INTERNATIONAL STANDARD

ISO/IEC 27031

First edition
2011-03-01

Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

Technologies de l'information — Techniques de sécurité — Lignes directrices pour mise en état des technologies de la communication et de l'information pour continuité des affaires

Reference number
ISO/IEC 27031:2011(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 27031 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

Over the years, information and communication technology (ICT) has become an integral part of many of the activities which are elements of the critical infrastructures in all organizational sectors, whether public, private or voluntary. The proliferation of the Internet and other electronic networking services, and today's capabilities of systems and applications, has also meant that organizations have become ever more reliant on reliable, safe and secure ICT infrastructures.

Meanwhile, the need for business continuity management (BCM), including incident preparedness, disaster recovery planning, and emergency response and management, has been recognized and supported with specific domains of knowledge, expertise, and standards developed and promulgated in recent years, including the BCM International Standard developed by ISO/TC 223.

NOTE ISO/TC 223 is in the process of developing a relevant business continuity management International Standard (ISO 22301).

Failures of ICT services, including the occurrence of security issues such as systems intrusion and malware infections, will impact the continuity of business operations. Thus managing ICT and related continuity and other security aspects form a key part of business continuity requirements. Furthermore, in the majority of cases, the critical business functions that require business continuity are usually dependent upon ICT. This dependence means that disruptions to ICT can constitute strategic risks to the reputation of the organization and its ability to operate.

ICT readiness is an essential component for many organizations in the implementation of business continuity management and information security management. As part of the implementation and operation of an information security management system (ISMS) specified in ISO/IEC 27001 and business continuity management system (BCMS) respectively, it is critical to develop and implement a readiness plan for the ICT services to help ensure business continuity.

As a result, effective BCM is frequently dependent upon effective ICT readiness to ensure that the organization's objectives can continue to be met in times of disruptions. This is particularly important as the consequences of disruptions to ICT often have the added complication of being invisible and/or difficult to detect.

In order for an organization to achieve ICT Readiness for Business Continuity (IRBC), it needs to put in place a systematic process to prevent, predict and manage ICT disruption and incidents which have the potential to disrupt ICT services. This can be best achieved by applying the Plan-Do-Check-Act (PDCA) cyclical steps as part of a management system in ICT IRBC. In this way IRBC supports BCM by ensuring that the ICT services are as resilient as appropriate and can be recovered to pre-determined levels within timescales required and agreed by the organization.

Table 1 — Plan-Do-Check-Act cycle in IRBC

Plan	Establish IRBC policy, objectives, targets, processes and procedures relevant to managing risk and improving ICT readiness to deliver results in accordance with an organization's overall business continuity policies and objectives.
Do	Implement and operate the IRBC policy, controls, processes and procedures.
Check	Assess and, where applicable, measure process performance against IRBC policy, objectives and practical experience, and report the results to management for review.
Act	Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the IRBC.

If an organization is using ISO/IEC 27001 to establish an ISMS, and/or using relevant standards to establish a BCMS, the establishment of IRBC should preferably take into consideration existing or intended processes linked to these standards. This linkage can support the establishment of IRBC and also avoid any dual processes for the organization. Figure 1 summarizes the interaction of IRBC and BCMS.

In the planning and implementation of IRBC, an organization can refer to ISO/IEC 24762:2008 in its planning and delivery of ICT disaster recovery services, regardless of whether or not those services are provided by an outsourced vendor, or internally to the organization.

