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 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 sources – 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 (see ISO 22313).

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 affecting ICT;

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.

Business continuity strategies influencing IRBC can be:

- stopping business for a certain time frame;
- relocating business to an alternative site;
- cooperating with supplier or partner.

Decisions can be:

- prioritized business operations or processes and time frames for these;
- ICT services and their related RPO and RTO.

IRBC should provide the capability for organizations to use ICT during adverse situations when BCM is in operation. Two cases can occur:

a) IRBC is unable to meet the RPO or RTO for some processes/functions. In such a case, the organization is required to align the BCP for these processes/functions to allow operations without ICT until it is available according to the time provided by IRBC.

b) IRBC can meet the RPO or RTO for all processes/functions. Then, the BCP of the organization is aligned.

An organization should determine the ICT minimum business continuity objectives (MBCOs) based upon recovery point objectives (RPOs) and recovery time objectives (RTOs) within the ICT scope.

7 Business expectations for IRBC

7.1 Risk review

7.1.1 General

The information security risk management process is explained in greater detail in ISO/IEC 27005, which is also aligned with the guidelines for risk management given in ISO 31000.

ICT business continuity supports incident handling when a major incident affecting ICT has occurred. The IRBC modifies information security risks related to availability with a low likelihood, but with significant consequences.

The IRBC strategies should be resilient and adaptable, any change to the ICT services which can affect the IRBC capability should be implemented only after the business continuity implications of the change have been assessed, addressed and approved.

To ensure that the IRBC strategies and plans remain appropriate for the organization:

a) top management should ensure that the IRBC strategies continue to support the organization's BCM requirements (see 13.2);

b) the change management process should include all parties responsible for the IRBC strategies, both in their planning and implementation;

c) the development process for new ICT services should include a sign-off that IRBC resilience has not been compromised by even the simplest of upgrades or improvements;

d) due diligence on merger and acquisition activity; and

e) IRBC should consider any ICT component decommissioning.

The organization should establish a process to monitor and detect the emergence of ICT security threats including, but not limited to, the following areas:

f) retention of staff, skills and knowledge;

g) management of facilities that house ICT equipment (e.g. by monitoring the number and nature of security incidents/vulnerabilities related to computer rooms);

h) changes in supporting technology, plant, equipment, networks, applications and databases;

i) finance or budget allocation; and

j) effectiveness of external services and suppliers (supplies).

7.1.2 Monitoring, detection and analysis of threats and events

Monitoring of the ICT systems and their critical components is the first line of defence to allow detection of abnormal situations, such as vulnerabilities that can be exploited to become an event, and further develop into an incident and an ICT disruption that can cause the activation of the IRBC capability and processes.

Detection of unwanted events and situations, such as misconfigured controls, deviations to policies, or mechanical failures, is also essential as the incident response can only start as soon as the event is reported to the Point of Contact (PoC) and assessed by the incident coordinator (see ISO/IEC 27035-1).

Threat analysis is another way of seeing in advance what can harm the ICT systems as the threats are generally still outside direct concern and control. This will happen by being continuously informed by specialized bodies and verifying if an organization’s ICT can be potentially hit, harmed and impacted by the threat. If so, the vulnerability management capability should be activated to prepare the improvement of the current protection.

7.2 Inputs from business impact analysis

7.2.1 General

The organization should categorize its activities according to their priority for continuity as determined by a business impact analysis (see ISO/TS 22317). It should also define the minimum level at which each critical activity should be performed upon resumption. Top management should agree to the organization's business continuity requirements (see 13.2). These requirements should result in a RTO and a RPO for the MBCO for each product, service or activity. These RTOs start from the point at which the disruption occurs and run until the product, service or activity are recovered.

7.2.2 Understanding critical ICT services

A number of ICT services can be considered critical and required to enable recovery to take place. Each of these critical ICT services should have their own documented RTO and RPO and MBCO of the ICT service (these can include aspects of ICT service delivery, such as a help desk). The RTO of critical ICT services will invariably be lower than the RTO of the business activity, due to the interdependencies between ICT services.

The organization should identify and document its critical ICT services and include brief descriptions and names that are meaningful to the organization at service user level. This ensures common understanding between business and ICT staff, as there can be different names used for the same service. Each critical ICT service listed should identify the organization's product or service that it supports. Via the BIA process, top management should agree to the ICT services and their associated IRBC requirements, listing the ICT components/services that support the critical business processes.

For each critical ICT service identified and agreed within the BCM process, all the ICT components of the end-to-end service should be described and documented, showing how they are configured or linked to deliver each service. Both the normal ICT service delivery environment and the ICT continuity service delivery environment configurations should be documented.

For each critical ICT service, the current continuity capability should be examined from the point of view of the risk analysis review mechanism, in order to assess the risks of service interruption or degradation, and determine the appropriate level of readiness. Any dependencies between services, including reliance on external services and resources, should be included to determine continuity capability to be covered by the

IRBC. This is often the case for certain services that should be available in order for a critical service to be available to the business.

An ICT critical service is identified as one that, if interrupted, will produce an impact considered as unacceptable by the organization or stakeholders, for example, to safety, information security and business operations. A typical example is the dependence of external mail communication on the availability of the internet.

7.2.3 Assessing ICT readiness against business continuity requirements

For each critical ICT service, the current ICT readiness arrangements should be monitored, such as prevention, detection, response and recovery. These ICT readiness arrangements should also be compared with business continuity requirements (see ISO/TS 22317) and any gaps should be documented.

Top management should be informed of any gaps between IRBC capability and business continuity requirements. Such gaps can indicate business risks and the need for additional recovery resources, such as:

a) staff, including number, skills and knowledge;

b) facilities that house ICT systems, e.g. computer room;

c) supporting technology, plant, equipment and networks (technology);

d) information applications and databases;

e) finance or budget allocation; and

f) external services and suppliers (supplies).

Top management (see 13.2) should sign off the ICT business continuity strategy, the documented list of critical ICT services and the risks associated with gaps identified between IRBC capability and business continuity requirements. The options for addressing the gaps and risks identified should then be explored by determining IRBC strategies.

7.3 Coverage and interfaces

7.3.1 General

IRBC should be focused on:

- supporting business objectives in adverse situations;
- identification of the correct status of the ICT within the organization by ICT staff and partners because they are critical resources for identifying, setting up, documenting, operating, maintaining and improving ICT;
- checks in the ICT lifecycle phases that IRBC inputs are transposed in operational working level and service level agreements;
- pragmatic observations on ICT and cybersecurity staff or partners ability to sustain readiness factors before, during and after exercise, and finally, on real conditions.

The coverage should include:

- ICT architecture, infrastructures and services;
- how the ICT lifecycle is designed, built and run, regardless of the lifecycle framework.

The boundaries should limit to the following:

- business continuity management inputs:
  - BIAs;
- Contextualized inputs from cybersecurity and information security management:
  - penetration-test outcomes;
  - accepted risks scenario;
  - likely attacks leading to loss of data.

7.3.2 ICT dependencies for the scope

The organization should define and keep as a documented information, an architecture of the ICT within the context of the IRBC. This is done in order to identify the product, service or activity supported by ICT, any limitations, their dependencies, and their potential related risks.

