INTERNATIONAL STANDARD

ISO/IEC 24762

First edition
2008-02-01

Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services

Technologies de l'information — Techniques de sécurité — Lignes directrices pour les services de secours en cas de catastrophe dans les technologies de l'information et des communications

Reference number
ISO/IEC 24762:2008(E)

© ISO/IEC 2008

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2008 – All rights reserved

Not for Resale

Contents

Page

Foreword v

0 Introduction vi
0.1 General vi
0.2 Structure vi
0.3 Framework vii
0.4 Interpretation of clauses viii

1 Scope 1
1.1 General 1
1.2 Exclusions 1
1.3 Audience 1

2 Normative references 2

3 Terms and definitions 2

4 Abbreviated terms 3

5 ICT disaster recovery 3
5.1 General 3
5.2 Environmental stability 4
5.3 Asset management 4
5.4 Proximity of site 5
5.5 Vendor management 5
5.6 Outsourcing arrangements 7
5.7 Information security 8
5.8 Activation and deactivation of disaster recovery plan 9
5.9 Training and education 11
5.10 Testing on ICT systems 12
5.11 Business continuity planning for ICT DR service providers 12
5.12 Documentation and periodic review 14

6 ICT disaster recovery facilities 14
6.1 General 14
6.2 Location of recovery sites 14
6.3 Physical access controls 16
6.4 Physical facility security 19
6.5 Dedicated areas 24
6.6 Environmental controls 25
6.7 Telecommunications 26
6.8 Power supply 27
6.9 Cable management 29
6.10 Fire protection 30
6.11 Emergency operations center (EOC) 32
6.12 Restricted facilities 34
6.13 Non-recovery amenities 37
6.14 Physical facilities and support equipment life cycle 38
6.15 Testing 40

7 Outsourced service provider's capability 41
7.1 General 41
7.2 Review organization disaster recovery status 41
7.3 Facilities requirements 43
7.4 Expertise 43
7.5 Logical access control 45

© ISO/IEC 2008 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.6 ICT equipment and operation readiness 47
7.7 Simultaneous recovery support 49
7.8 Levels of service 50
7.9 Types of service 50
7.10 Proximity of services 51
7.11 Subscription ratio for shared services 52
7.12 Activation of subscribed services 52
7.13 Organization testing 53
7.14 Changes in capability 53
7.15 Emergency response plan 54
7.16 Self assessment 57

8 Selection of recovery sites 58
8.1 General 58
8.2 Infrastructure 59
8.3 Skilled manpower and support 59
8.4 Critical mass of vendors and suppliers 59
8.5 Local service providers' track records 59
8.6 Proactive local support 60

9 Continuous Improvement 60
9.1 General 60
9.2 ICT DR trends 60
9.3 Performance measurement 61
9.4 Scalability 62
9.5 Risk mitigation 62

Annex A (informative) **Correspondence between ISO/IEC 27002:2005 and this International Standard 64**

Bibliography 67

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 24762 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

0 Introduction

0.1 General

This International Standard is aimed at aiding the operation of an Information Security Management System (ISMS) by providing guidance on the provision of information and communications technology disaster recovery (ICT DR) services as part of business continuity management.

Information security management is the process by which management aims to achieve effective confidentiality, integrity and availability of information and service. When an organization implements an ISMS the risks of interruptions to business activities for any reason should always be identified.

ISO/IEC 27001 and ISO/IEC 27002 include a control objective for information security aspects of business continuity management (refer to Control Objective 14.1 in ISO/IEC 27002:2005), the implementation of which will reduce those risks. That control objective is supported by controls to be selected and implemented as part of the ISMS process.

Business continuity management is an integral part of a holistic risk management process that safeguards the interests of an organization's key stakeholders, reputation, brand and value creating activities through:

identifying potential threats that may cause adverse impacts on an organization's business operations, and associated risks;

providing a framework for building resilience for business operations;

providing capabilities, facilities, processes, action task lists, etc., for effective responses to disasters and failures.

In planning for business continuity, the fallback arrangements for information processing and communication facilities become beneficial during periods of minor outages and essential for ensuring information and service availability during a disaster or failure for the (complete) recovery of activities over a period of time. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services.

0.2 Structure

This International Standard provides guidelines for the ICT DR services, which include both those provided in-house and outsourced. It covers facilities and services capability and provides fallback and recovery support to an organization's ICT systems. It includes the implementation, testing and execution aspects of disaster recovery. It does not include other aspects of business continuity management.

The guidelines are applicable to both "in-house" and "outsourced" ICT DR service providers of physical facilities and services in varying degrees. ICT DR service providers should interpret the intent of these guidelines within the context of the services they offer.

These guidelines include the requirements for implementing, operating, monitoring and maintaining ICT DR services, divided into two areas:

a) ICT disaster recovery (Clause 5); and

b) ICT disaster recovery facilities (Clause 6).

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Clause 7, “outsourced service provider’s capability”, specifies the capabilities which outsourced ICT DR service providers should possess, and the practices they should follow, for them to be able to provide basic secure operating environments and facilitate organizations’ recovery efforts. The capabilities required are specified in terms of the infrastructure and services needed to enable organizations to implement and execute their ICT DR plans. (It should be noted that although this clause is targeted at outsourced service providers, the guidelines it contains are also recommended for adoption by service providers in general.)

Clause 8, “selection of recovery sites”, provides guidance for:

a) organizations that are in the process of selecting an external recovery site as part of their ICT DR practices;

b) ICT DR service providers who are in the process of building (additional) recovery sites to expand their operations.

Factors such as environmental stability, good infrastructure and availability of skilled manpower locally, may provide a favourable environment for the operation of ICT DR recovery sites. Further, the presence of other ICT DR service providers and their suppliers may create a critical mass for a vibrant local industry. The track record of key players is another indicator of the maturity and vibrancy of the local ICT DR industry. Where applicable, proactive support of the local authority may also contribute to the growth and expansion of this industry.

Clause 9, “continuous improvement”, provides guidance for ICT DR service providers on ensuring continuous improvement to their ICT DR services through a set of practices. These practices can enable service providers to continuously maintain and improve the level of their services and thus provide an additional level of assurance to organizations engaging these services.

0.3 Framework

0.3.1 ICT DR service provision framework

This International Standard is based on a multi-tier framework comprising different elements in the ICT DR services provision, as illustrated in Figure 1. The “foundation” layer comprises the important aspects of ICT DR services, namely Policies, Performance Measurement, Processes and People. This layer helps to define the supporting infrastructure and services capability. The “continuous improvement” layer highlights practices that help to improve ICT DR activities in specific areas, and represents an added level of provision to the services provided. Thus the guidelines in this International Standard are drawn from a composite view of these layers, and with a balance between cost effectiveness and standard rigor considerations.

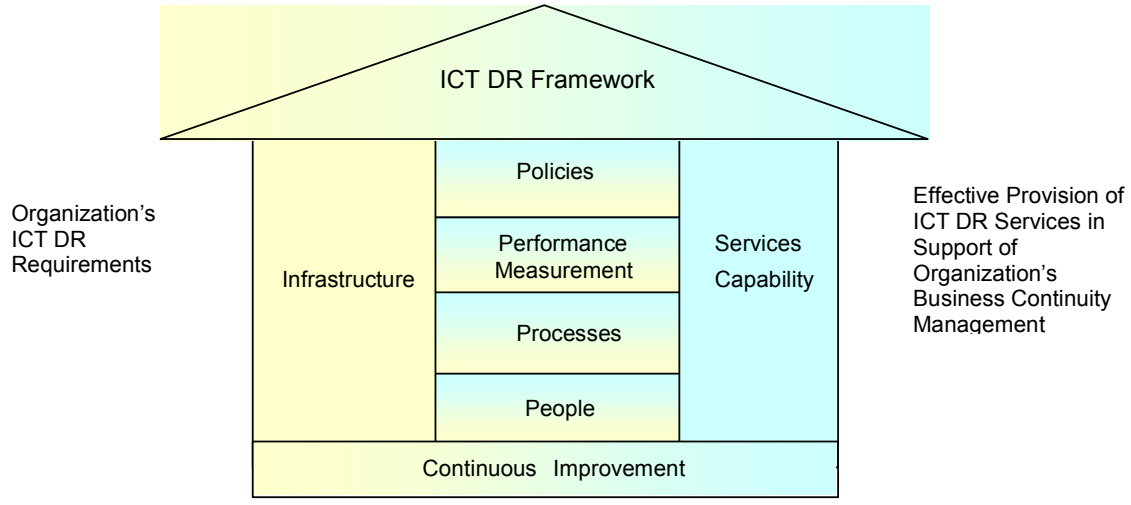

Figure 1 — ICT DR service provision framework

© ISO/IEC 2008 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

0.3.2 Policies

“Policies” enable ICT DR service providers to set the direction on the other, related, areas of their ICT DR services, and also enable clear communication to the relevant parties on the requirements that can be met by ICT DR service provider facilities.

The “Policies” aspect is elaborated on in clauses 5 to 9 of this International Standard. An established policy is usually expressed as “the system should include the following policies …” or “there should be documented policies and procedures …”.

0.3.3 Performance measurement

“Performance Measurement” enables ICT DR service providers to review and improve their services, and at the same time provides a means for service providers to demonstrate that their services meet organization requirements. This will in turn help to promote the ICT DR industry service level as a whole.

The “Performance Measurement” aspect is elaborated on in clause 9.3 of this International Standard, which explains the need for measuring the performance of ICT DR services and illustrates some examples of measurement metrics that service providers can select.”

0.3.4 Processes

“Processes” ensures that a consistent approach will be adopted in the other areas of ICT DR services, making possible the continuous maintenance of service levels and the ease of training of ICT DR personnel.

The “Processes” aspect is elaborated on in clauses 5 to 9 of this International Standard. An established process is usually expressed as “… according to appropriate established procedures”, “establish a set of procedures to ensure …”, or “there should be documented policies and procedures …”.

0.3.5 People

“People”, relates to the pool of skilled and knowledgeable service provider, organization and as relevant, third party personnel needed to help operate, uphold and maintain ICT DR practices. Further, the safety and welfare of personnel is also one of the aspects ICT DR service providers will need to take care of.

The “People” aspect is elaborated in various clauses of this International Standard. Clause 5.9 covers the general training and education guidelines, and clause 7.4 elaborates on the need for service provider management expertise. Clauses 6.10 and part of 6.12 cover personnel health and safety, and clause 6.13 provides guidance on personnel welfare aspects.

0.4 Interpretation of clauses

0.4.1 Statements on capability expectations

Statements on capability expectations typically contain the phrase – “ … service providers should be capable of providing organizations with … " – meaning that service providers should possess certain capabilities. Such capabilities could be a latent potential that can be swiftly activated by service providers if there is organization demand. For example, additional resources could be readily channelled from another unit (e.g. from elsewhere in the region or country, or from overseas) in response to an organization requirement. Obviously the actual provision of a particular stated capability to any organization would be subject to contract negotiations between service provider and organization.

0.4.2 Supplementary requests by organizations

Certain statements in this International Standard can lead organizations to making supplementary requests to service providers based on their specific ICT DR requirements. Such requests will be subject to further negotiations between service providers and organizations and not within the purview of this International Standard. For example, organizations may request audits of their service providers. The latter may levy fees for such requests.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

0.4.3 Service level agreement (SLA)/Service level commitment (SLC)

Certain subjects raised in this International Standard can be SLA/SLC issues. However, they do not dictate the content of the SLA/SLC between service providers and organizations. The subjects raised are intended to build common understanding and expectation between service providers and organizations. In particular they serve to draw organizations' attention to the typical items that could be included in SLA/SLC negotiations.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services

1 Scope

1.1 General

This International Standard describes the basic practices which ICT DR service providers, both in-house and outsourced, should consider.

It covers the requirements that service providers should meet, recognizing that individual organizations may have additional requirements that are specific to them (which would have to be addressed in the agreements/contracts with service providers). Examples of such organization requirements may include special encryption software and secured operation procedures, equipment, knowledgeable personnel and application documentation. Such additional organization specific requirements, if necessary, are generally negotiated on a case-by-case basis and are the subject of detailed contract negotiations between organizations and their ICT DR service providers and are not within the scope of this International Standard.

1.2 Exclusions

This International Standard does not:

a) provide any guidance on business continuity management as a whole for organizations;

b) take precedence over any laws and regulations, both existing and those in the future;

c) have any legal power over the Service Level Agreements (SLAs) included in negotiated contracts between organizations and service providers;

d) address requirements, legal or otherwise, governing normal business operations to be adhered to by service providers. Examples of such requirements include detailed regulations covering building and fire safety, occupational health and safety, copyright regulation and prevailing human resource practices;

e) provide an exhaustive list, and thus technical security controls are not covered. Readers should refer to ISO/IEC 27001 and ISO/IEC 27002, vendor literature and other technical references, as necessary.

1.3 Audience

This International Standard applies to:

a) all organizations requiring the ICT DR services as part of their business (whether in-house and/or outsourced);

b) ICT DR service providers in their provision of ICT DR services;

c) communities of organizations with reciprocal or mutual arrangements.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
computing and related equipment
computer, network, telecommunications and peripheral equipment that support the information processing activities of organizations

3.2
ICT systems
hardware, software and firmware of computers, telecommunications and network equipment or other electronic information handling systems and associated equipment

NOTE ICT systems include any equipment or interconnected systems or subsystems of equipment that are used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data/information.

3.3
information security
preservation of confidentiality, integrity and availability of information

NOTE 1 In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

NOTE 2 Adapted from ISO/IEC 27002:2005.

3.4
infrastructure
facilities and equipments to enable the ICT DR services, including but not limited to power supply, telecommunications connections and environmental controls

3.5
organizations
entities which utilize ICT DR services

3.6
outsourced service providers
external service providers of ICT DR services

3.7
service providers
in-house teams or external parties providing ICT DR services to organizations

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3.8
service level agreement
written agreement between a service provider and an organization that documents services and agreed service levels

NOTE In the case of outsourced service providers, the service level agreement is a written contractually binding agreement

3.9
service level commitment
commitment from a service provider (usually an internal service provider) to an organization that defines services and agreed service levels

4 Abbreviated terms

DBA Data Base Administrator

EMF Electro Magnetic Field

ICT DR Information and Communications Technology Disaster Recovery

MDF Main Distribution Frame

PDA Personal Digital Assistant

SLA Service Level Agreement

SLC Service Level Commitment

UPS Uninterruptible Power Supply

USB Universal Serial Bus

VFI Voltage and Frequency Independent

WAR Work Area Recovery

5 ICT disaster recovery

5.1 General

ICT DR service provision, irrespective of whether it is provided in-house or outsourced, should follow best practice guidelines as outlined in the following clauses. If the guidelines are followed there will be assurance that ICT DR services have been implemented after due consideration of unforeseen events that could affect the ability to fulfil service obligations, and related risk mitigation via prior arrangements with other service providers in the industry.

It should be noted that:

a) these guidelines will be applicable to ICT DR service providers (of physical facilities and services) in varying degrees. ICT DR service providers should interpret the intent of the guidelines in the context of the particular facilities and services they offer or intend to offer;

b) the issue of site proximity should be taken into consideration when ICT DR service providers contract and agree SLAs with organizations.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.2 Environmental stability

Environmental stability is important for the direct operation of a recovery center as well as personnel travel, safety and welfare. The utilities required for the operation of a recovery center, such as power supply and telecommunications, can be affected by environmental instability. Personnel travel and safety to/from a recovery center can be affected by disruption to the transportation system. Personnel welfare and social activities after work can also be limited by an unsafe external environment. The frequent occurrence on a large scale of the following type of activities would indicate underlying environmental instability:

a) strikes;

b) demonstrations;

c) riots;

d) violent crimes;

e) natural disasters;

f) pandemics;

g) deliberate attacks, e.g. terrorist bombing, biological attacks.

5.3 Asset management

5.3.1 General

Service providers should ensure that assets placed in their ICT DR premises are capable of being uniquely identified, located and retrieved in a timely manner when required by organizations. In addition to computing and related equipment, assets include: application software, vital records stored on media (magnetic or otherwise), and necessary operational documentation placed in service providers' operational premises to facilitate recovery from disasters and failures.

5.3.2 Organization ownership rights and privileges

Service providers should explicitly document and maintain the listing of assets that are in their ICT DR premises. In the case of outsourced service providers, the asset list should be included in service contracts with appropriate clauses inserted to identify their ownership rights and privileges.

