

# Company Management System

## Company Governance and Guidelines

Written by:

Verified by:

Approved by:

*The document is:  
**WRITTEN** if contains the writer's signature,  
**VERIFIED** if also contains the verifier's signature,  
**APPROVED** if contains all the signatures*

Document Code

1-CMS-2009-017-06

*Company–Project/Service–Year–Doc. number–Version*

Classification

Public

Application Domain

SIA-SSB



---

## COVER KEY

### Document Status

The signatures on the cover sheet of this document refer to the SIA-SSB Spa internal standard for company document management: they serve to ensure the control of the document's configuration and indicate its working status.

Specifically, the document is understood to be **WRITTEN** if it bears the author's signature; **VERIFIED** if it bears the verifier's signature; and **APPROVED** if it bears the signature for approval.

A document lacking signatures is in draft form.

*It is noted that the signature for approval authorises the dissemination of the document, limited to the distribution list.*

### Classification

**A document may be classified as follows:**

- **PUBLIC**, if the document may be disseminated without restriction;
- **INTERNAL**, if the document may be disseminated only within SIA-SSB;
- **CONFIDENTIAL**, if the document may only be distributed to a limited number of recipients;
- **STRICTLY CONFIDENTIAL**, if the document may only be distributed to a limited number of recipients and each copy is controlled;

### Application Domain

SIA-SSB Group companies to which the document applies:

**SIA-SSB GROUP** if the document is valid for all companies controlled by the Group

**SIA-SSB, KEDRIOS, RA COMPUTER, TSP, SINSYS, PERAGO, GBC,...**

**...ALL GROUP COMPANIES ...**

---

## VERSION HISTORY

This Reference Manual, firstly published in November 2007 for the new SIA-SSB company, has been completely updated; in particular Quality, Information Security and Business Continuity High-Level Policy have been updated.

## TABLE OF CONTENTS

|   |           |
|---|-----------|
| <b>1. APPROACH AND MANAGEMENT</b> .....                       | <b>6</b>  |
| <b>1.1 Company Presentation</b> .....                         | <b>6</b>  |
| <b>1.2 Application scope</b> .....                            | <b>8</b>  |
| <b>1.3 Exclusions</b> .....                                   | <b>8</b>  |
| <b>1.4 Glossary of terms</b> .....                            | <b>9</b>  |
| <b>1.5 Regulatory References</b> .....                        | <b>9</b>  |
| <b>1.6 SIA-SSB’s Mission and Responsibilities</b> .....       | <b>10</b> |
| <b>1.7 Organisational Structure</b> .....                     | <b>10</b> |
| <b>1.8 Business Process System</b> .....                      | <b>10</b> |
| 1.8.1 Business Processes.....                                 | 11        |
| 1.8.2 Governance Processes.....                               | 11        |
| 1.8.3 Support Processes.....                                  | 11        |
| <b>1.9 SIA-SSB Management responsibilities</b> .....          | <b>13</b> |
| <b>1.10 SIA-SSB High – Level Policy</b> .....                 | <b>13</b> |
| 1.10.1 Quality Policy.....                                    | 13        |
| 1.10.2 Security Policy.....                                   | 15        |
| 1.10.3 Business Continuity Policy.....                        | 15        |
| <b>1.11 Personnel fulfilments</b> .....                       | <b>15</b> |
| <b>1.12 SIA-SSB Management System</b> .....                   | <b>16</b> |
| 1.12.1 The Quality Management System.....                     | 16        |
| 1.12.1.1 Planning.....  | 16        |
| 1.12.1.2 Objectives.....                                      | 16        |
| 1.12.1.3 Management.....                                      | 16        |
| 1.12.1.4 Quality Management Representative.....               | 16        |
| 1.12.1.5 Customer Care.....                                   | 16        |
| 1.12.2 The Information Security Management System (ISMS)..... | 17        |
| 1.12.3 The Business Continuity Management System (BCMS).....  | 18        |
| <b>1.13 Management Review</b> .....                           | <b>19</b> |
| 1.13.1 Quality Review.....                                    | 19        |
| 1.13.2 Information Security Management Review.....            | 20        |
| 1.13.3 Business Continuity Management Review.....             | 21        |
| <b>2. THE PROCESSES SYSTEM</b> .....                          | <b>22</b> |
| <b>2.1 Business Processes</b> .....                           | <b>22</b> |
| 2.1.1 Sales Process.....                                      | 22        |
| 2.1.2 Contract Management Process.....                        | 22        |
| 2.1.3 Feasibility Process.....                                | 23        |

