FINAL DRAFT
International Standard

ISO/IEC FDIS 27031

Cybersecurity — Information and communication technology readiness for business continuity

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2024-06-26

Voting terminates on:
2024-08-21

Reference number
ISO/IEC FDIS 27031:2024(en)

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

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.

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.

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/

3.1
failure mode
manner by which a failure is observed

Note 1 to entry: This generally describes the way failure occurs and its impact on the operation of the system.

3.2
information and communication technology disaster recovery
ability of the information and communication technology elements of an organization to support its critical processes and activities to an acceptable level within a predetermined period of time following a disruption

3.3
information and communication technology readiness
state of an information and communication technology (ICT) function in which it has the knowledge, skills, processes, architecture, infrastructure and the related technologies in preparation for a potential event that would lead to either an intolerable disruption of ICT or an intolerable data loss

Note 1 to entry: This does not mean that the ICT function is all knowing and able to do everything, but rather it is fit for purpose and in readiness for the preparation, the response and the recovery at hand, if such a contingency occurs.

3.4
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

3.5
recovery point objective
RPO
point to which information used by an activity is restored to enable the activity to operate on resumption

Note 1 to entry: Can also be referred to as “maximum data loss”.

3.6
recovery time objective
RTO
period of time following an incident within which a product and service or an activity is resumed, or resources are recovered

3.7
restoration
level of recovery of data, ICT systems and business operations to the normal state after a disruption with a minimal loss, if any

3.8
trigger
event that causes the system to initiate a response

Note 1 to entry: Also known as triggering event.

4 Abbreviated terms

BCP business continuity plan

BIA business impact analysis

HVAC heating, ventilation and air-conditioning

ICT information and communication technology

IRBC ICT readiness for business continuity

MBCO minimum business continuity objective

RPO recovery point objective

RTO recovery time objective

5 Structure of this document

5.1 General

The intention of each clause of this document is as follows:

— Clause 6 explains how IRBC is linked to BCM and other organizational processes that are related to IRBC;

— Clause 7 explains how the business continuity for the organization sets objectives that IRBC should try to meet;

— Clause 8 provides guidance on what is needed to define the ICT current characteristics that affect the IRBC;

— Clause 9 provides guidance on different strategies that can be used and should be determined for IRBC pending the objectives and current characteristics of ICT that ICT continuity plans should follow;

— Clause 10 provides guidance on how to design ICT continuity plans based on determined strategies and how to address different types of adverse situations to meet the continuity objectives for ICT;

— Clause 11 provides guidance on how to test and finalize the ICT continuity plans;

— Clause 12 provides guidance on how to establish final RPOs and RTOs based on the ICT continuity plans and determine the ability to meet the business requirements;

— Clause 13 provides guidance on the feedback of IRBC to top management to approve the plans or risk treatment decisions, if the business objectives have not been met.

Specific planning and verifications of ICT are instrumental to build and ensure that ICT can face events. Without such readiness, the organization would suffer intolerable disruptions of prioritised activities or data losses.

Such events, potentially coming from technical failures or cybersecurity incidents, should motivate the ICT function to interface its governance, planning and operation with requirements coming from the decision-making activity of business continuity management and information security management.

6 Integration of IRBC into BCM

6.1 General

Disruption related risk within information security and ICT primarily relates to availability when an adverse situation occurs that disrupts the availability of ICT services to business activities.

The related risks have the characteristics of very low likelihood, meaning that they can happen very rarely or even never, but have a huge consequence and business impact if they occur. It should be noted that business continuity is the activity that should minimize the consequences if such risks do occur, as in most cases the likelihood for such risks can never be fully eliminated.

Determination of risk to business process can evolve from the risk management process and the controls to mitigate them to support business continuity.

Prioritized activities are identified through business impact analysis (BIA) on the business processes and functions where the ICT dependencies can be determined, and critical time frames are set.

The actual events or risk scenarios on how the ICT services are interrupted can be hard for businesses to determine and are generally on a high level based on different threats. Such threats and sources can include:

— environmental – fire, flooding, etc.;

— technical hardware, software failures or power and air conditioning (e.g. HVAC) shortages or breakdowns;

— unintentional human risk source – mistakes in change management, wrongly configured back up, etc;

— intentional human risk source – hacking, malware, sabotage;

— societal – pandemic, strikes, social unrest, etc;

— cyberattacks – DOS, DDOS;

— specific to the ICT-supply chain:

  — perturbation on the communication channel with a data/service provider;

  — disruption of a cloud service provider;

  — unclear information security requirements within contract terms covering ICT services provided by external parties.

These threats or events can significantly disrupt the ICT services and trigger business continuity strategies, resulting in the following:

— loss of critical ICT hardware and software;

— loss of critical ICT service;

— loss of facilities;

— loss of critical ICT service from supplier;

— loss of key personnel.