5.3.3 Asset protection

For all assets located in their ICT DR premises, service providers should ensure that:

a) a list of the assets is maintained [this could be through use of a configuration management "system" and associated processes that maintain details of current versions of documentation, software, and all other assets (ISO/IEC 20000 provides guidance on establishing configuration management)];

b) all assets are tagged/marked in a manner that uniquely identifies ownership;

c) in the case of outsourced ICT DR service provision, organizations and outsourced service providers do not display explicit organization names in the asset tagging/marking to ensure that security is not compromised. For example, equipment mounted on shared racks should not have explicit organization names as part of the tag/mark.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Service providers should establish "systems"[1)] to protect, maintain, locate, retrieve and return all organization tagged/marked assets located at their premises, and ensure that organization ICT DR assets are:

a) located and kept in safe environments;

b) maintained in good operating conditions, with the installation of appropriate environmental controls;

c) not used or redeployed for other than contracted purposes;

and that the location of organizations' ICT DR assets is accurately tracked for retrieval.

In the case of outsourced ICT DR service provision, outsourced service providers should ensure that:

a) organizations are informed when their assets are being relocated;

b) organizations' assets are retrieved and returned within a predetermined and agreed timeframe when requested by organizations;

c) organizations are forewarned and their assets returned to them according to appropriate established and agreed procedures before the onset of any seizure or stoppages.

Organizations should consider the implications of disaster recovery data and other assets being stored across national boundaries, and ensure that compliance is maintained with all relevant legal and regulatory requirements.

5.3.4 Availability of documentation

Service providers (if required by their SLAs) and organizations should maintain duplicate copies of plans, disaster/failure procedures and other essential information for managing disasters and failures, including details of how to contact staff and of access points for emergency services. Such duplicate plans, procedures and other essential information should be kept off site at easily accessible locations.

5.4 Proximity of site

DR sites should be in geographic areas that are unlikely to be affected by the same disaster/failure events as organizations' primary sites. The issue of site proximity and associated risks should be taken into consideration when ICT DR service providers contract and agree SLAs with organizations.

5.5 Vendor management

5.5.1 General

Service providers should assess the relevant risks and then take adequate steps to ensure that critical equipment and services can be provided by their vendors within predetermined and agreed timeframes. Such vendors could include original equipment manufacturers and/or suppliers.

The following guidelines are applicable only to equipment supplied by service providers. Organizations that place their equipment in a recovery site should make their own arrangements with their equipment vendors or suppliers.

1) "Systems" are composed of integrated and interacting components of processes, resources and implementation elements (such as technical implementation of controls or practices) to achieve their stated purpose.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.5.2 Critical equipment support

Service providers should establish procedures to ensure dedicated support of critical equipment from their vendors, e.g. procedures to ensure replacement and delivery of critical ICT components within a predefined and agreed time.

5.5.3 Procurement system

Service providers should ensure that a procurement "system" is established to govern the supply of equipment, both new purchases and replacement. The "system" should encompass the following:

a) delivery modes and lead time of equipment and spares;

b) warranty period in case of any emerging defects;

c) associated support offered in terms of installation, commission and training, as appropriate;

d) for each critical ICT component, the provision of additional information, including:

    1) description – name, device number and date purchased;

    2) manufacturers;

    3) suppliers;

    4) availability;

    5) delivery and installation time.

5.5.4 Equipment supplied by third-parties

Service providers should ensure that, as equipment may be supplied by third-party vendors on a rental or lease basis, the contractual agreements with these vendors includes the following provisions:

a) repair and replacement of faulty parts in the event of equipment malfunction;

b) identification of equipment not covered by insurance;

c) terms and conditions for withdrawal of rental equipment by suppliers.

5.5.5 Staff supplied by third-parties

Service providers should establish procedures to ensure the quality and integrity of vendor staff directly involved in the support of their recovery services. This should encompass personnel supplied by vendors to:

a) maintain and repair facilities and equipment, both on site and off site;

b) provide permanent support to services at the service provider premises, as contracted staff to service providers. The contracts should encompass the:

    1) provision of replacements within predetermined and agreed times if the supplied contract staff are not available or unable to perform the assigned ICT DR tasks;

    2) confirmation of any required security clearances of these contract staff.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.6 Outsourcing arrangements

5.6.1 General

Service providers could make outsourcing arrangements with their vendors on a temporary or permanent basis. Unlike with third-party vendor management relating to equipment and services supplied by vendors, service providers may have a lesser degree of control in any outsourcing arrangement. Thus, greater emphasis should be placed on the selection and management of outsourced vendors. This includes ensuring vendor awareness of the peculiarity of service provider business needs, more stringent contractual agreements, more thorough periodic review of outsourced arrangements, and close review of vendor security controls and the quality of vendor staff.

Such outsourcing arrangements should not affect the ability of service providers to fulfil their services to organizations. In addition, the primary service responsibility still lies with service providers and cannot be transferred to these outsourced parties.

5.6.2 Vendor awareness

Service providers should ensure that all external parties involved in outsourcing, including subcontractors, are made aware of their responsibilities and liabilities in support of service provider services, e.g. periodic briefings should be held for all outsourced vendors.

5.6.3 Contractual agreement

Service providers should ensure that the responsibilities and liabilities of outsourced vendors, including their subcontractors, are spelt out formally in contractual agreements, e.g. outsourced vendors should replenish supplies within a predetermined and agreed period of time.

5.6.4 Periodic review

Service providers should review the risks of outsourcing to vendors at least once a year. The reviews should examine the following concerns:

a) financial health and viability of the vendors;

b) new avenues for alternate supplies.

5.6.5 Vendor security controls

Service providers should ensure that the same level of physical, logical and other security controls are adopted by all parties involved in outsourcing arrangements, to restrict, limit and protect access to service provider outsourced functions. This should encompass all associated equipment, computer hardware and software, and facilities.

Service providers should also ensure that they regularly audit all physical, logical and other relevant security controls put in place by outsourced parties.

5.6.6 Quality of vendor staff

Service providers should ensure that their outsourced vendors have formal policies and procedures in place in relation to the hire of staff to provide services. These policies and procedures should be included as part of contractual agreements with outsourced vendors, and include the required:

a) staff qualifications and experience;

b) security clearance(s) of vendor staff, as appropriate;

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

c) policies on such as ethics, behaviour, sexual or racial harassment;

d) policies and procedures on performance monitoring;

e) policies and procedures on replacement of staff.

5.7 Information security

5.7.1 General

Service providers should ensure that organizations' information security is not compromised, and in doing so may need to invest in additional resources to segregate and maintain organizations' information security.

Service providers should communicate the physical, logical and other relevant security arrangements (including for information security incident (and weakness) management) to organizations, and agree with organizations the applicability of the security arrangements were a disaster plan to be activated. The DR facilities and equipment should be assessed to be sure that they meet the protection requirements of organizations.

Service providers should consider adopting ISO/IEC 27001 and ISO/IEC 27002 to ensure that relevant security requirements will be met.

5.7.2 Isolation of ICT systems

Service providers should ensure that information from one organization's ICT system is not accessible or made known to another organization's ICT system, unless authorised. Service providers should establish a means to identify and physically and logically isolate the different ICT systems which are located in their premises, and are:

a) supported and maintained by different external vendors;

b) subscribed to by different organizations.

5.7.3 Personnel restriction and segregation

Service providers should establish a means to identify and segregate different personnel at their recovery facilities from access to ICT systems and information, based on the need, to ensure that:

a) there are restrictions on physical access to facilities housing ICT systems. For example, ICT systems with different protection requirements should be located in separate buildings or areas/rooms to enable physical access control to be properly implemented;

b) work areas used by service provider, organization and vendor personnel are planned and designed with information privacy and confidentiality as a prime consideration, e.g. with buildings and/or assigned separate areas/rooms for use by different personnel.

5.7.4 Data transfer

Service providers should ensure that the integrity and confidentiality of organization DR data are maintained whilst being transferred (either electronically or physically) to and from DR sites, subject to contractual obligations with organizations.

5.7.5 Information security incident management

Service providers should ensure that all security incidents and weaknesses are promptly reported to the relevant authority and that appropriate action is taken. There should be an information security incident management scheme in place that is fully compatible with ISO/IEC 18044:2004.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.7.5.1 Procedures

A formal set of procedures should be established to deal with information security incidents (and weaknesses) (including physical). This should encompass:

a) detection of all information security incidents (and weaknesses), and related escalation procedures and channels;

b) reporting and logging of all information security incidents (and weaknesses);

c) logging the responses, and preventive and corrective action taken;

d) periodic evaluation of all information security incidents (and weaknesses);

e) learning from reviews of information security incidents (and weaknesses), and making improvements to security and to the information security incident (and weakness) management scheme.

5.7.5.2 Assessment criteria

All information security incidents (and weaknesses) should be assessed, as relevant aided by examining log files. The assessment criteria for information security incidents (and weaknesses), and/or personnel responses, should be made based on:

a) detection: How was the information security incident (or weakness) detected? Can detection be improved by technical measures or otherwise?

b) notification: How was the information security incident (or weakness) reported to the relevant personnel? Were all parties affected informed at the appropriate juncture? Are there alternate and better notification or escalation channels?

c) response: How were the decisions and responses made? Can further improvements be made to improve the decision-making process?

d) effectiveness: Were assessments of the information security incident (or weakness) and/or the related damage appropriate? Was the response effective, e.g. in terms of containing or preventing further information security incidents (and weaknesses) and/or related damage?

5.8 Activation and deactivation of disaster recovery plan

5.8.1 General

Service providers should establish with organizations the conditions and procedures for invoking and deactivating disaster recovery services.

Organizations, together with their service providers (subject to service provider contractual obligations with organizations), should maintain duplicate copies of plans, disaster/failure procedures and other essential information (such as contact lists and ‘call trees’) for managing disasters and failures.

5.8.2 Prior agreements

Service providers should ensure that, to prevent confusion and misunderstanding, prior agreements are established between themselves and organizations. These agreements should be documented and communicated to all relevant personnel. They should include:

a) a list of authorized organization representatives who can invoke or deactivate subscribed services;

b) the communication media to be adopted between service provider and organization representatives for notification, confirmation, activating and deactivating the subscribed services;

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

c) conditions whereby organizations can invoke or deactivate subscribed services;

d) a protocol for notifying either party of key personnel departures and changes (to guard against wrongful invocations etc.);

e) a list of organization personnel authorized to access the ICT DR facility following plan activation.

5.8.3 Notification

Service providers should ensure that agreements made with organizations include the following notification procedures as appropriate:

a) initial notification from organization representatives to service provider representatives;

b) confirmation by service provider representatives to organization representatives;

c) notification to service provider staff directly involved in the subscribed services to be on stand by;

d) notification to service provider external vendors or suppliers involved in the subscribed services to be on stand by;

e) consultation with organization representatives on one of the following courses of action:

   1) continue to stand by;

   2) stand down the notification;

   3) activate the subscribed services within a pre-determined period.

All communications between service provider and organization representatives in the notification stage should be via the communication media pre-agreed between service providers and the organizations.

5.8.4 Activation

Service providers should ensure that agreements to be made with the organizations include the following procedures for activating the subscribed services as appropriate:

a) informing service provider management of organization activation;

b) collection of vital records from secure storage (subject to contractual obligations with organizations);

c) activation of service provider staff directly involved in the subscribed services;

d) activation of service provider external vendors or suppliers involved in the subscribed services;

e) preparation of subscribed services, e.g. recovery site, for handover to organization recovery staff;

f) handover of subscribed services, e.g. recovery site and equipment by service providers to organization recovery staff.

The response times for the above procedures should also be included in the agreements with each organization.

5.8.5 Deactivation

Service providers should ensure that agreements made with organizations include procedures to effect the orderly handover of facilities and equipment from organizations to service providers when services are deactivated.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.9 Training and education

5.9.1 General

Service providers and organizations should ensure that ICT DR training is provided for all service provider staff and any relevant organization staff, and in particular that all new staff are appropriately trained to assume and discharge their job responsibilities in a competent manner. They should be assessed as competent before being assigned their responsibilities. The training can be conducted by own in-house staff or provided by external parties. Introduction DR training should be provided for all personnel, and specific training for staff assigned with key DR functions and roles.

5.9.2 Service provider staff training

Service providers should ensure that a "system" is established to ensure that all staff directly involved in providing ICT DR services to organizations, including those operating the physical facilities, are appropriately trained and educated. This should include:

a) all service provider staff undergoing formal ICT DR training and education commensurate with their roles in organization recovery. Those operating the physical facilities should undergo formal training and education commensurate with their operational roles. For key functions and roles there should be formal assessment of the trainees during and/or at the end of each training course;

b) all training exercises documented, with the results recorded and steps taken to address exceptions and failures.

5.9.3 Organization staff training

Organizations should establish programmes for training their personnel who will be assigned at the time of a disaster or failure (e.g. DBA, senior application development staff, communications managers, first aid workers, fire wardens and possibly some senior user staff) in order to ensure satisfactory outcomes during disaster/failure activation. For similar reasons, relevant organization personnel should also be involved in exercises of DR plans.

Organizations should also ensure that deputies for key staff are trained and involved in DR exercises in case the primary persons are not available when needed.

Organization testing, including simulated disaster/failure invocation, though valuable should not be regarded as the only part of formal training. These events provide practical experience, but do not provide systematic and thorough training.

5.9.4 Types of training

Service providers and organizations should ensure that the types of training to be provided to staff are commensurate with their assigned tasks and responsibilities. The types of training include:

a) introduction training, to provide basic understanding and awareness;

b) advanced level training, to equip staff with specific knowledge and skills to undertake assignments;

c) continuous training, to keep staff up-to-date and ensure that they remain competent in performing their assigned tasks;

d) training to assess and maintain the competency and readiness of staff.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.9.5 Scope and frequency of training

Service providers and organizations should schedule appropriate training for all staff, and maintain records of the training delivered, encompassing:

a) for all new staff, introduction level training on joining;

b) for specific staff, advanced level training to prepare them to undertake key tasks.

Training should be conducted at least once a year for staff performing key functions and roles, and for all staff as relevant after significant changes to the facilities and services that could affect those offered to organizations.

5.9.6 Assessment

Service providers and organizations should ensure, as far as practicable, that all training is assessed. Assessment should evaluate staff on one or more of the following:

a) staff understanding and interpretation of policies, procedures and operation of equipment and facilities, e.g. revocation of physical access upon staff resignation;

b) staff response to specific events, e.g. physical intrusion.

5.10 Testing on ICT systems

Service providers should ensure that all ICT systems essential for disaster recovery are tested regularly to ensure their continuing capability to support DR plans.

Tests should also be conducted when there are any significant changes in organization requirements and/or changes in service provider capacity and capability that affect services to organizations. Examples of such changes include relocation of DR sites, major upgrades of ICT systems or new ICT systems commissioned.

5.11 Business continuity planning for ICT DR service providers

Service providers should ensure that they have properly addressed their own business continuity, including disaster recovery, needs.

The end result for service providers should be to have business continuity plans produced, tested, maintained and updated covering all business functions. However, service providers should not go directly to producing the plans without some critical work beforehand. Service providers should first identify their business priorities and then the correct and most cost effective business continuity strategy appropriate to their business environment. Only when service providers have agreed business continuity strategies, and thus know their best way forward, should they produce, test and use the business continuity plans. They should also manage the risks to further reduce the likelihood of having to invoke the plans, and/or reduce the impact of a disaster or failure should one occur. The overall recommended approach to follow for business continuity planning is shown in Figure 2 below.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale



Figure 2 — Business Continuity Planning Approach

The recommended approach consists of a number of discrete stages, together aimed at achieving a comprehensive and viable business continuity plan that will fully meet the requirements of service providers' business in the event of a disaster or failure. These stages are:

a) Establishing business recovery priorities, timescales and requirements (including first conducting business impact analysis review and risk assessment);

b) Business continuity strategy formulation;

c) Business continuity plan production;

d) Business continuity plan testing;

e) Ensuring business continuity awareness for all staff;

f) Ongoing business continuity plan maintenance;

g) Risk reduction.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The first five stages are consecutive. When a plan has first been produced and tested, the sixth stage follows on over time, and is conducted at regular intervals and after any significant changes that might affect the validity of the plans, revisiting any of the other stages for update purposes as is necessary. The seventh stage is conducted in parallel with the other stages.

5.12 Documentation and periodic review

All policies, plans and provisions made should be documented. Staff at the relevant levels should be assigned to ensure that each document is reviewed and updated periodically. A configuration management system should be used to maintain current versions of documents, as well as of such as software and asset inventories.

6 ICT disaster recovery facilities

6.1 General

Basic requirements need to be fulfilled by ICT DR service providers so that they can provide secure physical operating environments to facilitate organization recovery efforts. In addition to covering basic physical facility requirements, requirements for environmental controls, telecommunications, continuous power supply and non recovery amenities such as parking and accessibility to food and drinks also need to be considered. For service providers with multiple recovery sites, the guidance should be equally applied to each and every site.