|            |  |           |
|------------|--|-----------|
| 2.1.3.1    | Requirements Review .....  | 23        |
| 2.1.4      | Service & Product Development Process .....                                  | 23        |
| 2.1.4.1    | Processes Related to the Customer .....                                      | 23        |
| 2.1.4.2    | Design and Development Planning .....  | 24        |
| 2.1.4.3    | Input of Design and Development.....   | 24        |
| 2.1.4.4    | Output of Design and Development.....  | 25        |
| 2.1.4.5    | Design and Development Review .....  | 25        |
| 2.1.4.6    | Design and Development Testing.....  | 25        |
| 2.1.4.7    | Design and Development Validation .....                                      | 25        |
| 2.1.4.8    | Design and Development Change Control .....                                  | 26        |
| 2.1.5      | Service Management Processes .....   | 26        |
| 2.1.5.1    | Control of Activities for Service Production and Delivery.....               | 26        |
| 2.1.5.2    | Validation of the Delivery Process .....                                     | 27        |
| 2.1.5.3    | Identification and Traceability.....   | 27        |
| 2.1.5.4    | Customer Property.....   | 27        |
| 2.1.5.5    | Products Maintenance.....  | 27        |
| 2.1.5.6    | Management of Monitoring and Measuring Devices .....                         | 27        |
| <b>2.2</b> | <b>Governance Processes .....</b>  | <b>28</b> |
| 2.2.1      | Quality .....  | 28        |
| 2.2.2      | Security.....  | 28        |
| 2.2.3      | Business Continuity .....  | 28        |
| 2.2.4      | Project Control Methodology.....   | 28        |
| <b>2.3</b> | <b>Support Processes .....</b>   | <b>30</b> |
| 2.3.1      | Legal.....   | 30        |
| 2.3.2      | Human Resource Management .....  | 30        |
| 2.3.3      | Supply.....  | 30        |
| 2.3.3.1    | Supply Process.....  | 31        |
| 2.3.3.2    | Vendor Management Process.....   | 31        |
| 2.3.4      | Facilities .....   | 32        |
| 2.3.4.1    | Infrastructure.....  | 32        |
| 2.3.4.2    | Work Environment.....  | 32        |
| 2.3.5      | Communication and Image.....   | 33        |
| 2.3.6      | Administration.....  | 33        |
| <b>2.4</b> | <b>Relationship between Business Processes and Security Guidelines .....</b> | <b>34</b> |
| <b>3.</b>  | <b>MONITORING AND CONTROL.....</b>   | <b>36</b> |
| 3.1        | The Quality Management System.....   | 36        |
| 3.1.1      | Customer Satisfaction .....  | 36        |
| 3.1.2      | Internal Quality Inspections.....  | 36        |

|            |  |           |
|------------|--|-----------|
| 3.1.3      | Monitoring and Measuring Processes, Products and Services .....    | 36        |
| 3.1.3.1    | Monitoring and Measurement .....                                   | 36        |
| 3.1.3.2    | Data Analysis .....  | 36        |
| 3.1.3.3    | Non-Compliance Management .....                                    | 37        |
| 3.2        | The Information Security Management System .....                   | 37        |
| 3.2.1      | ISMS Monitoring.....   | 37        |
| 3.2.2      | Security Inspections.....  | 38        |
| 3.3        | The Business Continuity Management System.....                     | 39        |
| 3.3.1      | BCMS Monitoring .....  | 39        |
| 3.3.2      | Business Continuity Inspections .....                              | 40        |
| 3.4        | Continuous Improvement.....  | 40        |
| <b>4.</b>  | <b>THE DOCUMENT SYSTEM (CMS) AND DOCUMENTATION MANAGEMENT.....</b> | <b>42</b> |
| <b>4.1</b> | <b>General Requirements .....</b>                                  | <b>42</b> |
| <b>4.2</b> | <b>Documentation Requirements .....</b>                            | <b>42</b> |
| 4.2.1      | General Information .....  | 42        |
| 4.2.2      | Company Governance and Guidelines.....                             | 43        |
| 4.2.3      | Documents Control .....  | 43        |
| 4.2.4      | Records Control.....   | 43        |