7.3.3 Determine any contractual aspects of dependencies

For each ICT product, service or activity, including the connection and use of internet services, a list of the suppliers and service providers should be established and documented, in order to determine the nature of support delivered and their associated responsibilities. This documentation should be maintained and kept up to date to ensure it is continuously relevant.

An analysis should be performed to identify gaps between the business continuity capability of the service provider and the approved RTO of the service contracted with the service provider.

8 Defining prerequisites for IRBC

8.1 Incident based – preparation before incident

8.1.1 General

For any ICT incident there should be an incident response to:

a) confirm the nature and extent of the incident;

b) take control of the situation;

c) resolve the incident; and

d) communicate with stakeholders.

Resolving the incident requires a team of competent people known as the incident response team (IRT), to stop the cause of the incident, its mode of action, its effect, and to recover the operation of the business activity by putting the ICT system back in operation.

The incident response should trigger an appropriate IRBC action (if required). If IRBC action is required, this response should be integrated with an overall BCM incident response, and can invoke an incident management team or, in a small organization, a single individual with the responsibility for incident and business continuity management.

A larger organization can use a tiered approach and establish different teams to focus on different functions. Within ICT, this can be based on technical or service-related issues.

Those responsible for incident management should have plans for the activation, operation, coordination and communication of the incident response.

A coordinated programme should be implemented to ensure that processes are in place to regularly promote IRBC awareness in general, as well as assess and enhance competency of all relevant personnel key to the successful implementation of IRBC.

ISO/IEC 27035-1 proposes the generic process and ISO/IEC 27035-3 explains the response on ICT systems.

There should be a linkage between crisis management and incident management. Sometimes incident response requires IRBC procedures to be activated without activation of the BCM. Sometimes the authority and responsibility to manage the incident should be given to the IRBC team when the conditions are present (when RTO or RPO, even potentially, cannot be achieved, or when several or even one critical business processes are impacted); when the crisis situation is solved, responsibility to finalize and close the incident can then be passed again to the incident coordinator.

The difference between the incident management and IRBC lies in the condition of activation, the extent of the business impact and possible consequences, and the level of authority to coordinate the actions; the processes are identical.

In addition to these response activities, the installation and operation of "workarounds" (see 10.4), which allow the business process to continue with the least possible disruption, can be permitted.

8.1.2 ICT Recovery capabilities

The main objective of the planning phase is to establish the organization's ICT readiness requirements, including:

a) the IRBC strategy and IRBC plan that are required to support the business requirements defined through BIA process;

   NOTE Legal requirements can apply.

b) the performance criteria needed by the organization to monitor the degree of ICT readiness it requires to achieve those aims and objectives;

c) list the resources (technical and other) to allow the IRBC team(s) to perform within the agreed time schedule.

8.1.3 Establishing an IRBC

IRBC is likely to be more efficient and cost effective when designed and built into ICT services from their inception as part of an IRBC strategy which supports the organization's business continuity objectives. This ensures that ICT services are better built, better understood and more resilient. Retrofitting IRBC can be complex, disruptive and expensive.

The organization should develop, implement, maintain and continually improve a set of documented processes which supports IRBC.

These processes should ensure that the IRBC objectives are clearly stated, understood and communicated, and that top management's commitment to IRBC is demonstrated.

8.1.4 Setting objectives

A basic approach should use the known incident scenarios and related events to establish the response baselines for each category of incidents and related events, as follows.

a) All known incidents and event indicators should be established as input and monitored or tracked to trigger to the next steps.

b) A set of known incidents should be specified (e.g. password intrusion attack, server failure due to insufficient hard disk space).

c) A list of events leading to those incidents should be identified (e.g. failed login attempts, hard disk utilization).

d) A time frame should be set to establish an adequate detection time (e.g. threshold for events to be reported/alerted to the system/administrator).

e) A time frame should be determined to establish suitable response time (e.g. timeline for an administrator to take action to prevent an incident to materialize);

f) Events should be classified into groups of desired response time blocks and response action types; events can be classified by threat group, application group, response action group and/or response time group.

g) Matrices and measures should be refined by testing scenarios and drills or exercises.

h) Tests should be carried out to determine whether the response actions are workable and whether the objectives are achievable.

i) Categories, expected event response time, and expected event response actions (e.g. seek alternative method to monitor, detect, and act) should be refined, and the new baselines should be updated as appropriate.

j) The situation should be improved by recording new incidents and failure scenarios, then repeating the process.

8.1.5 Determining possible outcomes and benefits of IRBC

The benefits of effective IRBC for the organization are that IRBC:

a) captures the organization’s understanding of the risks to continuity of ICT services and their vulnerabilities;

b) identifies the potential consequences of disruption to ICT services, and the sequence of the activities in the response;

c) encourages improved collaboration between its business managers and its ICT service providers (internal and external);

d) develops and enhances competence in its ICT staff by demonstrating credible responses through exercising ICT continuity plans and testing IRBC arrangements;

e) provides assurance to top management that it can depend on predetermined levels of ICT services and receive adequate support and communications in the event of a disruption;

f) provides assurance to top management that information security (confidentiality, integrity and availability) is properly preserved, ensuring adherence to information security policies;

g) provides additional confidence in the business continuity strategy through linking investment in ICT solutions to business needs and ensuring that ICT services are protected at an appropriate level given their importance to the organization;

h) has ICT services that are cost-effective and not under- or over-invested through an understanding of the level of the organization’s dependence on those ICT services; and the nature, location, interdependence and usage of components that make up the ICT services;

i) can enhance its reputation for prudence and efficiency;

j) potentially gains competitive advantage through the demonstrated ability to deliver business continuity and maintain product and service delivery in times of disruption; and

k) understands and documents stakeholders' expectations and their relationships with, and use of, ICT services.

Thus, IRBC provides a meaningful way to determine the status of an organization's ICT services in supporting its business continuity objectives by addressing the question of whether an organization's ICT is capable of responding, and whether it is secure.

8.1.6 Equipment redundancy planning

Concerning ICT, the IRBC can run on several strategies for its planning, depending on the time needed to replace the defective equipment:

- cold backups: equipment are present, possibly in storage (or can be ordered and provided within a very short time frame) but should be configured and installed to replace the defective one;
- warm backup: equipment is in operation for another function and can be easily and rapidly reconfigured;
- hot backup: equipment is ready to use and can directly be swapped with the defective one;
- high-redundancy: two identical equipment items are running simultaneously but each has the capacity to provide the whole service. The removal of the defective one will have no impact on operations.

Another IRBC possibility in the plan is to define and prepare “workarounds” that allow the business activity to continue with the least disruption while the response team works on recovering the “normal” system. It can be a fully manual, a semi-manual or a fully automated solution that performs the service with a reduced performance.

The concept of cold and warm backup can be extended to processing facilities, where a decision is made, with the necessary contracts and planning, to organize the resumption of all or part of the activities (including ICT) in another facility (see 9.2.3).