6.2 Location of recovery sites

6.2.1 General

Locations of recovery sites could have certain undesirable vulnerabilities, which could mean that the best designed and equipped recovery site had residual risks that could not be mitigated. Examples of such potential threats are described below.

6.2.2 Natural hazards

Recovery sites should not be located in areas exposed to natural hazards, or the risks should be assessed and mitigated or accepted. The natural hazards include but are not limited to:

a) volcanoes and earthquakes;

b) typhoons, hurricanes and storms;

c) low lying grounds adjacent to rivers which are susceptible to flooding after rain;

d) lightning.

6.2.3 Weather changes

Extreme and sudden changes in the environment could impact physical facilities and accessibility to recovery sites. Recovery sites should be selected based on assessments of the extent and speed of climatic changes and probable impact to:

a) physical facilities, e.g. sudden changes in environmental temperature could cause a water pipe to burst and flood basement areas;

b) accessibility, e.g. heavy downpours could affect large transportation system segments and limit or restrict accessibility to recovery sites.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.2.4 Industrial and commercial hazards

Recovery sites should not be located near potential industrial or commercial hazards, including such as:

a) nearby facilities processing chemicals or explosive materials;

b) directly under an airport flight path;

c) nearby busy hospitals, particularly those that will deal with certain disasters such as pandemics (e.g. bird flu, SARS), with consequent traffic congestion;

d) buildings or locations with business operations such that they are likely targets for public demonstration or other threats.

6.2.5 Accessibility

Recovery sites should be located in areas with good accessibility. It should be possible to move organization staff and equipment into recovery sites without undue delay. Accessibility should be measured by:

a) well connected air links (as relevant, from international to local airports);

b) quality rail links;

c) comprehensive road system;

d) convenient transportation from airports and rail stations to recovery sites;

e) convenient transportation from hotels to recovery sites;

f) as relevant, the ease of cross-border or trans-national entry.

Organization prime sites and recovery sites should be as far away from each other as possible, but with the condition that, should organization staff be required to implement DR plans at DR sites the recovery time objectives can still be met.

6.2.6 Alternate routes

Alternate routes of access to recovery sites are needed if unexpected congestion, cut-off or blockage occurs along normal access routes to recovery sites and bypass access is not possible without undue difficulty for personnel and equipment. For example, a recovery site accessible only via a bridge could suffer from physical isolation if the bridge was damaged. An alternate access route bypassing the bridge would be needed in such a case.

6.2.7 Shared premises

Special consideration should be given by service providers to recovery sites located in shared premises, due to the greater risks where other organizations and their personnel are in close proximity, compared with the use of dedicated single occupancy premises. Service providers should ensure that:

a) formal risk assessment and risk reduction reviews of shared premises are performed:

   1) periodically, at least once a year;

   2) when there are significant changes in shared premises, e.g. new tenants and change of use by existing tenants;

b) details of residual risks which cannot be mitigated are provided to organizations for review.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.2.8 Public utilities

Recovery sites should not be located near facilities providing public and other utilities such that the sites are susceptible to influences that could affect operations. Such utilities could produce vibration, interference or be sabotaged. Examples of such facilities include:

a) power plants;

b) telecommunications transmission towers;

c) underground and overground railway lines.

6.2.9 Cabling infrastructure

Telecommunications and power supply cabling from vendors to recovery sites should not be unduly exposed to external physical damage. For example, a cabling system suspended on transmission poles would be exposed to greater risk of physical damage than an underground cabling system, and should be avoided.

6.2.10 Risk mitigation

For recovery sites which are exposed to potential risks that cannot be eliminated, there should be corresponding risk mitigation procedures and efforts to minimize these risks to an appropriate level. An example of such potential risks is the building of a new facility for processing hazardous materials nearby.

6.3 Physical access controls

6.3.1 General

Physical access controls are key elements in the protection of recovery sites, and it is crucial that such controls are in place and maintained at all building entrances and exits. Upon entry, organization staff should have access to all the facilities allocated - without the imposition of additional access control when they move from one part of subscribed recovery facilities to another (unless absolutely necessary).

Thus service providers should ensure that physical access control facilities, policies and procedures are established, documented and implemented, commensurate with the assessed risks and the services provided to organizations, to control and monitor physical access into and out of, and within, service provider premises.

6.3.2 Personnel security categorization

A formal system of security categorization for personnel should be established. The categorization should cater for the following personnel categories:

a) service provider staff;

b) organization employees;

c) vendors and contractors;

d) visitors.

6.3.3 Security zones

Separate physical security zones should be identified and established in service provider premises, with:

a) restricted facilities – areas/rooms housing key equipment and facilities such as servers and other computer equipment, communications switches and other related equipment and cabling, data media archives, air conditioning facilities, and main distribution frames for the power supply;

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

b) common facilities – areas/rooms used by all personnel and not subject to any internal security restrictions, such as reception areas, conference rooms, cafeterias and toilets.

A formal system of access control of personnel to each security zone based on their security categorization should be established and enforced around the clock.

6.3.4 Staff

Formal procedures should be established to deal with staff joining or leaving service providers. These should cover:

a) new staff joining a service provider, for the determination of what level of authorized access is applicable and for the subsequent issue of the appropriate physical access control badges/cards;

b) staff resignation, for the immediate notification to the security function of the staff resignation, revoking of all related access authorizations and retrieval of physical access control badges/cards.

6.3.5 Access control

Formal policies and procedures should be established for the control of entry into service provider premises, to ensure that all entry is only at designated entrances and that the identity of all personnel, including visitors, is verified at the entrances.

6.3.6 Non-staff

Formal policies and procedures should be established to control the movement of other than service provider staff into and within service provider premises, to ensure that:

a) requests for entry into service provider premises and access to facilities are predetermined and arranged, e.g. with permission obtained through means such as prior e-mail and conversation (if the requesting person is well known to the relevant service provider staff member – who then issues confirmation of authorization to security personnel), or by formal signed authorization form submission;

b) security staff at the entrance countercheck with service provider staff concerned;

c) visitors are always held at the entrance or escorted to designated supervised waiting areas until reception by service provider staff;

d) entry of contractors located on site for a predetermined purpose and period of time is restricted to only the areas/rooms that are necessary to accomplish their specific authorized tasks. This applies to cleaners, caterers and other outsourced support service personnel;

e) all visitors to restricted areas are escorted by service provider staff at all times;

f) vendor staff on maintenance work in restricted areas are physically supervised to prevent their obtaining access to systems outside of their area of activity (monitoring via CCTV is also acceptable where resource limitations would prohibit physical monitoring);

g) badges are issued for all outsiders entering service provider premises, including permanent contractors such as cleaners and cafeteria operators. Subclause 6.4.8 outlines the usage of badges to control movement of personnel in the premises;

h) a log is maintained for the entry of outsiders into service provider premises, including permanent contractors. The log should include:

   1) outsiders' particulars, including name and organization identity;

   2) purpose of entry;

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3) service provider staff visited;

4) time in and out;

5) remarks;

6) signature of the personnel in the log.

6.3.7 Organization staff

Formal policies and procedures should be established to handle organization staff access to service provider premises, covering:

a) in normal times, with authorised organization staff allowed visits to a recovery site at pre-agreed times as provided in the service provider contract with an organization, e.g. during testing periods;

b) during a disaster/failure, with organization staff accorded round the clock access to designated areas/rooms for their recovery operations.

6.3.8 Personnel behaviour in restricted security zones

Formal policies and/or guidelines should be established governing personnel behaviour in restricted facilities such as server rooms, computer centers, and data media archives. These policies should include:

a) prohibition of smoking;

b) prohibition of food and drink;

c) conditions for the use of devices generating radio frequency, e.g. mobile phones, near sensitive equipment;

d) conditions for use of storage devices and photo-taking devices , e.g. PDAs, USB drives and mobile phones with in-built cameras.

6.3.9 Security functions and roles

Service providers should establish functions and roles for maintaining security, with specific staff assigned to them. These should encompass the:

a) appointment of specific staff for physical security functions and roles, e.g. for escalation/reporting purpose when there is an information security incident;

b) appointment of deputies for critical functions and roles, who should be competent to discharge the full duties in the event of the primary appointment holders being unavailable or otherwise unable to work;

c) adequate training of all appointed staff before they are assigned to their security functions and roles;

d) attendance at periodic refresher or update courses by all appointed staff for their security functions and roles, to ensure that they remain competent in undertaking their assignments;

e) procedures established to test staff assigned to security functions and roles to ensure that their alertness and knowledge is maintained. The tests should be conducted on a periodic basis, e.g. once a year. The evaluation of staff responses during the test should comply with the evaluation criteria given in clause 5.7.5.2.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.3.10 Tests

Testing strategy, test objectives, test plans, tests and test results should form an integral part of maintaining the integrity of the physical access control system. The policies and procedures governing planning, conduct, documentation, review and life cycle of tests are given in clause 6.15.4 below.

6.3.11 Physical security incidents (and weaknesses)

All physical security incidents (and weaknesses) should be promptly reported to the relevant authority and appropriate action taken. The handling of information security incidents (and weaknesses) (including physical) is referenced in clause 5.7.5 above.

6.3.12 Non-working hours

Policies and procedures should be established to govern personnel access to recovery premises outside their designated working hours, e.g. personnel access during public holidays. These should include:

a) authorisation and notification procedures;

b) emergency procedures, e.g. during on-site disaster recovery by an organization.

6.3.13 Authorisation

Authorisations for all physical access into service provider premises, and the restricted facilities therein, should be:

a) granted based on 'need-to-know' and 'need-to-hold' principles;

b) reviewed and updated on a periodic basis.

6.3.14 Continuity

All implemented facilities, policies and procedures should be operational on a basis of 24 hours a day, for every day in the year (hereinafter referred as 24 x 7).

6.4 Physical facility security

6.4.1 General

In line with risk assessment results, there should be physical security controls and procedures in place to protect both service provider and organization electronic information systems, buildings, facilities and equipment from unauthorised physical access, alteration and damage. Thus, all facilities provided by service providers to organizations should be physically secured and monitored, with safety and health protection of personnel as a prime consideration.

6.4.2 Protection concept

A unified protection concept should be established to integrate all physical security protection and procedures. This protection concept should form the underlying basis of all physical security protection and procedures such that they integrate and complement each other. For example, a protection concept focusing only on a high wall perimeter would be ineffective against other forms of intrusion. The protection concept employed should be one of the following approaches:

a) multi-layered, with premises divided into multiple layers from the outer perimeter to the inner center with corresponding increases in restrictions imposed, e.g. with additional personnel 'clearance' from gate entry permission required to enter into a server room;

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

b) sector-based, with premises divided into distinct sectors, e.g. sectors A, B, C and D, and each sector accorded different access protection criteria to limit cross-over from one sector to the next;

c) composite, with a combination of the multi-layered and sector-based approaches, and the premises divided into distinct sectors with increased restriction imposed from the outer perimeter to the inner center for each sector.

The protection concept should be implemented based on proper planning, design, building and management of physical facilities.

6.4.3 Physical building

Physical buildings housing recovery sites should be planned, designed and built with security in mind. For non-dedicated buildings, e.g. shared premises, appropriate controls should be implemented and maintained to mitigate the associated security risks.

6.4.3.1 External

The perimeters and exteriors of all recovery facility buildings should be physically secured against break-ins and vandalism. The security controls should include:

a) External walls of buildings of solid construction;

b) All doors and relevant windows appropriately protected against unauthorised access, e.g. with strong construction, and locks and alarms fitted.

In addition, buildings should be protected against lightning and induced electrical surges that could damage building exteriors and/or cause permanent or temporary malfunction of electrical and electronic equipment housed within. Examples of relevant security controls include lightning arrester and over-voltage protection devices for critical equipment.

6.4.3.2 Internal

The physical barriers for restricted facilities within buildings, e.g. computer rooms, should include walls extended from true floor to ceiling, i.e. slab to slab, to prevent unauthorised entry and environmental contamination, e.g. by smoke or fire. If this is not possible, service providers should implement other barriers.

6.4.3.3 Inspections

All recovery facility buildings should be inspected on a periodic basis, with inspections covering at least:

a) all entrances into and exits from service provider premises;

b) areas immediately surrounding the perimeter of service provider premises;

c) perimeter fences and/or walls of service provider premises;

d) any unused side entrances of buildings (i.e. checking that they are always locked);

e) goods lifts (i.e. checking that they are protected via access card or other security controls, including disabling after office hours).

6.4.4 Physical security surveillance

Physical security surveillance should be established to monitor personnel movement in and around service provider premises. Security surveillance should be established using a mixture of equipment (such as CCTV and motion detectors) and security guards, and should be operational round the clock and fully manned.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Procedures should be established for the installation, maintenance, repair and upgrade of the physical security surveillance equipment to ensure that there are no lapses in security. For example, security guards may be posted to oversee the affected areas/rooms during these activities.

Staff responsible for physical security surveillance should be adequately trained, and tested periodically to check responses to physical intrusion and attack. The requirements for training and related evaluation criteria are provided in clause 5.9 above.

The physical areas to be put under surveillance should include, if applicable:

a) all entrances into and exits from service provider premises;

b) all entrances and exits of restricted facilities, e.g. computer rooms and media storage facilities;

c) areas immediately surrounding the perimeter of service provider premises;

d) perimeter fences and/or walls of service provider premises;

e) areas between perimeter fences and/or walls and buildings within service provider premises.

Service providers may outsource the provision of physical security surveillance, e.g. security and monitoring, to external vendors but subject to the guidance provided in clause 5.6.

6.4.5 Detection and alarm systems

6.4.5.1 General

Physical detection and alarm systems should be established to detect intrusions, attacks and such as fire and flood, and provide early warnings of their occurrence to the appropriate personnel. The detection and alarm systems should encompass the features described in the clauses below.

6.4.5.2 Design

Detection and alarm systems should be implemented using one of the following approaches:

a) centralized, with all detection devices connected to a centralized facility that is manned on a 24 hours basis;

b) decentralized, with all detection devices operated and managed locally;

c) composite, with a combination of the centralized and decentralized approaches, e.g. using a centralized facility to monitor alarms for restricted facilities and local management of other alarms.

Ideally all alarms should also have links to the local police and fire services.

6.4.5.3 Types of warning

Detection and alarm systems should at least provide warning for the following threats, where applicable:

a) smoke;

b) fire;

c) water seepage;

d) break-ins.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.4.5.4 Facilities covered

Detection and alarm systems should include coverage of restricted facilities, with the areas/rooms housing those restricted facilities fitted with the appropriate types of detection and alarm devices. Restricted facilities should include:

a) server rooms;

b) other computer rooms;

c) data media archive rooms;

d) environmental control plant rooms (housing air-conditioning equipment);

e) main communications switch rooms;

f) UPS rooms;

g) battery rooms (if not combined in UPS rooms);

h) power switch/generator set area/rooms;

i) MDF / meet-me rooms;

j) other telecommunications rooms (e.g. housing distribution framework for wiring and patching).

6.4.6 Operations

Service provider staff should be adequately trained and tested periodically to check responses to warnings from detection and alarm systems. The evaluation criteria for staff responses alarms are described in clause 5.7.5.2, and information on staff training, education and testing is described in clause 5.9.

6.4.7 Storage facility

Service providers should be capable of providing organizations with secure storage facilities and accessories to store their vital records, magnetic media and supplies. The following should be adhered to for the provision of secure storage:

a) a formal set of procedures established to handle and secure the collection, transportation, receipt, marking, storage and retrieval of vital records, magnetic media and supplies - to and from organization premises, and to on-site and off site storage facilities, as well as recovery sites. For example, outgoing tapes of vital records may be kept in secured cabinets in mailrooms before collection and delivery to organizations;

b) appropriate environmental controls in place to maintain the integrity of organization records during transportation and storage;

c) for storage facilities not located within recovery sites:

   the criteria for the selection of sites for storage facilities should be the same as for the selection of the recovery sites. For example, storage facilities should be located away from natural hazards and with ease of access and alternate access routes;

   storage facilities accorded a similar level of physical access control and environmental protection as for recovery sites.

d) secure storage cabinets with locking capabilities available at recovery sites to hold organization vital records, magnetic media and supplies.

Service providers could outsource the provision of storage facilities to external vendors, but subject to the guidelines provided in clause 5.6 above.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.4.8 Badges

Some form of visible badge identification should be in place to facilitate monitoring and control of personnel movement within service provider premises, with the following requirements:

a) each badge should uniquely identify a given person;

b) badges should not be easily duplicated or forged;

c) each person should be given only one badge at any one time;

d) each person should be responsible for the security and appropriate use of the given badge;

e) loss of badge should be reported immediately;

f) badges should be prominently worn at all times while in service provider premises;

g) badges for staff should be distinctly different from those issued to visitors;

h) badges issued to visitors should be returned when the persons leave service provider premises;

i) badges should be returned on the last working days of members of staff, as part of security exit procedures.

