ISO/IEC ~~DIS~~ FDIS 27031:~~2023~~2024(E)

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Date: ~~2023~~2024-06-~~20~~12

Secretariat: DIN

Cybersecurity — Information and communication technology readiness for business continuity

Contents

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~~www.iso.org/directives or ~~www.iec.ch/members_experts/refdocs~~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~~.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~~.www.iso.org/iso/foreword.html. In the IEC, see ~~www.iec.ch/understanding-standards~~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~~www.iso.org/members.html and ~~www.iec.ch/national-committees~~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 ~~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.

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 Objectiveminimum 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 Planningbusiness continuity planning.

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

This document describes how ICT departmentdepartments plan and prepare to contribute to the resilience objectives desired byof 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 managementand 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