8.1.7 Determining the scope of ICT services related to the objectives

The key elements of IRBC can be summarized as follows:

a) people: the specialists with appropriate skills and knowledge, and competent backup personnel;

b) facilities: the physical environment in which ICT resources are located, including critical HVAC equipment;

c) technology:

- hardware (including racks, servers, storage arrays, tape devices and fixtures);
- network (including data connectivity and voice services), switches and routers;
- software, including operating systems and application software, links or interfaces between applications and batch processing routines;
- data: application data, voice data and other types of data;
- processes: including supporting documentation to describe the configuration of ICT resources and enable the effective operation, recovery and maintenance of ICT services; and
- suppliers: other components of the end-to-end services where ICT service provision is dependent upon an external service provider or another organization within the supply chain, e.g. a financial market data provider, telecoms carrier or internet service provider.

Figure 1 illustrates how the respective IRBC element supports a typical ICT disaster recovery timeline and in turn, supports the business continuity activities. IRBC implementation enables the organization to respond effectively to new and emerging threats, as well as being able to react and recover from disruptions.

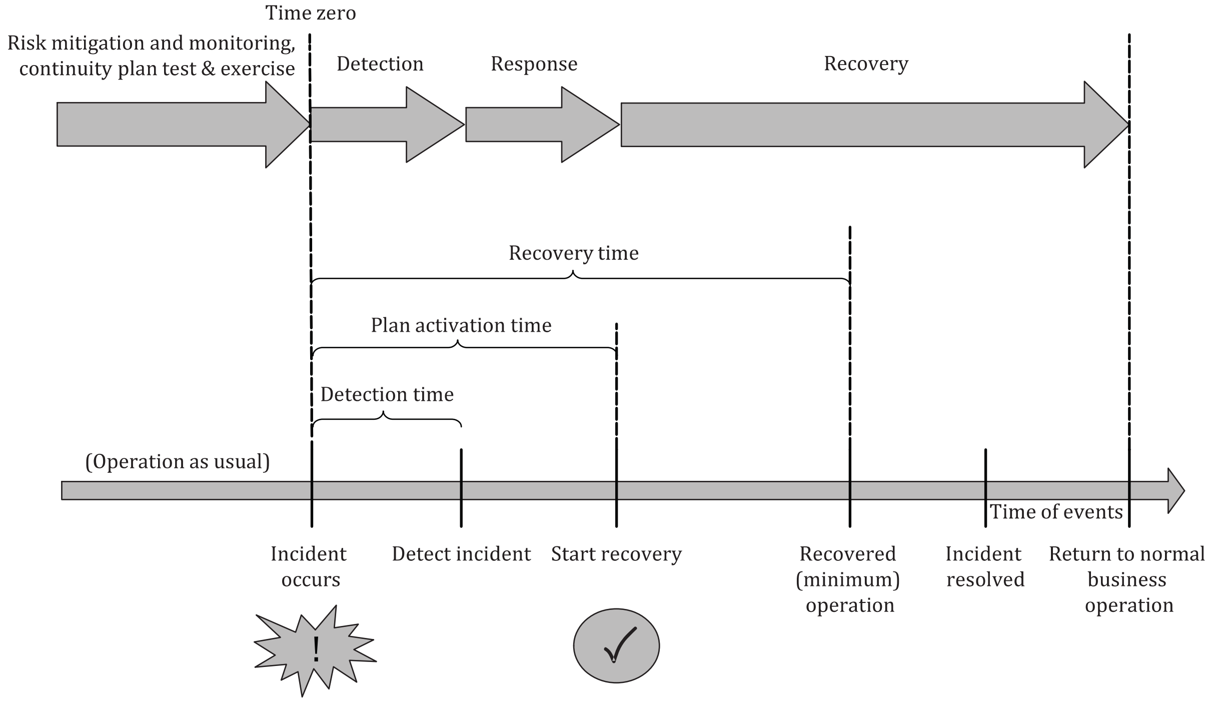

Figure 1 — Scope of IRBC on a typical ICT disaster recovery timeline

8.2 Determining target ICT RTO and RPO

From a business continuity perspective, there is one RTO per product, service or activity. This RTO starts from the point at which the disruption occurs and runs until the product, service or activity is recovered. A number of ICT services can be required to enable this and each of these ICT services can comprise a number of ICT systems or applications. Each of the components, ICT systems or applications will be restored by their respective RTOs, so that the dependent ICT products, ICT services and ICT activities will be restored by their approved RTO.

The RPO is related to the amount of information a business process can afford to lose and is expressed in time (e.g. a day, half a day or 30 minutes). This means that time is required to recover lost data and to return to the normal situation. The data backup policy should ensure the needed exploitable data are available within the RPO.

MBCO refers to the most critical business configurations (and related ICT equipment and services) that are needed to continue providing the services or to achieve minimal business objectives.

Some services can be stopped to provide equipment to support more crucial processes. It is only after the restoration phase that the business services are again fully operational.

It can be necessary to scale up recovered ICT services to support an increasing volume of activity, potentially up to the point at which the product, service or activity is fully recovered to normal transaction volumes. Subsequently, at some point along the timeline, restoration is feasible and desirable and disaster recovery operations are transitioned back to normal operations. The returned normal operations can be either the original state or environment before the disruption, or a new operation arrangement (especially when the disaster disruption has forced a permanent change upon the business).

The target ICT RTO, ICT RPO and MBCO should be defined with a validity period and thus reviewed on a regular basis.

Annexes A and B provide considerations on risk management methodologies for ICT recovery.

9 Determining IRBC strategies

9.1 General

The organization should consider a range of options for the incident readiness of its critical ICT services. The options should consider increasing protection, as well as provision for recovery and restoration from an unplanned disruption, and can include internal arrangements, services delivered to the organization, and services provided externally by one or more third parties.

The options should take account of the various components required to ensure the continuity and recovery of critical ICT services.

IRBC strategies should define the approaches to implement the required recovery capability so that the principles of incident prevention, detection, response, recovery and restoration are put in place.

A range of IRBC strategy options should be evaluated. The strategies chosen should be capable of supporting the business continuity requirements of the organization.

The organization should take into account the implementation and ongoing resource requirements when developing the strategy. External suppliers can be contracted to provide specialist services and skills that play an important role in supporting the strategy.

IRBC strategy should be flexible enough to cater for different business strategies in support of its own business requirements. In addition, the strategy should take into account internal constraints and factors, such as:

a) business objectives and priorities;

b) business continuity strategies;

c) budget;

d) resource availability;

e) potential costs and benefits;

f) technological constraints;

g) the organization's risk appetite;

h) the organization's existing IRBC strategy.

9.2 IRBC strategy options

9.2.1 General

The IRBC strategic options depend on the ICT structure. This structure can be very complex. Strategies should also take into account different scenarios, including when:

- ICT facilities are not available;
- ICT physical hardware is lost;
- ICT software is compromised;
- ICT data are compromised;
- ICT supply chain is compromised;
- competent ICT staff are not available.

In general, strategies can apply on a high level for IRBC, and they can be combined for different services. Such strategies include:

a) Dual site, which means there are multiple data centres;

b) Cooperation, meaning a similar organization can take over;

c) Fallback to secure state, which means implementing documented procedures for restoring systems;

d) Recovery of data, meaning the implementation of data backup strategies;

e) Suppliers take over, meaning the delegation of activities to suppliers;

f) Alternative sourcing, identification of alternative suppliers to ensure redundancy of functions provided internally;

g) Minimization, meaning the isolation of ICTs and the identification of parameters that allow minimum service to be provided until it is fully restored.