6.4.9 Keys

All keys (including such as magnetic stripe cards, smart cards and codes for digital key pads) that allow physical access to recovery site buildings and areas/rooms, and such as cabinets therein, should be centrally organised and managed.

The following policies and procedures should govern the management of these keys:

a) general issue and control of keys to personnel, e.g. issue of keys to new staff and return of the keys upon resignation;

b) specific issue and control of keys to personnel for key facilities, e.g. keys for entry into server rooms should be strictly restricted to only a few essential staff;

c) safekeeping of spare keys, e.g. in specially controlled key box or press;

d) loss of keys, e.g. compulsory changing of corresponding locks and re-issuing of new keys.

6.4.10 Flammable materials

Easily flammable materials such as lighter fuel should not be stored in rooms housing restricted facilities.

6.4.11 Portable equipment

Portable equipment such as notebooks, mobile phones, PDAs, cameras, USB drives, or other media drives should not be brought into areas/rooms housing sensitive facilities unless these are under the control of authorized service provider and/or organization staff. Such control could be decided on a case by case basis.

6.4.12 Maps and directories

Facility maps, telephone directories and other documents capable of associating or identifying sensitive information processing facilities should only be made available to relevant authorized personnel.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.4.13 Incoming and outgoing inspection

All incoming and outgoing materials to service provider premises should be inspected for potential hazards and security incidents.

6.4.14 Document and media disposal

Service providers should make available appropriate equipment and facilities at recovery sites for organizations to dispose of unwanted documents, media and other materials. Examples of equipment used for disposal include paper shredders that can ensure secured disposal of unwanted printouts, equipment that provides degaussing of magnetic tapes, and compact disc shredding/cross-cutting equipment. Disposals should be undertaken in such a way that no inference can be drawn regarding previously stored data.

6.4.15 Continuity

All physical security provisions and procedures implemented should be operational on a 24 x 7 basis.

6.4.16 Personnel health and safety

Procedures should be in place to ensure an appropriate level of safety and health protection for personnel at recovery sites. This includes periodic building and fire safety inspections covering areas such as air ventilation, fire load reduction, unblocked escape routes and emergency lighting.

6.5 Dedicated areas

6.5.1 General

Provisions should be made to set aside specific areas/rooms at service provider premises for organization equipment and usage during recovery. These areas/rooms should not be re-allocated for other usage during normal times. If an area/room is reassigned during normal operation then the service provider should have a process in place to immediately convert/use it for the purpose needed during a disaster or failure.

6.5.2 Assembly area

Service providers should provide adequate assembly areas with public address systems to enable organizations to gather and brief all their recovery staff. Assembly areas could be open spaces, halls or auditoriums that could:

a) accommodate expected large numbers of recovery staff from various recovery teams;

b) be operational and comfortable for personnel under all weather conditions;

c) fulfill organization confidentiality requirements such that any briefing or conversation in the areas cannot be overheard from adjacent areas.

6.5.3 Holding area

Service providers should provide holding areas for loading, unloading and inspection of organization computer and related equipment.

Service providers should establish policies and procedures to govern the movement of organization equipment in holding areas – including the presence and supervision by organization and service provider representatives as appropriate, and procedures to deal with irregularities and exceptions.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.5.4 Staging area

Service providers should provide staging areas with adequate power supply for testing of computer and related equipment. The power supply in staging areas should be isolated from that in other parts of recovery facilities to prevent accidental “trips” from affecting the power supply in other parts of recovery facilities during equipment testing. Considerations should also be given to the isolation of networks in staging areas if networking is to be tested in them.

Service providers should establish policies and procedures to govern the movement and testing of organization equipment in the staging areas – including the presence and supervision by organization and service provider representatives as appropriate, and procedures to deal with irregularities and exceptions.

6.5.5 Other areas

Provision should be made by service providers to enable organizations to site their computing and related equipment in secured environments. This is to prevent unauthorised physical access, alteration or removal. For example, areas/rooms could be set aside for printers and fax machines, and secured cabinets used for routers and modems.

6.6 Environmental controls

6.6.1 General

Service providers should ensure that policies and procedures are in place to protect service provider and organization electronic information systems, equipment and facilities from natural and/or environmental hazards. These policies and procedures should include coverage of the implementation and provision to organizations of facilities with suitable construction and accessories to prevent degradation of media used for storage. For example, proper temperature and humidity controls should be maintained within storage location for magnetic media.

6.6.2 Personnel and equipment

Procedures should be in place to achieve an appropriate level of environment quality for equipment and personnel at recovery sites. These procedures should ensure environmental controls for:

a) temperature;

b) ventilation;

c) humidity;

d) vibration and noise.

Procedures to ensure suitable monitoring and control of EMF strength should also be established whenever applicable.

6.6.3 Facilities

Service providers should ensure that environmental controls are provided for:

a) server rooms;

b) other computer rooms;

c) data media archive rooms;

d) environmental control plant rooms (housing air-conditioning equipment);

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

e) main communications switch rooms;

f) UPS rooms;

g) battery rooms (if not combined in UPS rooms);

h) power switch/generator set area/rooms;

i) MDF / meet-me rooms;

j) other telecommunications rooms (e.g. housing distribution framework for wiring and patching).

6.6.4 Redundancy

Service providers should ensure that all equipment providing environmental controls is installed with additional redundancy to cater for maintenance and/or failure and prevent adverse impacts on service levels. For example, additional air-conditioning units should be installed to provide a backup service during maintenance of the main air-conditioning system.

6.7 Telecommunications

6.7.1 General

Telecommunications provides vital links between recovery sites and the external world. All information (voice, data and possibly video) needs to be conveyed in a timely, efficient and effective manner, with all transmission from and into recovery sites made without disruption or quality degradation, and with no interception.

The following guidance applies to telecommunications links from the point of physical entry into service provider premises up to the physical equipment racks. (Telecommunications links outside service provider premises and under the control of telecommunications vendors are not covered by this International Standard).

6.7.2 Vendors

Service providers should have procedures and resources in place to assist organizations in negotiating with and bringing in any telecommunications service providers to meet minimum redundancy, reliability, security and quality standards.

6.7.3 Telecommunications single points of failure

Service providers should ensure that telecommunications single points of failure are minimised by having alternate telecommunications sources to permit switch over when failure occurs. Any alternate source should be an independent, different and non-shared set of telecommunications facilities and lines into a service provider recovery site. Thus service providers should ensure that there are no single points of failure in network facilities and lines entering into/out of their sites, and that there are alternate network links to permit switch-over when failure occurs, accomplished by:

a) network diversity;

b) telecommunications service provider diversity, which could be accomplished either by provision of a link to a different network service provider or by demonstrating connectivity to another node, building or facility where there is at least another network service provider.

6.7.4 Protection

Service providers should ensure that all telecommunications cabling supporting data/information and/or voice and video services within their premises is protected from interference, interception or damage, including by:

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

a) segregating power and telecommunications cables to prevent interference, and possible damage;

b) segregating telecommunications cabling based on fiber from other cables;

c) avoiding cabling through public areas to minimize the chances of eavesdropping;

d) providing conduits and/or trays with appropriate material strength to protect cables within from physical damage.

(Also see clause 6.9.2.)

6.7.5 Connectivity and capacity

Service providers should ensure that they are capable of providing telecommunications links with sufficient capacity and connectivity to enable organizations to connect internationally and to key information services and information feed providers without undue transmission limitations and delays.

6.7.6 Mobile communications

Service providers should ensure that when organization staff are located at their premises, they are able to communicate to external parties outside the premises using their mobile phones from pre-designated locations. For example, service providers could make arrangements with vendors providing telecommunications services and (if not themselves) the owners of the sites/buildings housing the recovery sites to improve mobile communications reception. Similar arrangements could also be made for the application of wireless network technology at service provider premises.

Service providers should also ensure diversity of mobile phone carriers so that there is no reliance on a single carrier.

All of the aspects regarding mobile communications will be subject to the contractual arrangements between service providers and organizations.

6.8 Power supply

6.8.1 General

All computing equipment depends on a continuous and stable source of power supply for normal operations, and interruptions to or disruptions of power supply could cause vital information to be lost or hinder recovery efforts. Thus service providers should ensure that policies and procedures are put in place to facilitate an adequate supply of electrical power always being available.

The following guidance applies to power supply links from the point of physical entry into service provider premises up to the physical equipment racks. (Power supply links outside service provider sites and under the control of power supply vendors are not covered in this International Standard.)

6.8.2 Power Supply Vendors

Service providers should ensure that they have procedures in place to be sure that the power supply provided by vendors meets minimum redundancy, reliability, security and quality standards, including procedures for the monitoring of incoming power supply and to resolve outstanding problems with vendors as they arise.

6.8.3 Power Supply single points of failure

Service providers should ensure that power supply single points of failure are minimised by having alternate power supply sources to permit switch-over when failure occurs, including:

a) generators (see clause 6.8.5.2);

b) Uninterruptible Power Supply (UPS) facilities and equipment (see clause 6.8.5.3).

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In addition, service providers should, where possible, have incoming power supplies into their recovery sites from independent, different and non-shared facilities and lines, for example with power supplies drawn from different power sub-stations.

6.8.4 Protection

Service providers should establish procedures and install the necessary facilities to isolate and protect all of their own and organization equipment operating in their premises against damage due to power increases and/or surges, lightning or other unforeseen circumstances. The types of power failure for which protection is needed include:

a) total failures (sometimes known as blackouts);

b) severely reduced voltage (sometimes known as brownouts);

c) spikes;

d) surges.

Further, adequate consideration should be given to potential electrical noise and its impact on sensitive equipment.

6.8.5 Alternate power supplies

6.8.5.1 General

Service providers should ensure that there are alternative power supplies in place for recovery sites for use on a temporary basis (when normal power supplies fail), and which are capable of catering for all organization recovery needs until resumption of normal power supplies.

6.8.5.2 Generators

Service providers should make available and install the necessary number of power generators as standby for use in preventing major power failures from affecting recovery operations. Power generators procured should meet capacity requirements and minimum safety, reliability and quality standards.

Power generators should be located where they cannot disturb operations at recovery sites nor pose any operational hazard or security breach, e.g. from noise pollution, fire or explosion.

Fuel tanks for generators should be located to minimise risks (e.g. sabotage and fire), preferably below ground level, with the amount of fuel maintained at a level that will enable the availability of standby power for a period not less than the contracted fuel supply lead time as specified in the supplier contract. Arrangements should be made for the immediate replenishment of fuel after use in the event of a disaster or failure. Fuel quality should be tested on a regular basis by qualified laboratories.

Power generators should be regularly tested by powering them up and using them, to ensure that a standby level of readiness is maintained. All tests of power generators should be undertaken in accordance with manufacturers' procedures and specifications.

6.8.5.3 Uninterrupted power supply (UPS)

Service providers should procure, install and maintain the necessary UPS units to enable organization mission critical networks and computing equipment to operate and shut down in an orderly manner.

UPS systems of the VFI-Class type (with no switch-over time), where power is supplied continuously from an inverter, should be used for mission critical networks and computing equipment requiring high availability.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

All UPS should be maintained and regularly tested in accordance with manufacturers' procedures and specifications to ensure operational readiness of the UPS to support the organization systems during disaster or failure.

As all UPS have innate potential hazards, they should be segregated or located at a safe distance from critical networks and computing equipment requiring high availability.

All batteries used in standby power supply units should be maintained, tested and/or replaced periodically, e.g. annually, according to manufacturers' specifications.

6.8.5.4 Safe switch-over

Service providers should establish procedures and facilities to ensure that switch-overs from normal power sources to power generators during power disruptions are accomplished in a safe manner and without affecting normal operations. The procedures and facilities should also ensure safe switch-overs to normal power sources when they are resumed.

6.8.5.5 Switch-over Alert

Service providers should ensure that any switch-over from normal power source to the alternate supply is detected and alerts are provided to the appropriate personnel for monitoring and action.

6.8.6 Emergency circuit-breakers

When required by organizations, service providers should ensure that emergency power circuit breakers are installed in organization designated areas where there are potential fire hazards due to heat given off by electrical devices. Disaster/failure situations could arise if electrical power supplies contributed to the stimulation and/or encouragement of the spread of fire inside the relevant areas/rooms. Emergency power circuit breakers should:

a) be installed for areas/rooms which contain equipment that consumes large amounts of power, e.g. three-phase electrical devices;

b) be installed next to entrance doors (either just inside or just outside) for areas/rooms wholly designated to an organization;

c) be installed near individual organization designated areas for areas/rooms shared by organizations;

d) be protected with covers against accidental activation;

e) cause all power supplies, including UPS, to be cut off from areas/rooms during emergencies.

The instructions for the operation of emergency power circuit breakers should be prominently displayed.

6.9 Cable management

6.9.1 General

As cables are needed to convey electrical power supplies as well as electronic information, service providers should ensure that steps are taken to protect cables from external damage and interference. These steps should include well-planned design, careful installation, production and maintenance of quality documentation (e.g. drawings and functions), and maintenance of that installed. The designs should cater for both current and projected future capacity and for ease of installation and maintenance.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.9.2 Protection

Service providers should establish procedures and facilities to isolate and protect all cabling, including that:

a) telecommunications and power cables are isolated from each other to prevent interference, e.g. by using separate risers or employing appropriate shielding;

b) cabling running through areas/rooms visited by the public or which cannot be guarded, are protected by such as concealed wiring of lines, conduits and/or trays with appropriate material strength to protect lines within from physical damage, running lines in mechanically solid and lockable ducts, and locking of distributors;

c) cables are selected based on the transmission requirements and the external environment. For example, strain-relieved cables should be used for overhead lines and extreme gradients (albeit the use of overhead cabling is not recommended), function-preserving cables should be used for areas exposed to heat and fire hazards, shielded cables should be used for areas with strong electrical and inductive interference fields, and armored cables should be used for situations where sufficient mechanical protection cannot be assured in any other way, e.g. for provisional layouts on floors and walls;

d) all cabling, cabling trays and ducts are checked periodically for damage, unauthorised modification, wire-tapping, or any other potential risk areas For example, renovation or alteration of site usage could result in shielded cabling being exposed accidentally.

(Also see clause 6.7.4.)

6.9.3 Routing plans

Service providers should ensure that precise and up-to-date location plans are kept for all cabling. Such plans provide useful information for cabling installation, maintenance, troubleshooting and repair, and also help to identify potential danger spots.

Individual detailed routing plans should be kept for each of the following cabling:

a) telecommunications/networking (data);

b) telecommunications/networking (voice);

c) telecommunications/networking (data/voice/video, i.e. IP convergence);

d) power supply.

Service providers should also ensure that general cabling plans showing the routing of all cabling are produced and maintained, containing details of:

a) physical routing across different portions of recovery sites, e.g. locations of any cable trays and inter-floor risers;

b) generic cable types, e.g. differentiating between power and telecommunication cables;

c) markings, as appropriate, to identify specific cable usage, e.g. of network user groupings.

6.10 Fire protection

6.10.1 General

Service providers should ensure that appropriate fire detection and suppression systems are in place to protect computing equipment and personnel working at their recovery sites. The capacity of these systems should be in proportion to the area/room sizes and the extent of protection required.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The following clauses contain the pertinent guidance for fire detection and suppression systems and the safety of personnel in recovery sites.

6.10.2 Regulatory compliance

Service providers should ensure that existing fire and safety regulations and requirements, as imposed by building inspectorates and/or similar bodies, are complied with.

6.10.3 Fire protection officer

Service providers should ensure that members of staff are designated to oversee compliance with fire and safety regulations. These staff could be fire protection officers or others who have been adequately trained in fire and safety regulations. Deputies should also be appointed, who should be competent to discharge the full duties in the event of the primary appointment holders being unavailable or otherwise unable to work.

6.10.4 Fire escape routes

Service providers should ensure that fire escape routes are planned, documented and communicated to all staff.

Fire escape routes should:

a) be clearly marked with exit signs which are illuminated during such as fire and power failure;

b) Not be obstructed at any time, e.g. bulky items should not be placed along escape routes thereby blocking or impeding movement along passage ways.

Whilst it should not be possible to open fire exit doors from the outside, for safety reasons they should not be locked from the inside.

All organization staff should be briefed on fire escape routes on arrival at recovery sites for DR plan testing or activation in the event of disaster or failure.

6.10.5 Fire response plan

Service providers should ensure that plans and procedures are established to deal with fire and smoke outbreaks, that include coverage of the:

a) procedures to be adopted for different fire and smoke situations;

b) evacuation plans for people located in different parts of recovery sites;

c) assembly areas for personnel briefing;

d) details for notifying the emergency services;

e) reporting and command chain;

f) procedures to deal with shortcomings uncovered by test drills, and personnel who do not comply.

