



DPC: 23 / 30431842 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 20 April 2023

Origin: International

Latest date for receipt of comments: 5 June 2023

Project No. 2020/03472

Responsible committee: IST/33 Information security, cybersecurity and privacy protection

Interested committees:

Title: BS ISO/IEC 27031 Information technology - Cybersecurity - Information and communication technology readiness for business continuity

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 5 June 2023**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Mr Delme Stephenson (BSI)**
Direct tel: **020 8996 7213**
E-mail: **delme.stephenson@bsigroup.com**

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27031

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Voting begins on:
2023-04-12

Voting terminates on:
2023-07-05

Information technology — Cybersecurity — Information and communication technology readiness for business continuity

ICS: 35.030; 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



Reference number
ISO/IEC DIS 27031:2023(E)
Documents
AVA Document Sharing Hub
© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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	2
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 The organization's BCM strategies and alignment for IRBC	6
7 Business Requirements 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 (BIA)	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, interfaces and dependencies	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 performance objectives	12
8.1.5 Determining possible outcomes and benefits of IRBC	12
8.1.6 HVAC redundancy planning	13
8.1.7 Determine the scope of ICT services related to the objectives	13
8.2 Determine target ICT RTO and ICT RPO	14
9 Determine IRBC strategies	15
9.1 General	15
9.2 IRBC Strategy Options	16
9.2.1 General	16
9.2.2 Skills and Knowledge	16
9.2.3 Facilities	16
9.2.4 Technology	17
9.2.5 Data	18
9.2.6 Processes	18
9.2.7 Suppliers	18
10 Determine ICT continuity plan	19
10.1 Prerequisites for the development of plans	19
10.1.1 Determine and set the recovery organization	19

10.1.2	Determine time frames for plan development, reporting and testing	19
10.1.3	Resources	20
10.1.4	Competency of IRBC staff	21
10.1.5	Technological solutions	21
10.2	Recovery plan activation	21
10.2.1	ICT BCP Activation	21
10.2.2	Escalation	22
10.3	ICT recovery plans	22
10.3.1	ICT RPO and ICT RTO plans	22
10.3.2	Facilities	22
10.3.3	Technology	22
10.3.4	Data	23
10.3.5	Processes	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	24
11.1	Internal test requirements	24
11.1.1	Performance criteria	24
11.2	Testing dependencies	24
11.2.1	Test and exercise	24
11.2.2	Test and exercise program	24
11.2.3	The 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 ICT RPO and RTO	29
12.1	General	29
13	Top Management responsibilities regarding evaluating the IRBC	29
13.1	General	29
13.2	Management Responsibilities	29
Annex A (Informative) General consideration for risk comparing ICT RTO and ICT RPO to business objectives for ICT recovery		31
Annex B (Informative) Risk reporting for FMEA		33
Bibliography		34

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization. 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.

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 ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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.

This document was prepared by Technical Committee ISO/IEC JTC 1, Information technology, 27, IT Security Techniques.

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

The main changes compared to the previous edition are as follows:

- The structure of the document has been changed
- The scope has been changed to ensure a clarification
- Technical content have been put within the following clauses:
 - [6.4](#) Risk management and applicable controls for IRBC
 - [6.5](#) Incident management and relationship to IRBC
 - [6.6](#) The organization's BCM strategies and alignment for IRBC
 - [9.2](#) IRBC Strategy Options
 - [10.1.5](#) Technological solutions

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.

Introduction

This document describes the concepts and principles of information and communication technology (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.

Over the years, ICT has become an integral part of many of the activities which are elements of the critical infrastructures in all organizational sectors, whether public, or private. 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 BCMS International Standard developed by ISO/TC 292.

ICT services failures including those caused by 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 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.

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 – ISO/IEC 22301) respectively, it is critical to develop and implement a ICT 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 during 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.

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 achieved by coordinating IRBC with the ISMS and BCM processes. In this way IRBC supports BCM by ensuring that the ICT services are appropriately resilient and can be recovered to pre-determined levels within timescales required and agreed by the organization.

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.

ISO/IEC 27031 complements the information security controls relating to Business Continuity in ISO/IEC 27002 along with aligning to support the information security risk management process as standardized in ISO/IEC 27005 (as part of an Information Security Management System (ISMS) according to ISO/IEC 27001).

Furthermore, the approach to ICT readiness for business continuity supports an organization having a Business Continuity Management System (BCMS) according to ISO 22301.

