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.

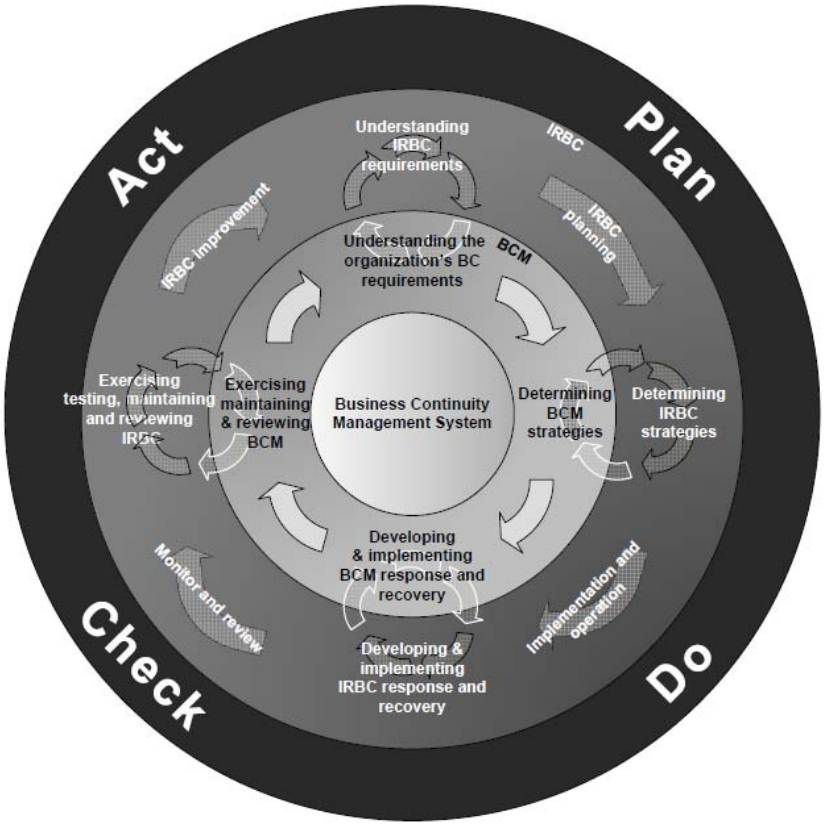

Figure 1 — Integration of IRBC and BCMS