

ISO/IEC ~~DIS~~ FDIS 27031:20232024(E)

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Date: ~~2023~~2024-06-2012

Secretariat: DIN

Cybersecurity — Information and communication technology readiness for business continuity

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO/IEC FDIS 27031](https://standards.itih.ai/catalog/standards/iso/c30dba04-327f-4ac4-b6fc-d3ac16306214/iso-iec-fdis-27031)

<https://standards.itih.ai/catalog/standards/iso/c30dba04-327f-4ac4-b6fc-d3ac16306214/iso-iec-fdis-27031>

© ISO/~~IEC~~ 2023, 2024

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/~~ISO's~~ member body in the country of the requester.

ISO ~~copyright office~~Copyright Office

CP 401 • ~~Ch. de Blandonnet 8~~

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

~~Fax: +41 22 749 09 47~~

~~Email: copyright@iso.org~~

~~Email: copyright@iso.org~~

Website: ~~www.iso.org~~www.iso.org

Published in Switzerland.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 27031

<https://standards.iteh.ai/catalog/standards/iso/c30dba04-327f-4ac4-b6fc-d3ac16306214/iso-iec-fdis-27031>

Contents

Foreword	4
Introduction	5
1 — Scope	7
2 — Normative references	7
3 — Terms and definitions	7
4 — Abbreviated terms	8
5 — Structure of this document	9
5.1 — General	9
6 — Integration of IRBC into BCM	9
6.1 — General	9
6.2 — Enabling governance	10
6.3 — Business continuity management objectives	11
6.4 — Risk management and applicable controls for IRBC	12
6.5 — Incident management and relationship to IRBC	12
6.6 — The organization's BCM strategies and alignment for IRBC	12
7 — Business Requirements for IRBC	13
7.1 — Risk review	13
7.1.1 — General	13
7.1.2 — Monitoring, detection and analysis of threats and events	14
7.2 — Inputs from business impact analysis (BIA)	14
7.2.1 — General	14
7.2.2 — Understanding critical ICT services	14
7.2.3 — Assessing ICT readiness against business continuity requirements	15
7.3 — Coverage, interfaces and dependencies	15
7.3.1 — General	15
7.3.2 — ICT dependencies for the scope	16
7.3.3 — Determine any contractual aspects of dependencies	16
8 — Defining prerequisites for IRBC	16
8.1 — Incident based — preparation before incident	16
8.1.1 — General	16
8.1.2 — ICT Recovery capabilities	17
8.1.3 — Establishing an IRBC	17
8.1.4 — Setting performance objectives	18
8.1.5 — Determining possible outcomes and benefits of IRBC	19
8.1.6 — HVAC redundancy planning	19
8.1.7 — Determine the scope of ICT services related to the objectives	20
8.2 — Determine target ICT RTO and ICT RPO	21
9 — Determine IRBC strategies	22
9.1 — General	22
9.2 — IRBC Strategy Options	23
9.2.1 — General	23
9.2.2 — Skills and Knowledge	23
9.2.3 — Facilities	23
9.2.4 — Technology	24
9.2.5 — Data	25

9.2.6	Processes	25
9.2.7	Suppliers	26
10	Determine ICT continuity plan	26
10.1	Prerequisites for the development of plans	26
10.1.1	Determine and set the recovery organization	26
10.1.2	Determine time frames for plan development, reporting and testing	27
10.1.3	Resources	28
10.1.4	Competency of IRBC staff	28
10.1.5	Technological solutions	28
10.2	Recovery plan activation	29
10.2.1	ICT BCP Activation	29
10.2.2	Escalation	29
10.3	ICT recovery plans	30
10.3.1	ICT RPO and ICT RTO plans	30
10.3.2	Facilities	30
10.3.3	Technology	30
10.3.4	Data	30
10.3.5	Processes	31
10.3.6	People	31
10.4	Temporary work around plans	31
10.5	External contacts and procedures	31
11	Testing, exercise, and auditing	31
11.1	Internal test requirements	31
11.1.1	Performance criteria	31
11.2	Testing dependencies	32
11.2.1	Test and exercise	32
11.2.2	Test and exercise program	32
11.2.3	The scope of exercises	33
11.2.4	Planning an Exercise	33
11.2.5	Alert based and different recovery stages	34
11.2.6	Managing an Exercise	35
11.3	Learning from tests	36
11.4	Auditing the IRBC	36
11.5	Control of documented information	37
12	Final ICT RPO and RTO	37
12.1	General	37
13	Top Management responsibilities regarding evaluating the IRBC	37
13.1	General	37
13.2	Management Responsibilities	38
Annex A (Informative) General consideration for risk comparing ICT RTO and ICT RPO to business objectives for ICT recovery		39
Annex B (Informative) Risk reporting for FMEA		40
Bibliography		41
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	2