9.2.2 Skills and knowledge

The organization should identify appropriate strategies for maintaining core ICT skills and knowledge. This may extend beyond employees to contractors and others who possess extensive ICT specialist skills and knowledge. Strategies to protect or provide those skills can include:

a) documentation of the way in which critical ICT services are performed;

b) multi-skill training, also known as cross-training, of ICT staff and contractors to enhance skill redundancy;

c) separation of core skills to reduce the concentration of risk (this can entail physical separation of staff with core skills or ensuring that more than one person has the requisite core skills); and

d) knowledge retention and management.

9.2.3 Facilities

According to identified risks, the organization should devise strategies for reducing the impact of the unavailability of the normal ICT facilities. This can include one or more of the following:

a) alternative facilities (locations) within the organization, including displacement of other activities;

b) alternative facilities provided by other organizations;

c) alternative facilities provided by third-party specialists;

d) working from home or at other remote sites;

e) other agreed suitable working facilities;

f) use of an alternative workforce in an established site; and

g) alternative facilities that can be transported to the site of the disruption and used to provide direct replacement of some of the physical assets involved.

Strategies for ICT facilities can vary significantly, and a range of options can be available. Different types of incidents or threats can require the implementation of multiple strategies (a pick and mix approach) which will be driven in part by factors such as the organization's size, breadth of activities, locations, technologies and budget.

In considering the use of alternative premises, the following risk mitigation aspects should be taken into consideration:

h) site security;

i) staff access;

j) proximity to existing facilities;

k) availability;

l) cloud risk profiles.

9.2.4 Technology

The ICT services upon which prioritized processes and activities depend should be available in advance, upon the resumption of their dependent business activities.

Thus, solutions are required which ensure the availability of applications within specific time frames, e.g. the RTOs being determined as part of the BIA. Technology platforms and application software should be put in place within timescales demanded by the organization as a whole.

The technologies that support critical ICT services frequently require complex arrangements to ensure continuity, so the following should be considered when selecting IRBC strategies:

a) RTOs and RPOs for critical ICT services which support the prioritized activities identified by the BCM programme;

b) location and distance between technology sites;

c) number of technology sites;

d) remote access to systems;

e) cooling requirements;

f) power requirements;

g) information security requirements;

h) the use of un-staffed (dark) sites as opposed to staffed sites;

i) telecoms connectivity and redundant routing;

j) the nature of “failback” (whether manual intervention is required to activate alternative ICT provision or whether this needs to occur automatically);

k) level of automation required;

l) technology obsolescence; and

m) outsourced service provider's connectivity and other external links.

9.2.5 Data

Additionally, prioritized processes and activities can depend on the provision of up-to-date or near-up-to-date data. Data continuity solutions should be designed to meet the RPO of each prioritized business activity of the organization as they relate to the business activities.

The selected IRBC options should ensure the ongoing confidentiality, integrity and availability of data that support critical activities (see ISO/IEC 27001 and ISO/IEC 27002).

Data storage and IRBC strategies should meet the organization's business continuity requirements, and should take account of:

a) ICT RPO requirements;

b) how data are stored, e.g. disk, tape or optical media; appropriate backup and restoration mechanisms should be in place to ensure the data are secure and in a safe environment;

c) where information is stored, transported or transmitted, distance, location, network links, etc. (onsite, offsite or third party) and expected timescales for the retrieval of backup media; and

d) restore timescales, driven by the volume of data, how they are stored and the complexity of the technical restore process, along with the requirements of the service user and the needs of organizational continuity.

An understanding of the “end-to-end” use of data throughout the organization is critical. This can include information feeds to and from third parties.

It should be considered that the nature, update status and value of data varies enormously within an organization.

9.2.6 Processes

In selecting its IRBC strategy, the organization should consider the processes necessary to ensure the viability of that strategy, including those necessary in the incident prevention, incident detection, incident response and disaster recovery. The organization should also identify any factors necessary for the effective implementation of those individual processes, e.g. key skill sets, critical data, key enabling technologies, or critical equipment or facilities.

For more details on information security incident management, refer to ISO/IEC 27035-1.

9.2.7 Suppliers

The organization should identify and document external dependencies which support ICT service provision and take adequate steps to ensure that critical equipment and services can be provided by their suppliers within predetermined and agreed time frames. Such dependencies can exist for hardware, software, telecoms, applications, third-party hosting services, utilities, and environmental issues, such as air conditioning, environmental monitoring, and fire suppression.

Strategies for these services can include:

a) storage of additional equipment and software copies at another location;

b) arrangements with suppliers for the delivery of replacement equipment at short notice;

c) rapid repair and/or replacement of faulty parts in the event of an equipment malfunction;

d) dual supply of utilities such as power and telecoms;

e) emergency generating equipment; and

f) identification of alternative/substitute suppliers.

The organization should include ICT and business continuity management requirements in contracts with its partners and service providers. Contract schedules should include reference to each party's obligations, agreed service levels, response to major incidents, cost assignment, exercising frequency and corrective actions.

For more details on information security for supplier relationships, refer to ISO/IEC 27036-1.

10 Determining the ICT continuity plan

10.1 Prerequisites for the development of plans

10.1.1 Determining and setting the recovery organization

The organization should, based on the IRBC strategy and plan, define the capability based on a structure, roles and responsibilities. On top of this capability, top management determines who takes the overall responsibility for IRBC.

IRBC strategies should only be implemented after top management's approval. At this point, the implementation stage begins. This clause provides recommendations for implementing an organization's chosen IRBC strategies along with the necessary organization structure, plans and procedures required to support the implementation.

The organization should manage resources (see 10.1.3), procedures and operation of IRBC, as well as implement training and awareness programmes. Implementation should be managed as a project through the organization's formal change control process and BCM project management controls in order to ensure full management visibility and reporting.

Reference should be made to relevant international standards during the implementation of incident detection and response, including ISO/IEC 27035-1 for the incident response process.

10.1.2 Determining time frames for plan development, reporting and testing

The RPO can also relate to the maximum amount of data that can be lost and unrecoverable due to the disruption. This is represented on the timeline as the amount of time between the last good backup and when the disruption event occurs. The RPO and MBCO that can be achieved depends on the ICT service recovery strategy employed, particularly on the backup arrangement.

As data can also be lost if there is a disruption in the incoming and outgoing data flows, organizations should include this consideration in their plans.

For example, at time zero, the critical ICT system is intruded by a hacker and services are brought down. The first milestone after the ICT service disruption event occurs is a direct detection of the security incident (i.e. the intrusion event) or an indirect detection of service loss (or degradation), for which there will be an elapsed time before the notification. For example, in some instances, the IT helpdesk is notified via a call from a user.

It can take several hours from the onset of ICT service disruption until a decision is taken to invoke IRBC, once communication and decision-making time is taken into account. The invocation decision can require careful consideration in some situations, since invoking IRBC often impacts upon normal business operations. An example of this is where the service has not been entirely lost or there seems to be a strong prospect of imminent service recovery.

Once invoked, ICT service recovery can commence. This can be divided into infrastructure (network, hardware, operating system, backup software, etc.) and application recovery (database, application, batch processes, interfaces, etc.).

Once the ICT service has been recovered and system testing has been conducted by ICT staff, the service can be made available for user acceptance test before it is released to staff for use in business continuity operations.