Periodic fire related evacuation drills should be conducted to test different aspects of these fire/smoke response plans and procedures.

Water supply points for fire fighting should be clearly marked such that they can be quickly located during a fire, and, if required by local regulation, copies of the plans indicating water supply points should be lodged with the local emergency services.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.10.6 Hand-held fire extinguishers

Service providers should ensure that:

a) hand-held fire extinguishers are located in areas/rooms requiring protection, e.g. server and other computer rooms;

b) staff and long-term on-site contractors are briefed on the use of hand-held fire extinguishers, with demonstrations and hands-on usage as appropriate;

c) hand-held fire extinguishers are in such a way that they can be easily reached, taken down and activated for use during fire;

d) appropriate types of fire extinguisher are selected for usage in areas containing equipment which would be damaged if water was used to put out a fire, e.g. those that are carbon-dioxide based;

e) fire extinguishers should be clearly visible or have indicators as to where to find them;

f) fire extinguishers should be properly maintained according to manufacturers specifications and best practices.

6.10.7 Personnel safety

As the oxygen repressing/quenching gases used in some fire detection and suppression systems not only smother flames but can cause people to be asphyxiated, service providers should seriously consider systems that use non noxious gases – particularly for areas/rooms that contain large numbers of people. If it is not possible to install systems that use non noxious gases then the personnel that work in the areas/rooms fitted with systems deploying oxygen repressing/quenching gases must be fully briefed before working in those areas/rooms on the need to leave very quickly when a fire detection and suppression system is activated, and the exit route to follow. Appropriate warning posters should be produced and permanently displayed in prominent places in the areas/rooms to reinforce the dangers.

6.11 Emergency operations center (EOC)

6.11.1 General

Service providers should provide Emergency Operation Centers (EOCs) at their recovery sites that are appropriately equipped to enable organizations to supervise and maintain communications with their business units and external parties during disasters or failures. (In the context of this International Standard, the following clauses do not relate to EOCs set up by organizations at other than service provider sites.)

6.11.2 Equipment and supplies

Service providers should provide basic equipment and supplies to enable organizations to operate their EOCs, including:

a) telecommunications equipment, e.g. dedicated telephones lines and telephones, fax machines;

b) office equipment, e.g. PCs, printers, paper shredders and photocopiers;

c) office supplies, e.g. pens, pencils, markers, flashlights and spare batteries, scissors and printing paper.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.11.3 Dedicated physical facilities

6.11.3.1 General

Service providers should ensure that EOCs have dedicated physical facilities and associated equipment, with areas/rooms to cater for the requirements described below in clauses 6.11.3.2 to 6.11.3.4.

6.11.3.2 Voice communications room

Service providers should ensure that communications areas/rooms are provided to facilitate conversations by telephone, and should be:

a) equipped with the appropriate number of dedicated telephone lines (for incoming and outgoing calls) for organization usage;

b) equipped to receive external news, e.g. with television sets for the viewing of local, and as relevant, national and international news;

c) free from audible noise interference from other sources, e.g. noise generated from printers.

6.11.3.3 Meeting areas/rooms

Service providers should ensure that meeting areas/rooms are provided for organization staff to hold meetings and discussions, and should be:

a) large enough to comfortably accommodate the required maximum number of organization staff, e.g. leaders of recovery teams;

b) equipped with status boards to monitor and track recovery progress, e.g. white boards and wall-mounted presentation pads;

c) appropriately equipped to receive external news, e.g. with television connections and television sets if televised press conferences are required.

6.11.3.4 Media briefing areas/rooms

Service providers should ensure that media briefing areas/rooms are provided to facilitate communications with the press and outsiders, and should be:

a) sited at separate locations away from other EOC rooms to prevent unauthorized access by members of the press or visitors to recovery site and organization personnel, and confidential information, e.g. sited at a location outside the main recovery site perimeter;

b) accessible only to invited members of the press or visitors, with entry into the areas/rooms controlled;

c) appropriately equipped and furnished to support briefings to the media, e.g. with adequate space to accommodate estimated numbers of press representatives likely to attend disaster/failure related briefings.

6.11.4 Work area recovery team workspace

Service providers should ensure that workspace is provided for use by representatives from the various recovery teams, and should be appropriately furnished to support organization needs, e.g. with telephone lines, telephones, fax machines and associated office furniture.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.12 Restricted facilities

6.12.1 General

Service providers should ensure that facilities are provided that are restricted to authorized access for designated purposes only and have the related levels of protection, including:

a) server rooms;

b) other computer rooms;

c) data media archive rooms;

d) environmental control plant rooms (housing air-conditioning equipment);

e) main communications switch rooms;

f) UPS rooms;

g) battery rooms (if not combined in UPS rooms);

h) power switch/generator set area/rooms;

i) MDF / meet-me rooms;

j) other telecommunications rooms (e.g. housing distribution framework for wiring and patching).

6.12.2 Areas/rooms housing main computer systems

6.12.2.1 General

Service providers should ensure that areas/rooms housing main computer systems are designed and built with levels of security additional to that provided for normal areas/rooms, in line with that described in the following clauses 6.12.2.2 to 6.12.2.5.

6.12.2.2 Physical access

Service providers should ensure that the doors providing access to areas/rooms housing restricted facilities are of strong construction, are fitted with high-quality access control mechanisms and good security locks, and that the windows, at minimum for those on the ground and first floors, are fitted with unbreakable glass and good security, and, if appropriate, security shutters.

All access should be monitored on a continuous basis.

6.12.2.3 Potential hazards

Service providers should ensure that there is adequate isolation, protection against, avoidance from, and removal of potential sources of disruption from areas/rooms housing restricted facilities, with the following measures taken:

a) avoiding routes taken in buildings by service pipes and cables, both overhead and below, e.g. pipes carrying water should not pass through server rooms;

b) incorporating appropriate protection in the design of areas/rooms, e.g. with raised flooring, dry-pipe water sprinklers, water/liquid seepage detectors with automatic solenoid valves and fire extinguisher systems that would not be destructive to delicate equipment when activated.

Service providers should also ensure that adequate consideration is given to protection against potential electro-magnetic interference from nearby cellular network transmission facilities, three-phase generators, transformers and high voltage/high current power lines, e.g. by using shielding or maintaining safe distances from electro-magnetic interference sources.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.12.2.4 Power supply

Service providers should ensure that each of the areas/rooms housing restricted facilities have electrical supplies that are separated and isolated from the electrical supplies to the rest of the buildings, with:

a) separate power distribution boards and associated circuit breakers for these areas/rooms;

b) all power distribution boards properly enclosed.

6.12.2.5 Electrical connectivity

Service providers should ensure that as heat can be generated from loose electrical connections, thus presenting a potential hazard, electrical connectivity from distribution boards to critical facilities and equipment is checked periodically, e.g. by conducting infra red scanning of distribution boards on a periodic basis.

6.12.3 Air-conditioning

Service providers should ensure that:

a) temperature and humidity measurements are carried out in areas/rooms housing restricted facilities to check whether air-conditioning systems are operating in conditions as required by ICT systems and equipment installed in the areas/rooms;

b) measurements are taken at different times of the day;

c) air-conditioning systems are:

   1) capable of maintaining room temperature and humidity within limits required by the ICT systems in the areas/rooms;

   2) designed to cater for breakdown or maintenance of individual air-conditioning units, e.g. by design with spare capacity or additional back-up air-conditioning units.

6.12.4 Fire and smoke

Heat, smoke and fumes from a fire can pose a significant threat to both human lives and sensitive computing equipment. Thus, service providers should ensure that not only is fire protection directly afforded to heat sensitive computing equipment, but also that sufficient fire breaks are installed to prevent heat radiation and fire, smoke and fumes from spreading. It should be noted that separate fire and smoke protection zones may well be needed for different parts of recovery sites.

6.12.5 Personnel health and safety

6.12.5.1 General

Service providers should ensure that personnel health and safety takes priority over all protection policies and procedures for facilities and ICT equipment.

6.12.5.2 Ventilation

Service providers should ensure that areas/rooms that are continuously occupied are ventilated to provide sufficient levels of fresh air for occupants, e.g. with the number of air-changes per hour in a given area/room calculated on the basis of the heat generated by the equipment in the area/room and the cooling needed.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.12.5.3 Lighting

Service providers should ensure that adequate lighting is provided for safe operations conducted by personnel in the areas/rooms housing restricted facilities, including emergency lighting for use during emergencies, e.g. if the power supply was cut off during a fire.

6.12.5.4 Fire suppression systems

There are dangers to people from the oxygen repressing/quenching gases used in some fire detection and suppression systems – see clause 6.10.7 above for more detail.

6.12.5.5 Electrically controlled doors

Service providers should ensure that areas/rooms where all doors are locked electrically to control personnel access are capable of being opened from within during power failure or fire to facilitate the safe departure of personnel from the areas/rooms, e.g. there should be manual overrides of electrical door locking systems from within during power failure or fire, or the doors should be designed to be in the open status during such situations.

6.12.5.6 Public announcement system

Service providers should ensure that public announcement (PA) systems or equivalents are installed and regularly tested at recovery sites to enable audible announcements to be made to all personnel, e.g. during a fire situation at a recovery site, a PA system could be used to alert all personnel to leave the site.

6.12.6 Alarm systems

Service providers should ensure that appropriate detection and alarm devices are installed that at minimum provide warnings of smoke, fire, water/liquid seepage and physical break-ins and are capable of being heard both inside and outside the areas/rooms concerned.

6.12.7 General installation consideration

Service providers should ensure that areas/rooms housing restricted facilities do not have any marking regarding their use, to help protect confidentiality and enhance security, e.g. signboards bearing organization names should not be posted on the doors of organization subscribed facilities. Further, the areas/rooms housing restricted facilities should:

a) be designed and located away from public areas such as reception points and toilets, and with facilities to prevent access from unauthorised persons;

b) be unobtrusive from outside the building perimeter, e.g. by shielding all windows or having no windows at all;

c) include appropriate protection design considerations such as dry-pipe water sprinklers, water seepage detectors with automatic solenoid valves and a fire extinguisher system that is not destructive to equipment when activated;

d) either have in use special grade glass that is not easily breakable or be equipped with glass breaking detection, if they are fitted with glass walls or windows that are accessible from outside the building;

e) have a load rating for all supporting structures, particularly for raised floors and ramps, that has been planned with current and potential future load considerations in mind;

f) have placement of equipment within them that takes into account the circulation of hot and cold air such as not to cause undue concentration of heat within certain parts of the areas/rooms;

g) have a design that has accounted for both current and future requirements, e.g. with adequate power supply and air-conditioning capacities covering current and projected future consumption.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.12.8 Areas for exclusion

Service providers should ensure that areas/rooms housing restricted facilities are not sited in the following locations if any of the related dangers are present:

a) in basement areas, if they are susceptible to pipe burst, water leakage or flooding;

b) in areas immediately below flat roofs, if they are susceptible to rainwater seepage;

c) in ground floor areas, if they are facing public traffic zones and susceptible to attacks, vandalism and force majeure due to traffic accidents in the vicinity of the buildings;

d) areas in close proximity (areas/rooms next door, a floor above or below) to other areas/rooms that are used for the handling or storing of hazardous materials such as easily combustible fabric, chemicals or explosives.

6.13 Non-recovery amenities

6.13.1 General

Service providers should ensure that, in addition to providing facilities and equipment to enable actual recovery, they provide facilities that will cater for the well-being and welfare of organization staff stationed at their premises during recovery.

6.13.2 Personnel

Service providers should ensure that they provide adequate basic amenities to cater for organization staff working at their premises during recovery, including:

a) rest areas;

b) toilets;

c) drinking water;

d) three meals each day (subject to contractual arrangements with organizations).

6.13.3 Parking

Where circumstances permit, service providers should ensure that adequate parking facilities are available for organization staff when working at the service provider premises during recovery, and that, if the premises are used solely by the service provider, access to these parking facilities is monitored and controlled on a 24 $\times$ 7 basis.

6.13.4 Transportation

Service providers should ensure that the locations of their recovery sites are accessible to organization staff on a 24 $\times$ 7 basis, e.g. by locating their recovery sites near public transportation drop off points and/or, subject to contractual arrangements with organizations, providing chartered vehicles to pick up organization staff from selected public transport drop off points and return them to those points.

6.13.5 Medication

Service providers should ensure that they can make provision to supply light medication to organization staff who may be working under tremendous work and time stress at recovery sites during recovery, e.g. by having a first aid kit at the premises.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.14 Physical facilities and support equipment life cycle

6.14.1 General

Through facility\equipment life cycle management, service providers should ensure that all physical facilities and support equipment are fit for their intended purposes on a continuous basis, in order to assure accessibility of organizations to subscribed services.

Service providers should institute proper systems of care and attention covering the life span of each facility and equipment item used, with the life span covering building, installation, commission, operation, repair, maintenance, upgrade and replacement of the physical facilities and equipment as appropriate.

6.14.2 Policies and procedures

Service providers should ensure that policies and procedures are established for physical facilities and equipment, covering installation, commission, operation, repair, maintenance, upgrade and replacement, e.g. including a policy stating that all attempts should be made to repair equipment on site before removal to a supplier's site.

6.14.3 Compliance with requirements

Service providers should ensure that all physical facilities and support equipment complies fully with current recommendations by equipment manufacturers, professional standards/practices and/or regulatory requirements.

6.14.4 Qualified professionals

Service providers should ensure that all physical facilities and support equipment are handled by qualified professionals, e.g. that high tension electrical installation and commissioning is undertaken by qualified professional engineers.

6.14.5 Service situations

Service providers should ensure that policies and procedures are established to handle the following situations during repair, maintenance, upgrade or replacement of physical facilities and equipment:

a) on-site – as additional equipment may be employed by vendors during servicing, steps should be taken to ensure that the additional equipment does not impact on the security and operations of recovery facilities and equipment. Proper isolation of equipment should be undertaken during servicing, e.g. with appropriate procedures in place for the replacement of faulty equipment and installation of new equipment;

b) off-site – for which, whilst there are similar issues to on-site servicing, because direct vendor supervision is difficult, additional steps must be taken, e.g. if a malfunctioning item of equipment needs to be taken back to the vendor site for thorough investigation, extra checks and tests for security and functionality should be undertaken before the repaired item of equipment is put back into operational service;

c) unavailability - as equipment could be unavailable during servicing, appropriate steps should be taken to ensure services offered to organizations are not unduly affected and the situation remains under control during this period, e.g. by activating standby or alternative backup equipment before equipment maintenance is performed;

d) re-connection - equipment to be put back to service after repair, maintenance, upgrade or replacement should be checked and tested to ensure that they are set to the correct functioning modes and integrated back into the relevant systems, e.g. a replaced intrusion detector connected to the main physical security system must be re-tested for connectivity.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.14.6 Reviews

6.14.6.1 General

Service providers should ensure that:

a) procedures are established for periodic audit reviews of each physical facility and equipment item in their premises, as part of the physical facility and equipment audits;

b) appropriately qualified personnel, either internal or external, are designated with the authority and responsibility to conduct physical facility and equipment audit reviews.

6.14.6.2 Review reporting

Service providers should ensure that reports are generated after each review, with the report format including:

a) scope and objectives;

b) steps and procedures followed;

c) findings and results;

d) corrective actions to be taken;

e) deviations, and supporting rationale for future review and action.

6.14.6.3 Scope

Service providers should ensure that the scopes of reviews include:

a) recovery site premises and perimeter physical protection;

b) physical security equipment;

c) environmental control equipment;

d) ICT equipment and facilities;

e) telecommunications equipment and facilities;

f) power supply;

g) fire and smoke protection;

h) water/liquid protection.

6.14.6.4 Triggers

Service providers should ensure that reviews of physical facilities and equipment are undertaken when there are significant changes in organization requirements, e.g. when an organization adds extra pieces of high power consumption equipment, the capacity of existing power supply, UPS and generators should be reviewed.

6.14.7 Decommissioning

Service providers should ensure that all physical facilities and equipment that have reached the end of their useful life are decommissioned and/or removed by appropriately qualified personnel and according to current

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

recommendations by equipment manufacturers, professional standards/practices and/or regulatory requirements.

6.14.8 Spares and accessories

Service providers should ensure that adequate spares and accessories are kept on hand to enable the necessary repair, maintenance and replacement of physical facilities and equipment in a manner that will minimise disruption to normal operations. The extent and types of spares and accessories to be kept should reflect the downtime figures in the SLAs that service providers have with organizations and the capability of vendors to supply and repair failed equipment within stipulated time frames.

6.14.9 Inventory

Service providers should ensure that they maintain up-to-date inventories of their physical facility and equipment items.