---

## 1. APPROACH AND MANAGEMENT

### 1.1 Company Presentation

Created by the merger between **SIA** (Società Interbancaria per l'Automazione) and **SSB** (Società per i Servizi Bancari) in May 2007, is one of the leaders in Italy and among the top companies in Europe offering complete and integrated services in the areas of:

**Debit and Credit Card Processing** with full processing services, and system and accessory services.

#### Payment cards framework

According to experts and industry analysts, the European market for payment cards presents interesting growth opportunities, mainly due to the expansion of the Euro zone and the resulting growth in the Eastern European market.

The possibilities for payment volume growth represent an enormous opportunity for the banking industry. Market operators must improve efficiency levels, reduce costs and increase volumes in order to compete in the new scenario that will be created by 2010 under SEPA (Single Euro Payment Area).

Based on current trends of aggregation and consolidation in the banking industry, it is important to respond quickly to the challenges presented by SEPA: in fact, only those operators that are able to reach a European size, create economies of scale and, at the same time, innovate using the most advanced technologies will survive.

The SIA-SSB Group, due to its professional skills and experience gained over the years, is able to offer – through its SINSYS subsidiary – processing, issuing and acquiring services to manage national, international and private payment cards, guaranteeing competitive prices and high service levels.

Our current geographic coverage includes Italy and 8 other countries: Belgium, Germany, Netherlands, Poland, Czech Republic, Slovakia, Ukraine, and Hungary.

**Payment Systems** with clearing, corporate banking and interbank services, solutions for central and commercial banks, and system services.

#### Payment systems framework

The European Parliament's recent approval of the PSD (Payment Services Directive) initiates a process that will completely change the European payments system, through the creation of the SEPA (Single Euro Payment Area).

In the payment systems area, the SIA-SSB Group has an integrated offer that will satisfy the needs of commercial and central banks, businesses and government agencies.

The Group offers itself as a **banking system partner** to meet the challenges of **SEPA**, with the **efficiency and range of service** characteristics of a market leader at the European level.

Furthermore, the SIA-SSB Group is able to offer a complete range of solutions to meet the needs of continuous improvement in effectiveness and efficiency in banking **back-office** processes, drawing on its experience as a leading player in the **central clearing and settlement systems**.

**Central banks** can benefit from the Group's know-how in solutions for wholesale payment management to support the process of development and improvement of payment systems.

Companies can optimize their **treasury and supply chain management** processes required for SEPA and for changes in **Corporate Banking**, with the integrated offer of services and solutions capable of meeting the needs of national companies as well as large international groups.

SIA-SSB Group supports **government agencies** in **automating payment systems** both centrally and locally, with benefits in terms of efficiency and service quality for end users.

**Capital Markets** with market platform management services, securities back-office and financial information system, surveillance solutions for financial intermediaries, access systems to fixed income markets

### Capital markets framework

Particularly in recent years the European financial markets integration process is experiencing significant changes, with positive acceleration and considerable commitment from EU Institutions and Members to create a common regulatory framework with equity, efficiency and transparency criteria which will safeguard investors and competition.

The **MiFID** (Markets in Financial Instruments Directive) regulation was developed as part of this initiative, with the objective of **governing services and financial markets** and will lead to the design of the **new European Financial Market**. The process began in 2000 under FSAP - Financial Service Action Plan, and has already starting generating **epic changes in financial market operations** through the Prospectus and Market Abuse directives.

SIA-SSB's Capital Markets BU continues to support the evolution of the European economic system through its **interactions with key players** in financial markets as well as European and Italian institutions by proposing a **new integrated offer** of technology solutions, able to support market operators in **adapting to regulatory changes**.

This offer, in cooperation with other Group companies, anticipates the **significant changes** such as the expiration of the **concentration requirement for exchange of shares**, **"best execution"** certainty and more stringent requirements for **pre- and post-trade transparency**, that require financial operators to integrate, consolidate and confront, in an efficient and timely manner and at sustainable costs, the multiple information flows related to investment transactions with a growing need to **excel in the execution process**.

