INTERNATIONAL STANDARD

ISO/IEC 27031

First edition
2011-03-01

Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

Technologies de l'information — Techniques de sécurité — Lignes directrices pour mise en état des technologies de la communication et de l'information pour continuité des affaires

Reference number
ISO/IEC 27031:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27031 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

Over the years, information and communication technology (ICT) has become an integral part of many of the activities which are elements of the critical infrastructures in all organizational sectors, whether public, private or voluntary. The proliferation of the Internet and other electronic networking services, and today's capabilities of systems and applications, has also meant that organizations have become ever more reliant on reliable, safe and secure ICT infrastructures.

Meanwhile, the need for business continuity management (BCM), including incident preparedness, disaster recovery planning, and emergency response and management, has been recognized and supported with specific domains of knowledge, expertise, and standards developed and promulgated in recent years, including the BCM International Standard developed by ISO/TC 223.

NOTE ISO/TC 223 is in the process of developing a relevant business continuity management International Standard (ISO 22301).

Failures of ICT services, including the occurrence of security issues such as systems intrusion and malware infections, will impact the continuity of business operations. Thus managing ICT and related continuity and other security aspects form a key part of business continuity requirements. Furthermore, in the majority of cases, the critical business functions 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.

ICT readiness is an essential component for many organizations in the implementation of business continuity management and information security management. As part of the implementation and operation of an information security management system (ISMS) specified in ISO/IEC 27001 and business continuity management system (BCMS) respectively, it is critical to develop and implement a 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 in times of 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.

In order for an organization to achieve ICT Readiness for Business Continuity (IRBC), it needs to put in place a systematic process to prevent, predict and manage ICT disruption and incidents which have the potential to disrupt ICT services. This can be best achieved by applying the Plan-Do-Check-Act (PDCA) cyclical steps as part of a management system in ICT IRBC. In this way IRBC supports BCM by ensuring that the ICT services are as resilient as appropriate and can be recovered to pre-determined levels within timescales required and agreed by the organization.

Table 1 — Plan-Do-Check-Act cycle in IRBC

Plan	Establish IRBC policy, objectives, targets, processes and procedures relevant to managing risk and improving ICT readiness to deliver results in accordance with an organization's overall business continuity policies and objectives.
Do	Implement and operate the IRBC policy, controls, processes and procedures.
Check	Assess and, where applicable, measure process performance against IRBC policy, objectives and practical experience, and report the results to management for review.
Act	Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the IRBC.

If an organization is using ISO/IEC 27001 to establish an ISMS, and/or using relevant standards to establish a BCMS, the establishment of IRBC should preferably take into consideration existing or intended processes linked to these standards. This linkage can support the establishment of IRBC and also avoid any dual processes for the organization. Figure 1 summarizes the interaction of IRBC and BCMS.

In the planning and implementation of IRBC, an organization can refer to ISO/IEC 24762:2008 in its planning and delivery of ICT disaster recovery services, regardless of whether or not those services are provided by an outsourced vendor, or internally to the organization.

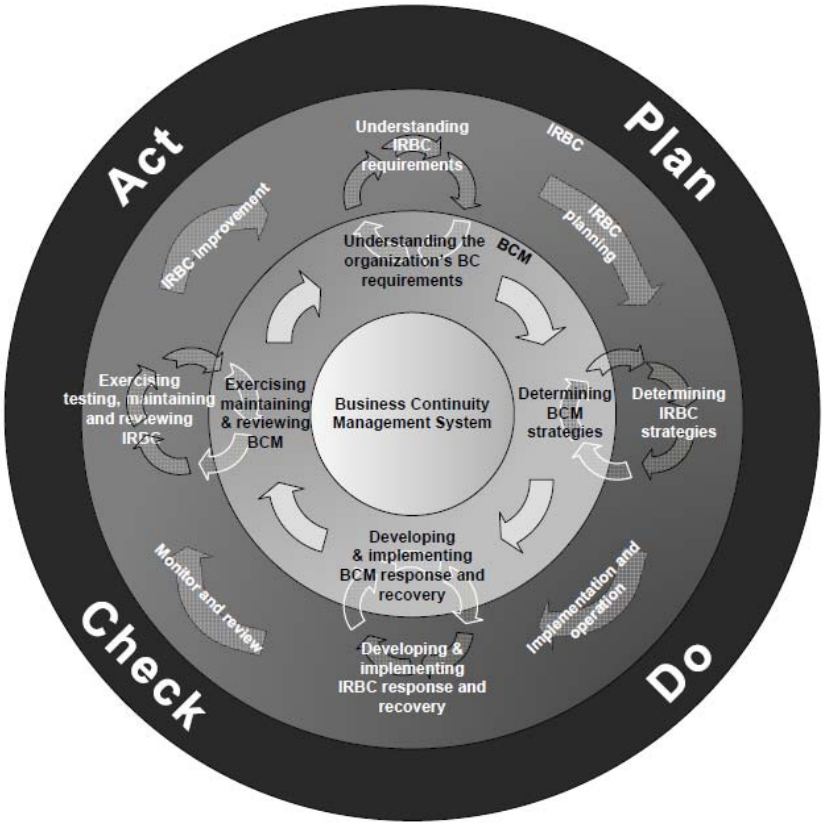

Figure 1 — Integration of IRBC and BCMS

Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

1 Scope

This International Standard describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. It applies to any organization (private, governmental, and non-governmental, irrespective of size) developing its ICT readiness for business continuity (IRBC) program, and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions. It also enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner.

The scope of this International Standard encompasses all events and incidents (including security related) that could have an impact on ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.

2 Normative references

The following referenced documents are indispensable for the application 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 TR 18044:2004 [1)], *Information technology — Security techniques — Information security incident management*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

1) ISO/IEC TR 18044:2004 is to be revised and renumbered as ISO/IEC 27035.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC TR 18044, ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and the following apply.

3.1
alternate site
alternate operating location selected to be used by an organization when normal business operations cannot be carried out using the normal location after a disruption has occurred

3.2
business continuity management
BCM
holistic management process that identifies potential threats to an organization and the impacts to business operations whose threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

3.3
business continuity plan
BCP
documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption

NOTE Typically this covers resources, services and activities required to ensure the continuity of critical business functions.

3.4
business impact analysis
BIA
process of analysing operational functions and the effect that a disruption might have upon them

3.5
critical
qualitative description used to emphasize the importance of a resource, process or function that must be available and operational constantly or available and operational at the earliest possible time after an incident, emergency or disaster has occurred

3.6
disruption
incident, whether anticipated (e.g. hurricane) or unanticipated (e.g. power failure/outage, earthquake, or attack on ICT systems/infrastructure) which disrupts the normal course of operations at an organization location

3.7
ICT disaster recovery
ability of the ICT elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disruption

3.8
ICT disaster recovery plan
ICT DRP
clearly defined and documented plan which recovers ICT capabilities when a disruption occurs

NOTE It is called ICT continuity plan in some organizations.

3.9
failure mode
manner by which a failure is observed

NOTE It generally describes the way the failure occurs and its impact on the operation of the system.