Although ICT staff have the opportunity to carefully plan the restoration and schedule it to take place during a natural low activity period, this is nevertheless a substantial task.

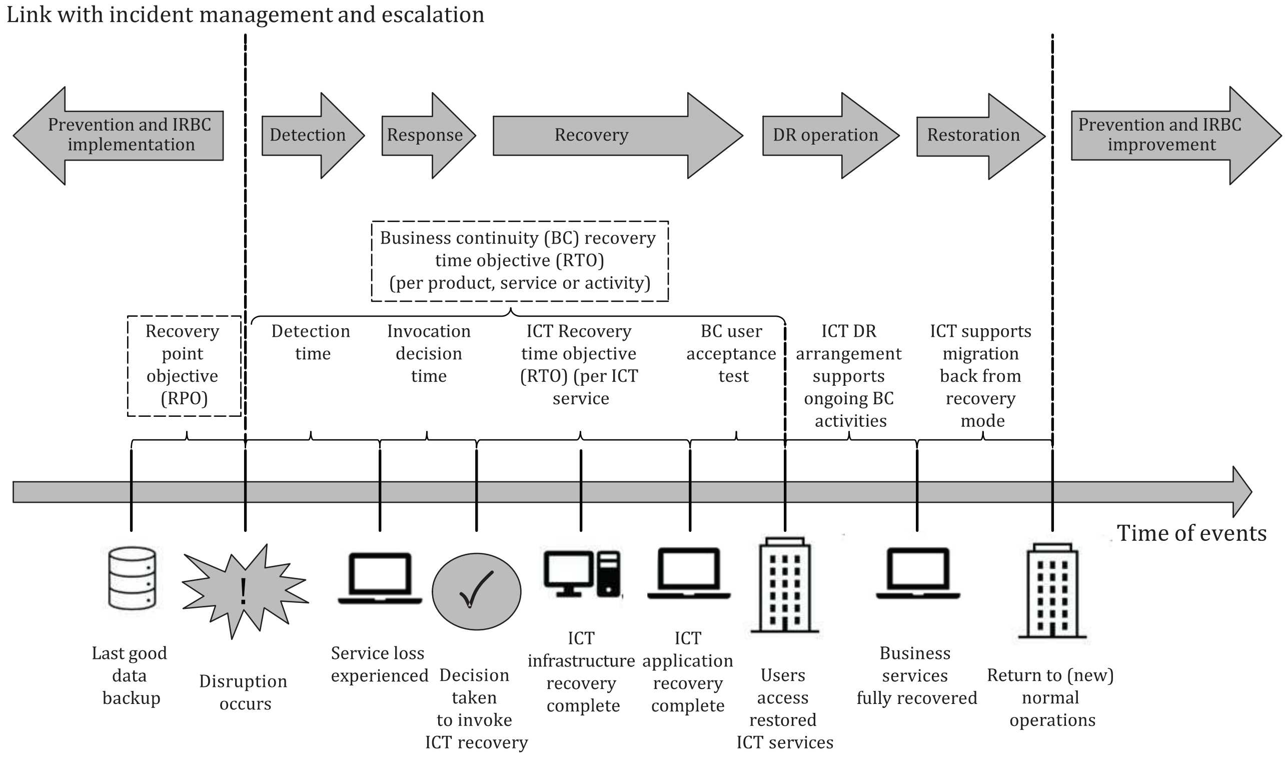
Link with incident management and escalation
Prevention and IRBC implementation
Detection
Response
Recovery
DR operation
Restoration
Prevention and IRBC improvement
Business continuity (BC) recovery time objective (RTO) (per product, service or activity)
Recovery point objective (RPO)
Detection time
Invocation decision time
ICT Recovery time objective (RTO) (per ICT service
BC user acceptance test
ICT DR arrangement supports ongoing BC activities
ICT supports migration back from recovery mode
Time of events
Last good data backup
Disruption occurs
Service loss experienced
Decision taken to invoke ICT recovery
ICT infrastructure recovery complete
ICT application recovery complete
Users access restored ICT services
Business services fully recovered
Return to (new) normal operations

Figure 2 — IRBC and milestones during a disruption timeline

The arrows across the top of Figure 2 indicate how the principles of IRBC detailed in this document align with the disruption timeline.

Figure 2 illustrates how elements of IRBC support key milestones during a major disruption. Events and milestones happen along a timeline starting at time zero when an ICT service disruption/disaster event occurs. An example of the disaster scenario is one that has arisen from a targeted system intrusion attack (commonly called “hacking”) to the organization's critical ICT system.

10.1.3 Resources

As part of the policy mandate, the organization should define the need for an IRBC programme as part of its overall BCM objectives, and determine and provide the resources needed to establish, implement, operate and maintain this programme.

IRBC roles, responsibilities, competencies, and authorities should be defined and documented.

Top management should:

a) appoint or nominate a person with appropriate seniority and authority to be accountable for IRBC policy and implementation;

b) appoint one or more competent persons, who, irrespective of other responsibilities, should implement and maintain the IRBC as described in this document; and

c) appoint a team of competent people that will operate the IRBC tasks and procedures.

10.1.4 Competency of IRBC staff

IRBC staffing should be made up by qualified and trained personnel to perform their assigned duties and responsibilities to ensure IRBC success. IRBC staff should receive up-to-date training to stay current with threats and vulnerabilities to the ICT organization.

10.1.5 Technological solutions

The potential points of failure should be categorized in terms of business impact, in order to escalate the response. In ICT, “high availability” refers to systems or components that are continuously operational for a desirably long period of time. Availability can be measured relative to “100 % operational” or “never failing.” There is a widely held but difficult-to-achieve standard of availability for a system or product which is known as “five 9s” (99,999 %) availability.

A computer system or a network is made up of many components, all of which usually should be present and functional in order for the whole to be operational. While planning for high availability often focuses on backup and failover processing and data storage and access, other infrastructure components such as power and cooling are equally important.

For example, power availability can be assured by such measures as:

a) uninterruptible power supply (UPS);

b) emergency power generating capacity;

c) dual sources of power from a grid.

Data backup and availability can be attained using a variety of storage technologies such as redundant array of disks (RAID) and storage area network (SAN).

Application availability should also be considered and is often achieved through clustering.

Such technologies can only be really effective in delivering high availability through concurrent implementation at more than one geographically dispersed location. For example, simply having a “failover” server at the same location as a primary or “production” server is not going to provide the necessary levels of resilience if that site is affected by a serious environmental disruption. Both servers will be affected by the same environmental disruption. The “failover” server and other supporting technologies would have to be located at another site for required levels of availability to be achieved.

For many organizations, the cost and effort involved in achieving such levels of high availability can be daunting. For that reason, there has been an increased use of third-party service providers who are able to offer the skills, resources and resilient technologies at an affordable price either through the provision of managed or cloud services. It is important to keep in mind however, that while high availability is an effective route to enhanced resilience, the possibility of failure remains. Thus, it is vital that well planned and tested DR processes and procedures are in place.

