

Geregistreeerde Belgische norm

NBN ISO/IEC 27031

1e uitg., november 2014

Normklasse: Z 07

Informatietechnologie - Beveiligingstechnieken - Richtlijnen voor de paraatheid van informatie- en communicatietechnologie met betrekking tot bedrijfscontinuïteit (ISO/IEC 27031:2011)

Technologies de l'information - Techniques de sécurité - Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité (ISO/IEC 27031:2011)

Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity (ISO/IEC 27031:2011)

Toelating tot publicatie: 28 november 2014

Deze norm ISO/IEC 27031:2011 heeft de status van een Belgische norm.

Deze norm bestaat in twee officiële versies (Engels, Frans).

***norme belge
enregistrée***

NBN ISO/IEC 27031

1e éd., novembre 2014

Indice de classement: Z 07

Technologies de l'information - Techniques de sécurité - Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité (ISO/IEC 27031:2011)

Informatietechnologie - Beveiligingstechnieken - Richtlijnen voor de paraatheid van informatie- en communicatietechnologie met betrekking tot bedrijfscontinuïteit (ISO/IEC 27031:2011)

Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity (ISO/IEC 27031:2011)

Autorisation de publication: 28 novembre 2014

La présente norme ISO/IEC 27031:2011 a le statut d'une norme belge.

La présente norme existe en deux versions officielles (anglais, français).

**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*

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 2011

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

Contents

Page

Foreword	v
Introduction.....	vi
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions	2
4 Abbreviations.....	3
5 Overview.....	3
5.1 The role of IRBC in Business Continuity Management.....	3
5.2 The Principles of IRBC.....	5
5.3 The Elements of IRBC.....	6
5.4 Outcomes and benefits of IRBC	7
5.5 Establishing IRBC	7
5.6 Using Plan Do Check Act to establish IRBC.....	8
5.7 Management Responsibility.....	8
5.7.1 Management leadership and commitment.....	8
5.7.2 IRBC policy	8
6 IRBC Planning.....	9
6.1 General	9
6.2 Resources	9
6.2.1 General	9
6.2.2 Competency of IRBC staff	9
6.3 Defining requirements	10
6.3.1 General	10
6.3.2 Understanding critical ICT services	10
6.3.3 Identifying gaps between ICT Readiness capabilities and business continuity requirements.....	10
6.4 Determining IRBC Strategy Options.....	11
6.4.1 General	11
6.4.2 IRBC Strategy Options.....	11
6.5 Sign Off.....	14
6.6 Enhancing IRBC Capability	14
6.6.1 Enhancing Resilience	14
6.7 ICT Readiness Performance Criteria	15
6.7.1 Identification of performance criteria.....	15
7 Implementation and Operation	15
7.1 General	15
7.2 Implementing the Elements of the IRBC Strategies	15
7.2.1 Awareness, Skills and Knowledge	15
7.2.2 Facilities	16
7.2.3 Technology	16
7.2.4 Data.....	16
7.2.5 Processes.....	17
7.2.6 Suppliers	17
7.3 Incident Response.....	17
7.4 IRBC Plan Documents.....	17
7.4.1 General	17
7.4.2 Content of Plan Documents	18
7.4.3 The ICT Response and Recovery Plan Documentation	19

ISO/IEC 27031:2011(E)

7.5	Awareness, competency and training program	20
7.6	Document Control.....	21
7.6.1	Control of IRBC records.....	21
7.6.2	Control of IRBC documentation	21
8	Monitor and Review	21
8.1	Maintaining IRBC	21
8.1.1	General.....	21
8.1.2	Monitoring, detection and analysis of threats	22
8.1.3	Test and exercise.....	22
8.2	IRBC Internal Audit.....	26
8.3	Management Review	26
8.3.1	General.....	26
8.3.2	Review Input.....	27
8.3.3	Review Output.....	27
8.4	Measurement of ICT Readiness Performance Criteria.....	28
8.4.1	Monitoring and measurement of ICT Readiness	28
8.4.2	Quantitative and Qualitative Performance Criteria	28
9	IRBC improvement.....	28
9.1	Continual improvement.....	28
9.2	Corrective action.....	28
9.3	Preventive action	29
	Annex A (informative) IRBC and milestones during a disruption	30
	Annex B (informative) High availability embedded system	32
	Annex C (informative) Assessing Failure Scenarios	33
	Annex D (informative) Developing Performance Criteria	35
	Bibliography	36

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.

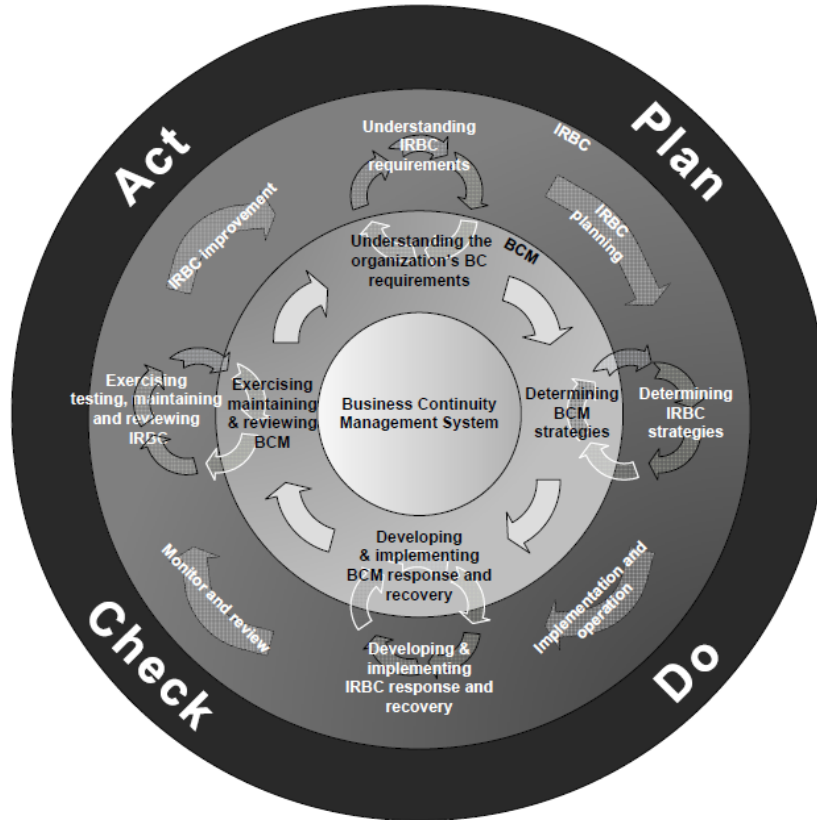


Figure 1 — Integration of IRBC and BCMS

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 18044:2004¹⁾, *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.