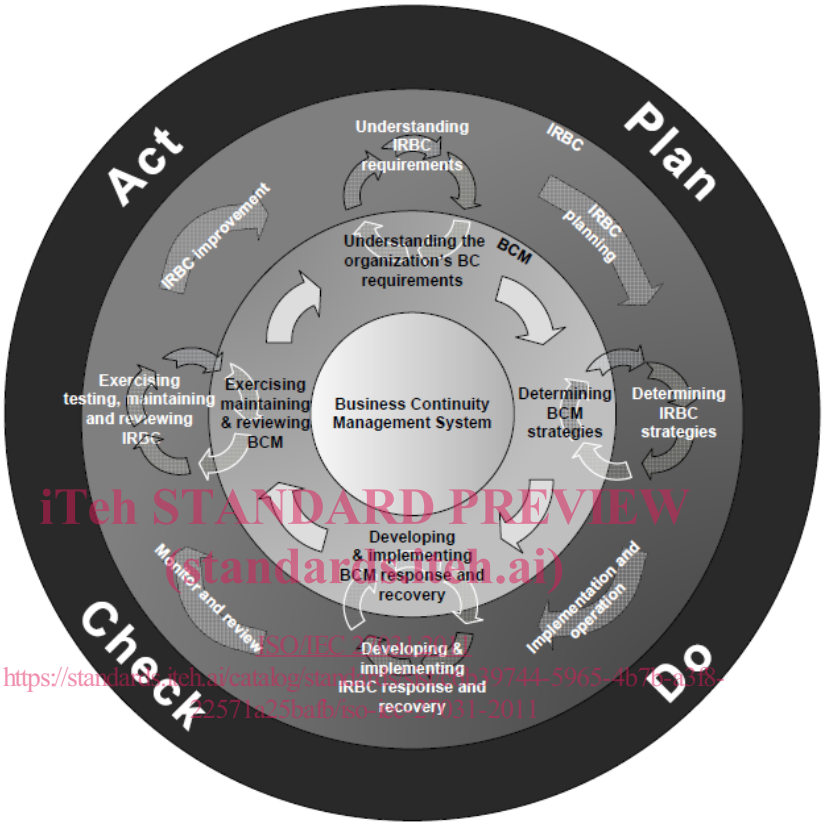

Figure 1 — Integration of IRBC and BCMS

Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

1 Scope

This International Standard describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. It applies to any organization (private, governmental, and non-governmental, irrespective of size) developing its ICT readiness for business continuity (IRBC) program, and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions. It also enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner.

The scope of this International Standard encompasses all events and incidents (including security related) that could have an impact on ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.

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 TR 18044:2004 [1)], *Information technology — Security techniques — Information security incident management*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

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

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

1) ISO/IEC TR 18044:2004 is to be revised and renumbered as ISO/IEC 27035.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC TR 18044, ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and the following apply.

3.1
alternate site
alternate operating location selected to be used by an organization when normal business operations cannot be carried out using the normal location after a disruption has occurred

3.2
business continuity management
BCM
holistic management process that identifies potential threats to an organization and the impacts to business operations whose threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

3.3
business continuity plan
BCP
documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption

NOTE Typically this covers resources, services and activities required to ensure the continuity of critical business functions.

3.4
business impact analysis
BIA
process of analysing operational functions and the effect that a disruption might have upon them

3.5
critical
qualitative description used to emphasize the importance of a resource, process or function that must be available and operational constantly or available and operational at the earliest possible time after an incident, emergency or disaster has occurred

3.6
disruption
incident, whether anticipated (e.g. hurricane) or unanticipated (e.g. power failure/outage, earthquake, or attack on ICT systems/infrastructure) which disrupts the normal course of operations at an organization location

3.7
ICT disaster recovery
ability of the ICT elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disruption

3.8
ICT disaster recovery plan
ICT DRP
clearly defined and documented plan which recovers ICT capabilities when a disruption occurs

NOTE It is called ICT continuity plan in some organizations.

3.9
failure mode
manner by which a failure is observed

NOTE It generally describes the way the failure occurs and its impact on the operation of the system.

3.10
ICT readiness for business continuity
IRBC
capability of an organization to support its business operations by prevention, detection and response to disruption and recovery of ICT services

3.11
minimum business continuity objective
MBCO
minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption

3.12
recovery point objective
RPO
point in time to which data must be recovered after a disruption has occurred

3.13
recovery time objective
RTO
period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions must be recovered after a disruption has occurred

3.14
resilience
ability of an organization to resist being affected by disruptions

3.15
trigger
event that causes the system to initiate a response

NOTE Also known as triggering event.

3.16
vital record
electronic or paper record that is essential for preserving, continuing or reconstructing the operations of an organization and protecting the rights of an organization, its employees, its customers and its stakeholders

4 Abbreviations

IRBC ICT Readiness for Business Continuity

ISMS Information Security Management System

5 Overview

5.1 The role of IRBC in Business Continuity Management

Business Continuity Management (BCM) is a holistic management process that identifies potential impacts threatening an organisation's continuity of business activities and provides a framework for building resilience and capability for an effective response that safeguards the interests of the organization from disruptions.