**Network Services** for connectivity and value-added data transfer services.

### Network services framework

The financial community's operations are based on the continuous transmission of a large amount of data between commercial and central banks, debit and credit card processors, stock markets, content management systems, information services providers and traders.

SIA-SSB Group is the **primary provider of connectivity services** and **value-added data transfer services** for the Italian banking and financial system and is one of the leaders in Europe.

The Group offers a **unique technology infrastructure of integrated networks** that meets the most complex needs, surpassing the traditional separation of the connectivity offer (typical of telecommunications providers) from that of the value-added data transfer services offer.

Due to its exclusive **"peer-to-peer"** network architecture, it is possible to transfer data in total security, ensuring **compliance with data confidentiality regulations**.

The numbers are the best evidence of the high reliability and performance of the network infrastructure: in 2006, through more than **600 network gateways** and **1,200 connections**, over **8 terabytes of data** (or 8 thousand billion bytes) were transferred for a total of **6.7 million transfer transactions**, **476 million messages sent** and **290 million transactions carried out**.

Furthermore, the network was designed to support the volumes required by **SEPA** and the new **Interbank Corporate Banking services**.

More than 20 years after the development of the Italian National Interbank Network (RNI), the infrastructure currently connects **more than a thousand financial institutions**, is integrated with the **Italian Public Connectivity System (SPC)** and with **SWIFT**, the international network for financial markets and payments.

**Globalisation** is the key factor that guides the development of the Group: it allows us to respond effectively, in a timely manner, and with knowledge and expertise as the primary technology provider of payment clearing platforms, to the profound changes brought about the SEPA Directive – the Single Euro Payments Area - and MiFID Directive– Markets in Financial Instruments Directive.

The SIA-SSB Group consists of the parent company SIA-SSB and the subsidiaries Kedrios, Perago, RA Computer, SiNSYS, TSP and GBC.

## 1.2 Application scope

The scope of the current Quality, Security and Business Continuity Systems is:

**Conception, design, development, selling and provision on card processing services on national/international networks, electronic payment systems, products, information and technological systems connected with banking, financial and market sectors, also of institutional service, networking services and technological infrastructures for financial market operators.**

## 1.3 Exclusions

There are no exclusions to the application scope related to SIA-SSB S.p.A. activities.

## 1.4 Glossary of terms

| Term                     | Description  |
|--------------------------|--|
| BCMS                     | Business Company Management System   |
| CMS                      | Company Management System  |
| Customer                 | Organisation or person that receives a product   |
| Effectiveness            | Degree of implementation of planned activities and achievement of planned results  |
| Efficiency               | Ratio between the results achieved and the resources used to obtain the results  |
| Organisational Structure | Set of responsibilities, authorities and interrelationships between individuals  |
| Process                  | Set of related or interacting activities that transform input into output  |
| Product                  | Result of a process  |
| Project                  | Single process that consists of a set of coordinated and controlled activities, with start and end dates, undertaken to achieve an objective conforming to specific requirements, including time, cost and resource limits |
| Supplier                 | Organisation or person that supplies a product   |

This section includes certain definitions from ISO 9000:2005. For other terms, please refer to the specific reference documents.

## 1.5 Regulatory References

|                             |  |
|-----------------------------|--|
| Legislative Decree 231/2001 | Administrative liability of companies                                |
| Legislative Decree 81/08    | Measures to protect worker health and safety                         |
| Legislative Decree 196/2003 | Code on protection of personal data – Privacy code                   |
| UNI EN ISO 9000:2005        | Quality Management Systems – Fundamentals and Definitions            |
| UNI EN ISO 9001:2008        | Quality Management Systems - Requirements                            |
| UNI EN ISO 9004:2000        | Quality Management Systems – Guidelines for performance improvements |
| ISO 27001:2005              | Information Technology – Security Techniques                         |
| BS 25999-1.2006             | Business Continuity Management – Part 1: Code of practice            |

BS 25999-2:2007

Business Continuity Management – Part 2: Specification

## 1.6 SIA-SSB's Mission and Responsibilities

The demand for quality, security and continuity in production processes, products/services, decisional and administrative procedures and customer support constitutes an important element in development and competition for today's companies.

SIA-SSB has implemented a **Company Management System (CMS)** with the aim of increasing customer satisfaction, improving internal processes and the quality and security level of services, by adopting international reference standards recognised on a global level.