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

Information technology — Cybersecurity — Information and communication technology readiness for business continuity

1 Scope

The scope of this document is delimited on information and communication technology (ICT) readiness for business continuity.

Readiness of ICT for business continuity means that ICT and its operational capabilities demonstrate the ability to achieve desired business continuity objectives in case of a disruption affecting ICT.

This document serves the following business continuity objectives for ICT:

- Maximum Tolerable Period of Disruption (MTPD)
- Recovery Point Objective (RPO),
- Recovery Time Objective (RTO) as part of the ICT Business Continuity Planning.

This document applies to an ICT context serving a given activity (private, governmental, and non-governmental), irrespective of size.

This document describes how ICT function should plan and get ready to contribute to the resilience objectives desired by the organization.

2 Normative references

There are no normative references in this document.

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, ISO Guide 73 and the following apply.

ISO and IEC maintain terminological 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 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

3.2 failure mode

manner by which a failure is observed

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

3.3

ICT disaster recovery

ability of the ICT elements of an organization to support its critical processes and activities to an acceptable level within a predetermined period of time following a disruption

3.4

ICT readiness

state of an 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 doesn't 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 may such a contingency occurs.

3.5

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

3.6

recovery point objective

RPO

point in time to which data must be recovered after a disruption has occurred

Note 1 to entry: RPO also represents the maximum data loss tolerated by an organization.

3.7

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

3.8

restoration

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

3.9

trigger

event that causes the system to initiate a response

Note 1 to entry: Also known as triggering event.

4 Abbreviated terms

BCMS	business continuity management system
BIA	business impact analysis
HVAC	heating, ventilation and air-conditioning
ICT	information and communication technology
IRBC	ICT readiness for business continuity
ISMS	information security management system

5 Structure of this document

5.1 General

The intent of each part of this document are the following:

- [Clause 6](#), this clause explains how IRBC is linked to BCM and other organizational processes that have a relation to IRBC;
- [Clause 7](#), this clause explains how the business continuity for the organization sets objectives that IRBC should try to meet;
- [Clause 8](#), this clause provides guidance on what is needed to define the ICT current characteristics that will affect the IRBC;
- [Clause 9](#), this clause provides guidance on what different strategies 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](#), this clause provides guidance on how to design ICT continuity plans based on determined strategies and addressing different types of adverse situations to meet the continuity objectives for ICT;
- [Clause 11](#), this clause provides guidance on how to test and finalize the ICT continuity plans;
- [Clause 12](#), this clause 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](#), this clause 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 is able to face events, which, without such readiness, would lead the organization to 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 instances of business continuity management and information security management.

6 Integration of IRBC into BCM

6.1 General

Business continuity risk within information security and ICT relates primarily with availability when adverse situation occurs that disrupts the availability of ICT services to critical business processes.

The related risks have the characteristics of very low likelihood meaning that they may 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 the likelihood for such risks can in most cases never be fully eliminated.

Determination of risk of business process can evolve from the risk management process that takes part within an ISMS and the controls to mitigate them and maintain business continuity.

The determination of prioritised activities can be concluded through BIA (business impact analysis) 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 can be interrupted may be hard for business to determine and are generally on a high level based on different threats. Such threats and sources are typically:

- Environmental – Fire, flooding, etc.;
- Technical hardware, software failures or power and air conditioning (HVAC) shortages or breakdowns;
- Human error – Mistakes in change management, wrongly configured back up, etc.;
- Human intentional – hacking, malware, sabotage;
- Societal – Pandemic, strikes, social unrest, etc.;
- Cyberattacks - DOS, DDOS;
- ICT- supply chain specifics:
 - Perturbation on the communication channel with a data/service provider;
 - Disruption of a cloud service provider;
 - Unclear information security requirements on ICT dependencies provided by external parties.

The threats above generally result in the following states of major impacts in the ICT services that lasts for critical timeframes:

- 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 and their competence

All these scenarios should be addressed 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. ICT may through their risk management determine vulnerabilities or other weaknesses that may cause severe disruption. It is through risk assessment and risk treatment that risks can be mitigated but still this mitigation will not eliminate the need for IRBC to be in place as there will always be a risk that something unforeseen will happen.

6.2 Enabling governance

General knowledge of the readiness of the different elements of ICT should be made including as applicable:

- ICT services;
- ICT facilities;
- technology (hardware, software, architecture);
- data;
- processes;
- suppliers, as well as their critical components; and
- staff competencies.