10.2 Recovery plan activation

10.2.1 ICT BCP Activation

ICT BCP activation is part of the BCM structure for the whole organization. ICT BCP activation is applicable when a severe incident affects ICT operations. The decision to activate should be made according to the mandate set by the BCM. ICT management activates relevant BCP pending the character of the incident according to the IRBC. The activation decision flow can be as follows:

- Incident management determines the incident as severe and ICT related.
- Incident management notifies ICT management and/or crisis management as applicable.
- Authorized management decides to activate ICT BCP.
- BCP for other parts of the organization can also be activated and crisis management is already active.

10.2.2 Escalation

Escalation from incident management to IRBC is a process that:

- puts the responsibility and authority to a higher level,

— depends on criteria and conditions that should be set out and applied both by incident management and BC/IRBC management.

These criteria/conditions should consider the time to resolve the incident with regard to the RTO, and the size of the impact of the incident on business continuity. A process should be developed to ensure the swift transfer of the responsibility in both directions (escalation and de-escalation). When the crisis (IRBC condition) is finished, it is possible that the incident is not yet resolved, especially if the business impact and parties in the resolution involved external resources and teams. The incident coordinator (or the incident management capability) should recover control to complete the incident report and prepare the recommendations for improvements.

10.3 ICT recovery plans

10.3.1 RPO and RTO plans for ICT

ICT RPO and ICT RTO should be established for each product, services and activities and reproduced on several locations and in different kind of support, allowing each person with the appropriate responsibility to have the most appropriate support to use if/ when necessary.

10.3.2 Facilities

ICT recovery systems and critical data backup should, where possible, be physically separated from the operational site to prevent them being affected by the same incident.

Consideration should be given to the location of all ICT environments when implementing the strategy.

The overall scalability, manageability, supportability, performance and cost characteristics of the different implementation techniques should be examined to identify the most appropriate techniques for the chosen strategies which support the overall business continuity aims and objectives.

10.3.3 Technology

ICT technology plans should be implemented based on the chosen IRBC strategy. The implementation depends on one or more of the following implementations and arrangements:

a) hot standby, where ICT infrastructure plan and implementation enable replication across two geographically dispersed sites;

b) warm standby, where the plan and implementation enable that recovery takes place at a secondary site where ICT infrastructure is partially prepared;

c) cold standby, where the plan and implementation enable that infrastructure is built or configured from scratch at an alternative location;

d) ship-in arrangements, where the plan and implementation cover which external service providers provide hardware; and

e) composite arrangement of the preceding strategies, where the plan and implementation enable a "pick-and-mix" approach of d).

For more information about virtual environments, see ISO/IEC 21878.

10.3.4 Data

The implementation and plan arrangements for the availability of identified data should be aligned with the IRBC strategies that can include:

a) additional storage for data in a format that ensures its availability aligned with the strategies identified within the IRBC; and

b) definition of alternative locations for data storage, which can be physical or virtual, provided the security and confidentiality of the data are maintained. Thus, appropriate access procedures should be in place and, if arrangements are made through third parties for the storage of that information, the information owners should satisfy themselves that appropriate controls are in place.

For more information about virtual environments, see ISO/IEC 21878.

10.3.5 Response and recovery procedures

IRBC procedures should be documented clearly and in sufficient detail to enable competent staff to execute them.

NOTE Some of these procedures can differ from the daily operation.

IRBC procedures can be dependent on the situation that unfolds. In practice, it is possible that such procedures should be adapted in light of the disruption (e.g. the degree of loss or damage), the organization's operational priorities or the stakeholders demands.

10.3.6 People

It is essential that the organization makes available the necessary human resources to perform the critical activities and to help in the operation of the IRBC.

Staff should be trained to allow personnel performing other duties in time of IRBC activation.

10.4 Temporary work around plans

Critical business processes should be the least impacted in case of ICT disruption. During the period necessary to rebuild the necessary ICT infrastructure, organizations should allow the activation of “workarounds”, which are a temporary fix or other way to perform the business activity or restore the ICT service failure to a usable level, without correcting the root cause. A workaround reduces the impact of an incident or problem for which a solution/resolution is not yet ready. This can be manual, semi-manual or fully automated services activated internally or eventually with external partners. The efficiency can be lower than for the normal conditions.

Disrupted activity owners should follow their workaround procedures. For details about workaround strategies, refer to ISO/TS 22331.

10.5 External contacts and procedures

The organization should ensure that critical suppliers are able to support the IRBC service capabilities required by the organization.

This includes having documented and tested business continuity and IRBC plans with the capacity to support concurrent activations of incident or recovery plans by customers.

The organization should establish a process to evaluate the capacity and capability of the suppliers before engaging their services, as well as regularly monitoring and reviewing the ability of the suppliers after the engagement.

Conformity to requirements or good practices in relevant standards is a useful means of determining the capability of supplier.

11 Testing, exercise, and auditing

11.1 Performance criteria

Performance criteria for IRBC can be qualitative or quantitative.

Qualitative criteria are subjective when used to determine the performance of IRBC but usually require less resources in the measurement process (which can be appropriate for a small or medium size organization subject to resource constraints). It can include determining the efficiency of the processes used in planning, preparing, and executing the activities of IRBC and can be measured through:

a) a survey using a structured or unstructured questionnaire;

b) feedback from participants and stakeholders;

c) conducting feedback workshops and other focused group meetings.

More details on metrics and measurements in the field of information security can be found in ISO/IEC 27004.

11.2 Testing dependencies

11.2.1 Test and exercise

The organization should exercise not only the recovery of the ICT service, but also its protection and resilience elements in order to determine whether:

a) the service can be protected, maintained and/or recovered regardless of the incident severity;

b) the IRBC management arrangements can minimize the impact on the business;

c) the procedures for return to business as usual are valid.

11.2.2 Test and exercise program

In most instances, the whole set of IRBC elements and processes, including ICT recovery, cannot be proven in one test and exercise.

A progressive training programme can therefore be appropriate towards building a full simulation of a real incident.

The programme should include different levels of exercise from familiarization to computer room resilience and should consider all aspects of the end-to-end ICT service delivery.

There are risks associated with tests and exercises and such activities should not expose the organization to an unacceptable level of risk.

The exercise programme should define how risks identified_during individual exercises are addressed or will be addressed in future.

Top management selected on the programme should be obtained and a clear explanation of the associated risks documented.

The test and exercise programme objectives should be fully aligned to the wider business continuity management scope and objectives, and complementary to the organization's broader exercise programme.

Each test and exercise should have both business objectives (even where there is no direct business involvement) and defined technical objectives to test or validate a specific element of the IRBC strategy.

Exercising individual elements in isolation at the component level is complementary to full systems exercising and should be maintained as part of an ongoing test and exercise programme.

The test and exercise programme should define the frequency, scope and format of each exercise. The following are high-level examples of exercise scopes:

a) data recovery: recovery of a single file or database following corruption;

b) recovery of a single server (including a full rebuild);

c) recovery of an application (this can consist of several servers, sub applications and infrastructure);

d) failover of services hosted on a high availability platform;

e) data recovery from tape (recovery of single files or a series of files from offsite tape storage);

f) network testing;

g) communications infrastructure failover tests.

Exercises should be progressive to include an increasing test of dependencies, inter-relationships and should be relevant for end-user communities.