Compliance with these standards is certified by the achievement of [ISO 9001:2008](#), [ISO 27001:2005](#) and [BS 25999-2:2007](#) for conception, design, implementation, marketing and delivery of:

- Card processing services on national and international circuits
- Electronic payment systems and services
- Information products and services to support banking, credit and financial market operations, including institutional operations
- Network services and technology platforms for transmitting data related to financial activities

Within the scope of **Group Governance** and in addition to business certifications, SIA-SSB has also obtained [ISO 9001:2008 Corporate](#) certification, to give greater visibility to the overall skills that all companies of the Group can offer to the market.

## 1.7 Organisational Structure

SIA-SSB is organised into Departments which have the responsibility of the company's business, designing and delivering products and services, and in Staff Departments for all business support activities.

## 1.8 Business Process System

CMS is a set of processes, methodologies, procedures and responsibilities that provides the organisational reference to SIA-SSB's operating units, from conception to supply of services and products.

All CMS processes are:

- developed by Organisation and Quality together with the other business departments involved
- verified with the applicable business departments
- approved by General Management
- published by Organisation and Quality

The CMS system is constantly updated and improved to reflect customers' needs and the organisational requirements of the company.

In order to achieve this objective, the company has:

- identified the main, or Business, processes
- identified the Governance processes
- identified the Support processes
- established the sequence and interactions among these processes
- defined the measurement criteria to verify the effectiveness of processes
- ensured that the necessary resources are available to guarantee the correct functioning of the processes
- prepared checkpoints to verify if the processes have achieved the expected results and if they may be improved.

SIA-SSB ensures control on outsourced processes which may have effects on product requirements compliance.

The Company Management System defines the methods for controlling outsourced processes.

In particular, all external suppliers, including companies within the Group, are governed by contracts that define the methodology for delivering service and the service level agreement.

The company has defined its processes, differentiating between business, governance and support processes.

### **1.8.1 Business Processes**

The general map of SIA-SSB business processes indicates how the Company Management System is integrated and interacts with the primary processes that make up the business of SIA-SSB, specifically:

- sales process
- contract management process
- feasibility process
- service & product development process
- service management processes (incident management, problem management, change management, release management, configuration management, SLA management, availability & continuity management.....)

### **1.8.2 Governance Processes**

The governance processes, fundamental to defining business objectives and verifying their achievement, are identified as follows:

- Quality
- Security
- Business Continuity
- Project Control

### **1.8.3 Support Processes**

The support processes, essential to the functioning of the business processes, are identified as follows:

- legal (contract management, ...)

- human resource management (education and training management, recruiting management, selection and hiring of personnel,...)
- purchasing (supply management, vendor management,...)
- facilities (access management,...)
- communication and image
- administration (customer accounting, supplier accounting, financial statements,...)

## 1.9 SIA-SSB Management responsibilities

SIA-SSB Management commits to:

- communicating to all partners that the respect for Customer requirements and the related legal requirements must always be our first consideration
- defining the Quality Policy, the Security Policy and the Business Continuity Policy and communicate them to all personnel so that the stated objectives may be reached and the necessary resources may be made available
- appointing a Quality Management Representative
- assigning to managers responsibilities related to the business and to the company goals
- ensuring that updates and changes to the processes are communicated to all personnel throughout the organisation
- ensuring specific training sessions if significant changes to CMS occurs.

## 1.10 SIA-SSB High – Level Policy

SIA-SSB considers Quality, Information Security and Business Continuity an essential elements for the protection of its information assets and a strategic factor, such as competitive advantage within the national and international market position and in the delivery provided services.

The excellence of its services delivery and customer satisfaction are attained by ensuring efficiency and reliability of services provided through the company processes system and also through the adoption of Security and Business Continuity solutions developed in compliance with relevant international best practices.

SIA-SSB has decided to develop the Quality Policy, the Security of Information Policy and the Business Continuity Policy because considers their implementation to be essential in relationships with customers, suppliers, group companies and shareholders. These policies allow to answer appropriately to the needs of customers and the requirements of market and to achieve business goals, through the guarantee of an adequate processes system and an adequate information security level consistent with laws, regulations and requirements stated by the Supervisory bodies.