6.14.10 Continuous monitoring

Service providers should ensure that critical physical facility and equipment items are monitored on a continuous basis to ensure their availability, e.g. the UPS system for a main computing system should be connected to the network operations center and monitored from there.

6.14.11 Software and firmware

Service providers should ensure that policies and procedures pertaining to the operation of physical facility and equipment items are equally applicable to associated firmware and software, either embedded or constituting part of the facility or equipment operation, as appropriate.

6.15 Testing

6.15.1 General

Service providers should ensure that testing forms an integral part of maintaining physical facilities and equipment in the required high quality condition to support the services offered to organizations.

6.15.2 Scope

Service providers should ensure that physical facilities and equipment, including those listed from in clause 6.14.6.3 above, are periodically checked and/or tested.

6.15.3 Staff

Service providers should ensure that the staff operating their recovery facilities and equipment, and their operational procedures, are also tested - ideally in conjunction with the testing of the physical facilities and equipment.

6.15.4 Test life cycle

Service providers should ensure that the planning, conduct, documentation and review of tests encompasses:

a) tests conducted at least once a year for critical capability and capacity that affects services to organizations;

b) tests conducted when there are any significant changes in organization requirements and/or changes in service provider capacity and capability that affect their services to organizations, e.g. upgrades of physical facilities, equipment, telecommunications and power supply resources;

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

c) all tests, whether announced or unannounced, properly planned and designed not to cause any damage, either of a permanent nature or which can only be rectified with difficulty;

d) steps taken to ensure that situations remain under control during tests;

e) critical tests approved and authorised by service provider management;

f) for critical tests, service provider management and organizations informed before the start of each test;

g) all tests, test objectives, test plans and test results documented for follow up review or audit for effectiveness;

h) shortcomings discovered in tests rectified at the earliest possible moment and no later then the next set of tests;

i) shortcomings (not rectified) justified and clearly communicated to service provider management, with the potential consequences of each omission presented;

j) a schedule established to ensure all possible tests are executed at some juncture, e.g. the different tests should have been tested at least once every five years;

k) Tests different from year to year where possible, also serving to introduce variety and remove predictability for the participants, e.g. this year tests should not be exactly the same as those conducted last year.

7 Outsourced service provider's capability

7.1 General

Outsourced ICT DR service providers should provide the basic service capabilities required by organizations. This includes having qualified staff, the capacity to support simultaneous invocations of DR plans by different organizations, all capabilities and services offered to organizations audited on a regular basis, and their own fully documented and tested business continuity, including disaster recovery, plans in place.

7.2 Review organization disaster recovery status

Unless it is clear in contracts between outsourced service providers and organizations (on which disaster recovery services are to be provided) that there is no service provider liability for any incidents that might occur due to deficiencies in organisation disaster recovery planning and any subsequent business related consequences, it is important that service providers check organization disaster recovery status before contracts are signed. Service providers should check that:

a) an organisation has properly addressed disaster recovery and thus has a quality DR plan in place;

b) an organization's DR plan has been produced by following the recognized sequence of required disaster recovery tasks. Service providers should ensure that an organisation:

   1) has first conducted a business impact analysis and thence a risk assessment, and then on the basis of the results identified and documented its business recovery priorities and requirements;

   2) on the basis of the agreed business recovery requirements, has identified and documented the correct and most cost effective disaster recovery strategy appropriate to its business environment;

   3) next, when the disaster recovery strategy has been agreed, and thus the organisation knows its best way forward, produced (and if possible tested) the DR plan;

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4) implemented risk reduction controls to reduce the likelihood of having to invoke the DR plan in the first place and/or which will reduce the impact of a disaster or failure should one occur.

The overall recommended approach that organizations should follow for disaster recovery planning is shown in Figure 3 below.

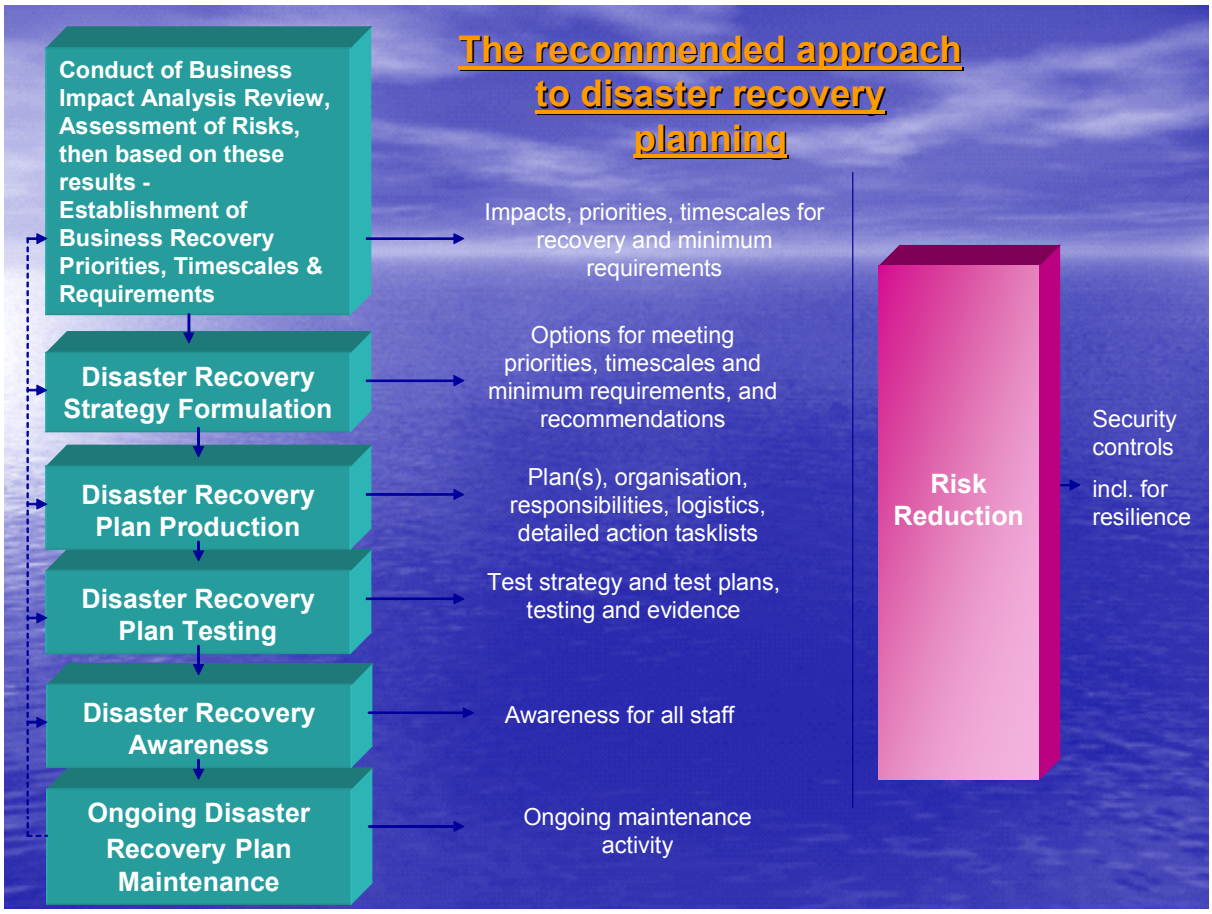

Figure 3 — Disaster Recovery Planning Approach

Thus, in summary the recommended approach to disaster recovery that should be followed by any organization, and thus checked by service providers, consists of a number of discrete stages, together aimed at achieving a comprehensive and viable DR plan that fully meets the requirements of the organisation's business in the event of a disaster or failure. These stages are:

a) establishing business recovery priorities, timescales and requirements (based on the results of business impact analysis review and thence risk assessment);

b) disaster recovery strategy formulation;

c) DR plan production;

d) DR plan testing;

e) ensuring disaster recovery awareness for all staff;

f) ongoing DR plan maintenance;

g) risk reduction.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The first five stages are consecutive. When a DR plan has first been produced and tested, the sixth stage follows on over time, and is conducted at regular intervals and after any significant changes that might affect the validity of the plan, revisiting any of the other stages for update purposes as is necessary. The seventh stage is conducted in parallel with the other stages.

In particular, each organization also needs to identify the individuals (and their deputies) who will perform the following functions should a disaster or failure occur:

a) the person in charge of determining how best to address the disaster or failure;

b) the composition of the team who will take the decisions to invoke the DR Plan as the disaster or failure unfolds (Refer to clause 5.8.3 and 5.8.4 above);

c) the person who invokes use of third parties.

Organizations and their service providers should also:

a) instruct the staff on where they should go to work (or stay at home) and what they should do;

b) identify deputies (possibly 3rd or lower choices) for key people and provide them with appropriate training.

7.3 Facilities requirements

All the requirements to be met by service providers as specified in clause 5 apply to outsourced service providers.

7.4 Expertise

7.4.1 General

The capability of outsourced service providers to offer and support their services depends on their expertise. This can be the experience they have acquired over the years through supporting organization testing and actual recovery, and/or the expertise residing in the experience of the staff they hire. Related to this, it is important that outsourced service providers have ‘systems’ in place to retain their expertise.

7.4.2 Experience

Outsourced service providers should ensure that they can provide organizations with summary lists describing their ICT DR project team expertise, covering:

a) planning – the experience of their staff sited locally, elsewhere in the country or overseas, who undertake planning;

b) operations - the experience of the local staff who support recovery operations;

c) track record - details of capability and capacity including of:

   1) the diversity and number of organizations supported across different business environments in the past and at present;

   2) the duration, costs and resources deployed.

   (The outsourced service provider should take precautions to ensure that any confidentiality agreements signed with organizations, e.g. which will prevent the quoting of organization names as references without organizations’ agreements and/or the revealing of any details of organizations’ ICT DR plans, are adhered to.)

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The following should be used as indicators of track records:

3) diversity and experience - including summary descriptions across the various industries of those organizations subscribing to their services;

4) types of services offered - including summary descriptions of their services subscribed to by organizations;

5) regional experience – including summary descriptions of experiences in supporting organizations across the region.

d) extent of involvement - outsourced service providers should provide summary descriptions of the extent of their involvement and expertise in the areas of:

1) project management;

2) risk assessment and management, including:

i) business impact analysis;

ii) risk evaluation;

iii) risk treatment;

3) business recovery requirements determination;

4) disaster recovery strategy formulation and selection;

5) DR plan development;

6) disaster recovery awareness and training;

7) DR plan testing;

8) actual recovery using DR plans;

9) DR plan maintenance.

7.4.3 Knowledge retention

Outsourced service providers should ensure that they establish a 'system' to capture details and maintain a knowledge base of the past and present ICT DR projects they have undertaken and the organizations they have provided ICT DR services to, with the 'system' encompassing:

a) a human resource backup and succession plan for key personnel;

b) in-house knowledge sharing;

c) information on the recovery effort for past projects;

d) the knowledge base preferably being software based and fully automated, e.g. web enabled, and, if not, either manually recorded and maintained, e.g. with hardcopy files and cabinets, or a composite of automated and manual repositories used.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.4.4 Management of staff

Outsourced service providers should ensure that, as staff are the main source of their expertise, a proper "system" is established to manage the staff directly involved in organization recovery operations that includes:

a) formal designations identifying appointments (rather than the actual staff names), that indicate the roles, accountability, responsibility and authority of all operations staff directly involved in providing recovery services to organizations during disasters/failures;

b) all operations staff made aware of their designations and recovery tasks;

c) back-up and succession plans for key personnel directly involved in providing recovery services to organizations during disasters/failures;

d) all designated back-up personnel appropriately trained to be competent to fulfil the related roles in the event of the main designated personnel being unavailable or unable to fulfil their roles;

e) the pre-designation of ICT DR co-ordinators to oversee and coordinate the support for each organization during recovery, with:

   1) ICT DR co-ordinators with the appropriate training, experience and competency in the relevant ICT DR areas;

   2) each ICT DR co-ordinator overseeing and coordinating only ONE actual recovery at any one time (ensuring staff dedication to each organization during simultaneous recoveries);

   3) deputy ICT DR co-ordinators who are competent to discharge all duties if the relevant ICT DR co-ordinators are unavailable or unable to fulfil their roles;

f) the provision to each organization of the list of the key operations staff who will be involved in the organization's actual recovery, including their designations, tasks, and ICT DR qualifications as appropriate;

g) all staff directly involved in supporting organization recovery operations preferably being dedicated staff employed specifically for ICT DR activities and not supporting non-ICT DR operations on concurrent or secondary appointments.

7.5 Logical access control

7.5.1 General

Logical access control is applicable to outsourced service providers that provide operational support for organization computer systems at their recovery sites, including where they supply their own staff to operate those organization computer systems during recovery. The guidelines should enable outsourced service providers to describe their abilities and capabilities to operate organization computer systems. For organizations that choose to use their own staff to operate their computer systems at provider recovery sites, these guidelines will need to be interpreted and moderated as appropriate.

Service providers should ensure that the policies and associated procedures for day-to-day operations at their recovery sites are fully documented and maintained. Further, service providers should ensure that the selection, development, and use of security controls within their recovery sites are commensurate with the assessed risks and the services provided to organizations.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

With regard to the provision of logical access control, the underlying principles for service providers should be that:

a) one organization's information cannot be disclosed to another even though shared computing and related equipment is used at a recovery site;

b) the responsibility for maintenance of logical access control is handed over to organizations that operate dedicated provider supplied computer systems with their own staff during recovery;

c) organizations that operate their own computer systems at service provider sites are responsible for the logical access control facilities in place for their operations during recovery.

7.5.2 Deployment

Outsourced service providers should ensure that all computer systems at recovery sites are provided with logical access control facilities commensurate with the assessed risks and recognized standards, at minimum with secure access control lists indicating for every valid username/user id and password combination what each combination can access – record, file, etc., and for what purposes – read, write, delete, execute etc. and combinations thereof.

7.5.3 Authorization

Outsourced service providers should ensure that authorizations for all logical access are granted based on the "need-to-know" and "need-to-hold" principles, and that all logical access authorizations are documented, reviewed and updated on a periodic basis.

7.5.4 Staff resignation

Outsourced service providers should ensure that formal processes are in place to deal with staff joining or leaving, e.g. the security personnel should be notified immediately of staff resignation and all access revoked accordingly.

7.5.5 Temporary access

Outsourced service providers should ensure that the policies and procedures for logical access control address the needs of such control on a temporary basis, e.g. where a guest account is required for a limited time period, and cover the following:

a) authorization and creation of 'guest' logical access control profile;

b) usage timing and duration;

c) activity log checking;

d) expiry.

7.5.6 Monitoring

Outsourced service providers should ensure that procedures are in place and operational on 24 x 7 basis for the monitoring and logging of all logical access to computer systems.

7.5.7 Remote access

Outsourced service providers should ensure that, where there is remote access to recovery computer systems, policies and procedures are in place for the control of that remote access, e.g. a policy should be documented on the use of laptops and other portable devices and remote log-ins to recovery facilities from home and other types of remote location.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.5.8 Security functions and roles

Outsourced service providers should ensure that:

a) security functions and roles are established to monitor and control logical access, including for the periodic analysis of log files and other checks of selected ICT systems;

b) the responsibilities of the security functions and roles are assigned to specific staff;

c) deputies are appointed for all critical functions and roles who are competent to fulfill all duties in the event that primary appointment holders are unavailable or unable to fulfill their roles;

d) all appointed staff are adequately trained before being assigned their security functions and roles, to ensure that staff remain competent in undertaking their assignments;

e) periodic refresher or update courses are arranged for all security functions and roles, to ensure that appointed staff remain competent in undertaking their assignments;

f) to maintain alertness, procedures are established to test staff assigned with security functions and roles on a periodic basis, e.g. once a year;

g) the staff responses during tests are assessed against the criteria given in clause 5.7.5.2.

7.5.9 Tests

Outsourced service providers should ensure that test objectives, test plans, test executions and test results form an integral part of maintaining the integrity of logical access control systems. (The policies and procedures for the planning, conduct, documentation, and life cycle of tests are given in clause 7.16.4 below.)

7.5.10 Logical security incidents

Outsourced service providers should ensure that the handling of logical security incidents follows the information security incident management process referred in clause 5.7.5.

7.6 ICT equipment and operation readiness

7.6.1 General

Outsourced service providers should ensure that there are adequate policies and procedures in place so that their computing and related equipment provided to support organization continuity and recovery needs are installed, operated and maintained in optimal condition. The underlying principle of equipment and operation readiness is accessibility of organizations to subscribed services. All computing and related equipment should be at a constant and ready state to respond to organization needs.