11.2.3 Scope of exercises

Exercises should be carried out to:

a) build confidence throughout the organization that the resilience and recovery strategy can meet the business requirements;

b) demonstrate that the critical ICT services can be maintained and recovered within agreed service levels or recovery objectives regardless of the incident;

c) demonstrate that the critical ICT services can be restored to pre-test state in the event of an incident at the recovery location;

d) provide the opportunity for staff to familiarize themselves with the recovery process;

e) train staff and ensure they have adequate knowledge of IRBC plans and procedures;

f) check that IRBC remains synchronized with ICT infrastructure and general infrastructure;

g) identify any improvements that are required to the IRBC strategy, architecture or recovery processes;

h) provide evidence for audit purposes and demonstrate the organization's ICT service competence.

Exercises should apply to the entire ICT environment identified within the IRBC scope and all the components that deliver the end-to-end service from the computer room through to the user desktop or any other service delivery channel.

11.2.4 Planning an exercise

An exercise should be carefully planned to minimize the risk of an incident undermining the service capability.

This risk management should be appropriate to the level of exercise being undertaken (i.e. the elements of service recovery). This can include:

a) ensuring that all data are backed up immediately prior to the exercise;

b) conducting exercises in isolated environments;

c) scheduling exercises “out of hours” or during quiet times in the business cycle, with the knowledge of the end users.

Exercises should be realistic, carefully planned and agreed with stakeholders, to ensure minimum risk of disruption to business processes. They should not, however, be carried out during incidents.

The scale and complexity of exercises should be appropriate to the organization's recovery objectives.

Each exercise should have a “term of reference”, agreed and signed off in advance by the exercise sponsor, which can include the following:

d) description;

e) objectives;

f) scope;

g) assumptions;

h) constraints;

i) risks;

j) success criteria;

k) resources;

l) roles and responsibilities;

m) high-level timeline/schedule;

n) exercise data capture;

o) issues log;

p) exercise/incident logging;

q) debriefing;

r) post-exercise actions (follow up and reporting).

Planning an exercise should enable the organization to achieve the success criteria identified.

11.2.5 Alert based and different recovery stages

The organization should exercise all elements of the ICT service recovery as appropriate to its size and, complexity and business continuity management scope.

The exercising should not focus solely on service recovery and resumption, but should include the reliability of the resilience capability, system monitoring and alert management.

The organization should perform exercises at component level through to the full location-based system testing stage in order to achieve high levels of confidence and resilience.

Figure 3 shows the different steps to be considered for a participant in the organization, who is involved in the BCM exercise.

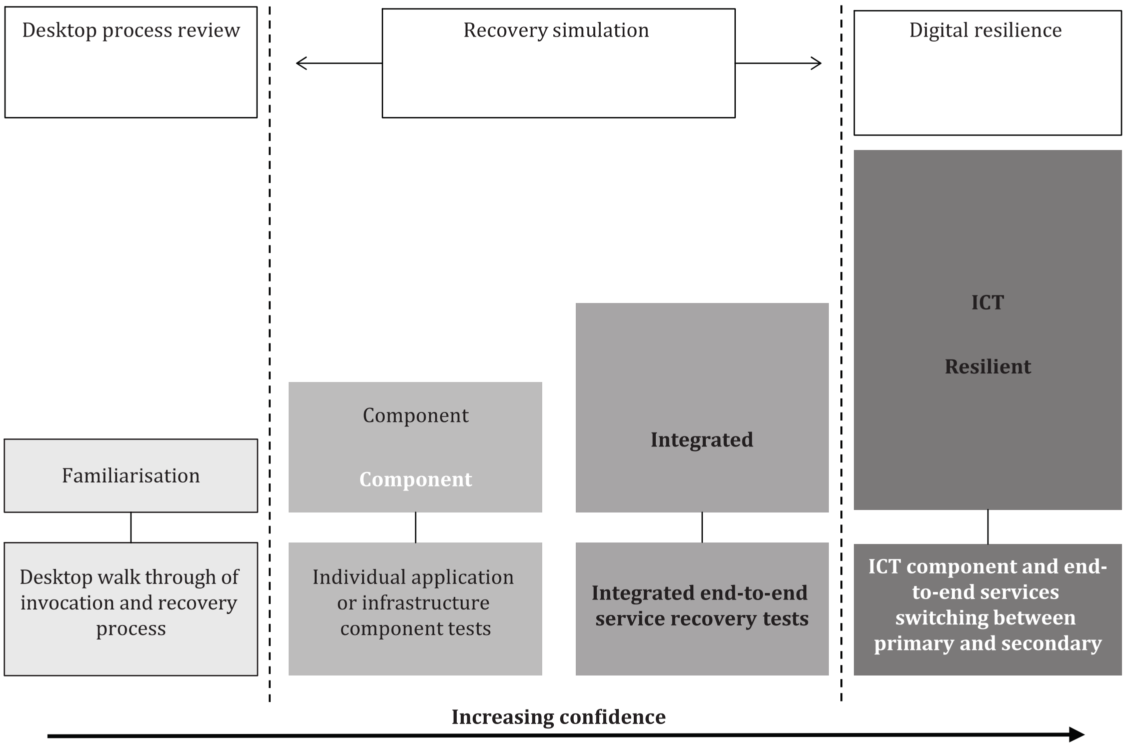
Desktop process review
Recovery simulation
Digital resilience
ICT
Resilient
Integrated
Component
Component
Familiarisation
Desktop walk through of invocation and recovery process
Individual application or infrastructure component tests
Integrated end-to-end service recovery tests
ICT component and end-to-end services switching between primary and secondary
Increasing confidence

Figure 3 — A progressive test and exercise program

The following elements should be considered in the exercise:

a) all devices related to physical security inside a computer room such as, fire and water leak detection systems; evacuation process; heating, ventilation and air conditioning; environmental monitoring; and alert protocols and electrical services;

b) infrastructure, including the overall resilience of the network connectivity; network diversity; and network security, including anti-virus protection and intrusion prevention and detection;

c) hardware, including servers, telecommunications equipment, storage arrays and removable media;

d) software;

e) data;

f) services;

g) processes;

h) people;

i) role and response of suppliers.

11.2.6 Managing an exercise

A clear exercise control structure should be developed with roles and responsibilities allocated to appropriate individuals. The exercise control structure can include:

a) exercise controller [participant(s) with overall control of the test and exercise]:

b) exercise communications;

c) confirmation that there are enough staff available to undertake the exercise safely;

d) sufficient observers and or facilitators to capture the exercise proceedings and maintain an issues log;

e) key exercise milestones;

f) end of exercise protocols;

g) emergency stop exercise protocols.

The exercise should be run through the exercise control to ensure that:

h) objectives and key milestones are met;

i) all exercise material and activities have appropriate levels of confidentiality;

j) any ongoing risks are monitored and mitigated;

k) any visitors/observers are authorized;

l) exercise proceedings are captured in a consistent manner;

m) all participants are debriefed, and feedback collated.

11.3 Learning from tests

At the end of an exercise its findings should be reviewed and followed up promptly. This should include:

a) gathering the results and findings;

b) analysing the results and findings against the exercise objectives and success criteria;

c) identifying any gaps;

d) assigning action points with defined timelines;

e) creating an exercise report for formal consideration by the exercise sponsor;

f) consolidating and following up exercise report actions.

11.4 Auditing the IRBC

The IRBC internal audit plan should define and document the audit criteria, scope, method and frequency. IRBC internal audits should be conducted annually.