### 1.10.1 Quality Policy

Company management has established and distributed to all personnel the Quality Policy, which includes:

- A satisfaction guarantee for customer requirements, in terms of external organisations which may provide services and internal structures that contribute to the effective and efficient fulfilment of said requirements.
- The continuous improvement of business processes through measuring and monitoring systems, both internal and external, in comparison with a benchmark market.
- The recognition and response by the corporate organisation to system regulations which were established according to a vision of processes based on quality requirements, consistent with international ISO 9001:2008 standards.
- Behavioural and technical education that is organised to guarantee a level of professionalism that can ensure customer satisfaction.
- Periodic review of the policy, in conjunction with the revision of the corporate strategic plan, in order to

ensure continued satisfaction of customer and market needs.

### 1.10.2 Security Policy

SIA-SSB has developed an Information Security Management System according with the rules and criteria prompted by the referential best practices and international standards (ISO27001) in order to address the issues of security, monitoring compliances, identifying risk areas and deal with risks in an appropriate way.

In particular, SIA-SSB has developed the Information Security Management System in order to ensure the fulfilment of the basic security requirements, such as:

- Confidentiality, which is the data' s property of being known only to those who are authorized
- Integrity, which is the data' s property of being modified only by those who are authorized
- Availability, which is the data' s property of being accessible and usable when required by the authorized processes and users
- Compliance, which is the data' s property of being treated in accordance with the referential laws and regulations.

The Company management undertakes to pursue the objectives of this policy with the appropriate resources and means.

### 1.10.3 Business Continuity Policy

SIA-SSB considers the Business Continuity an essential element for the provision of its own services consistent with customer agreements, Bank of Italy's Guidelines and, in general, with the referential methodologies and international standards.

In particular, SIA-SSB has established a Business Continuity Management System which includes the rules of behaviour, the processes, the command chain and the technological and logistics infrastructures of the Disaster Recovery for the emergency management, in case of events that may affect the continuity of the business.

Business Continuity Policy, defined by Company Management and released to SIA-SSB personnel, is based on the following principles:

- Adoption of a Business Continuity model recognized as a valuable reference in international context (SIA-SSB has adopted the BS25999 and the BCI – Business Continuity Institute methodology)
- Definition of the Business Continuity objectives for the various services in line with the customer agreements and the requirements stated by the Supervisory bodies
- Identification of technical and organizational solutions in line with the organization's economic compatibility
- Establishment of a Business Continuity multi-annual plan that provides repeated exercises and tests to ensure the verification of adequacy and continuous updating of the adopted solutions.

### 1.11 Personnel fulfilments

All personnel working in SIA-SSB, internal and external, due stick to the following rules:

- know the contents of the SIA-SSB High-Level Policies and help in implementing the directives and objectives set out in them
- develop and implement the Guidelines, Procedures and Operating Instructions on its own competence
- treat company information correctly

Any action that could endanger the SIA-SSB's, or customer's, or third parties' information security, is subject to the appropriate disciplinary action and / or legal advice.

## **1.12 SIA-SSB Management System**

### **1.12.1 The Quality Management System**

#### **1.12.1.1 Planning**

The Company Management defines and plans business objectives, in agreement with the various department managers. The objectives of the Quality System are formalised in the respective Policy, Management Review and Improvement Plans. The objectives are measurable and promote continuous performance improvement.

#### **1.12.1.2 Objectives**

Based on relevant organisational levels, analysis of data collected and information gathered from external sources (customers, suppliers, etc.) and results of process performance measurements, Company Management defines specific objectives consistent with the Quality Policy that are monitored and reviewed at established intervals based on their criticality.

#### **1.12.1.3 Management**

If an event occurs that influences the company organisation, such as, for example, organisational changes, acquisitions or divestments, process changes, changes in objectives, or results of internal audit controls, an impact analysis is performed on the system and appropriate actions are planned to preserve the effectiveness and efficiency of the system.

#### **1.12.1.4 Quality Management Representative**

The Quality Management Representative, having the authority and resources necessary to perform the role, and in cooperation with the Quality Manager, is responsible for:

- identifying and establishing the stages and interactions of the business processes in CMS, consistent with appropriate regulation and its application within the organisation
- ensuring that the necessary processes for CMS are established, implemented and updated
- establishing criteria and methods to ensure the effective performance and control of these processes through measurement, monitoring and analysis
- reporting to Company Management on CMS performance and on any improvement requirements
- ensuring the promotion of awareness of customer requirements across the organisation
- organising Management Reviews based on the established intervals
- prepare and implement Internal Inspection Plans.