As part of the BCM process, IRBC refers to a management system which complements and supports an organization's BCM and/or ISMS program, to improve the readiness of the organization to:

a) respond to the constantly changing risk environment;

b) ensure continuation of critical business operations supported by the related ICT services;

c) be ready to respond before an ICT service disruption occurs, upon detection of one or a series of related events that become incidents; and

d) to respond and recover from incidents/disasters and failures.

Figure 2 illustrates the desired ICT outcome to support the Business Continuity Management activities.

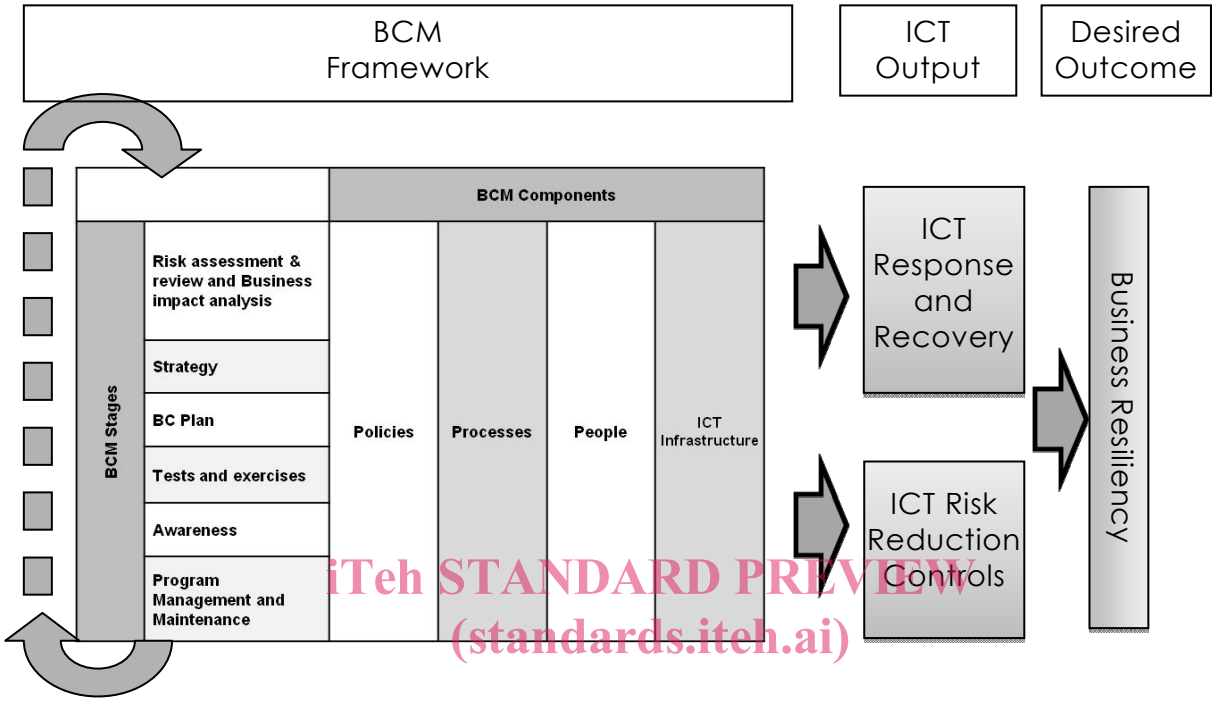

Figure 2 — Business Continuity Framework and its related ICT output and desired outcome

The BCM International Standard developed by ISO/TC 223 summarizes the BCM approach to preventing, reacting and recovering from incidents. Activities involved in BCM include incident preparedness, operational continuity management, disaster recovery planning (DRP) and risk mitigation which focus on increasing the resilience of the organization and by preparing it to react effectively to incidents and recover within pre-determined timescales.

An organization therefore sets out its BCM priorities and it is these which drive the IRBC activities. In turn BCM depends upon IRBC to ensure that the organization can meet its overall continuity objectives at all times, and particularly during times of disruption.

