International Standard

ISO/IEC 27031

Cybersecurity — Information and communication technology readiness for business continuity

Cybersécurité — Préparation des technologies de l'information et de la communication pour la continuité d'activité

Second edition
2025-05

Reference number
ISO/IEC 27031:2025(en)

© ISO/IEC 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **3**
5 Structure of this document **3**
5.1 General 3
6 Integration of IRBC into BCM **3**
6.1 General 3
6.2 Enabling governance 4
6.3 Business continuity management objectives 5
6.4 Risk management and applicable controls for IRBC 6
6.5 Incident management and relationship to IRBC 6
6.6 BCM strategies and alignment to IRBC 6
7 Business expectations for IRBC **7**
7.1 Risk review 7
7.1.1 General 7
7.1.2 Monitoring, detection and analysis of threats and events 8
7.2 Inputs from business impact analysis 8
7.2.1 General 8
7.2.2 Understanding critical ICT services 8
7.2.3 Assessing ICT readiness against business continuity requirements 9
7.3 Coverage and interfaces 9
7.3.1 General 9
7.3.2 ICT dependencies for the scope 10
7.3.3 Determine any contractual aspects of dependencies 10
8 Defining prerequisites for IRBC **10**
8.1 Incident based – preparation before incident 10
8.1.1 General 10
8.1.2 ICT Recovery capabilities 11
8.1.3 Establishing an IRBC 11
8.1.4 Setting objectives 11
8.1.5 Determining possible outcomes and benefits of IRBC 12
8.1.6 Equipment redundancy planning 13
8.1.7 Determining the scope of ICT services related to the objectives 13
8.2 Determining target ICT RTO and RPO 14
9 Determining IRBC strategies **15**
9.1 General 15
9.2 IRBC strategy options 15
9.2.1 General 15
9.2.2 Skills and knowledge 16
9.2.3 Facilities 16
9.2.4 Technology 17
9.2.5 Data 17
9.2.6 Processes 18
9.2.7 Suppliers 18
10 Determining the ICT continuity plan **19**
10.1 Prerequisites for the development of plans 19
10.1.1 Determining and setting the recovery organization 19
10.1.2 Determining time frames for plan development, reporting and testing 19

© ISO/IEC 2025 – All rights reserved

10.1.3 Resources 20
10.1.4 Competency of IRBC staff 20
10.1.5 Technological solutions 21
10.2 Recovery plan activation 21
10.2.1 ICT BCP Activation 21
10.2.2 Escalation 21
10.3 ICT recovery plans 22
10.3.1 RPO and RTO plans for ICT 22
10.3.2 Facilities 22
10.3.3 Technology 22
10.3.4 Data 22
10.3.5 Response and recovery procedures 23
10.3.6 People 23
10.4 Temporary work around plans 23
10.5 External contacts and procedures 23

11 Testing, exercise, and auditing 23
11.1 Performance criteria 23
11.2 Testing dependencies 24
11.2.1 Test and exercise 24
11.2.2 Test and exercise program 24
11.2.3 Scope of exercises 25
11.2.4 Planning an exercise 25
11.2.5 Alert based and different recovery stages 26
11.2.6 Managing an exercise 27
11.3 Learning from tests 28
11.4 Auditing the IRBC 28
11.5 Control of documented information 29

12 Final MBCO 29

13 Top management responsibilities regarding evaluating the IRBC 29
13.1 General 29
13.2 Management responsibilities 29

Annex A (informative) **Comparing RTO and RPO to business objectives for ICT recovery 31**

Annex B (informative) **Risk reporting for FMEA 32**

Bibliography 33

© ISO/IEC 2025 – All rights reserved

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27031:2011), which has been technically revised.

The main changes are as follows:

— the structure of the document has been changed;

— the scope has been changed for clarification;

— technical content has been added in 6.4, 6.5, 6.6, 9.2 and 10.1.5.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2025 – All rights reserved

Introduction

Over the years, information and communication technology (ICT) has become an integral part of many of the activities within the critical infrastructures in all organizational sectors, whether public or private. The proliferation of the internet and other electronic networking services, as well as the capabilities of systems and applications, has also resulted in organizations becoming 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 the development and endorsement of specific domains of knowledge, expertise, and standards, including ISO 22313.

Failures of ICT services, including those caused by security issues such as systems intrusion and malware infections, impact the continuity of business operations. Thus, managing ICT and related continuity, as well as other security aspects, form a key part of business continuity requirements. Furthermore, in the majority of cases, the critical processes and activities 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.

The advent and increasing dominance of Internet-based ICT services (cloud ICT services) has caused the nature of preparedness to change from relying on internal processes to a reliance on the quality and robustness of services from other organizations and the associated business relationships with such organizations.

ICT readiness is an essential component for many organizations in the implementation of business continuity management and information security management.

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

For an organization to achieve ICT readiness for business continuity (IRBC), it should put in place a systematic process to prevent, predict and manage ICT disruptions and incidents which have the potential to disrupt ICT services. This can be achieved by coordinating IRBC with the information security and BCM processes. In this way, IRBC supports BCM by ensuring that the ICT services can be recovered to pre-determined levels within timescales required and agreed by the organization.

If an organization is using relevant information security and business continuity standards, 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.

This document describes the concepts and principles of ICT readiness for business continuity (IRBC) and provides a framework of methods and processes to identify and specify aspects for improving an organization's ICT readiness to ensure business continuity.

This document complements the information security controls relating to business continuity in ISO/IEC 27002. It also supports the information security risk management process specified in ISO/IEC 27005.

Based upon ICT readiness objectives, this document also extends the practices of information security incident management into ICT readiness planning, training and operation.

© ISO/IEC 2025 – All rights reserved

Cybersecurity — Information and communication technology readiness for business continuity

1 Scope

This document describes the concepts and principles of information and communication technology (ICT) readiness for business continuity (IRBC). It provides a framework of methods and processes to identify and specify aspects for improving an organization's ICT readiness to ensure business continuity.

This document serves the following business continuity objectives for ICT:

— minimum business continuity objective (MBCO),

— recovery point objective (RPO),

— recovery time objective (RTO) as part of the ICT business continuity planning.

This document is applicable to all types and sizes of organizations.

This document describes how ICT departments plan and prepare to contribute to the resilience objectives of the organization.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

ISO/IEC 27035-1:2023, *Information technology — Information security incident management — Part 1: Principles and process*

ISO 22300, *Security and resilience — Vocabulary*

ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27035-1, ISO 22300, ISO 22301, and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

© ISO/IEC 2025 – All rights reserved