7.6.2 Policies and procedures

Outsourced service providers should ensure that policies and procedures are established for computing and related equipment covering installation, commission, operation, repair, maintenance, upgrade and replacement. For example, a maintenance policy should state that all data or information should be physically and completely erased, such that no inference can be drawn as regards previously stored data, before the equipment is removed from site.

7.6.3 Compliance with requirements

Outsourced service providers should ensure that all computing and related equipment is installed, commissioned, operated, repaired, maintained, upgraded and replaced according to current recommendations

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

by equipment manufacturers, professional standards/practices and/or regulatory requirements. For example, installation should be undertaken only by qualified professionals.

7.6.4 Service situation

Outsourced service providers should ensure that policies and procedures are established to handle the following situations during repair, maintenance, upgrade or replacement of computing and related equipment:

a) on-site. Additional equipment and software may be employed by vendors. Steps should be undertaken to ensure that these additional equipment and software do not impact the security and operation of the equipment subsequently. Proper isolation of equipment should also be undertaken during service duration. For example, diagnostic software may be installed or remotely activated to troubleshoot faulty equipment. These software should be completely disabled and erased before putting the repaired equipment back into service;

b) off-site. This is similar to on-site servicing. Direct vendor supervision would be difficult. Additional steps to those undertaken for on site procedures should be specified as appropriate. For example, where a malfunctioned piece of equipment needs to be taken back to the vendor's site for thorough investigation, extra tests for security and functionality should be undertaken before putting the repaired equipment back into service; (For guidance on controls, reference should be made to ISO/IEC 27001 and 27002.)

c) unavailability. Equipment would be unavailable during repair, maintenance, upgrade or replacement. Appropriate steps should be undertaken to ensure services offered to organizations are not unduly affected and the situation remain under control during this period, for example activating alternate standby or backup equipment before performing equipment maintenance;

d) reconnection. Equipment to be put back to service after repair, maintenance, upgrade or replacement should be checked and tested to ensure that they are set to the correct functioning mode and integrated back to the main system (wherever applicable), and powered down totally and re-started before being put back into service.. For example, a replaced router should be configured to the proper network setting and tested for connectivity and operations.

7.6.5 Spares and accessories

Outsourced service providers should ensure that adequate spares and accessories, where practicable, are kept on hand to effect the necessary repair, maintenance and replacement so as to minimise disruption to normal operation. For example, there should be an adequate supply of spare batteries for portable computers for their immediate use.

7.6.6 Portable equipment for recovery

Outsourced service providers should ensure that policies, procedures and guidelines are established for the usage of portable equipment (such as notebooks or mobile phones) for recovery purposes by outsourced service provider staff. For example, guidance should be provided to staff on how to deal with the loss or malfunction of a notebook used in crucial recovery activities due to theft or virus infection, and on the usage of mobile phones in close proximity to computing and telecommunications equipment.

7.6.7 Monitoring

Outsourced service providers should ensure that critical pieces of computing and related equipment are monitored on a continuous basis, for example with remote monitoring of critical network equipment in locked cabinets not easily accessible physically.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.6.8 Overvoltage protection

Outsourced service providers should ensure that, where practicable, all computing and related equipment is protected against electrical overvoltage surge. Overvoltage surge can be caused by lightning strike, cross-coupling and switching operations. The protection should include the following:

a) overvoltage protection devices installed, e.g. surge arresters and optocouplers;

b) overvoltage protection devices inspected and checked periodically and after incidents such as direct lightning strike and overvoltage peaks in the power supply system, and replaced if damaged;

c) potential equalisation for all computing and related equipment protected with overvoltage protection (for the latter to be effective).

7.6.9 Changes and upgrade

Outsourced service providers should ensure that any upgrade or change of computing and related equipment, e.g. to reflect current technology, does not affect the support of organizations' continuity and recovery needs according to contract requirements. Thus, outsourced service providers should establish procedures to check for compatibility of all upgraded or changed computing and related equipment.

7.6.10 Software and firmware

Outsourced service providers should ensure that policies and procedures to maintain equipment and operation readiness are equally applicable to firmware and software, as appropriate.

7.7 Simultaneous recovery support

7.7.1 General

Outsourced service providers should have sufficient facilities and staff to meet their contractual obligations when multiple clients simultaneously activate the DR services. This includes dedicated facilities, computing and related equipment, and personnel that can be deployed instantly without the need for sharing or to have undue restriction being imposed on organizations. Organizations should be able to use the full range of outsourced service provider resources as provided in their service contracts. These resources should be available on a continuous basis without disruption or interruption for the contracted duration. It is assumed that outsourced service providers will maintain the necessary spare capacity and redundancy in terms of facilities, computing and related equipment, and personnel to provide this capability.

7.7.2 Capability and capacity

Outsourced service providers should ensure that they can provide simultaneous recovery services at their recovery facilities for more than one organization, with each organization being able to operate its subscribed recovery facilities in a manner that is independent of others.

7.7.3 Scope

Outsourced service providers should ensure that all services and supporting resources (such as their recovery support staff, power supplies, IT and telecommunication) offered to affected organizations during simultaneous recoveries are not diminished, reduced or affected in any manner.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.8 Levels of service

7.8.1 General

Outsourced service providers should ensure that they can provide ranges of service levels to suit the varying needs of organizations, such that organizations can select the particular levels of service that best suit their recovery needs.

7.8.2 Round-the-clock service support

Outsourced service providers should ensure that they are capable of offering services on a 24 × 7 basis, either in remote or fully manned mode.

7.8.3 Hardware and software platforms

Outsourced service providers should ensure that they can:

a) support the prevailing hardware and software platforms of key industry vendors, at minimum for the hardware and up to the operating system level;

b) provide lists of the hardware and software corresponding to the services subscribed to by organizations, as part of contractual agreements;

c) communicate details of updates to hardware and software to organizations for their deliberations.

7.8.4 Categories

Outsourced service providers should be able to provide the following categories of service levels for their facilities and equipment:

a) shared, with organizations able to invoke their subscribed services on a first-come-first-served basis, and services offered to subsequent organizations invoking their contracted services subject to availability of facilities and equipment (i.e. not utilized by the preceding organizations);

b) dedicated, with organizations able to invoke and receive their subscribed services, with related facilities and equipment, on an exclusive sole use and reserved basis, and the reserved facilities and equipment not available for use by or sharing with other organizations.

7.9 Types of service

7.9.1 General

The following clauses describe the basic range of services that outsourced service providers should be capable of providing to organizations. The range is by no means inclusive, and it is foreseen that competition and technology changes will result in new services and that some unique to organization requirements may necessitate customization of specific services (subject to negotiation and contract agreement between the relevant outsourced service providers and organizations).

It should be noted that whilst outsourced service providers may choose to collaborate with external parties or consultants where it considers that some services can be better performed by these external suppliers, the responsibilities for such service collaboration remains with outsourced service providers. Guidelines on outsourcing are provided in clause 5.6.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2008 – All rights reserved
Not for Resale

7.9.2 Recovery site service

Outsourced service providers should be capable of providing the following categories of recovery site services:

a) cold site, with adequate space and associated infrastructure - power supply, telecommunications connections, environmental controls, etc - to support organization ICT systems, which will only be installed when DR services are activated;

b) warm site, that is partially equipped with some of the equipment, computing hardware and software, and supporting personnel, with organizations installing additional equipment, computing hardware and software, and supporting personnel when DR services are activated;

c) hot site, that is fully equipped with the required equipment, computing hardware and software, and supporting personnel, and fully functional and manned on a 24 × 7 basis so that it is ready for organizations to operate their ICT systems when DR services are activated.

These sites should be maintained in an operational status ready to receive organization staff and equipment when activated.

7.9.3 Work area recovery

Outsourced service providers should be capable of providing physical work areas for recovery (WAR) to organizations during recovery. Each WAR should be appropriately furnished to support organization needs as specified in clause 6.11.4.

Outsourced service providers should be capable of providing WAR to support more than one organization simultaneously. The policy and details for simultaneous support are described in clause 7.7.

(All WAR aspects will be subject to contractual arrangements between service providers and organizations.)

7.9.4 Information services/information feeds

Outsourced service providers should be capable of providing access for organizations to key information services/information feed providers, e.g. market data providers.

(All information service/information feed aspects will be subject to contractual arrangements between service providers and organizations.)

7.9.5 Transactional services

Outsourced service providers should be capable of providing access for organizations to transactional services providers.

7.10 Proximity of services

7.10.1 General

In general, disasters and failures can take various forms and are not necessarily limited to events which occur within close geographical proximity. There could be disruptions to common power supplies and telecommunications services, and two or more organizations could be affected simultaneously.

Outsourced service providers should ensure that they take account of the risks associated with simultaneous adverse impacts on one or more organizations by the same disaster or failure, and align their capabilities and capacities accordingly. For example, to mitigate against proximity related problems, outsourced service providers should only offer services to one organization of a group that are located in close proximity. They can also refrain from offering services to organizations that are located close to their own premises.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.10.2 Risk mitigation

Outsourced service providers should establish processes to minimize the risks associated with organizations that are in close proximity, including:

a) establishing plans for corresponding increases of capability and capacity to service simultaneous organizations during disaster recovery, e.g. with prior arrangements with external parties;

b) establishing procedures to ensure that recovery site locations are not likely to be impacted by the same disaster or failure, e.g. with recovery sites located at such a distance that the likelihood of the same disaster or failure affecting both organizations and outsourced service provider facilities is minimized, including in the case of fire and flooding.

7.10.3 Disclosure to organizations

Outsourced service providers should ensure that on request they disclose to organizations details of the proximities of other organizations to which they provide and/or are offering services. At minimum details should be provided of the industry types and numbers of organizations in adjacent buildings, in the nearby vicinity or sharing the same utility, which could be adversely impacted by the same disaster or failure.

7.11 Subscription ratio for shared services

7.11.1 General

Besides dedicated services, outsourced service providers should maintain sensible ratios of their service offerings and the number of organizations subscribing to each service offering. The principles underlying subscription ratios relate to outsourced service provider capabilities and capacities to service their organizations during simultaneous invocations in the event of disaster or failure.

7.11.2 Self-restraint

Outsourced service providers should establish processes to ensure that their shared services are not unduly oversubscribed without a corresponding increase in their capabilities and capacities. This should encompass:

a) both policy and procedural undertakings to monitor and maintain a balance between their shared services subscriptions and existing capability and capacity;

b) ensuring that the maximum subscription ratio for each work area recovery seat is not exceeded.

7.11.3 Privacy and confidentiality

Outsourced service providers should ensure that shared services are undertaken in such a way that organization security requirements for confidentiality and privacy are not compromised. For example, adequate procedures should be put in place to ensure information is not easily disclosed between organizations from shared computing and related equipment during simultaneous disaster recovery invocation and operations.

7.11.4 Disclosure to organizations

Outsourced service providers should ensure that they disclose their subscription ratios to organizations when requested.

7.12 Activation of subscribed services

Outsourced service providers should establish with each of their organizations the conditions and procedures for invoking and deactivating the subscribed services as described in clause 5.8. Agreements for DR service activation should be included in SLAs between outsourced service providers and organizations, with all

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

established on an individual one-to-one basis. Agreements should include the requirements described in clause 5.8.2, and also an additional requirement of the associated fees to be paid, e.g. for notification, activation and penalties for delay in handover.

7.13 Organization testing

7.13.1 General

Outsourced service providers should ensure that, as untested recovery plans cannot be relied upon during a disaster or failure, they cater for organization testing of subscribed services using the outsourced service provider facilities.

7.13.2 Provision for testing

Outsourced service providers should ensure that they make provision for organizations to test the subscribed services of their recovery plans at the start of the contract agreements and thereafter on a yearly basis.

7.13.3 Triggers

Outsourced service providers should make provision for organizations to test their subscribed services when significant changes occur in organization requirements or in their (outsourced service provider) capacity and capability that affects their ability to fulfil services offered to organizations. Examples of such changes include upgrades of physical facilities, equipment, telecommunications and power supply resources, and relocation of recovery sites.

7.13.4 Support

Outsourced service providers should ensure that they have in place the processes and facilities to support organization testing, including:

a) a coordinator from their staff appointed for each organization's testing, who will collect information and document tests and test results pertaining to the outsourced service provider services to organizations;

b) each coordinator submitting reports to outsourced service provider management immediately after testing on the success and shortcomings of services to the supported organization;

c) appropriate steps taken to rectify any shortcomings identified by testing, and organizations informed accordingly;

d) remedial steps taken before the next tests for each organization, with any omissions justified and clearly communicated to organizations.

7.14 Changes in capability

7.14.1 General

Changes in service capability can be due to additional investments in facilities, equipment, computer hardware and software, and/or increase in staff, thereby expanding the range of services offered. Outsourced service providers should ensure that all changes in capability are re-tested and affirmed to ensure that existing services will not be impaired, and that new services are able to fulfill organization requirements completely.

7.14.2 Change control

Outsourced service providers should have clearly defined change control processes to ensure all resources supporting services to organizations are maintained in an up-to-date and fit-for-purpose status.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.14.3 Revalidation and qualification

Outsourced service providers should ensure that:

a) existing services are regularly re-tested and re-validated unless they are superseded by new services;

b) new capacities, capabilities and services are confirmed as acceptable, e.g. through tests and test results;

c) all tests and test results for new and existing services are documented and audited.

7.14.4 Staff retraining

Outsourced service providers should ensure that all relevant staff are trained ready for when there are facility upgrades, new equipment and software to be installed, or when there are changes in equipment and software configuration to be made that can affect existing or new services offered to organizations.

7.14.5 Organization notification

Outsourced service providers should ensure that organizations are informed of changes in capacity and capability corresponding to their contracted services for their own internal deliberations, e.g. risk assessment. Summaries of new capacities, capabilities and services, and related tests and test results, should be submitted to organizations as appropriate.

7.14.6 Inventory update

Outsourced service providers should maintain up-to-date inventories of their capacities and capabilities, such as computing and related equipment, software and staff expertise.

7.14.7 Existing services

Outsourced service providers should ensure that any changes in their capabilities do not affect their continuing ability to support existing contracted services to organizations, e.g. as a required organization recovery may still need to be possible using older equipment, hardware and software.

7.15 Emergency response plan

7.15.1 General

Emergencies are any unplanned events that could disrupt the operations of outsourced service provider services to organizations. Such events could include:

a) deaths or significant injuries to key staff supporting recovery operations;

b) physical or environmental damage due to:

   1) fire;

   2) hazardous materials;

   3) flood;

   4) telecommunications failure;

   5) power failure;

   6) civil disturbance;

   7) explosion.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Outsourced service providers should establish emergency plans to cater for such unplanned events, with emergency plans commensurate with the range of ICT DR services offered to organizations.

7.15.2 Implementation

Outsourced service providers should have emergency plans in place for their own facilities and business operations, with those plans:

a) exercised on a yearly basis, in part if not in total;

b) audited on a yearly basis, with summary copies of the plan audit report sent to their organizations.

7.15.3 Plan content

Outsourced service providers should ensure that emergency plans at least contain the following components:

a) conditions for activating the plan, e.g. when human life is threatened;

b) procedures to be executed immediately upon activation of the plan, e.g. evacuation from relevant buildings;

c) procedures to recover and resume key business functions and operations, e.g. operations at a temporary “back-up” site;

d) procedures to restore and return to normal operations, e.g. replacement of damaged equipment.

7.15.4 Duties and responsibilities

Outsourced service providers should ensure that emergency duties and responsibilities are drawn up and assigned to nominated appointment holders. Alternates (deputies) should be nominated for critical appointments, e.g. key appointment holders.

7.15.5 Plan update

7.15.5.1 General

Outsourced service providers should keep their emergency plans up to date to reflect changes in business practices and technology to support the services offered to their organizations.

7.15.5.2 Risk assessment

Outsourced service providers should conduct risk assessments of their recovery facilities and equipment at least once every three years as part of their emergency plan updates.

7.15.5.3 Triggers

Outsourced service providers should ensure that changes to the following necessitate reviews and updates of the relevant parts of emergency plans:

a) key appointment holders;

b) business strategies;

c) relocation of primary facilities;

d) new legislation and/or regulation;

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

e) key service upgrades;

f) addition of key organizations;

g) contractors and suppliers.

7.15.6 Emergency drills

7.15.6.1 General

Outsourced service providers should conduct emergency drills on a periodic basis to maintain staff alertness and reduce the chances of confusion if one of the types of unplanned event listed in clause 7.15.1 were to occur.

7.15.6.2 Coverage of drills

The coverage of emergency drills should include the following:

a) notification, warning and communications procedures;

b) location and use of common emergency equipment;

In addition, emergency drills should also include the following considerations:

c) protective actions against hazards;

d) evacuation, shelter and accountability procedures;

e) emergency shutdown procedures.