As shown in Figure 3, such readiness activities aim to:

a) improve the incident detection capabilities;

b) prevent a sudden or drastic failure;

c) enable an acceptable degradation of operational status should the failure be unstoppable;

d) further shorten recovery time; and

e) minimize impact upon eventual occurrence of the incident.

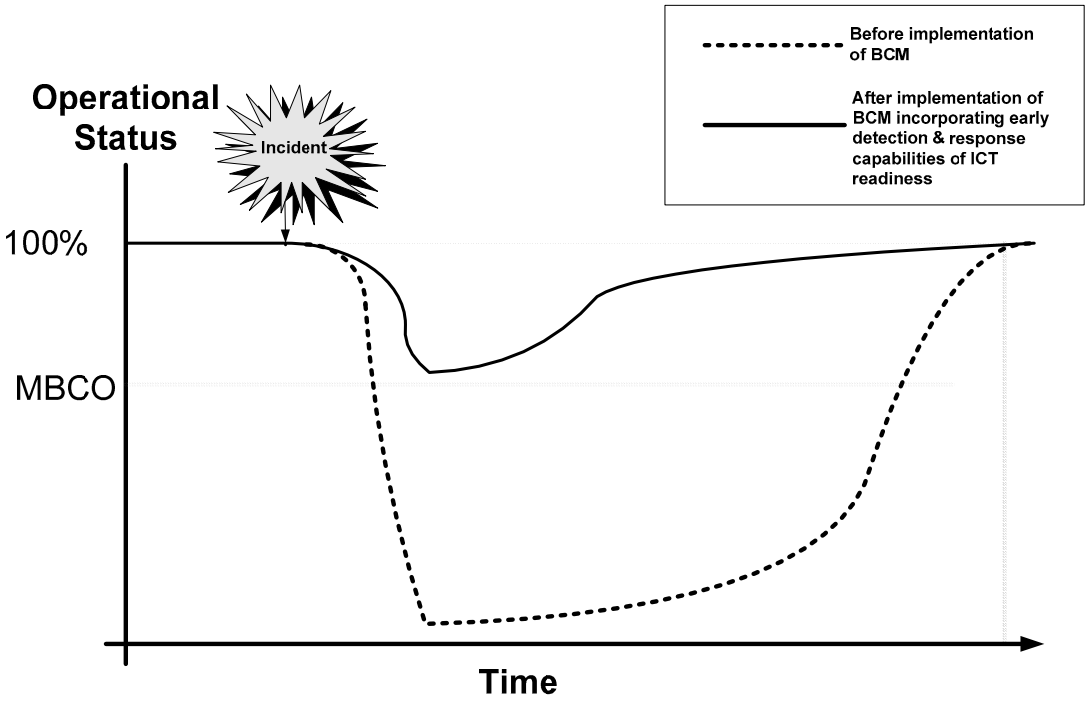

Figure 3 — Concept of ICT Readiness for Business Continuity

5.2 The Principles of IRBC

IRBC is based around the following key principles:

a) Incident Prevention - Protecting ICT services from threats, such as environmental and hardware failures, operational errors, malicious attack, and natural disasters, is critical to maintaining the desired levels of systems availability for an organization;

b) Incident Detection - Detecting incidents at the earliest opportunity will minimize the impact to services, reduce the recovery effort, and preserve the quality of service;

c) Response - Responding to an incident in the most appropriate manner will lead to a more efficient recovery and minimize any downtime. Reacting poorly can result in a minor incident escalating into something more serious;

d) Recovery - Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data. Understanding the recovery priorities allows the most critical services to be reinstated first. Services of a less critical nature may be reinstated at a later time or, in some circumstances, not at all; and

e) Improvement – Lessons learned from small and large incidents should be documented, analysed and reviewed. Understanding these lessons will allow the organization to better prepare, control and avoid incidents and disruption.

Figure 4 illustrates how the respective IRBC element supports a typical ICT disaster recovery timeline and in turn supports the business continuity activities. IRBC implementation enables the organization to respond effectively to new and emerging threats as well as being able to react and recover from disruptions.