4	Abbreviated terms	3
5	Structure of this document	3
5.1	General	3
6	Integration of IRBC into BCM	4
6.1	General	4
6.2	Enabling governance	5
6.3	Business continuity management objectives	6
6.4	Risk management and applicable controls for IRBC	7
6.5	Incident management and relationship to IRBC	7
6.6	BCM strategies and alignment to IRBC	7
7	Business expectations for IRBC	8
7.1	Risk review	8
7.1.1	General	8
7.1.2	Monitoring, detection and analysis of threats and events	9
7.2	Inputs from business impact analysis	9
7.2.1	General	9
7.2.2	Understanding critical ICT services	9
7.2.3	Assessing ICT readiness against business continuity requirements	10
7.3	Coverage and interfaces	10
7.3.1	General	10
7.3.2	ICT dependencies for the scope	11
7.3.3	Determine any contractual aspects of dependencies	11
8	Defining prerequisites for IRBC	11
8.1	Incident based - preparation before incident	11
8.1.1	General	11
8.1.2	ICT Recovery capabilities	12
8.1.3	Establishing an IRBC	13
8.1.4	Setting objectives	13
8.1.5	Determining possible outcomes and benefits of IRBC	13
8.1.6	Equipment redundancy planning	14
8.1.7	Determining the scope of ICT services related to the objectives	15
8.2	Determining target ICT RTO and RPO	16
9	Determining IRBC strategies	17
9.1	General	17
9.2	IRBC strategy options	18
9.2.1	General	18
9.2.2	Skills and knowledge	18
9.2.3	Facilities	19
9.2.4	Technology	19
9.2.5	Data	20
9.2.6	Processes	21
9.2.7	Suppliers	21
10	Determining the ICT continuity plan	21
10.1	Prerequisites for the development of plans	21
10.1.1	Determining and setting the recovery organization	21
10.1.2	Determining time frames for plan development, reporting and testing	22
10.1.3	Resources	24
10.1.4	Competency of IRBC staff	24
10.1.5	Technological solutions	24
10.2	Recovery plan activation	25

10.2.1 ICT BCP Activation	25
10.2.2 Escalation	25
10.3 ICT recovery plans	25
10.3.1 RPO and RTO plans for ICT	25
10.3.2 Facilities.....	25
10.3.3 Technology.....	26
10.3.4 Data.....	26
10.3.5 Response and recovery procedures	26
10.3.6 People	26
10.4 Temporary work around plans	27
10.5 External contacts and procedures.....	27
11 Testing, exercise, and auditing.....	27
11.1 Performance criteria.....	27
11.2 Testing dependencies	27
11.2.1 Test and exercise.....	27
11.2.2 Test and exercise program	28
11.2.3 Scope of exercises.....	28
11.2.4 Planning an exercise	29
11.2.5 Alert based and different recovery stages	30
11.2.6 Managing an exercise.....	31
11.3 Learning from tests.....	32
11.4 Auditing the IRBC	32
11.5 Control of documented information.....	33
12 Final MBCO.....	33
13 Top management responsibilities regarding evaluating the IRBC	34
13.1 General.....	34
13.2 Management responsibilities	34
Annex A (informative) Comparing RTO and RPO to business objectives for ICT recovery	35
Annex B (informative) Risk reporting for FMEA.....	36
Bibliography.....	37

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 ~~to ensure a 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.

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO/IEC FDIS 27031](https://standards.itih.ai/catalog/standards/iso/c30dba04-327f-4ac4-b6fc-d3ac16306214/iso-iec-fdis-27031)

<https://standards.itih.ai/catalog/standards/iso/c30dba04-327f-4ac4-b6fc-d3ac16306214/iso-iec-fdis-27031>

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 ~~failures~~, 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 ~~and, 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 part of the implementation and operation of an information security management system (ISMS) specified in ISO/IEC 27001 and a business continuity management system (BCMS), specified in ISO/IEC 22301, it is critical to develop and implement an 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 should put in place a systematic process to prevent, predict and manage ICT ~~disruption~~disruptions and incidents which have the potential to disrupt ICT services. This can be achieved by coordinating IRBC with the ISMS 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 ~~ISO/IEC 27001 to establish an ISMS, and/or using~~ relevant information security and business continuity standards ~~such as ISO 22301 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.

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.

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

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

[ISO/IEC FDIS 27031](https://standards.itih.ai/catalog/standards/iso/c30dba04-327f-4ac4-b6fc-d3ac16306214/iso-iec-fdis-27031)

<https://standards.itih.ai/catalog/standards/iso/c30dba04-327f-4ac4-b6fc-d3ac16306214/iso-iec-fdis-27031>

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~~ minimum business continuity objective (MBCO),
- ~~Recovery Point Objective~~ recovery point objective (RPO),
- ~~Recovery Time Objective~~ recovery time objective (RTO) as part of the ICT ~~Business Continuity Planning~~ business continuity planning.

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

This document describes how ICT ~~department~~ departments plan and prepare to contribute to the resilience objectives ~~desired by~~ 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 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

ISO/IEC 27005:2022, *Information ~~technology~~ — ~~Security techniques~~ — ~~Information security risk management, cybersecurity and privacy protection~~ — Guidance on managing information security risks*

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

ISO 22300, *Security and resilience — Vocabulary*

ISO 22301:~~2019~~, *Security and resilience — Business continuity management systems — Requirements*

~~ISO Guide 73, *Risk management — Vocabulary*~~

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 terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at ~~<https://www.iso.org/obp>~~<https://www.iso.org/obp>
- IEC Electropedia: available at ~~<https://www.electropedia.org/>~~<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 ~~doesn't~~**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”.

~~[SOURCE: ISO 22300:2021, 3.1.202]~~

3.6

recovery time objective

RTO