3.10
ICT readiness for business continuity
IRBC
capability of an organization to support its business operations by prevention, detection and response to disruption and recovery of ICT services

3.11
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

3.12
recovery point objective
RPO
point in time to which data must be recovered after a disruption has occurred

3.13
recovery time objective
RTO
period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions must be recovered after a disruption has occurred

3.14
resilience
ability of an organization to resist being affected by disruptions

3.15
trigger
event that causes the system to initiate a response

NOTE Also known as triggering event.

3.16
vital record
electronic or paper record that is essential for preserving, continuing or reconstructing the operations of an organization and protecting the rights of an organization, its employees, its customers and its stakeholders

4 Abbreviations

IRBC ICT Readiness for Business Continuity

ISMS Information Security Management System

5 Overview

5.1 The role of IRBC in Business Continuity Management

Business Continuity Management (BCM) is a holistic management process that identifies potential impacts threatening an organisation's continuity of business activities and provides a framework for building resilience and capability for an effective response that safeguards the interests of the organization from disruptions.

As part of the BCM process, IRBC refers to a management system which complements and supports an organization's BCM and/or ISMS program, to improve the readiness of the organization to:

a) respond to the constantly changing risk environment;

b) ensure continuation of critical business operations supported by the related ICT services;

c) be ready to respond 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/disasters and failures.

Figure 2 illustrates the desired ICT outcome to support the Business Continuity Management activities.

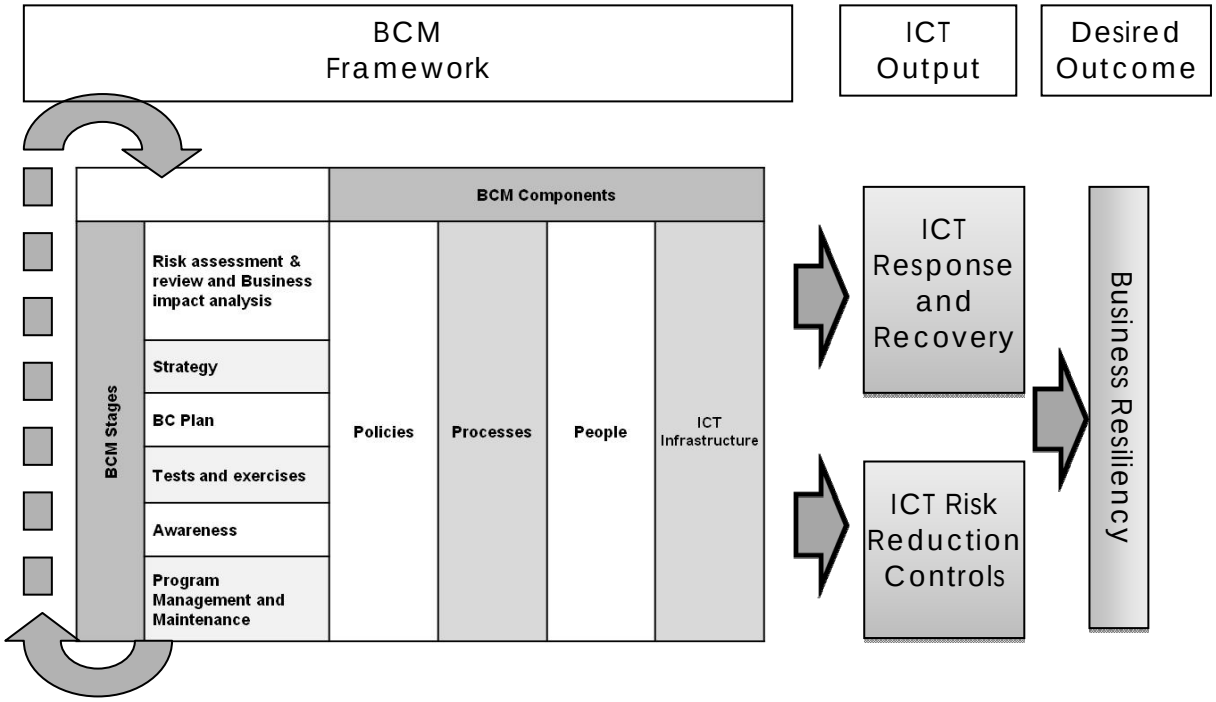

Figure 2 — Business Continuity Framework and its related ICT output and desired outcome

The BCM International Standard developed by ISO/TC 223 summarizes the BCM approach to preventing, reacting and recovering from incidents. Activities involved in BCM include incident preparedness, operational continuity management, disaster recovery planning (DRP) and risk mitigation which focus on increasing the resilience of the organization and by preparing it to react effectively to incidents and recover within pre-determined timescales.

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

As shown in Figure 3, such readiness activities aim to:

a) improve the incident detection capabilities;

b) prevent a sudden or drastic failure;

c) enable an acceptable degradation of operational status should the failure be unstoppable;

d) further shorten recovery time; and

e) minimize impact upon eventual occurrence of the incident.

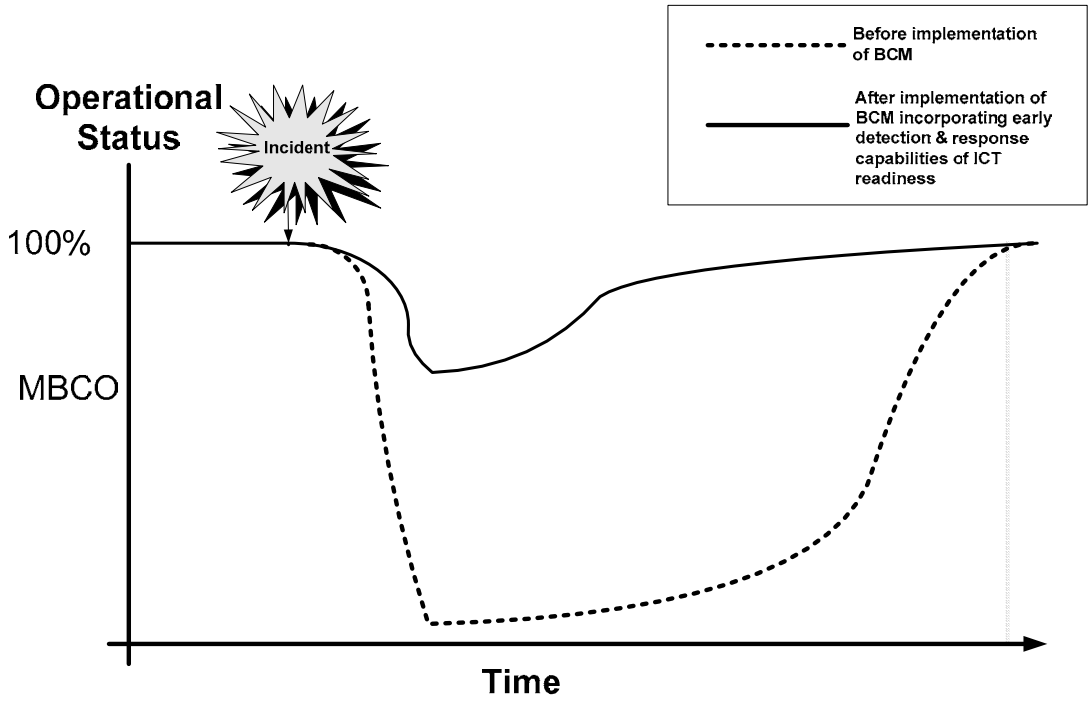

Figure 3 — Concept of ICT Readiness for Business Continuity

5.2 The Principles of IRBC

IRBC is based around the following key principles:

a) Incident Prevention - Protecting ICT services from threats, such as environmental and hardware failures, operational errors, malicious attack, and natural disasters, is critical to maintaining the desired levels of systems availability for an organization;

b) Incident Detection - Detecting incidents at the earliest opportunity will minimize the impact to services, reduce the recovery effort, and preserve the quality of service;

c) Response - Responding to an incident in the most appropriate manner will lead to a more efficient recovery and minimize any downtime. Reacting poorly can result in a minor incident escalating into something more serious;

d) Recovery - Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data. Understanding the recovery priorities allows the most critical services to be reinstated first. Services of a less critical nature may be reinstated at a later time or, in some circumstances, not at all; and

e) Improvement – Lessons learned from small and large incidents should be documented, analysed and reviewed. Understanding these lessons will allow the organization to better prepare, control and avoid incidents and disruption.

Figure 4 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.

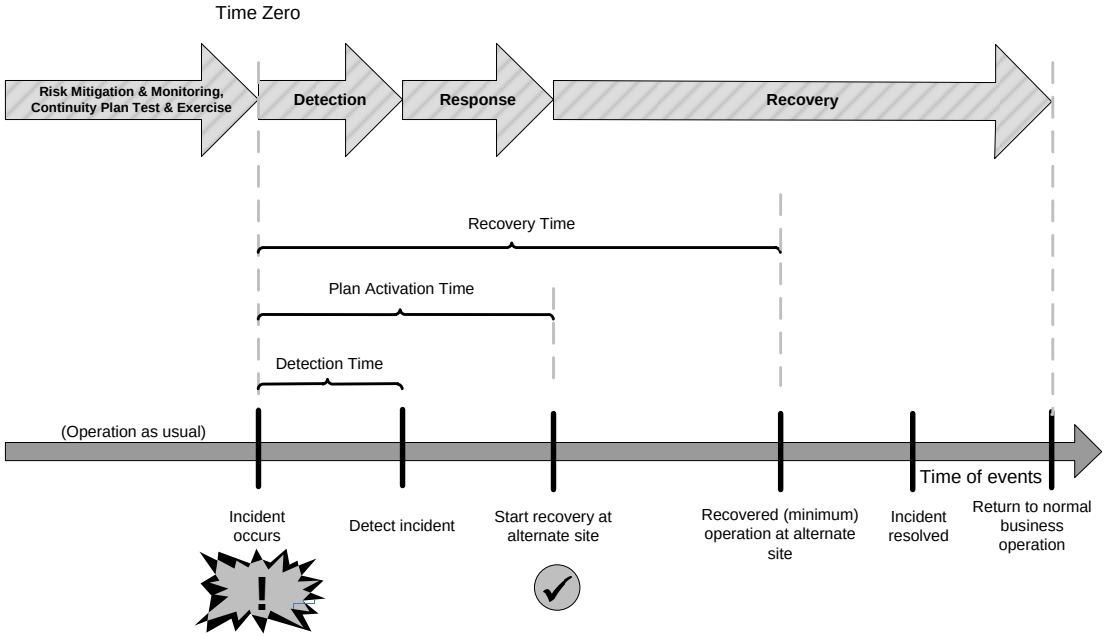

Figure 4 — The principles of IRBC on a typical ICT disaster recovery timeline

NOTE Recovery stage includes activities in the timely recovery/resumption of services, sustainable ICT DR operations, and the restoration & return to normal operation. For details refer to Figure A.1 in Annex A.

5.3 The Elements of IRBC

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;

c) Technology:

   1) hardware (including racks, servers, storage arrays, tape devices and fixtures);

   2) network (including data connectivity and voice services), switches and routers; and

   3) software, including operating system and application software, links or interfaces between applications and batch processing routines;

d) Data: application data, voice data and other types of data;

e) Processes: including supporting documentation to describe the configuration of ICT resources and enable the effective operation, recovery and maintenance of ICT services; and

f) 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.

5.4 Outcomes and benefits of IRBC

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

a) understands the risks to continuity of ICT services and their vulnerabilities;

b) identifies the potential impacts of disruption to ICT services;

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 upon 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 IT 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 its 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 “is our ICT capable of responding” rather than “is our ICT secure”.

5.5 Establishing 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 BC 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 will support IRBC.

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

Figure 5 presents graphically the activities in the different stages of IRBC.

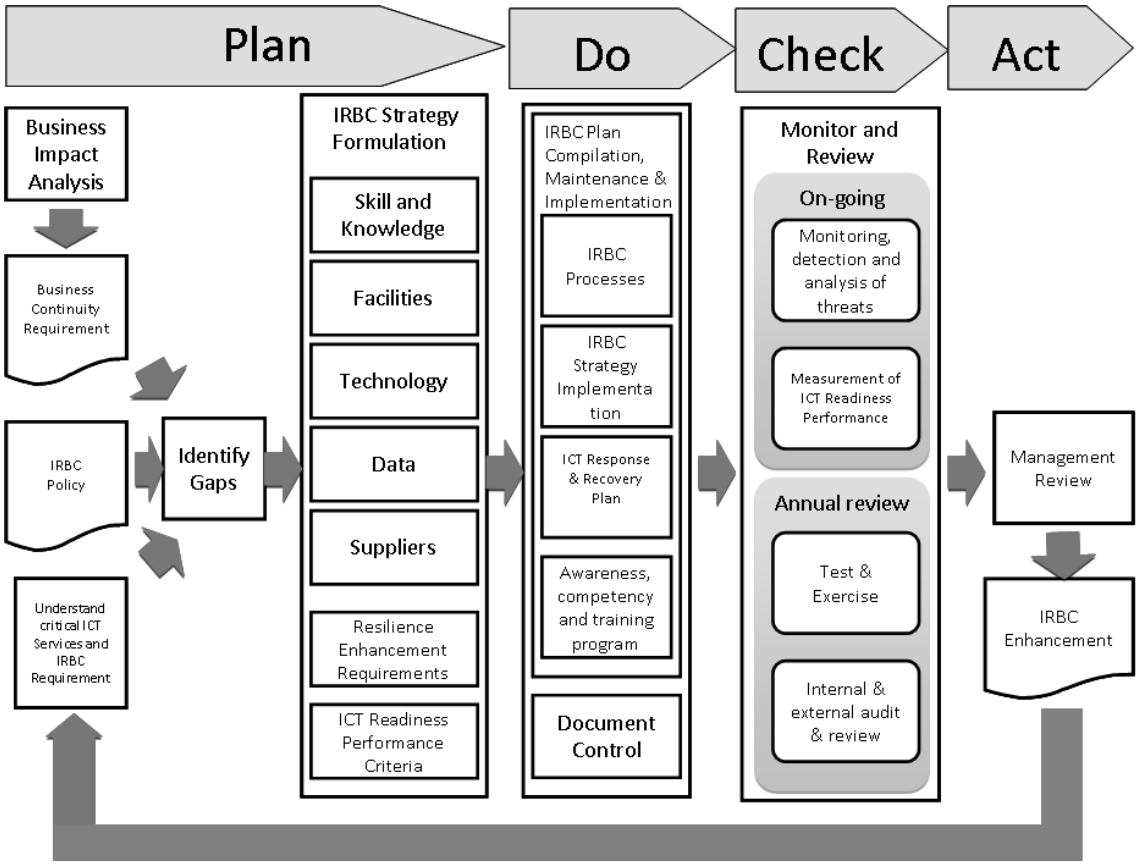

Figure 5 — Stages in IRBC

5.6 Using Plan Do Check Act to establish IRBC

IRBC involves the organization in establishing processes to develop and enhance its key IRBC elements (see 5.2) to improve their capability to respond to any type of disruption, including changing risk situations through the use of the Plan-Do-Check-Act (PDCA) approach. Figure 5 presents graphically the activities in the different stages of IRBC.

5.7 Management Responsibility

5.7.1 Management leadership and commitment

To be effective an IRBC program should be a process fully integrated with the organization's management activities, driven from the top of the organization, endorsed and promoted by top management. A number of professional IRBC practitioners and staff from other management disciplines and departments may be required to support and manage the IRBC program. The quantity of resources required to support such a program will be dependent upon the size and complexity of the organization.

5.7.2 IRBC policy

The organization should have a documented IRBC policy. Initially, this may be at a high level with further refinement and enhancement as the entire IRBC process matures. The policy should be regularly reviewed and updated in line with organization needs and should be consistent with the wider organizational BCM objectives.

The IRBC policy should provide the organization with documented principles to which it will aspire and against which its IRBC effectiveness can be measured. It should:

a) Establish and demonstrate commitment of top management to an IRBC program;

b) Include or make reference to the organization's IRBC objectives;

c) Define the scope of IRBC including limitations and exclusions;

d) Be approved and signed off by top management;

e) Be communicated to appropriate internal and external stakeholders;

f) Identify and provide relevant authorities for the availability of resources such as budget; personnel necessary to perform activities in line with the IRBC policy; and

g) Be reviewed at planned intervals and when significant changes, such as environmental changes, change of an organization's business and structure, occur.

6 IRBC Planning

6.1 General

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, legal, statutory and regulatory requirements relating to the defined scope and the achievement of the organization's business continuity aims and objectives; and

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

6.2 Resources

6.2.1 General

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

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; and

b) appoint one or more competent persons, who, irrespective of other responsibilities, should implement and maintain the IRBC management system as described in this International Standard.

6.2.2 Competency of IRBC staff

The organization should ensure that all personnel who are assigned IRBC responsibilities are competent to perform the required tasks. Refer to 7.2.1 for details.

6.3 Defining requirements

6.3.1 General

As part of its BCM program, the organization will have categorized its activities according to their priority for continuity (as determined by a Business Impact Analysis) and defined the minimum level at which each critical activity needs to be performed upon resumption. Top management should agree to the organization's business continuity requirements and these requirements will result in Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the Minimum Business Continuity Objective (MBCO) per product, service or activity. These RTOs start from the point at which the disruption occurs and run until the product, service or activity.

6.3.2 Understanding critical ICT services

There may be a number of ICT services that are considered to be critical and required to enable recovery to take place. Each of these critical ICT services should have its own documented Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the Minimum Business Continuity Objective (MBCO) of the ICT service. (These may include aspects of ICT service delivery, such as help desk.) The RTO of the critical ICT services will invariably be less than the business continuity RTO. (Refer to Annex A for detailed elaboration of RTO and RPO.)

The organization should identify and document its critical ICT services to include brief descriptions and names that are meaningful to the organization at service user level. This will ensure common understanding between business and ICT staff as there may be the use of different names for the same ICT service. Each critical ICT service listed should identify the organization's product or service that it supports and top management should agree to the ICT services and their associated IRBC requirements.

For each critical ICT service identified and agreed, 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 (e.g. existence of single point of failure) should be reviewed from a prevention perspective to assess risks of service interruption or degradation (which can be taken as part of the overall BCM risk assessment exercise). Opportunities should also be sought to improve ICT service resilience and thereby lower the likelihood and/or impact of service disruption. It may also highlight opportunities to enable early detection and reaction to ICT service disruption. The organization can decide if there is a business case to invest in identified opportunities to improve service resilience. This service risk assessment (which may form part of the organization's overall risk management framework) may also advise the business case for enhancing ICT service recovery capability.

6.3.3 Identifying gaps between ICT Readiness capabilities and business continuity requirements

For each critical ICT service the current ICT Readiness arrangements - such as prevention, monitoring, detection, response and recovery - should be compared with business continuity requirements and any gaps should be documented.

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

a) staff, including numbers, skills and knowledge;

b) facilities to house ICT facilities, 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 should sign off the ICT service definitions, the documented list of critical ICT services and the risks associated with gaps identified between critical IRBC capability and business continuity requirements. This should include, where appropriate, the sign-off of identified risks. The options for addressing the gaps and risks identified should then be explored by determining IRBC strategies.

6.4 Determining IRBC Strategy Options

6.4.1 General

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

A full 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 may 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 different markets. In addition, the strategy should take into account internal constraints and factors, such as:

a) budget;

b) resource availability;

c) potential costs and benefits;

d) technological constraints;

e) the organization's risk appetite;

f) the organization's existing IRBC strategy; and

g) regulatory obligations.

6.4.2 IRBC Strategy Options

The organization should consider a range of options for the incident readiness of its critical ICT services. The options should consider increasing protection and resilience, as well as provision for recovery and restoration from an unplanned disruption, and may include internal arrangement; services delivered to the organization; and service 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 may be achieved in many ways, and should address the elements of IRBC as described in 5.3.

6.4.2.1 Skills and Knowledge

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

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

b) multi-skill training of ICT staff and contractors to enhance skill redundancy;

c) separation of core skills to reduce the concentration of risk (this might 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.

6.4.2.2 Facilities

According to identified risks, the organization should devise strategies for reducing the impact of the unavailability of the normal ICT facilities. This may 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 may be available. Different types of incident or threat may require the implementation of multiple strategies (a pick and mix approach) which will be driven in part by the organization's size, breadth of activities, locations, technologies and budget etc.

In considering the use of alternative premises the following should be taken into consideration:

a) site security;

b) staff access;

c) proximity to existing facilities; and

d) availability.

6.4.2.3 Technology

The ICT services upon which critical business activities depend should be available in advance of the resumption of their dependent critical business activities. Thus solutions are required which ensure the availability of applications within specific timeframes, 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 need 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 critical activities identified by the BCM program;

b) location and distance between technology sites;

c) number of technology sites;

d) remote access to systems;

e) cooling requirements;

f) power requirements;

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

h) telecoms connectivity and redundant routing;

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

j) level of automation required;

k) technology obsolescence; and

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

6.4.2.4 Data

Additionally, critical business activities may depend on the provision of up-to-date or near-up-to-date data. Data continuity solutions should be designed to meet the Recovery Point Objectives (RPO) of each critical business activity of the organization as they relate to the critical business activities.

The selected IRBC options should ensure the ongoing confidentiality, integrity and availability of critical 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) RPO requirements;

b) how data are securely 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 may include information feeds to and from third parties.

It should be remembered that the nature, currency and value of data will vary enormously within an organization.

6.4.2.5 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 / facilities.

6.4.2.6 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 timeframes. Such dependencies may 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 may 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.

6.5 Sign Off

IRBC strategy options selected should be presented to top management, with recommendations for a decision 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 may 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 options 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; and

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

6.6 Enhancing IRBC Capability

6.6.1 Enhancing Resilience

The organization should include within its high level IRBC strategy and plans reference to specific enhancements of its IRBC capabilities which are required to fulfil its identified IRBC requirements. Such enhancements may be achieved through preventive and corrective actions (refer to 9.2 and 9.3), as well as other specific processes or methodologies which are relevant responses to the organization's BIA and its risk appetite.

Information on such processes and or methodologies can be found in Annexes B and C.

6.7 ICT Readiness Performance Criteria

6.7.1 Identification of performance criteria

Within any ICT environment there are many potentially threatening events – such as hardware failures, security intrusion etc – and an organisation should be capable of monitoring the threats and understanding if the IRBC system is capable of adequately dealing with them.

The organization should therefore define performance criteria to measure the effectiveness of its ICT readiness. Such criteria can be used to determine the desired quality of the response to a disruption, both in terms of its effectiveness and efficiency.

Performance criteria for IRBC should be based on the IRBC requirements as well as overall BCM objectives in terms of incident response and continuity requirements. (Refer 8.3.1)

7 Implementation and Operation

7.1 General

IRBC strategies should only be implemented after top management 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 7.2), 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 and disaster recovery components, including the following:

a) ISO/IEC 18043 for the selection and operation of intrusion detection systems;

b) ISO/IEC 18044 for the incident response process; and

c) ISO/IEC 24762 for the disaster recovery services.

NOTE ISO/IEC 18044 is being revised and renumbered as 27035.

7.2 Implementing the Elements of the IRBC Strategies

7.2.1 Awareness, Skills and Knowledge

General awareness of the readiness of the elements of ICT services (see 5.3) - people, facilities, technology, data, processes, and suppliers, as well as their critical components - is a crucial element in ensuring the required support for the business continuity governance and management system, including ICT readiness. The organization should therefore:

a) raise, enhance and maintain awareness through an ongoing education and information program 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 IRBC objectives.

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

a) determining the necessary competencies for such personnel;

b) conducting training needs analysis on such personnel;

c) providing training;

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

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

7.2.2 Facilities

ICT recovery systems and critical data 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. For example, if available, the training or development ICT systems should be logically separated from the production systems as there may be an opportunity for these to be reconfigured in the event of a disaster to quickly bring up the production service.

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.

7.2.3 Technology

ICT technology strategies should be implemented. These may include one or more of the following implementation and arrangements:

a) hot standby, where ICT infrastructure is replicated across two sites;

b) warm standby, where recovery takes place at a secondary site where ICT infrastructure is partially prepared;

c) cold standby, where infrastructure is built or configured from scratch at an alternative location;

d) ship-in arrangements, under which external service providers provide hardware; and

e) composite arrangement of the preceding strategies: a “pick-and-mix” approach.

7.2.4 Data

The arrangements for the availability of data should be aligned with the requirements identified within the IRBC management strategies, and may include:

a) additional storage for data in a format that ensures its availability within the timescales identified in the business continuity program; and

b) alternative locations for data storage, which may 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.

7.2.5 Processes

IRBC processes should be documented clearly and in sufficient detail to enable competent staff to execute them (some of these processes may differ from the daily operation).

IRBC procedures may be dependent on the situation that unfolds and in practice may need to be adapted in light of the disruption (e.g. the degree of loss or damage), the organization's operational priorities and the stakeholders demands.

7.2.6 Suppliers

The organization should ensure that critical suppliers are able to support the IRBC service capabilities required by the organization. This includes having their own 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 continuously monitoring and reviewing the ability of the suppliers after the engagement. Compliance with requirements/good practices in relevant standards is a useful means of determining the suppliers' capability, e.g. the adoption of ISO/IEC 24762 best practices by suppliers hosting/managing the alternate processing facility and providing ICT disaster recovery services.

7.3 Incident Response

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) contain the incident; and

d) communicate with stakeholders.

The incident response should trigger an appropriate IRBC action. This response should integrate with overall BCM incident response, and may 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 may use a tiered approach and may establish different teams to focus on different functions. Within ICT, this may 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.

7.4 IRBC Plan Documents

7.4.1 General

The organization should have documentation (plans) to manage potential disruption and thereby enable continuity of ICT services and the recovery of critical activities.

The organization's ICT incident management, business continuity and technical recovery plans may be activated in rapid succession or simultaneously.

The organization may develop specific plan documents to recover or resume ICT services back to a "normal" state (recovery plans). However, it might not be possible to define what "normal" looks like until some time after the incident, so that it might not be possible to implement recovery plans immediately. The organization should therefore ensure that the continuity arrangements are capable of extended operation in support of the wider business continuity, giving time for the development of recovery ("back-to-normal") plans.

7.4.2 Content of Plan Documents

A small organization may have a single plan document that encompasses all activity to recover the ICT services of its entire operations. A very large organization may have many plan documents, each of which specifies in detail the recovery of a particular element of its ICT services.

ICT response and recovery plans should be concise and accessible to those with responsibilities defined in the plans. Plans should contain the following elements.

a) Purpose and scope

The purpose and scope of each specific plan should be defined, agreed by top management, and understood by those who will invoke the plan. Any relationship to other relevant plans or documents within the organization, particularly to BC plans, should be clearly referenced and the method of obtaining and accessing these plans described.

Each incident management and ICT response and recovery plan should set out prioritized objectives in terms of:

i) the critical ICT services to be recovered;

ii) the timescales in which they are to be recovered;

iii) the recovery levels needed for each critical ICT service activity; and

iv) the situation in which each plan can be invoked.

Plans may also contain, where appropriate, procedures and checklists that support the post incident review process.

b) Roles and responsibilities

The roles and responsibilities of the people and teams having authority (both in terms of decision-making and authority to spend) during and following an incident should be clearly documented.

c) Plan invocation

NOTE Invariably time lost during a response cannot be regained. It is almost always better to initiate an ICT response and subsequently stand it down than to miss an opportunity to contain an incident early and prevent escalation.

Organizations therefore need to use the incident management escalation and invocation protocols contained within their wider business continuity incident management plans to form the basis for managing potential ICT-related service disruptions.

The method by which an ICT response and recovery plan is invoked should be clearly documented. This process should allow for the relevant plans or parts thereof to be invoked in the shortest possible time, either in advance of a potentially disruptive event or immediately following the occurrence of an event.

The plan should include a clear and precise description of:

i) how to mobilize the assigned individual or team;

ii) immediate rendezvous points;

iii) subsequent team meeting locations and details of any alternative meeting locations (in a larger organization these meeting places may be referred to as command centres) ; and

iv) circumstances under which the organization deems an IRBC response is not necessary (e.g. minor faults and outages, perhaps to critical ICT services, but which are managed by normal helpdesk and support arrangements and agreements).

The organization should document a clear process for standing down the ICT response team once the incident is over, and returning to business as usual.

d) ICT response and recovery plan documentation owner and maintainer

Management should nominate an owner for the ICT response and recovery plan documentation, holding them accountable for regular reviewing and updating the documentation.

A system of version control should be employed, and changes formally notified to all interested parties with a formal continuity plan document distribution record maintained.

e) Contact details

NOTE The contact records may include "out of hours" contact details. However, where plans reference such private details, respect for information privacy has to be a paramount consideration.

Where appropriate, each plan document should contain or provide a reference to the essential contact details for all key stakeholders.

7.4.3 The ICT Response and Recovery Plan Documentation

The ICT Response and Recovery Plan documentation should:

a) be flexible, feasible and relevant;

b) be easy to read and understand; and

c) provide the basis for managing serious issues that are deemed by the organization to merit an IRBC response (typically following a significant disruption event).

The documentation should define the overarching framework within which the recovery plans are organized, covering:

a) overall strategy;

b) critical services (with RTO/RPO);

c) timelines for recovery; and

d) recovery teams and their responsibilities.

The plans should be documented such that competent personnel can use them in the event of an incident. They should include:

a) Objectives: a short description of the objectives of the plans;

b) Scope: covering the following, with reference to the results of the BIA:

i) the criticality of services: description of the relevant services and identification of their criticality;

ii) technology: overview of the main technology that supports the services, including where it is housed;

iii) organization: overview of the organizations (departments, vital persons and procedures) that manage the technology; and

iv) documentation: overview of the main documentation for the technology, including the (offsite) locations where it is stored.

c) Availability requirements: business-defined requirements for the availability of services and related technology;

d) Information security requirements: requirements for the information security of services, systems and data, including their confidentiality, integrity and availability requirements;

e) Technology recovery procedures: description of the procedures to be followed to recover the ICT service, including the following:

i) a list of activities, e.g. desktop support and restore contact information;

ii) a list of activities to recover network, systems, applications, databases, etc., to an agreed level at an alternative location, taking into account the changed environment (e.g. this could affect line capacity, system-to-system communications, etc.);

iii) a list of activities to restore basic functionality such as security, routing and logging;

iv) coordination within the application, or between applications, data synchronization, and potential automated procedures for handling a backlog of information;

v) the process needed to restore the ICT services and turn them over to their users to operate in recovery mode;

vi) back-up procedures; and

vii) where and how people can get further information, instructions, etc., e.g. hotline numbers; and steps to take to return to normal.

f) Appendices

i) inventory of information systems, applications and databases;

ii) overview of network infrastructure and server names;

iii) inventory of hardware and systems software; and

iv) contracts and service level agreements.

g) Key ICT suppliers

i) business as usual suppliers; and

ii) recovery service suppliers.

7.5 Awareness, competency and training program

A co-ordinated program 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 (refer to 7.2.1).

7.6 Document Control

7.6.1 Control of IRBC records

Controls should be established over IRBC records in order to:

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

b) provide for their storage, protection and retrieval.

7.6.2 Control of IRBC documentation

Controls should be established over IRBC documentation to ensure that:

a) documents are approved for adequacy prior to issue;

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

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

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

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

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

8 Monitor and Review

8.1 Maintaining IRBC

8.1.1 General

With change comes risk; not only the risk of failure, but the risk of destabilizing existing policies and strategies. The IRBC strategies should therefore be resilient and adaptable.

Any change to the ICT services which may affect the IRBC capability should be implemented only after the business continuity implications of the change have been assessed and addressed.

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;

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 sign-off that resilience has not been compromised by even the most simple of upgrades or improvements;

d) due diligence on merger and acquisition activity should include a resilience assessment; and

e) ICT component decommissioning should be reflected within related IRBC management system.

8.1.2 Monitoring, detection and analysis of threats

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

a) retention of staff, skills and knowledge;

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

c) changes in supporting technology, plant, equipment and networks;

d) changes in information applications and databases;

e) finance or budget allocation; and

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

8.1.3 Test and exercise

8.1.3.1 General

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 to the business; and

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

8.1.3.2 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 exercising regime might therefore be appropriate towards building a full simulation of a real incident. The program should include different levels of exercise from familiarization to computer room resilience, as defined in Figure 5, 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 test and exercise program should define how the risk of individual exercise is addressed. Top management sign-off on the program should be obtained and a clear explanation of the associated risks documented.

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

The test and exercise program 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 may consist of several servers, sub applications and infrastructure);

d) failover of services hosted on a high availability platform (for example, clustering: simulating the loss of any member of a cluster – see Annex B);

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

f) network testing; and

g) communications infrastructure failover tests.

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

8.1.3.3 The scope of exercises

Exercising should be carried out to:

a) build confidence throughout the organization that the resilience and recovery strategy will 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; and

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

Exercising should apply to the entire ICT environment 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.

8.1.3.4 Elements of service recovery

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 exercise at component level through to full location-based system testing in order to achieve high levels of confidence and resilience.

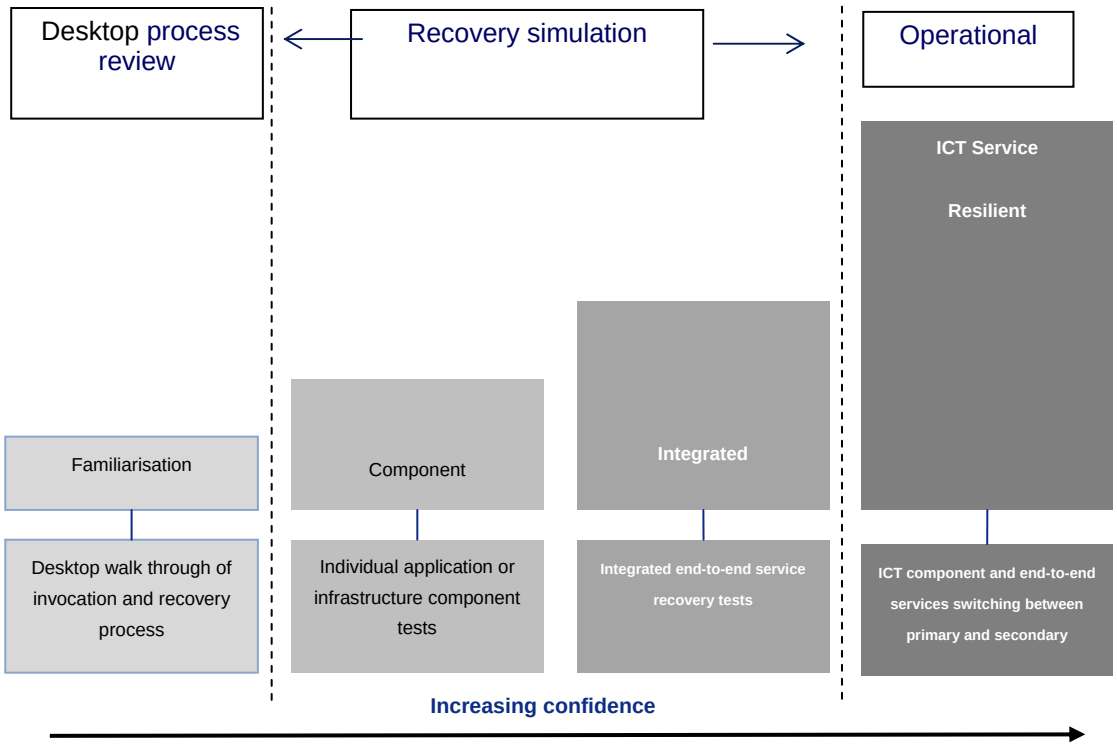

Figure 6 — A progressive test and exercise program

The following elements should be exercised:

a) computer room, such as physical security; 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; and

g) role and response of suppliers

8.1.3.5 Planning an Exercise

To ensure that an exercise does not cause incidents or undermine the service capability, an exercise should be carefully planned to minimize the risk of an incident occurring as a direct result of the exercise.

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

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

b) conducting exercises in isolated environments; and

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, so that there is 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 “terms of reference”, agreed and signed off in advance by the exercise sponsor, which may include the following:

a) description;

b) objectives;

c) scope;

d) assumptions;

e) constraints;

f) risks;

g) success criteria;

h) resources;

i) roles and responsibilities;

j) high-level timeline/schedule;

k) exercise data capture;

l) exercise/incident logging;

m) debriefing; and

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

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

8.1.3.6 Managing an Exercise

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

a) exercise commander (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 with safety;

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; and

g) emergency stop exercise protocols.

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

a) objectives and key milestones are met;

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

c) any ongoing risks are monitored and mitigated;

d) any visitors/observers are authorized;

e) exercise proceedings are captured in a consistent manner; and

f) all participants are debriefed and feedback collated.

8.1.3.7 Review, Report and Follow-up

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; and

f) consolidating and following up exercise report actions.

8.2 IRBC Internal Audit

The IRBC internal audit plan should define and document the audit criteria, scope, method and frequency (e.g. IRBC internal audit conducted annually). The audit plan should ensure that only qualified internal auditors are appointed for the audit. Selection of auditors and conduct of audit should ensure objectivity and impartially of the audit process. Auditors conducting IRBC internal audit shall be competent to undertake the task. For example, auditors should attend relevant auditor training so that they acquire the necessary skills and knowledge to conduct the audit.

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

8.3 Management Review

8.3.1 General

Top management should ensure that IRBC management system is reviewed at planned intervals. This review may take the input of internal or external audits, or self-assessments. The review should include assessing

opportunities for improvement and the need for changes to IRBC management, including the IRBC policy and objectives.

In addition, top management should review annually the signed off IRBC requirements, including ICT service definitions, the documented list of critical ICT services and the risks associated with gaps identified between critical ICT Readiness capability and business continuity requirements.

The results of the review should be clearly documented and records should be maintained.

8.3.2 Review Input

The input to a management review should include information on:

a) internal service levels;

b) external service providers' ability to maintain appropriate levels of service;

c) results of relevant audits;

d) feedback from interested parties, including independent observations;

e) status of preventive and corrective actions;

f) level of residual risk and acceptable risk;

g) follow-up actions from previous management reviews and recommendations;

h) lessons learnt from tests and exercises, incidents and the education and awareness program; and

i) emerging good practice and guidance.

8.3.3 Review Output

The output from the review should be signed off by top management and include:

a) varying the scope of IRBC management system;

b) improving the effectiveness of IRBC management system;

c) revised IRBC requirements, including ICT service definitions, the documented list of critical ICT services and the risks associated with gaps identified between critical ICT Readiness capability and business continuity requirements;

d) modifying IRBC strategy and procedures, as necessary, to respond to internal and/or external events that could impact on ICT services, including changes to:

   i) business requirements;

   ii) resilience requirements; and

   iii) levels of risk and/or levels of risk acceptance.

e) resource needs; and

f) funding and budget requirements.

8.4 Measurement of ICT Readiness Performance Criteria

8.4.1 Monitoring and measurement of ICT Readiness

The organization should monitor and measure its ICT readiness through the implementation of measurement process of the defined ICT Readiness Performance Criteria (refer to 6.7).

8.4.2 Quantitative and Qualitative Performance Criteria

Performance criteria for IRBC may be qualitative or quantitative.

Quantitative criteria may include:

a) over a given period time, the number of incidents that have not been detected prior to disruption (this can provide an indication of the completeness of detection and alert mechanisms);

b) detection time for incidents;

c) number of incidents that cannot be effectively contained to reduce impact;

d) availability of data sources to indicate emergence of incidents through trend monitoring of events; and

e) time to react and respond to detected emerging incidents.

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

a) survey using structured or unstructured questionnaire;

b) feedback from participants and stakeholders;

c) conduct of feedback workshops; and

d) other focused group meeting.

9 IRBC improvement

9.1 Continual improvement

The organization should continually improve IRBC through the application of preventive and corrective actions which are appropriate to the potential impacts determined by the organization's business impact analysis (BIA) and its risk appetite.

9.2 Corrective action

The organization should take action to correct any actual failure of ICT service and elements of IRBC. The documented procedure for corrective action should define requirements for:

a) identifying the failures;

b) determining the causes of failures;

c) evaluating the need for actions to ensure that nonconformities do not recur;

d) determining and implementing the corrective action needed;

e) recording results of action taken; and

f) reviewing of corrective action taken.

9.3 Preventive action

The organization should identify potential weaknesses in the elements of IRBC, and establish a documented procedure for:

a) identifying potential failures;

b) identifying the causes of failures;

c) determining and implementing preventive action needed; and

d) recording and reviewing results of action taken.

Annex A
(informative)

IRBC and milestones during a disruption

Figure A.1 illustrates how elements of IRBC support key milestones during a major disruption. Events and milestones happen along a time line 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.

The Recovery Point Objective (RPO) relates to the amount of data that are lost and unrecoverable due to the disruption. This is represented on the time line as the amount of time between the last good backup and when the disruption event occurs. The RPO varies according to the ICT service recovery strategy employed, particularly on the backup arrangement.

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

Further time could elapse whist while the ICT service disruption is investigated, analysed, communicated and a decision taken to invoke IRBC. It might 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 might require careful consideration in some situations, for example where the service has not been entirely lost or there seems to be a strong prospect of imminent service recovery, because invoking IRBC often impacts upon normal business operations.

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.). (Refer to ISO/IEC 24762 for further information).

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.

From a business continuity perspective there is an Recovery Time Objective (RTO) per product, service or activity and that this RTO starts from the point at which the disruption occurs and runs until the product, service or activity is recovered, but there might be a number of ICT services required to enable this and each of these ICT services could comprise a number of ICT systems or applications. Each of these component ICT systems or applications will have its own RTO as a subset of the end-to-end ICT service RTO and this should be less than the business continuity RTO, taking into account the detection and decision making time and the user acceptance testing time (unless the business continuity product, service or activity can be supported without ICT for a period, for example using manual procedures).

Recovered ICT services typically operate for a period of time supporting business continuity activity and if this is an extended period then recovered ICT services might need to be scaled up 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 will be feasible and desirable and DR operations will be 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).

Whilst 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 in its own right.

The arrows across the top of the diagram indicate how the principles of IRBC detailed in ISO/IEC 27031 align with the disruption time line.

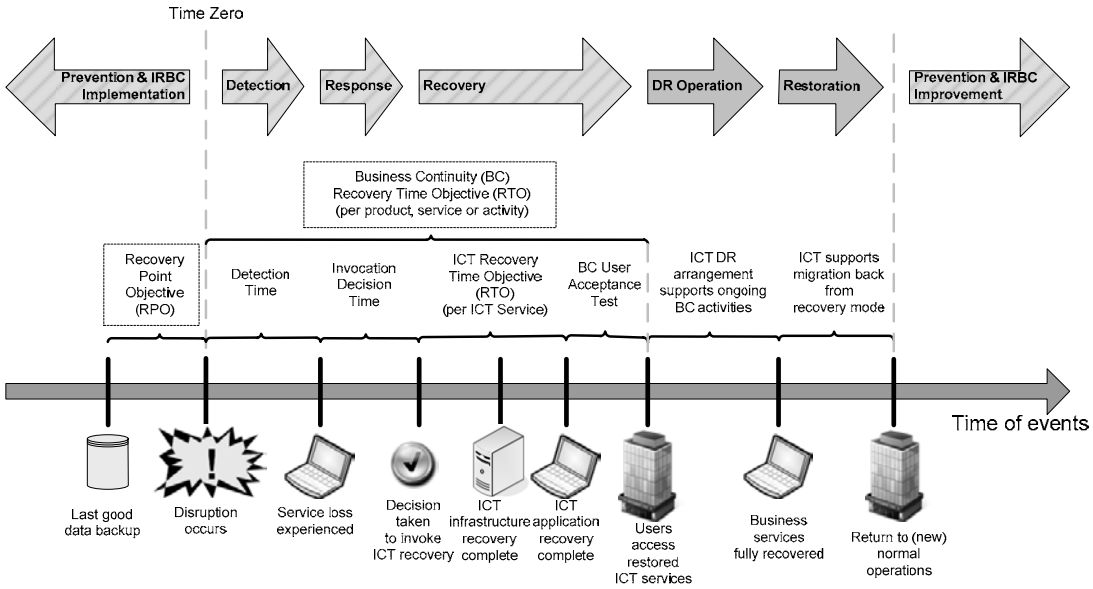

Figure A.1 — IRBC and milestones during a disruption

Annex B
(informative)

High availability embedded system

In information and communications technology, “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 percent) availability.

A computer system or a network is made up of many components, all of which usually need to be present and functional in order for the whole to be operational, and while planning for high availability frequently 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; and

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), storage area network (SAN) etc.

Application availability also needs to 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 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 disruption. Both servers will be affected by the same 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 organisations the cost and effort involved in achieving such levels of high availability can be daunting and in recent years there has been a huge growth in the 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 should be remembered 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.

Annex C
(informative)

Assessing Failure Scenarios

C.1 General

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

ISO 31010-2009 “Risk Management – Risk Assessment Techniques” is intended to reflect current good practices in the selection and utilization of risk assessment techniques. Reference should be made to this standard to determine which is the most appropriate technique to be used within an organization.

The assessment of failure scenarios is one technique which may be beneficial in enhancing the efficacy of IRBC and this annexe provides additional information on how it may be implemented.

C.2 Assessment Methodology

Unknown risk issues may emerge between assessments as a result of changes in and external to the organization environment which may hamper business continuity and resilience. The purpose of failure scenario assessment is to identify suitable event indicators and 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). For demonstration purpose, this annex elaborates on the specific FMEA methodology although an organization should select a methodology appropriate to its environment and framework.

Failure Mode Effect Analysis (FMEA) is a process for identifying and analyzing 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 standard, FMEA may 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 FMEA approach, may be applied to each critical component of the ICT service as described in 6.3.2.

For each critical component:

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 each result;

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

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

e) identify the direct and indirect events that are related, and will 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; categorize the event indicators by the availability of monitoring methods and ease of monitoring; and

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

C.3 Assessment result

The FMEA output includes a list of potential failure modes and effects, related events – may be used to determine event indicators that need to 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 life of the product or service.

Annex D
(informative)

Developing Performance Criteria

As the performance of IRBC differs from organization to organization, each organization should develop its IRBC performance criteria, and maintain them as part of the continuous improvement process.

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

a) As part of ISMS and BCM processes, the known incidents and event indicators have been established as input to the next steps.

b) Give a set of known incidents (e.g., password intrusion attack, server failure due to insufficient hard disk space).

c) Determine events leading to those incidents (e.g., failed login attempts, hard disk utilization).

d) Determine suitable detection time (e.g., threshold for events to be reported/alerted to the system/administrator).

e) Determine suitable response time (e.g., timeline for administrator to take action to prevent an incident to materialize);

f) Categorize events into groups of response time block desired and types of response actions; events may be categorized by threat group, application group, response actions group, and/or response time group.

g) Refine the matrices and measurements through scenario testing and drills/exercises.

h) Conduct test to determine whether the response actions are workable, and whether target achievable.

i) Refine categories, expected event response time, and expected event response actions (e.g., seek alternative method to monitor, detect, and act).

j) Improve by capturing new incidents and failure scenarios and repeat the process.

Bibliography

[1] SS 540:2008, Singapore Standard for Business Continuity Management

[2] BS 25999-1:2006, *Business continuity management — Part 1: Code of practice*

[3] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[4] ISO/IEC 18043:2006, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems*

[5] ISO/IEC 20000-1:2005, *Information technology — Service management — Part 1: Specification*

[6] ISO/IEC 20000-2:2005, *Information technology — Service management — Part 2: Code of practice*

[7] ISO 22301, *Societal security — Preparedness and continuity management systems — Requirements*[2)]

[8] ISO/IEC 24762:2008, *Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services*

[9] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*

[10] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*

[11] ISO 31010:2009, *Risk management — Risk assessment techniques*

2) Under preparation.

ICS 35.040

Price based on 36 pages