The above scenarios should be considered in the business continuity planning for ICT if they are relevant to the ICT provided to the business. Overall strategies should be determined and BCP developed and tested to determine residual risks to be handled in the risk management process. Vulnerabilities or other weaknesses that cause severe disruption to the ICT can be determined through risk management. It is through risk assessment and risk treatment that risks can be mitigated. However, this mitigation does not eliminate the need for IRBC to be in place, as there is always a risk that something unforeseen will happen.

6.2 Enabling governance

Organizations should have general knowledge of the readiness of the different ICT elements, including the following:

— ICT services;

— ICT facilities;

— technology (hardware, software, architecture);

— data;

— processes;

— suppliers, as well as their critical components; and

— staff competencies.

The knowledge of the structure of ICT is a crucial element in ensuring the required support for the governance of the business continuity, including ICT readiness. The organization should therefore:

a) raise, enhance and maintain awareness through ongoing training, education and information programme for relevant staff, and establish a process for evaluating the effectiveness of the awareness delivery; and

b) ensure that staff are aware of how they contribute to the achievement of the ICT readiness for business continuity (IRBC) objectives.

The organization should ensure that all personnel who are assigned IRBC management responsibilities are competent to perform the required tasks by:

c) determining the necessary competencies for such personnel;

d) conducting training needs analysis on such personnel;

e) providing training;

f) ensuring that the necessary competence has been achieved; and

g) maintaining records of education, training, skills, experience and qualifications.

Top management or their delegates should ensure that a clear and complete distribution of roles has been established with enough granularity to identify each individual role in the IRBC. For assigned roles, an identification of the linked responsibilities should be documented.

An IRBC training program should be planned, developed, and implemented to ensure relevant personnel with IRBC roles can fulfil their responsibilities when an event occurs.

NOTE For more details on awareness and training related to information security incident management, refer to ISO/IEC 27035-2.

6.3 Business continuity management objectives

Business continuity management is the process for implementing and maintaining capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption.

As part of the BCM process, IRBC refers to a process to improve the readiness of the organization to:

a) respond to the constantly changing risk environment;

b) ensure continuation of related ICT services that support prioritized activities;

c) anticipate and prepare a response 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 and failures affecting ICT.

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

Such readiness objectives include:

e) improving the incident detection capabilities;

f) preventing a sudden or drastic failure;

g) enabling an acceptable degradation of operational service if the failure is unpreventable;

h) further shortening recovery time; and

i) minimizing consequence upon eventual occurrence of the incident.

6.4 Risk management and applicable controls for IRBC

The risk management process includes information security risks where risk related to loss of availability of ICT services in adverse situations is applicable to ICT readiness and business continuity. These risks are characterized by very low likelihood and very high impact.

The risk treatment should include business continuity controls.

Such controls are crucial to modify and lower the risk, and to reduce the impact on the business by having an IRBC. The extent and capability of the IRBC should then, through the risk management process, be determined that it is in line with business risk appetite and the business impact analysis.

The risk management and risk status reporting supports the business in determining the risk and possible risk acceptance on a strategic and long-term perspective.

IRBC supports the actual implementation of the control specified in ISO/IEC 27002:2022, 5.30.

For further information on information security risk management, see ISO/IEC 27005.

6.5 Incident management and relationship to IRBC

The incidents applicable to IRBC are on the highest classification level of the incident organization's incident classification.

Incidents that IRBC can help mitigate are typically considered highly unlikely but have a significant or catastrophic impact on the ICT services if they occur. The objective of IRBC is to develop strategies that help the organization to prevent, respond and recover from incidents that impact ICT services.

Triggers for activating IRBC plans should be defined as part of the organization's incident management process, including information security incident response plans that can include the following interactions during the flow of information security events and incidents:

— a link should be established between the incident coordinator (see ISO/IEC 27035-1) and the responsible IRBC as soon as the potential effect of the incident on business continuity is identified;

— communication channels and procedures should be prepared to enable the handover of operational responsibility between incident management and IRBC response elements prepared to avoid uncontrolled loss of time and meet agreed deadlines;

— transfer of responsibility from the responsible IRBC to the incident coordinator should be foreseen to allow for the preparation of the incident report and introduce their proposal for improvement via "learn lessons". Refer to ISO/IEC 27035-1:2023, Clause 5 for more details.

For further general information on information security incident management, see ISO/IEC 27035-1.

6.6 BCM strategies and alignment to IRBC

An organization's dependency on ICT in an adverse situation can vary and the characteristics of an adverse situation can also affect the ICT dependency. The BCM strategy should provide the time frames and priorities for IRBC.