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 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

Contents

Page

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*.

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).

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.

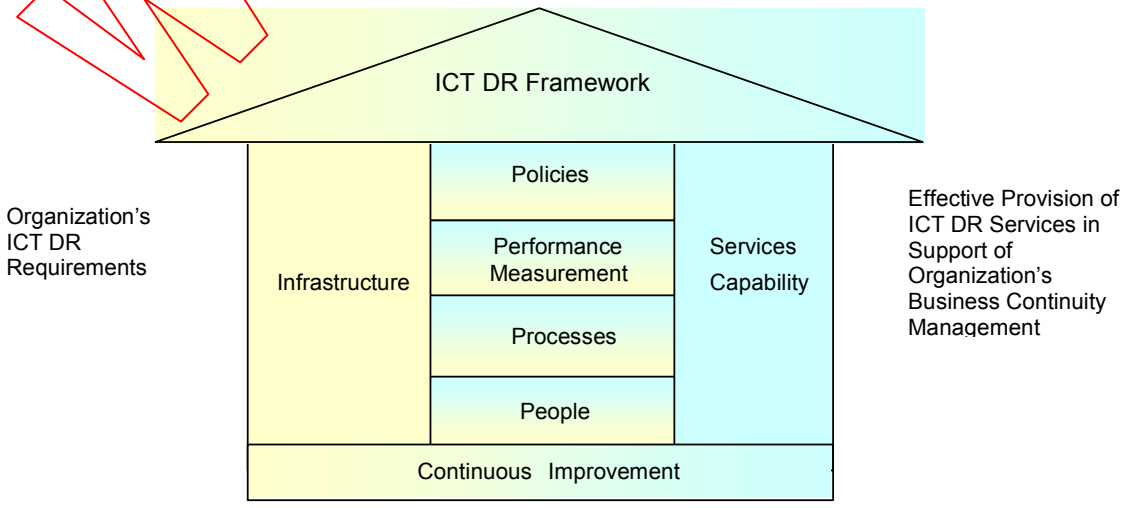

Figure 1 — ICT DR service provision framework

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.

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.

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.

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*