



Company Management System

Business Continuity in SIA

Document code: 1-CMS-2010-056-03
Company–Project/Service–Year–Document No.–Version

Classification: Public



INDEX

1. INTRODUCTION	3
2. SIA'S BUSINESS CONTINUITY MANAGEMENT SYSTEM AND REFERENCE STANDARD	4
3. BCM PROGRAMME MANAGEMENT	5
3.1 The provisions of BS 25999	5
3.2 The SIA scenario	5
4. UNDERSTANDING THE ORGANIZATION	6
4.1 The provisions of BS-25999	6
4.2 The SIA scenario	6
4.2.1 Business Impact Analysis	6
4.2.2 Risk Assessment	6
5. DETERMINING BCM STRATEGY	8
5.1 The provisions of BS-25999	8
5.2 Business Continuity in SIA	8
6. DEVELOPING AND IMPLEMENTING BCM RESPONSE	9
6.1 The provisions of BS-25999	9
6.2 The SIA scenario	9
6.2.1 Organizational solutions: Emergency and Crisis Management Process	9
6.2.2 Organizational solutions: Business Continuity Plan (BCP) for Departments.....	10
6.2.3 Organizational solutions: Disaster Recovery Plans (DRP)	11
6.2.4 Logistics solutions.....	11
6.2.5 Technology solutions	11
6.2.6 Involvement of the customers	12
6.2.7 Business Continuity and Disaster Recovery Documentation.....	12
6.2.8 Review of the Business Continuity Management System.....	12
7. EXERCISING, MAINTAINING AND REVIEWING	13
7.1 The provision of BS-25999	13
7.2 The SIA scenario	13
7.2.1 Drills.....	13
7.2.2 Maintenance.....	13
7.2.3 Revision	14
8. EMBEDDING BCM IN THE ORGANIZATION'S CULTURE	15
8.1 The provisions of BS-25999	15
8.2 The SIA scenario	15
8.2.1 Awareness and Training	15
9. ATTACHMENT 1 - BUSINESS CONTINUITY MANAGEMENT GLOSSARY	16

1. INTRODUCTION

SIA considers Business Continuity to be a crucial element in the provision of its services in full conformity with the contracts it enters into with customers, with Bank of Italy Guidelines and, more generally, in conformity with the international methodologies and standards of reference. SIA has therefore developed, and maintains, a Business Continuity Management System that includes logistics, organizational and technological solutions. This system is designed to support the organization in an efficient and timely manner in the case of emergency situations.

The main objective of SIA's Business Continuity Management System is to ensure that the organization is able to react in case of damaging events threatening its existence or reputation.

The principles which establish the priorities in the management of emergencies/crises and guide decisions are:

- protect the life and safety of people;
- prevent further consequences arising from the original incident;
- protect business continuity and safeguard the reputation of the company;
- cooperate to guarantee continuity in the provision of services for the credit-financial system;
- safeguard the assets the company has or is responsible for, while respecting the environment.

These principles are consistent with the Bank of Italy's *Guidelines for service continuity of qualified payment systems infrastructures* and with the best practices and standards such as BS 25999 and ISO 27001.

For SIA, managing Business Continuity means:

- **guiding choices** in emergency and crisis situations,
- **defining plans, procedures and technical, human and logistical resources** to ensure Business Continuity within the company in emergency and crisis situations,
- **reacting promptly in order to reduce** downtime of business processes and ensure that they are restored efficiently.

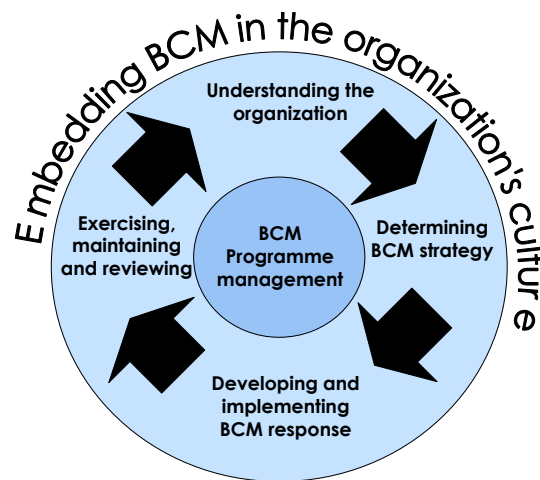
2. SIA'S BUSINESS CONTINUITY MANAGEMENT SYSTEM AND REFERENCE STANDARD

In the development of its Business Continuity Management System, SIA has adopted the **BS 25999** standard and, in 2008, was awarded the certification BS 25999 through a qualified third party for the entire corporate perimeter.

The lifecycle of the Business Continuity Management System is made up of six phases:

1. BCM Programme management
2. Understanding the organization
3. Determining BCM strategy
4. Developing and implementing BCM response
5. Exercising, maintaining and reviewing
6. Embedding BCM in the organization's culture

The phases, which are not necessarily in this order but that need to be repeated periodically over time, are represented as follows:



The following chapters describe the methods adopted by SIA to be compliant with the standard in each phase.

3. BCM PROGRAMME MANAGEMENT

3.1 The provisions of BS 25999

BCM Programme Management is an ongoing management and governance process that, supported by the Company's Top Management and by an adequate allocation of resources, ensures that the necessary steps are taken in order to identify the impact of potential losses, to maintain recovery plans and strategies in place and to ensure continuity of products and services through training, testing and drill programs and continuous updating and reviewing activities.

3.2 The SIA scenario

SIA is structured in order to identify roles and responsibility within the organization itself to face organizational (Business Continuity), technological (Disaster Recovery) and logistical issues.

In addition, it has set up a Business Continuity/Disaster Recovery Steering Committee to coordinate the master plan of actions relating to Business Continuity and Disaster Recovery. This Committee reports periodically to the Company's Top Management.

Lastly, there is an Auditing function that reports directly to the Chairman. This function intervenes on the Business Continuity and Disaster Recovery programmes through independent verifications, assessments, and by offering opinions and recommendations.

4. UNDERSTANDING THE ORGANIZATION

4.1 The provisions of BS-25999

The aim of this phase is to promote the understanding of the company through the identification of its key services and **critical activities**, and of the necessary resources for their maintenance. This analysis also aims at guaranteeing that the Business Continuity management programme is in line with the corporate mission, the regulations in force and the agreements with customers.

The pursuit of this objective is realized through the following activities:

- Business Impact Analysis
- Risk Assessment

4.2 The SIA scenario

4.2.1 Business Impact Analysis

Business Impact Analysis (BIA) is the evaluation of the impact on the business in case of significant events that could compromise corporate activities and the provision of services. In order to select the appropriate Business Continuity solutions, service requirements are identified.

SIA produces the Business Impact Analysis with these objectives:

- list the services that are important to the corporate business
- identify the impacts connected to the unavailability of the service
- identify the timescale needed for the restoration of services at contractual/regulatory level
- identify the most critical services
- identify the activities to be restored at a later time

SIA's BIA mainly includes the analysis of business services and the identification of critical activities using evaluation parameters that take into account regulatory and contractual obligations, the relevance of the service/activity for the corporate business, and the strategic relevance of the service/activity for the company.

SIA's BIA is updated annually with the information provided by the corporate departments involved and is made available to the company for the preparation of Disaster Recovery plans.

4.2.2 Risk Assessment

The activity of Risk Assessment is aimed at identifying and evaluating the threats that could damage the assets of the company and make them unavailable for a given period of time.

When carrying out the Risk Assessment, SIA has the following main objectives:

- Identify the events that could result in a loss of confidentiality, integrity, availability and compliance of corporate services/processes
- Identify and manage existing vulnerable elements, and manage the risk arising from the occurrence of events identified as possible threats.

SIA's process and methods for the analysis of risks to security are based on the indications provided by the BS7799-3 standard and on the CobiT reference model (Process PO9 – Assess Risk).

The risks, calculated according to the security parameters Confidentiality, Integrity, Availability and Compliance, are analyzed by the parties involved and a specific Security Committee decides how to deal with them according to the appropriate balance between business, cost, technology and security requirements, namely:

- mitigate risks through the identification of actions, responsibilities and intervention priorities
- consciously accept risks
- avoid risks
- transfer risks to third parties.

On the basis of the decisions made, the Security Risk Management Plan is drawn up. This is regularly monitored and updated according to the indications provided by the Security Committee.

Also regularly carried out are the:

- Analysis and management of security risks of processes and infrastructures used in the provision of corporate business services
- Physical Security Analysis and Safety Analysis.

5. DETERMINING BCM STRATEGY

5.1 The provisions of BS-25999

The activities of this phase allow the company to determine an adequate Business Continuity strategy that allows it to guarantee an appropriate response for each service, both in terms of operating levels and acceptable restoration timescales, during and after an incident.

5.2 Business Continuity in SIA

Every year, SIA submits the Business Continuity Plan to its Board of Directors for approval. This includes the company's strategy, the actions carried out and those still to be performed.

SIA's Business Continuity strategy is based on the following guiding principles:

- The adoption of a Business Continuity model recognized at international level. SIA has chosen as its reference the BS 25999 standard and the methodology of the Business Continuity Institute (BCI)
- Breakdown of Business Continuity objectives by service, consistent with the commercial contracts entered into with customers and with the requirements of the Supervisory Authorities
- Identification of adequate technical and organizational solutions
- Definition of a multi-year Business Continuity plan to include repeated tests aimed at guaranteeing the appropriateness and constant updating of the solutions adopted
- Use of Bank of Italy's Terms of Reference (TOR) as a tool to verify the appropriateness of the Business Continuity system.

6. DEVELOPING AND IMPLEMENTING BCM RESPONSE

6.1 The provisions of BS-25999

The objective of the Developing and Implementing BCM Response phase is to guarantee that the corporate structure develops plans, instructions and processes and makes available rooms and equipment in preparation for a prompt response to incidents and crises.

The structure must allow:

- Confirmation of the nature and extent of the incident
- Initiation of an appropriate Business Continuity response
- Set up of plans, processes and procedures for the activation, coordination, communication, management and closing of the emergency
- Availability of resources to support plans, processes and procedures during the incident management phase
- Communication with the stakeholders.

The development and realization of a Business Continuity response derive from the creation of a model and a structure to manage the incident, and of Business Continuity and Disaster Recovery plans detailing the actions to be carried out during and after an incident in order to maintain or restore operations.

6.2 The SIA scenario

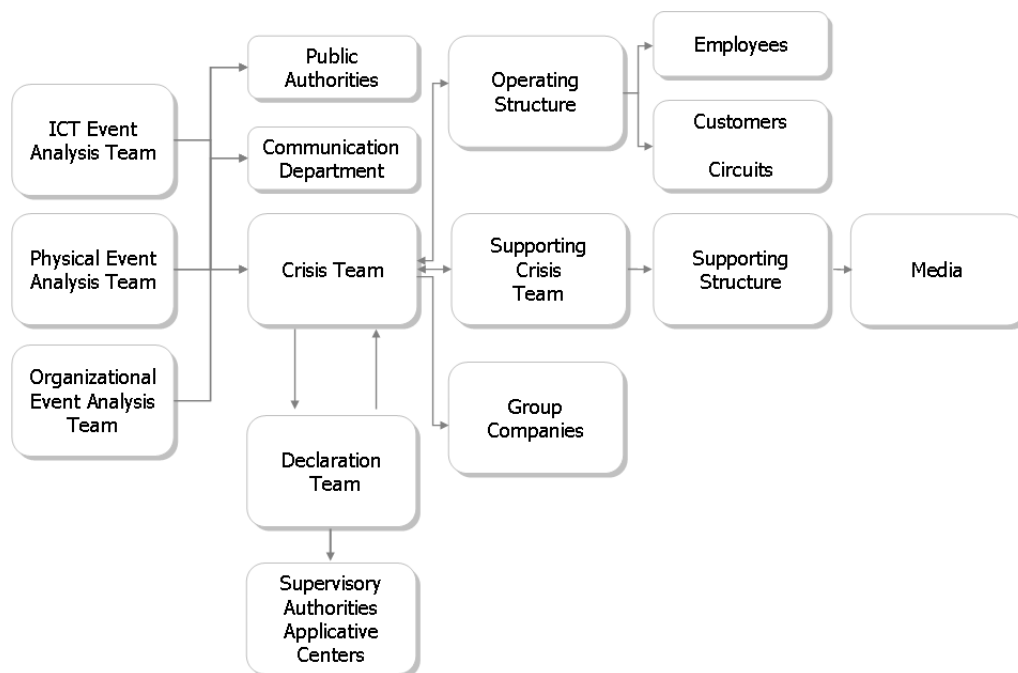
In order to be ready to deal with an emergency and/or crisis in the best way possible, SIA has developed:

- Organizational solutions
- Logistics solutions
- Technological solutions

6.2.1 Organizational solutions: Emergency and Crisis Management Process

SIA has defined the organizational structure necessary to manage the escalation procedure for the assessment and possible declaration of a Crisis Situation and the subsequent activation of the Business Continuity operative teams. It has also created an Emergency and Crisis Management Process that describes the methods of activation, the responsibilities and the contacts necessary to manage an emergency and/or crisis within the company.

The flow chart that follows illustrates the methods of activation of Business Continuity Management Teams, their relative responsibilities and the methods for transferring information inside and outside the company.



The Emergency and Crisis Management Process is broken down into five phases: Event Analysis, Activation of Crisis Teams, Reaction, Crisis Management and Closing of the Crisis.

The status of emergency and/or crisis may originate from two types of event: "ICT" and "NON ICT".

ICT identifies everything concerning the technology, applications and operations necessary for the provision of services (under the responsibility of the ICT Event Analysis Team).

NON ICT means all aspects relating to physical security, logistics and auxiliary equipment (under the responsibility of the Physical Event Analysis Team), and relating to the company's organization such as issues concerning personnel, legal matters, administration, the media, etc. (under the responsibility of the Organizational Event Analysis Team).

The actions to be performed and the responsibilities connected to them in the case of an emergency that calls for the evacuation of the building or some of its areas to ensure the safety of the occupants are described in a specific Emergency Plan that is reviewed at regular intervals.

6.2.2 Organizational solutions: Business Continuity Plan (BCP) for Departments

The Emergency and Crisis Management Process activates the Business Continuity Plans (BCP) for the Departments.

The Business Continuity Plans describe the organizational procedures that each Department must follow in order to restore its services following the Declaration of an Emergency and/or Crisis within the company by the Declaration Team.

The Business Continuity Plans describe the potential disaster scenarios, the management of contacts and communication activities during the emergency or crisis (company staff, suppliers, customers, subsidiary companies), the containment and/or contrast actions planned for each scenario and the relevant documentation.

In addition, the Business Continuity Plans contain the names of the operative personnel that must be involved.

6.2.3 Organizational solutions: Disaster Recovery Plans (DRP)

SIA has set up and maintains the Disaster Recovery Plans, a collection of documents that detail the activities necessary to restore the technical and applicative infrastructures and the methods and timescale of reactivation at the Disaster Recovery site.

6.2.4 Logistics solutions

In order to protect itself from events that could threaten the security of the company, SIA has equipped itself with the most modern and sophisticated physical security measures, including access control, intrusion detection, perimeter defence, flood and infiltration detection, smoke detection and fire prevention systems, CCTV and continuity generators. Furthermore, the building is constructed in compliance with earthquake standards and the electricity is supplied by two separate power plants.

In addition to the measures described above, in order to provide an appropriate response to disaster events, SIA has at its disposal different offices (where both equipment and human resources are dislocated) and a Disaster Recovery site outside the city containing the infrastructure necessary to manage the re-start of services following a disaster event (the services deemed critical by the company and those that are the subject of contracts entered into with the customers). Separate rooms contain network and security equipment, local network devices and the other equipment necessary to reactivate the services.

Also available are data-rooms equipped with workstations, links to several providers, satellite telephones, cash and documentation instruments.

6.2.5 Technology solutions

The Disaster Recovery site is equipped with technology platforms featuring a processing capacity equivalent to those of the primary site.

The basic hardware devices are either redundant or possess adequate fault-tolerant features both at the primary and at the Disaster Recovery site.

Also in place are specific maintenance contracts with adequate Service Levels with regard to the timescales of intervention or resolution.

The Disaster Recovery architectural solutions adopted allow the creation of specific technology infrastructure configurations in order to meet Service Levels and Institutional requirements.

The architecture of the local network, of the SIANet.NG geographical network and of access to the telephone network have been designed and realized to guarantee the same level of reliability and the same scope of the network as are present at the production site. The primary site and the DR site are connected using fibre optic cabling that is dedicated and have diversified paths and suppliers.

All the data necessary to activate systems and services in the Disaster Recovery phase are replicated in the secondary site, in "synchronous" or "consistently asynchronous" mode, thus allowing for a Recovery Point Objective (RPO) that varies from zero to some minutes according to contractual SLAs and defined performance requirements.

6.2.6 Involvement of the customers

The complete realization of Business Continuity must be in line with the development of a direct collaborative relationship with the Customers to enable the analysis, definition and implementation of all the joint crisis management measures and to restore support services and technologies such as lines, security devices and connections to International Circuits.

For this purpose, SIA agrees with its customers methods of reciprocal collaboration, namely the definition of RTOs and RPOs, the connections to be used in case of disaster events, the staff to be contacted for general communications, the actions to be carried out in case of activation of the technical-applicative infrastructure at the Disaster Recovery site, and test planning.

For any communication concerning the services supplied, SIA provides its Customers with a Service Desk, which can be contacted at the telephone number:

+39 02 6084 3060

or via email at:

mo.service.management@sia.eu

6.2.7 Business Continuity and Disaster Recovery Documentation

The electronic version of the documents issued for the Business Continuity Management System (BCMS) is filed in the corporate document system.

In order to have a copy of the Business Continuity and Disaster Recovery documents immediately available, also in the case of an emergency or crisis, the Disaster Recovery sites have filing cabinets containing the paper format of the documents themselves.

6.2.8 Review of the Business Continuity Management System

SIA periodically, or in the case of significant variations, carries out a revision of the entire Business Continuity Management System (BCMS) in order to ensure its correspondence and compliance with regulatory, organizational, strategic and legislative changes.

7. EXERCISING, MAINTAINING AND REVIEWING

7.1 The provision of BS-25999

A Business Continuity Management System cannot be considered reliable if it is not tested at regular intervals and adequately updated.

This phase includes three activities:

- Drills
- Maintenance
- Revision

7.2 The SIA scenario

7.2.1 Drills

SIA periodically carries out Business Continuity and Disaster Recovery tests and drills, which could concern the:

- **Organization** (for example: Test of the emergency management process, test of Business Continuity Plans, etc.)
- **Logistics** (building evacuation drills)
- **Technology** (Disaster Recovery tests)

SIA, in its role as Qualified Infrastructure, also takes part in systematic tests organized by the CODISE group (Bank of Italy).

The Business Continuity tests are performed to verify the effectiveness and efficiency of the Emergency Management Process, the adequacy, completeness and practicability of the Business Continuity Plans and relative support procedures, to assess the preparation of the Business Continuity management teams and the effectiveness of the awareness/training programme, and to develop and spread awareness of Business Continuity issues within the company.

Disaster Recovery tests are necessary to assess the practicability and efficiency of technology infrastructure back-ups and to update the skills of the staff involved.

Every year, SIA draws up both the Plan of Business Continuity Tests and the Plan of Disaster Recovery Tests.

7.2.2 Maintenance

SIA has put in place a document updating process thanks to which each change, at internal and external level, impacting the company is included in the Business Continuity/Disaster Recovery management procedures.

7.2.3 Revision

SIA regularly carries out a revision of its Business Continuity Management System in order to assess its effectiveness, efficiency and adequacy as well as its policies, strategies and objectives and to identify possible needs for updating. It then performs the appropriate corrective actions and improvements.

The system revision activity is carried out through:

- Management Review
- Regular Internal Inspections
- External Inspections (Maintenance of the Certification with DNV)

The Management Review is regularly carried out with the Company's Top Management. Its objective is the assessment of the degree of adequacy of the Business Continuity Management System following the evolution of rules and requirements of reference standards/regulations and to identify specific activities aimed at guaranteeing its maintenance.

Every year, SIA draws up the annual Plan of Checks and carries out Internal Checks.

8. EMBEDDING BCM IN THE ORGANIZATION'S CULTURE

8.1 The provisions of BS-25999

In order to enhance and spread Business Continuity culture within the company, it is necessary that the BCMS is perceived as a key value for the company itself and is sponsored by the top management. In order to achieve this, SIA carries out the following activities:

- Education and information (Awareness)
- Training
- Drills (Tests/inspections)

8.2 The SIA scenario

8.2.1 Awareness and Training

The success of the Business Continuity process also depends on the knowledge of the staff with regard to processes and services and the activities to be carried out to guarantee their continuity.

SIA has set up a training programme to spread awareness among the staff regarding the importance of the BCMS.

The Training programme is aimed at both the management and the operative staff.

SIA carries out its training programmes in classes, training sessions for staff employed in specific tasks and drills on the basis of the Business Continuity Awareness/Training Programme drawn up at regular intervals.

9. ATTACHMENT 1 - BUSINESS CONTINUITY MANAGEMENT GLOSSARY

From: BS 25999-2:2007 British standard-Business Continuity Management - Part 2: Specification

Terms	Definitions
Activity	process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products or services
Audit	systematic examination to determine whether activities and related results conform to planned arrangements and whether these arrangements are implemented effectively and are suitable for achieving the organization's policy and objectives
business continuity	strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level
business continuity management (BCM)	holistic management process that identifies potential threats to an organization and the impacts to business operations that those 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
business continuity management lifecycle	series of business continuity activities which collectively cover all aspects and phases of the Business Continuity Management Programme
business continuity management personnel	those assigned responsibilities defined in the BCMS, those accountable for BCM policy and its implementation, those who implement and maintain the BCMS, those who use or invoke the business continuity and incident management plans, and those with authority during an incident
business continuity management programme	ongoing management and governance process supported by top management and appropriately resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products and services through training, exercise, maintenance and review
business continuity management response	element of BCM concerned with the development and implementation of appropriate plans and arrangements to ensure continuity of critical activities, and the management of an incident
business continuity management system (BCMS)	that part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity
business continuity plan (BCP)	documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical activities at an acceptable predefined level
business continuity strategy	approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major incident or business disruption
business impact analysis (BIA)	process of analysing business functions and the effect that a business disruption might have upon them

Terms	Definitions
consequence	outcome of an incident that will have an impact on an organization's objectives
cost-benefit analysis	financial technique that measures the cost of implementing a particular solution and compares this with the benefit delivered by that solution
critical activities	those activities which have to be performed in order to deliver the key products and services which enable an organization to meet its most important and time-sensitive objectives
disruption	event, whether anticipated (eg. a labour strike or hurricane) or unanticipated (eg. blackout or earthquake), which causes an unplanned, negative deviation from the expected delivery of products or services according to the organization's objectives
emergency planning	development and maintenance of agreed procedures to prevent, reduce, control, mitigate and take other actions in the event of a civil emergency
exercise	activity in which the business continuity plan(s) is rehearsed in part or in whole to ensure that the plan(s) contains the appropriate information and produces the desired result when put into effect
gain	positive consequence
impact	evaluated consequence of a particular outcome
incident	situation that might be, or could lead to, a business disruption, loss, emergency or crisis
incident management plan (IMP)	clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process
internal audit	audit conducted by, or on behalf of, the organization itself for management review and other internal purposes, and which might form the basis for an organization's self-declaration of conformity
invocation	act of declaring that an organization's business continuity plan needs to be put into effect in order to continue delivery of key products or services
likelihood	chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies or mathematical probabilities
loss	negative consequence
management system	system to establish policy and objectives and to achieve those objectives
maximum tolerable period of disruption	duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed
nonconformity	non-fulfilment of a requirement
organization	group of people and facilities with an arrangement of responsibilities, authorities and relationships
process	set of interrelated or interacting activities which transforms inputs into outputs
product and services	beneficial outcomes provided by an organization to its consumers, recipients and stakeholders, eg manufactured items, car insurance, regulatory compliance and community nursing
recovery time objective	target time set for resumption of product, service or activity delivery after an incident
resilience	ability of an organization to resist being affected by an incident

Terms	Definitions
resources	all assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objectives
risk	something that might happen and its effect(s) on the achievement of objectives
risk assessment	overall process of risk identification, analysis and evaluation
risk management	structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating, and controlling responding to risk
stakeholders	those with a vested interest in an organization's achievements
system	set of interrelated or interacting elements
top management	person or group of people who direct and control an organization at the highest level