The audit plan should ensure that qualified auditors are appointed for the audit (where required). Selection of auditors and conduct of the audit should ensure objectivity and impartiality of the audit process. For example, auditors should attend relevant auditor training so that they acquire the necessary skills and knowledge to conduct the audit.

A remediation schedule or programme should be established to ensure that deficiencies identified in IRBC internal audits are rectified.

The audit plan should also encompass external parties. For example, outsourcing vendors should be audited for their capability to support the organization's IRBC strategies and plans during daily operation and response to and recovery from disaster.

An internal audit should be conducted when there are significant changes to the critical ICT services, business continuity requirements (as relevant to IRBC scope), or IRBC requirements.

The results of IRBC audit should be recorded and reported. The management should review the results of IRBC audits and the status of the follow-up corrective action.

11.5 Control of documented information

Controls should be established over IRBC records in order to:

a) ensure that they remain legible, readily identifiable and retrievable;

b) provide for their storage, protection and retrieval;

Controls should be established over IRBC documentation to ensure that:

c) documents are approved for adequacy prior to issue;

d) documents are reviewed and updated as necessary and re-approved;

e) changes and the current revision status of documents are identified;

f) relevant versions of applicable documents are available at points of use;

g) documents of external origin are identified, and their distribution controlled;

h) the unintended use of obsolete documents is prevented, and such documents are suitably identified if they are retained for any purpose.

12 Final MBCO

Depending on the situation, it is possible that IRBC is unable to initially meet the MBCO set by the business using ICT. In such a case, the IRBC is not fulfilling the continuity requirements set by the business. If there is a gap between the requirement and the capability, then there are only two options:

- close the gap by enhancing the capability;
- accept the gap and include it in the risk register.

When closing the gap then depending on the cost of improving IRBC, an organization should review its business requirements as well as the possibilities to improve the IRBC so that in future, the MBCO for ICT can be improved and come closer to achieving the business continuity requirements. This IRBC review and improvement should be done through the BCM by the appropriate management (see Clause 13).

NOTE For further information, see Annex A.

13 Top management responsibilities regarding evaluating the IRBC

13.1 General

To be effective, an IRBC programme should be a fully integrated process within the organization's management activities, driven from the top of the organization and endorsed by top management.

A number of professional IRBC practitioners and staff from other management disciplines and departments can be required to support and manage the IRBC program.

The quantity of resources required to support such a programme is dependent upon the size and complexity of the organization.

13.2 Management responsibilities

The IRBC strategy options which are selected should be presented to top management. The decision should be based on risk appetite and cost.

Top management should be advised if IRBC strategy options selected are unable to meet the business continuity requirements, in which case they can be informed of current capability.

Top management should select the IRBC strategies from the options presented to them and approve and sign off the documented options to confirm that the actions have been properly undertaken and that they support the overall business continuity requirements.

The selected IRBC strategy options should:

a) cater for likely risks and effects of disruption;

b) integrate with the organization's chosen business continuity strategies;

c) be appropriate to meet the organization's overall objectives within its risk appetite;

d) be reviewed by the appropriate management.

Annex A
(informative)

Comparing RTO and RPO to business objectives for ICT recovery

A range of potential risk management techniques exist which can assist in the assessment of IRBC and in developing an appropriate framework for the continued development and enhancement of ICT resilience.

IEC 31010:2019 is intended to reflect current good practices in the selection and utilization of risk assessment techniques. Reference should be made to this document to determine which is the most appropriate technique to be used within an organization. The assessment of failure scenarios is one technique which can be beneficial in enhancing the efficacy of IRBC. This annex and Annex B provide additional information on how it can be implemented.

Unknown risk issues can emerge between assessments as a result of changes in and external to the organization environment, which can hamper business continuity and resilience.

The purpose of failure scenario assessment is to identify suitable event indicators, ensure that IRBC plans are capable of detecting such emerging risk issues and able to prepare the organization to ensure appropriate actions can be taken before failure occurs.

A number of specific methodologies are available for such a purpose, including failure mode effect analysis (FMEA) and component failure impact analysis (CFIA).

If this methodology is selected, it can be deployed as follow:

FMEA is a process for identifying and analysing the potential failure modes of a system for the classification by severity or determination of the failures affect upon the system. In the context of this document, FMEA can be applied to determine the critical event indicators that should be monitored in order to detect potentially severe failure modes in an organization ICT system. The process, based on the FMEA approach, can be applied to each critical component of the ICT service.

For each critical component, the following can be done:

a) identify the potential failure mode;

b) determine the potential impact to the ICT service i.e. the severity of each failure mode, and what consequences would result;

c) identify the frequency of occurrence of a failure mode that the organization has already experienced, as well as the ease of monitoring and detection of the failure mode;

d) identify the indicators that provide a signal or information that the component is failing;

e) identify the direct and indirect events that are related, and change the state of each indicator;

f) identify the existing controls that prevent the critical components from failing, or can detect such failures occurring;

g) identify related data sources, and possible methods of monitoring to detect changes to the value of the indicator;

h) categorize the event indicators by the availability of monitoring methods and ease of monitoring;

i) identify if suitable risk reduction or elimination controls can be applied to prevent its occurrence.

Annex B
(informative)

Risk reporting for FMEA

The failure mode effect analysis (FMEA) output that includes a list of potential failure modes and effects, and related events, can be used to determine event indicators that should be monitored.

The failures modes identified through the FMEA process can be prioritized according to the assessed severity, their frequency of occurrence, and the ease of monitoring and detection.

An FMEA also documents current knowledge and actions about the risks of failures, for use in continuous improvement.

If FMEA is used during the design stage with an aim to avoid future failures, it can be used for process control, before and during ongoing operation of the process. Ideally, FMEA begins during the earliest conceptual stages of design and continues throughout the lifecycle.

Bibliography

[1] ISO/IEC 20000-1:2018, *Information technology — Service management — Part 1: Service management system requirements*

[2] ISO/IEC 21878:2018, *Information technology — Security techniques — Security guidelines for design and implementation of virtualized servers*

[3] ISO 22313:2020, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*

[4] ISO/TS 22317:2021, *Security and resilience — Business continuity management systems — Guidelines for business impact analysis*

[5] ISO/TS 22318:2021, *Security and resilience — Business continuity management systems — Guidelines for supply chain continuity management*

[6] ISO 22320:2018, *Security and resilience — Emergency management — Guidelines for incident management*

[7] ISO/TS 22331:2018, *Security and resilience — Business continuity management systems — Guidelines for business continuity strategy*

[8] ISO/TS 22332:2021, *Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures*

[9] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

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

[11] ISO/IEC 27004:2016, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[12] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

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

[14] ISO/IEC 27035-2:2023, *Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*

[15] ISO/IEC 27035-3:2020, *Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations*

[16] ISO/IEC 27036-1:2021, *Cybersecurity — Supplier relationships — Part 1: Overview and concepts*

[17] ISO 31000:2018, *Risk management — Guidelines*

[18] IEC 31010:2019, *Risk management — Risk assessment techniques*

[19] CEN/TS 17091:2018, *Crisis Management – Guidance for developing a strategic capability*

ICS 35.030

Price based on 33 pages

iso.org