7.15.6.3 Conduct of drills

The following should govern the planning, conduct, documentation and review of emergency drills:

a) emergency drills should be conducted at least once a year;

b) emergency drills should be conducted when there are any significant changes to outsourced service provider capacity and capability that affect their services to organizations. Examples of such changes include those to physical facilities, equipment, telecommunications and power supply resources;

c) all drills, whether announced or unannounced, should be properly planned and designed so as not to cause any disruption of outsourced service provider services to organizations;

d) steps should be taken to ensure that the situations remain under control during emergency drills;

e) all full scale drills should be approved and authorised by outsourced service provider management;

f) outsourced service provider management should be informed before the start of all full scale drills;

g) all drills, drill plans and drill results should be documented for follow up review and audit;

h) shortcomings uncovered in the drills should be rectified at the earliest possible moment and no later then the next audit or drill, whichever is earlier;

i) shortcomings not rectified should be justified and clearly communicated to outsourced service provider management. The potential consequences of each omission should be presented;

j) a schedule should be established to ensure that drills are undertaken for each possible type of unplanned event as listed in clause 7.15.1. For example, if there have been no significant changes, the different drills could be exercised at least once every five years.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.16 Self assessment

7.16.1 General

To ensure effectiveness and currency of service capability, outsourced service providers should put in place self assessment programmes. Internal audits could form an integral part of these programmes. In addition to reviewing existing policies and procedures, the self assessments would serve to assess the currency of provider capability to meet organization and industry requirements in a changing environment. These self assessments would provide added confidence to existing and potential organizations.

7.16.2 Assessment areas

Outsourced service providers should perform internal assessments of their service capacity and capability at least once a year. Service capacity and capability in the following areas should be assessed:

a) physical facilities and equipment;

b) computing and related equipment;

c) staff expertise and operational alertness;

d) emergency response planning;

e) customer service;

f) any significant business change.

To ensure impartiality, each of these areas should be assessed by an independent party to the area. For example, staff from another functional area should be appointed to assess a specific area service capacity and capability.

7.16.3 Audit

Audits form an integral part of self assessment. The following should govern the conduct of audits:

a) internal and external audits are mandatory when there are significant business changes which affect outsourced service provider ability to service their organizations. For example, when outsourced service providers decide to relocate and consolidate their recovery sites, internal and external audits should be conducted;

b) internal audits are mandatory when there are significant changes in organization requirements. For example, when an organization requires additional items of computing equipment with considerable power consumption to be supported, an audit of the capacity of the electrical power supply should be conducted;

c) internal audits are mandatory when significant changes are made following resolution of security incidents;

d) external auditors should possess formal qualifications in the ICT DR arena;

e) a summary of the latest external audit results should be made available to existing organizations upon request.

All assessments, by audits or otherwise, should have a clearly defined, documented and approved cycle and programme.

The results of all assessments should be properly documented and kept for at least three years, or any period as required by legal and regulatory requirements.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.16.4 Test life cycle

Testing forms an integral part of self assessment. Outsourced service providers should ensure that the following govern the planning, conduct, documentation, review and life cycle of tests:

a) tests should be conducted at least once a year for critical capacity and capability that affect services to organizations;

b) tests should be conducted when there are any significant changes to outsourced service provider capacity and capability that affect their services to organizations. Examples of such changes include those involving upgrades of physical facilities, equipment, telecommunications and power supply resources;

c) all tests, whether announced or unannounced, should be properly planned and designed so as not to cause any disruption of services to organizations;

d) steps should be taken to ensure that the situation remain under control during tests;

e) critical tests should be approved and authorised by outsourced service provider management;

f) for critical tests, outsourced service provider management should be informed before the start of each test;

g) all tests, test objectives, test plans and test results should be documented for follow up review or audit;

h) shortcomings discovered in tests should be rectified at the earliest possible moment and not later then the next tests;

i) shortcomings not rectified should be justified and clearly communicated to outsourced service provider management. The potential consequences of each omission should be presented;

j) schedules should be established to ensure that all possible tests are executed on an agreed periodic basis. For example, all tests should be conducted at least once every five years;

k) each test should be different from the last test. This also serves to introduce variety and remove predictability for the participants.

8 Selection of recovery sites

8.1 General

In addition to the stability of the external environment, good infrastructure and availability of skilled local manpower in the geographic region will contribute towards a favourable setting for ICT DR service providers to base and operate their recovery sites. Furthermore, the presence of other ICT DR service providers and their suppliers in the geographic region would create the critical mass for a vibrant local industry. The track record of key players is another indicator of the maturity and vibrancy of the local ICT DR industry. Depending on the local political environment and its possibilities, the availability of proactive support of the local authority would also play a crucial role in the growth and expansion of the ICT DR industry.

--`,,```,,,,````-`-`,,`,,`,`,,`--- © ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.2 Infrastructure

The external infrastructure of the geographical region where outsourced service providers locate their recovery sites will influence the extent and quality of the services that can be provided. In addition to accessibility, recovery operations from the recovery sites may be impacted if there are uncertainties, frequent fluctuations or disruptions in any of the following infrastructure components:

a) telecommunications;

b) power supply;

c) land transportation;

and, dependent on the particular local environment,

d) air links and transportation;

e) sea links and transportation.

8.3 Skilled manpower and support

There should be a ready pool of skilled and experience ICT DR professionals available locally. The manpower pool should be capable of being expanded by the geographic region having:

a) a high level of general worker skills such that they can be easily trained and equipped to take on ICT DR operational roles;

b) a comprehensive range of ICT DR education and training providers who can constantly retrain and upgrade expertise.

8.4 Critical mass of vendors and suppliers

There should be a critical mass and range of ICT DR vendors and their suppliers in the geographic region who can provide the necessary consultancy, equipment, hardware and software support and replacement on a 24×7 basis.

The range of ICT DR vendors and suppliers include:

a) consultants;

b) hardware, software and technology solutions providers;

c) recovery site and work area recovery providers;

d) telecommunications providers.

8.5 Local service providers' track records

The profile of the ICT DR service providers in the geographic region is indicative of the maturity of the local ICT DR industry. The profile can include the following:

a) number of years of local operations;

b) number of recovery tests undertaken during local operations;

c) number of organizations who have recovered from the local sites;

d) profile of the organizations supported.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.6 Proactive local support

Depending on the country and its political environment, and related possibilities, the support of the local and national authorities may play a crucial role for growth and expansion of the ICT DR industry. Dependant on the role of local and national authorities in a country, examples of local support could include:

a) establishing an ICT DR standard and certification programme;

b) facilitating major ICT DR vendors to establish their operations locally;

c) establishing a proactive telecommunications strategy to attract major ICT DR vendors to establish operations locally;

d) promoting the local ICT DR industry on a wide geographic basis;

e) allocating and pre-planning of land for use as recovery sites.

9 Continuous Improvement

9.1 General

Service providers should continuously improve their services through the following:

a) tracking ICT DR trends;

b) performance measurement;

c) scalability planning;

d) continuous risk mitigation.

9.2 ICT DR trends

9.2.1 General

Changes in the general business environment and related operations may affect the approach and manner in which ICT DR activities are planned, designed and implemented. ICT DR service providers should demonstrate their ability to keep abreast of industry trends through appropriate exposures and contributions.

9.2.2 Participation in industry activities

Recognizing that it is a matter of business direction choice, ICT DR service providers should ideally participate in the activities of the ICT DR industry on a periodic basis. Such activities could include:

a) membership in ICT DR interest groups;

b) attendance at national and international ICT DR conferences.

Participation can be in one or more of the following ways:

a) organizing committees of conferences and seminars;

b) exhibition of products and services;

c) presentation of papers at conferences and seminars.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.2.3 Tracking industry development

Service providers should establish their own capability to monitor, develop and track trends in ICT DR.

9.2.4 Organizations education and training

ICT DR service providers could find benefit from updating their organizations on a periodic basis on trends and developments in the ICT DR industry. This could take one or more of the following forms:

a) publishing periodic newsletter;

b) organizing end-user seminars or conferences.

9.3 Performance measurement

9.3.1 The need for ICT DR services performance measurement

In order to quantify how effective ICT DR services are being provided, it is best practice for ICT DR service providers to conduct performance measurements, and supply the measurements results to organizations as set out in the relevant SLAs or other agreed arrangements.

ICT DR services performance measurement will:

a) enable ICT DR service effectiveness be assessed and reviewed;

b) facilitate the estimation of the adverse impacts from unavailability of information and ICT system assets, which will provide input to business impact analysis activities and the other aspects of information security risk assessment (and, as relevant, operation risk analysis);

c) demonstrate to organizations the ability of ICT systems to recover from disasters and failures;

d) enable the comparison of ICT DR services over a period of time as part of continuous improvements;

e) enable benchmarking across the ICT DR services industry.

9.3.2 Types of performance indicators

The choice of types and numbers of performance measurements depends on the requirements of organizations. In the process of identifying performance metrics, ICT DR service providers can consider the following types of indicators:

a) resource and operation readiness indicators: e.g. percentage of staff who have received ICT DR training and qualifications, percentage of equipment and facilities under regular maintenance;

b) ICT DR plan maturity indicators: e.g. frequency of exercises, extent of exercises, percentage of ICT systems tested;

c) exercise effectiveness indicators: e.g. exercise effectiveness to achieve pre-set business objectives, exercise effectiveness to meet SLAs;

d) simultaneous disaster invocation risk indicators: e.g. subscription ratios for shared services;

e) industry best practice compliance indicators: e.g. number of internal or external audit findings, percentage of compliance to this International Standard.

© ISO/IEC 2008 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.4 Scalability

9.4.1 General

ICT DR service providers should cater for sudden unplanned increases in demand for services and service levels by their organizations due to unforeseen circumstances during disasters/failures. Such demands may exceed those specified in SLAs. ICT DR service providers should put in place policies and procedures to handle such unplanned demands. These demands may be within or over and above their existing capability and capacity. For the latter, pre-planning such as collaboration with other ICT DR service providers or utility suppliers for additional resources would enable ICT DR service providers to help their organizations in meeting unplanned requirements.

9.4.2 Scope

ICT DR Service providers should establish policies and procedures to deal swiftly with unplanned increases in demands for their services by organizations, for example during disasters/failures. These policies and procedures should cover the following areas:

a) telecommunications;

b) power supply;

c) computer and related equipment;

d) software;

e) recovery sites and facilities;

f) storage space for vital records and supplies;

g) work area recovery;

h) staff providing direct recovery support;

i) non-recovery amenities.

9.4.3 Non-recovery amenities

ICT DR service providers should establish policies and procedures to deal swiftly with unplanned increase in demands for their non-recovery amenities by organizations, e.g. during disasters/failures. These policies and procedures should encompass inclusion of:

a) provision of additional catering facilities;

b) arrangements with nearby clinics or health centers for medical attention.

9.5 Risk mitigation

9.5.1 General

ICT DR service providers, particularly outsourced service providers, should identify potential risks, and establish procedures to address each of the identified risks. Such risks may include those related to seizure or stoppages as a result of legal enforcement. The procedures should be pre-arranged and clearly documented. ICT DR service providers should also have clear risk mitigation policies and plans in place, with clear and specific documented steps to deal with identified risks.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9.5.2 Auxiliary arrangements

ICT DR service providers should ensure that arrangements are in place to address the loss of their own facilities and service capabilities. These arrangements should cater for a minimal set of facilities and service capabilities, e.g. arrangements made with external parties.

9.5.3 Insurance

9.5.3.1 General

Whilst insurance does not contribute directly to services offered by ICT DR service providers (depending on the national legal and regulatory environment), it may help to provide some form of recompense for certain types of loss that may be incurred by ICT DR service providers, particularly outsourced service providers. In certain circumstances, it may be possible for such recompense to be used to restore ICT DR service providers to their operational readiness state for service to their organizations at earlier dates than otherwise.

9.5.3.2 Property insurance

ICT DR service providers, particularly outsourced service providers, should purchase insurance against loss or damage of equipment and storage media, which could be caused by theft, fire, water pipe burst, failure of environmental control equipment, and computer abuse by staff.

9.5.3.3 Operational continuity

Dependent on the feasibility in a country's national legal and regulatory environment, ICT DR service providers, particularly outsourced service providers, may be able to arrange and purchase sufficient insurance coverage such that their recovery sites have a chance of being fully operated for a period of time without being affected by seizure or stoppages. This may provide sufficient prior warning for organizations to select and relocate their recovery requirements elsewhere. (However, it should be noted that in a number of countries, such insurance is not possible.)

© ISO/IEC 2008 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(informative)

Correspondence between ISO/IEC 27002:2005 and this International Standard

Table A.1 shows correspondence between recommendations provided in clause 5 - 7 of this International Standard and security controls listed in ISO/IEC 27002:2005. Note that security controls indicated in this table are not exhaustive but representative.

Table A.1 — Correspondence between ISO/IEC 27002:2005 and this International Standard

This International Standard	ISO/IEC 27002:2005
5 ICT Disaster Recover5	
5.1 General	
5.2 Environmental stability	
5.3 Asset management	Controls listed in Clause 7 (ASSET MANAGEMENT)
5.4 Proximity of site	
5.5 Vendor management	6.2.3 Addressing security in third party agreements Controls listed in Clause 8 (HUMAN RESOURCES SECURITY) 12.1.1 Security requirements analysis and specification
5.6 Outsourcing arrangements	Controls listed in Sub-clause 10.2 (THIRD PARTY SERVICE DELIVERY MANAGEMENT)
5.7 Information security	10.1.3 Segregation of duties 13.1.1 Reporting information security events
5.8 Activation of disaster recovery plan	6.1.3 Allocation of information security responsibilities 14.1.4 Business continuity planning framework
5.9 Training and education	8.2.2 Information security awareness, education, and training

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2008 – All rights reserved
Not for Resale

This International Standard	ISO/IEC 27002:2005
5.10 Testing on ICT systems	10.1.2 Change management 10.3.2 System acceptance 10.5.1 Information back-up 14.1.5 Testing, maintaining and re-assessing business continuity plans
5.11 Business continuity planning for ICT DR service providers	Controls listed in Clause 14 (BUSINESS CONTINUITY MANAGEMENT)
5.12 Documentation and periodic review	
6 ICT disaster recovery facilities	
6.1 General	
6.2 Location of recovery site	10.5.1 Information back-up
6.3 Physical access controls	9.1.1 Physical security perimeter 9.1.2 Physical entry controls
6.4 Physical facility security	
6.5 Dedicated areas	
6.6 Environmental controls	
6.7 Telecommunications	9.2.2 Supporting utilities 9.2.3 Cabling security
6.8 Power supply	
6.9 Cable management	
6.10 Fire protection	
6.11 Emergency operations center (EOC)	
6.12 Restricted facilities	
6.13 Non-recovery amenities	
6.14 Physical facilities and support equipment life cycle	
6.15 Testing	

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

This International Standard	ISO/IEC 27002:2005
7 Outsourced service provider's capability	
7.1 General	
7.2 Review organization disaster recovery status	(For organizations which are going to utilize professional DRS services) Controls listed in Clause 14 (BUSINESS CONTINUITY MANAGEMENT)
7.3 Facilities requirements *(Note: This expectation is for IDS service providers in general, and not limited for professional service providers)*	
7.4 Expertise	
7.5 Logical access control	
7.6 ICT equipment and operation readiness	
7.7 Simultaneous recovery support	
7.8 Levels of service	(For organizations which utilize professional DRS services) Controls listed in Sub-clause 10.2 (THIRD PARTY SERVICE DELIVERY MANAGEMENT)
7.9 Types of service	10.3.1 Capacity management
7.10 Proximity of services	
7.11 Subscription ratio for shared services	15.1.4 Data protection and privacy of personal information
7.12 Activation of subscribed services	14.1.4 Business continuity planning framework
7.13 Organization testing	14.1.5 Testing, maintaining and re-assessing business continuity plans
7.14 Changes in capability	12.1.1 Security requirements analysis and specification 12.5.1 Change control procedures
7.15 Emergency response plan	13.2.1 Responsibilities and procedures Controls listed in Clause 14 (BUSINESS CONTINUITY MANAGEMENT)
7.16 Self assessment	

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] SS 507:2004, *Singapore Standard for Business continuity/disaster recovery (BCDR) service providers*

[2] ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security incident management*

[3] ISO/IEC 20000-1:2005 *Information technology — Service Management — Part 1: Specification*

[4] ISO/IEC 20000-2:2005 *Information technology — Service Management — Part 2: Code of practice*

[5] High-level principles for business continuity, Consultative document, Basel Committee on Banking Supervision, The Joint Forum, December 2005

[6] Good Practice Guidelines, *A Framework For Business Continuity Management, The Business Continuity Institute, 2005*

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 67 pages

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale