SIA S.p.A.

via Francesco Gonin, 36 - 20147 Milan - Italy
p. +39 02 6084.1 - **f.** +39 02 6084 3920

Foreign branches:
Belgicastraat 1 - B-1930 Zaventem - Belgium
Winthontlaan 200 - 3526 KV Utrecht - Netherlands

www.sia.eu - info@sia.eu

Share capital € 22.274.619,51 fully paid-up
VAT number, tax code and Milan Register
of Companies no. 10596540152
Milan Economic and Administrative
Index no. 1385874

Business Continuity in SIA

January 2020

INDEX

EXECUTIVE SUMMARY

This document describes how SIA S.p.A. develops, implements and maintains its business continuity management system, applying what is stated in the company Business Continuity Guidelines, in compliance with the industry standards [3] and in line with the requirements of standard ISO 22301:2012 [1].

1. SCOPE

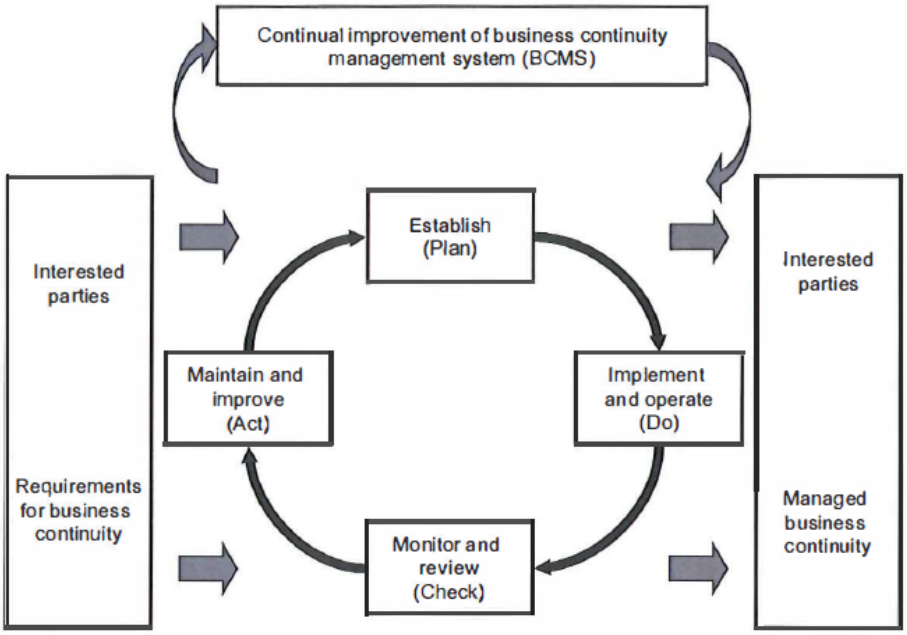
The scope of application of the Business Continuity Management System (valid also for the other Quality and Security certified Management Systems) is indicated in the ISO 22301 Certificate issued by the Certification Body DNV and available for consultation at www.sia.eu, SIA Group, Compliance.

2. NORMATIVE REFERENCES

SIA has since 2007 adopted the BS 25999 standard as the reference model for the creation of its own Business Continuity Management System. In 2008, it attained Business Continuity Certification in compliance with the model adopted.

In 2012, the BS 25999 standard was converted into ISO 22301 and in 2013 SIA updated its Business Continuity Management System to ensure its compliance with the new ISO 22301 standard.

The reference model adopted for the implementation of the BCMS is Plan – Do – Check – Act.



In particular, Sections 4 through 7 can be identified as *Plan*, Section 8 represents *Do*, Section 9 *Check* and finally Section 10 *Act*.

SIA's Business Continuity Management System also complies with the *Guidelines* issued by Banca d'Italia (the Bank of Italy) and in general with all regulations, guidelines or directives issued by Banca d'Italia concerning service continuity.

3. TERMS AND DEFINITIONS

An extract from the section 'Terms and definitions' of the ISO 22301:2012 standard with the items of greatest interest to SIA is included in the Appendix.

4. CONTEXT OF THE ORGANIZATION

4.1 Understanding of the organization and its context

The organization outlines its development strategy in the corporate Strategic Plan analyzing the international competitive scenario and defining the positioning of the company, activating processes of strategic intelligence to support the Top Management, also with the aim of identifying in advance any threats and opportunities in the various international areas of interest to the Group.

For the purpose of Business Continuity, the company management promotes the understanding of the organization through the identification of its key services and its critical activities as well as the resources necessary for their maintenance. This is achieved through the activities of Business Impact Analysis and Risk Assessment of new projects and services (see Section 8.2).

4.2 Understanding the needs and expectations of interested parties

In planning its activities, SIA takes into great consideration the needs and expectations of its stakeholders.

In particular, as far as Banca d'Italia is concerned, SIA participates in the CODISE (Service Continuity) group and in the Business Continuity tests this group organizes on a regular basis, involving the main players in the domestic financial system.

As far as its Customers are concerned, SIA undertakes to respect the contractual terms and requirements agreed with them and stated in the Business Impact Analysis of the business services.

SIA's organizational model represents the tangible application of the principles of legality, transparency, correctness and loyalty that have always characterized SIA's relationships with its stakeholders.

The SIA Code of Ethics expresses the company's ethical values, rights, obligations and responsibilities towards all the parties with which it comes into contact in the achievement of its corporate purpose.

Furthermore, it establishes the relevant standards and rules of conduct that must guide the behavior and activities of those working within the framework of SIA.

The adoption of the Code of Ethics is based on SIA's conviction that ethical behavior in the conduct of business is also a necessary condition for the company's success.

In its Code of Ethics, SIA sets out, in addition to the corporate values, the rights, obligations and

responsibilities of SIA towards all the parties with which it comes into contact in the achievement of its corporate purpose[1], the standards of reference and rules of conduct that must guide the behavior and activities of those working within the framework of SIA, be they Directors, Statutory Auditors, employees or external collaborators.

The Code of Ethics also falls within the framework of implementation of the provisions of Legislative Decree 231 of 8 June 2001, setting out the general principles of management, supervision and control on which the organizational models must be based, also regulating cases and conducts specific to the company.

Corporate Compliance is also guaranteed through the establishment of a specifically dedicated function, responsible for defining and administering the system of corporate compliance, namely the systematic governance of compliance with laws/regulations/ standards subject to certification applicable in the company.

4.3 Determining the scope of the business continuity management system

The activities of this phase permit the organization to develop a specific Business Continuity strategy to guarantee an appropriate response for each service, in terms of operating levels and acceptable restoration times, during and after a damaging event.

On an annual basis, SIA submits to its Board of Directors the Business Continuity Plan, which includes the corporate strategy, the actions carried out and the actions to be performed.

The SIA Business Continuity action strategies are based on the following guiding principles:

- reference to the "Banca d'Italia Guidelines for business continuity" to assess the adequacy of the Business Continuity structure;
- outline of the Business Continuity objectives for the various services consistent with the requirements set out by the Supervisory Authorities and with the business contracts with customers;
- adoption of a Business Continuity model recognized as a reference at international level. SIA has chosen as its reference the standard ISO 22301:2012;
- identification of technical and organizational solutions consistent with the evolutions of the technology and compatible with the economic requirements of the company;
- definition of a Business Continuity plan that provides for repeated tests to guarantee the adequacy and continual updating of the technical and organizational solutions adopted.

4.4 Business Continuity Management System

SIA has implemented a Business Continuity Management System (BCMS) with the aim of increasing the satisfaction of its clientele, improving internal processes and the levels of quality and security of the services, adopting international standards recognized at global level.

SIA puts to use a continual process of management and governance which, supported by the Top Management and by the appropriate allocation of resources, ensures that the necessary steps are taken to identify the impact of potential losses, to keep the restoration plans and strategies practicable and to ensure the continuity of the products and services through training programs, tests, drills and constant updating and revision activities.

[1] Internal relationships: with the employees, with the directors and statutory auditors, with the shareholders. External relationships: with the customers, with the suppliers, with public administration bodies, with the relevant institutions and authorities, with political parties, the trade unions and the other associations, with the media, with the competitors, with the corporate governance system and for environmental protection.

5. LEADERSHIP

5.1 Leadership and commitment

As far as the Business Continuity Management System (BCMS) is concerned, the Top Management:

- identifies the main Business Continuity roles within the individual corporate units, setting up a specific organizational body to manage and implement Business Continuity in the company and a predefined organizational body for the extraordinary management of emergencies and crises (see 5.4);
- defines and circulates the Business Continuity Policy, from which the Business Continuity Action Strategies, Guidelines and Objectives originate;
- promotes the understanding of the company through the identification of its key services and critical activities, as well as the resources necessary for their maintenance, through the performance of Business Impact Analysis and Risk Assessment activities;
- on an annual basis, submits the Business Continuity Plan to its Board of Directors (see 4.3).

Furthermore, it ensures that the organization:

- develops and keeps updated plans, instructions and processes that enable it to manage emergencies and crises promptly;
- creates a document framework containing the array of predefined plans detailing how the organization manages a damaging event and how it guarantees the continuity of its activities in case of a disaster event;
- organizes regular Business Continuity training programs;
- plans regular Business Continuity and Disaster Recovery tests and drills;
- regularly performs a revision of the entire Business Continuity Management System to ensure its conformity and adequacy in relation to regulatory, organizational, strategic and legislative changes.

5.2 Management commitment

The management of SIA believes unreservedly in the value and importance of Business Continuity and fully supports the implementation and development of the Business Continuity Management System.

To this end, SIA's Top Management actively:

- informs its staff of the fact that respect for the requirements of the customer and for the mandatory ones related to them is always of primary importance;
- defines the Business Continuity Policy and informs all personnel of it so that the objectives set out are achieved and that the resources necessary for this purpose are provided;
- grants to the various managers of the corporate functions the necessary authority to perform the duties assigned to them;
- ensures the distribution to all personnel of information concerning the updates and evolution of the processes;
- takes part in the Business Continuity tests, both internal (to assess the effectiveness and efficiency of the chain of contact of the Emergency and Crisis Management Process and to measure the time required to declare a Crisis) and external (e.g. CODISE test);

- sets up an appropriate organizational body responsible for managing and implementing Business Continuity in the company (see 5.4);
- takes part in the Management Review.

5.3 Policy

SIA considers Business Continuity to be an indispensible factor to protect its information capital and a factor of strategic value, that can be easily transformed into a competitive advantage in terms of its positioning in the domestic and international market and the supply of the services offered.

Excellence in the delivery of its services and customer satisfaction are achieved by guaranteeing the efficiency and reliability of the services supplied through the system of corporate processes, and also through the adoption of Security and Business Continuity solutions developed in compliance with industry best practices.

SIA decided to develop the Business Continuity Policy since it considers its implementation to be fundamental in relations with all the company's stakeholders.

By guaranteeing an adequate system of processes and an adequate level of information security and in compliance with the laws, regulations and requirements set out by the Supervisory Bodies, SIA is able to respond appropriately to the needs of its customers and to the market requirements and achieve its corporate objectives.

The Business Continuity Policy is available in the document SIA Management Processes and Systems.

5.4 Organizational roles, responsibilities and authorities

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.

A Committee has been set up to call to the attention of the Top Management to the most significant aspects to be managed in addition to a Business Continuity and Disaster Recovery Steering Committee to coordinate the development of issues relating to Business Continuity and resilience in the supply of services and in applicative and infrastructural projects.

A Risk Team has also been set up, with the aim of implementing and developing the Risk Management program and overseeing and monitoring the identification and analysis of risks and the plans to deal with the risks found. The Business Continuity and Risk functions take part in the respective Committees.

The company Departments and Divisions are responsible for the Business Continuity activities under their responsibility and identify, in agreement with the management, the processes and services critical to the company and the methods by which their continual functioning is guaranteed, also in critical situations.

In order to guarantee an operational link between Business Continuity body and the other company Departments and Divisions, appropriate Contact Persons have been appointed in the Divisions and Departments and appropriate operational relationships have been outlined.

6. PLANNING

6.1 Actions to address risks and opportunities

As far as the risk management strategy is concerned, SIA has established a function called *Risk* responsible for the definition and management of corporate risks.

One of the main activities of the Risk function is the Company Risk Analysis process, the objective of which is to guarantee a regular review of risks at Company level and subsequently align SIA's risk profile.

6.2 Business continuity objectives and plans to achieve them

The main objective of SIA's Business Continuity Management System is to guarantee that the company is able to react to events threatening its survival or image, while respecting the industry regulations and the terms of contracts entered into with customers.

In order to guarantee Business Continuity, it is necessary to establish a system that includes logistical, organizational and technological solutions (Disaster Recovery). This system must be able to support the company in an efficient and prompt manner in case of an emergency.

The Top Management of the Company defines and plans the Business Continuity objectives and agrees them with the various functions. The Business Continuity objectives are made formal in the relevant Policy, in the Management Review and in the Improvement Plans.

The principles that establish the priorities in the management of an emergency/crisis and that guide decisions are:

- protection of the life and safety of people;
- prevention of further consequences deriving from the original incident;
- protection of business continuity and of the company image;
- cooperation in ensuring the service continuity of the credit-financial system;
- protection of the assets owned by or under the responsibility of the Company and of the environment.

These principles are consistent with the Guidelines issued by Banca d'Italia (the Bank of Italy) and with the best practices and standards such as ISO 22301 and ISO 27001.

7. SUPPORT

7.1 Resources

The Top Management is committed to pursuing the Business Continuity objectives with adequate resources and means and grants the Business Continuity personnel the authority and resources necessary to perform their duties.

The company management supported the creation of a Business Continuity management system that is widespread and integrated in each corporate Department and Division as well as a predefined organizational structure for the extraordinary management of emergencies and crises.

Resources made available

The company management has identified and assigned the necessary resources for the implementation of the Business Continuity Management System in line with the Business Continuity policy and objectives aimed at achieving customer satisfaction.

Said resources are competent and adequately trained staff, support information and IT systems, infrastructures, the working environment and the technologies used.

Every year, the company management makes available in the corporate budget the resources necessary for the management and evolution of Business Continuity.

7.2 Competence

The company management believes that the competence and training of the staff are critical factors in the achievement of customer satisfaction.

The specific competences have been defined in the system of roles pertaining to all professional profiles, including those profiles that directly influence the quality of services and products.

The needs for managerial training are defined on a yearly basis according to the business guidelines and then translated into a training plan the effectiveness of which is assessed through suitable tests or certifications, where provided for, or in the training assessment forms.

7.3 Awareness

In order to strengthen and spread the Business Continuity culture within the company it is necessary for the BCMS to be seen as a key value for the company itself and to be sponsored by the top management.

The competences necessary for the management of Business Continuity are acquired through activities of:

- Awareness (training and information);
- Drills (tests).

Awareness

The success of the Business Continuity process also depends on employees' awareness of the processes and services in addition to the activities to be carried out to guarantee their continuity.

To this end, SIA has set up an ongoing training and information process (Awareness) aimed at promoting awareness regarding the importance of the BCMS among the staff.

Annually SIA draws up and performs the Business Continuity Awareness Program composed of at least 6 training sessions each year in dedicated training rooms, aimed at all the personnel and more specifically at the Business Continuity staff, which include both the management staff in charge of updating the plans and the operative staff who must perform the various activities indicated by the plans themselves.

Drills

Training activities are also performed through Business Continuity and Disaster Recovery tests planned and carried out at regular intervals.

Through the Business Continuity drills, SIA assesses the competence level of the Business Continuity Management Teams and the effectiveness of the awareness program.

7.4 Communication

During an emergency or crisis, the management of the communication process, both internal and external, is vital.

Each Department, supported by the Communication Department, is responsible for the communication process with customers during an emergency or crisis.

The Communication Department must also oversee the communication strategy to be adopted towards the media, interacting with the media themselves in a proactive manner or responding to their specific requests and drawing up the standard messages to be distributed to the external stakeholders.

7.5 Documented information

All the Business Continuity Management System (BCMS) documentation is files in electronic format in the document system *Sharedocs* in libraries containing the corporate documentation, the documentation of the departments, and the operative documentation used for the restoration of services.

In order to make Business Continuity and Disaster Recovery documentation immediately available in crisis situations, there are cabinets containing electronic or paper-format copies of said documentation both at the primary site and at the DR sites.

As far as the maintenance of the system is concerned, SIA has a process to update the documentation thanks to which each change, internal and external, which has an impact on the company, is acknowledged as part of the Business Continuity/Disaster Recovery management.

In addition, SIA carries out on a regular basis or in the case of significant variations, a revision of the entire Business Continuity Management System (BCMS) to guarantee its compliance and adequacy with regard to regulatory, organizational, strategic and legislative changes.

8. OPERATION

For SIA, managing Business Continuity means:

- guiding the choices in emergency and crisis situations;
- defining the plans, procedures and technical, human and logistical resources, to ensure Business Continuity to the company in emergency and crisis situations;
- reacting promptly to reduce the interruption time of the business processes and guarantee their effective restoration.

8.1 Operational planning and control

SIA carries out its activities in complex and highly competitive environments, supplying services that can have an impact on the entire domestic and international credit-finance system. For this reason, full compliance with the requirements of business continuity deriving from the relevant regulations, the requirements set out by the Supervisory Authorities and the contracts with customers are of fundamental importance.

To achieve this objective, SIA operates in compliance with the appropriate methodologies, best practices and international standards, producing and keeping up-to-date the BIA and Risk Assessment, defining the Business Continuity strategy, the organizational, logistical and technological procedures and performing regular drills and tests as illustrated here below.

8.2 Business impact analysis and risk assessment

The aim of this activity is to promote the understanding of the company through the identification of its key services and critical activities. This analysis is aimed at guaranteeing that the Business Continuity management program is aligned with the corporate mission, the regulatory restrictions and the agreements with customers.

The pursuit of this objective is achieved through the execution of the following activities:

- Business Impact Analysis;
- Risk Assessment.

Business Impact Analysis

Business Impact Analysis (BIA) is the assessment of the impact on the business in the case of significant events that may compromise the company's activities and the supply of services. In order to direct appropriate Business Continuity solutions, the requirements necessary to restart the services are identified.

SIA produces the Business Impact Analysis with the aim of:

- listing the services pertinent to the company business;
- identifying the impacts related to the unavailability of the service;
- identifying the restoration times at contractual/regulatory level;
- identifying the most critical services;
- identifying which activities need to be restored at a later stage.

SIA Business Impact Analysis principally includes the analysis of the business services and the identification of the critical activities using the assessment parameters, which take into account restrictions at regulatory level, contractual ties with customers, the significance of the service/activity for the company's business, and the strategic significance of the service/activity for the company.

The BIA is updated with the information provided by the company structures involved and is made available to all Divisions and Departments for the preparation of the Disaster Recovery plans.

Risk Assessment

The activity of Risk Assessment is aimed at preventing and counteracting 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 aims to protect the value of the company, pursue the objectives of the company and manage the risks that could result in a loss of confidentiality, integrity, availability and compliance of corporate services/processes.

The SIA's Risks Management Process is inspired by ISO31000 standard and takes into account the provisions of Bank of Italy.

The process describes how the risks are identified, analyzed, evaluated, managed, monitored and updated and the related responsibilities.

The decision about the processing of identified risks, based on the assessment of the correct balance between compliance with the mandatory regulations and the business, cost, technology and security needs, is divided into the usual options of treatment of risks (mitigate, accept, avoid, transfer).

On the basis of the decisions made, the so-called Risk Processing Plan is drawn up, containing the measures that SIA has decided to adopt to deal with the risks identified.

SIA regularly updates its Risk Processing Plan, which is systematically monitored.

A risk analysis must be performed for each new initiative (project or job order) and for SIA's business services.

SIA regularly produces the document Physical Security Risks for each of its corporate sites and performs a risk analysis at Safety level in compliance with Law 81/08.
This activity is a global assessment and documents all the risks to the health and safety of workers present in the organization. Its aim is to identify adequate prevention and protection measures and to draw up a program of measures able to guarantee the improvement of health and safety levels over time.

8.3 Business continuity strategy

The objective of the Business Continuity system is to ensure that the corporate structure is able to develop plans, instructions and processes and that it makes available the rooms and equipment for the prompt management of incidents and crises.

The development and implementation of a Business Continuity response derive from the creation of a management model and of a structure for the management of the disaster event, in addition to Business Continuity and Disaster Recovery plans detailing the steps to take during and after an incident in order to maintain or restore operations.

The system must permit:

- confirmation of the nature and the extent of the incident;
- start up of an appropriate Business Continuity response;
- plans, processes and procedures for the activation, coordination, communication, management and closure of the emergency;
- the availability of the resources needed to support the incident management plans, processes and procedures;
- communication with the stakeholders and the main actors involved.

In order to be able to tackle an emergency and/or crisis situation in the best possible manner, SIA has developed:

- Organizational solutions;
- Logistics solutions and
- Technological solutions.

8.4 Establish and implement business continuity procedures

SIA has drawn up an *Emergency and Crisis Management Process* describing the methods for the activation, the responsibilities and the contacts necessary when managing an emergency and/or crisis situation in the company.

The figure below illustrates the flow of activation of the Business Continuity Management Teams and the persons responsible for disclosing information inside and outside the company.

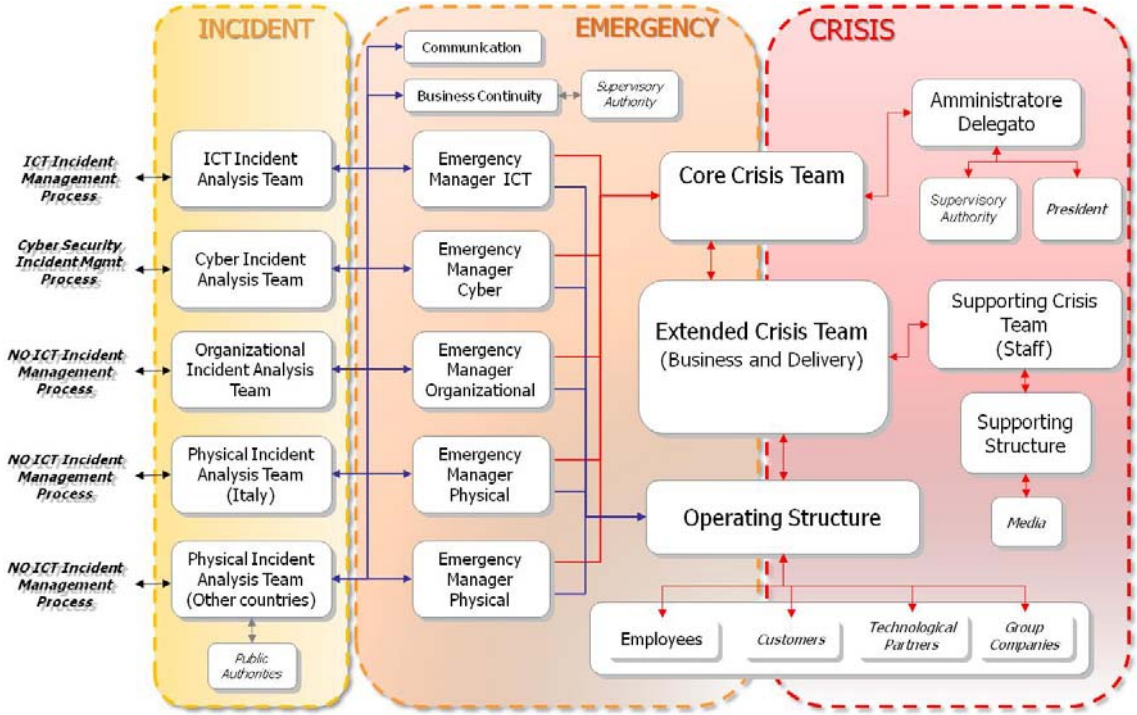


Figure 1 – Flow of the Emergency and Crisis Management Process

The Emergency and Crisis Management Process is made up of three phases: Incident, Emergency and Crisis.

The situations in the company that may lead to an emergency and/or crisis situation can essentially be subdivided into ICT, NON-ICT and Cyber categories, according to the type of event at the origin of the process within SIA.

The activation of the *Emergency and Crisis Management Process* is necessary when the event has risks and impacts of such a level of gravity that prevent it from being managed through the incident management procedures in place at the company.

The first phase (Incident) provides for the involvement of various Teams according to the type of event (ICT, NON-ICT of an Italian or foreign physical nature, NON-ICT of an organizational nature, Cyber).

ICT relates to all technology, applicative and operating aspects necessary for the supply of services.

NON-ICT are all the aspects relating to physical security, logistics and auxiliary equipment and the organizational aspects, such as problems concerning the personnel, legal issues, administration, Media, etc.

The activities to be implemented and the related responsibilities in case of an emergency requiring the evacuation of the building or of certain areas in order to protect the safety of people are described in specific documents.

The following are the macro scenarios managed and examples of events that can cause them.

	MACRO-SCENARI	Possibili Cause
ICT	HW failure	Failure in a server or ICT HW infrastructure (i.e. virtualization)
	Service halt	Failure in a system/service automatic procedure
	Total unavailability of a supply site - 1	Systems hang as a consequence of NON ICT Physical event Failure of multiservice technological infrastructure (i.e. SAN, LAN)
NO ICT Physical	Total unavailability of a supply site - 2	Power failure Conditioning failure Fire Overflows/Flooding Earthquake Structural failure / Collapses Bomb threats Chemical accident
	Partial unavailability of a supply site	
	Total or partial unavailability of the Offices	
NO ICT Organiz.	Unavailability of staff	Pandemic situation Public transport strike Socio-Political demonstrations/protests
	Inability to reach or inaccessibility of Offices	Overflows/Flooding Heavy snowfall Socio-Political demonstrations/protests
Cyber	Computer fraud	Exploit of software vulnerabilities to make fraudolent operations Use of stolen credential
	Attacks on availability (DoS)	Overloading of network devices or servers with spam traffic
	Information theft	Actions performed by unfaithful Employees, hackers, activists Use of malicious software (virus, worm, trojan) to infect organisation's computer
	Data modification / defacing	
	Blocking / malfunctions	

The natural continuation of the Emergency and Crisis Management Process is the Business Continuity Plans (BCP) produced by each Division/Department.

The BCPs describe the organizational procedures that each Division/Department must follow in order to restore and control its services.

More specifically, the BCPs describe:

- the possible disaster scenarios;
- the management of contacts and communications during emergencies or crises (internal resources, suppliers, customers, subsidiary companies);
- the possible containment and/or contrast actions for each scenario;
- reference documentation for each service.

The Business Continuity Plans also include the names of the members of the Operating Structure

or of the Supporting Structure of the relevant Division/Department.

The Disaster Recovery Plans are a set of documents drawn up for each individual infrastructure and describe the methods and time frame for reactivation at the Disaster Recovery site.

In order to be able to manage any emergencies or crises in the best possible manner, SIA has identified a Disaster Recovery site located outside the urban area and Business Continuity rooms at the company's premises.

As far as logistics solutions are concerned, the SIA office buildings have been equipped with rooms that can quickly be transformed into Business Continuity rooms. Said rooms are reserved for Directors and/or the staff of the Organizational Units who need a shared space from which to perform their respective activities.

The supply of services in Disaster Recovery mode is guaranteed by dedicated hardware, software and connectivity solutions and by the availability of adequately trained internal personnel.

Prevention, monitoring and control systems have been set up to tackle events relating to IT and logistics terrorism.

The technology solutions guarantee the interconnection between the sites and logical remote access to the sites themselves. The DR site has technology platforms possessing a processing capability equal to that of the primary site. The hardware equipment is either redundant or is *fault tolerant* in order to ensure the DR requisites of the services. The DR architectural solutions adopted permit the realization of specific types of configuration of the technology infrastructure, in order to meet the service SLAs and comply with the directives of the Institutions.

In order to improve efficiency and business continuity of services, for many SIA infrastructures, the setup based on a primary site and a secondary site (or DR site) is evolving towards a setup based on two equal sites, in which a number of services are supplied simultaneously from the two sites while others are supplied by one site but, when necessary, can be activated on the other.

The architecture of the local network, of the geographical network SIANet.NG and of access to the telephone network has been designed and created to guarantee the same level of reliability and the same sizing of the network present at the production site. The primary site and the DR site are connected via dedicated fiber optic cables with diversified paths and suppliers.

Specific maintenance contracts with adequate SLAs regarding the timeframe of intervention or solution have also been entered into.

All the data necessary for the activation of systems and services in DR mode are replicated in the secondary site as "synchronous" or "consistent asynchronous" thus allowing for a Recovery Point Objective (RPO) that varies from zero to several minutes according to the contractual SLAs and performance requisites defined.

Involvement of the customers

The complete realization of Business Continuity must include the development of a direct collaboration with the customers which, in turn, makes it possible to analyze, define and implement all the joint measures for the management of the crisis and the restoration of services and of support technologies such as, for example, lines, security equipment and connection to the International Circuits.

To this end, SIA agrees with its customers methods of mutual collaboration, such as: the definition of RTOs and RPOs, the connections to be used in case of disaster events, the persons to be contacted for general communications, the activities to be performed in case of activation of the technical-applicative infrastructure at the Disaster Recovery site, and the planning of tests.

Furthermore, specific contractual agreements regulating the positions of the counterparts have been stipulated.

8.5 Exercising and testing

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

SIA regularly performs Business Continuity and Disaster Recovery tests and drills, which may be of the following types:

- **Organizational** (for example: Tests of the Emergency Management Process, tests of the Business Continuity Plans, etc.);
- **Logistical** (building evacuation drills);
- **Technological** (Disaster Recovery tests).

In its role as a Qualified Infrastructure, SIA also takes part in tests of a systemic nature organized by the CODISE group of Banca d'Italia.

The Business Continuity tests are performed to assess the effectiveness and efficiency of the Emergency Management Process, to verify the adequacy, completeness and working of the Business Continuity Plans and the support procedures, to assess the competence of the Business Continuity management teams and the effectiveness of the awareness program and to develop and spread knowledge and awareness on Business Continuity issues within the company.
The Disaster Recovery tests are necessary to assess the working and effectiveness of the technology infrastructures and to keep the skills of the persons involved up-to-date.

The *Emergency and Crisis Management Process* tests (also called Call Tree test) are performed once a year, moreover on an annual basis, SIA updates the multi-year plan of Business Continuity Tests and Disaster Recovery Tests.

9. PERFORMANCE EVALUATION

9.1 Monitoring, measurement, analysis and evaluation

SIA measures the performances of the following Business Continuity activities:

- BC and DR tests;
- awareness;
- internal inspections;
- documentation management.

The performance indicator of the BC and DR tests is the Severity Code assigned to the tests performed.

The performance indicator of the Awareness activity is the degree of coverage of the members of the BC management team.

The performance indicator of the Internal Inspections activity is the degree of coverage of the Departments and Divisions.

The performance indicator of the documentation management is the number of documents updated out of the total of BCMS documents.

The objectives relating to the indicators described above are monitored in the Management

Review.

9.2 Internal audit

In order to pursue the continual improvement of the BCMS, SIA regularly performs a revision of its system in order to assess the effectiveness, efficiency and adequacy of the BCMS itself and of the related policies, strategies and objectives, in addition to identifying any needs for adjustment, carrying out suitable corrective and improvement actions.

The system review activity is implemented by:

- Business Continuity Inspections;
- The Management Review.

On an annual basis, SIA prepares the Business Continuity Inspections Plan and performs the Internal Inspections.

The results of the Business Continuity Inspections are documented and reviewed with the heads of the company units subject to inspection with the aim of agreeing on a plan of corrective actions of dealing with any points of non-compliance found.

If deemed appropriate, the corrective actions defined to solve any irregularities found during the Internal Inspections may be monitored in the BC/DR Committee.

9.3 Management Review

The Management Review, performed regularly, has the objective of assessing the degree of adequacy of the Business Continuity Management System following the evolution of the rules and requirements expressed in the relevant standards and regulations and of identifying specific activities aimed at guaranteeing its maintenance.

10. IMPROVEMENT

10.1 Non conformity and corrective action

During the performance of the activities related mainly to the BIA, the Tests, the Inspections and the Audits (both external and internal), areas of Non-conformity may arise and therefore the necessity to identify appropriate Corrective Actions may be found.

A Corrective Action is an action designed to eliminate the cause of a Non-conformity and prevent its reoccurrence.

The Corrective Actions identified may be included and monitored, if deemed appropriate, in the BC/DR Steering Committee, in the Committee with the Top Management and in the Management Review.

10.2 Continual improvement

SIA undertakes to improve continually its BCMS using as a guide the Business Continuity policies, the Business Continuity objectives, the results of the Business Continuity Inspections, the data analysis, the corrective actions and the Management Reviews.

This objective is pursued by systematically analyzing the indicators and objectives defined and performing the Management Review with particular attention to:

- the results of the data analysis;
- the outcomes of the inspections;
- the performances of the processes and services;
- the status of achievement of the objectives of the individual Organizational Units;
- the previous Management Reviews;
- the improvement actions underway.

On the basis of the data collected and the causes identified, the improvement actions are agreed, identifying the person responsible, the timescales and the resources necessary.

GENERAL INFORMATION

Acronyms

Acronym	Complete wording
BC	Business Continuity
DR	Disaster Recovery
BCP	Business Continuity Plan
BCMS	Business Continuity Management System

References

1. BS ISO 22301:2012 – Societal Security - Business Continuity Management Systems – requirements
2. ISO/IEC 27001:2013 - Information security management systems
3. Banca d'Italia - Linee guida in materia di continuità operativa per le infrastrutture dei mercati finanziari

Index of figures

APPENDIX

Source: ISO 22301:2012 Societal security – Business Continuity Management Systems – Requirements.

Term	Definition
Business Continuity (BC)	Capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident.
Business Continuity Management (BCM)	Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business Continuity Management System (BCMS)	Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity. NOTE The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes and resources.
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.
Business Impact Analysis (BIA)	Process of analyzing activities and the effect that a business disruption might have upon them.
Incident	Situation that might be, or could lead to, a disruption, loss, emergency or crisis.
Infrastructure	System of facilities, equipment and services needed for the operation of an organization.
Recovery Point Objective (RPO)	Point to which information used by an activity must be restored to enable the activity to operate on resumption. NOTE Can also be referred to as "maximum data loss".
Recovery Time Objective (RTO)	Period of time following an incident within which: — product or service must be resumed, or — activity must be resumed, or — resources must be recovered. NOTE For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.
Risk Assessment (RA)	Overall process of risk identification, risk analysis and risk evaluation.
Stakeholder	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity. NOTE This can be an individual or group that has an interest in any decision or activity of an organization.