#### **1.12.1.5 Customer Care**

Given the emphasis placed on meeting customer requirements (both explicit and implicit) and in order to monitor its achievement, Company Management has placed particular attention on the definition and control of business processes and measuring customer satisfaction, developing appropriate control tools such as the

Customer Satisfaction survey.

### 1.12.2 The Information Security Management System (ISMS)

As regards the Information Security Management System, the Company Management:

a) *identifies the primary security roles* within each business unit, determining an organizational structure to manage and implement information security. Furthermore:

- establishes a Security Committee, with the scope of determining the fundamental issues related to information security;
- identifies specific key roles in the area of information security within each BU/Department (e.g., Safety Manager).

b) *defines and distributes the information security policy for the ISMS system*, which establishes the objectives of the corporate ISMS System in terms of guaranteeing an adequate level of information security in the design, development and delivering of business services.

c) *defines and distributes the security guidelines of the ISMS system*. Specifically, at a minimum, the following security guidelines must be defined:

- Documentation Classification and Management
- Logical Access Control
- Intrusion Tests
- Separation of Processing Environments
- Security Education and Awareness
- Application and Technology Changes
- Use of Corporate Information Tools
- Use of Electronic Mail and Internet
- Physical Access
- Human Resource Behavioural Obligations
- Human Resource Selection
- Security Incidents
- Teleworking
- Information Back-up
- Managing Records
- Supplier Contracts

*All the employees must know and apply the Security Guidelines in performing their work tasks; in addition all*

*employees have the responsibility for the dissemination of the principles described within the Security Guidelines to its external partners and for verifying the application of the same.*

d) *defines a systematic approach to evaluating security risks*, or identifies a risk evaluation methodology that is suitable for the ISMS system, the business information as well as security, legal and regulatory requirements.

e) *defines a systematic approach for managing security risks*, based on the conclusions of the aforementioned risk evaluation. Regarding the criteria for risk management, the following options exist:

- mitigate the security risks by defining a security risk treatment plan that identifies the actions, responsibilities and priorities of intervention;
- knowingly accept the security risks
- avoid the security risks
- transfer security risks to third parties, i.e., insurers or suppliers

f) *defines a control process for security incidents in business services*, integrated with the security risk analysis process for business processes.

g) *defines a Security Key Indicators (SKI) system* integrated with the security risk analysis process for business processes.

h) *prepares periodic education programmes for security.*

### **1.12.3 The Business Continuity Management System (BCMS)**

As regards the Business Continuity Management System, the Company management:

a) *identifies the primary business continuity roles* within each business unit, determining two organizational structures, one to manage and implement the Business Continuity and the other one to manage crisis and emergency situations. Furthermore, it has been identified:

- Business Continuity and Disaster Recovery Committee
- The Interoperability Working group of Business Continuity (Referents of BC)

b) *defines and distributes the Business Continuity policy*, which states the objectives of the Business Continuity Management System, from which the Business Continuity Strategy, included in the Business Continuity Management, is determined. Business Continuity policy, also, states and releases the Guidelines in terms of operational continuity.

- c) promotes the understanding of the organization through the identification of its key services and the critical activities and resources that support them, carrying out Business Impact Analysis and Risk Assessment activities.
- d) develops and maintains updated plans, instructions and processes in order to be able to deal promptly with emergencies and crises and defines a documental system containing all predefined plans that detail how the organization manages any incident and continues its critical activities in case of disaster.
- e) prepares, at planned intervals, programmes (sessions) of Business Continuity training.
- f) prepares, at planned intervals, the Business Continuity and Disaster Recovery tests and exercises.
- g) reviews, at planned intervals, its BCMS (Business Continuity Management System) to ensure its adequacy and suitability in the face of regulatory, organizational, policy and legislation changes.

## **1.13 Management Review**

### **1.13.1 Quality Review**

Company management performs a Quality Review on an annual basis in order to evaluate its continued suitability, sufficiency, and effectiveness and to verify that the objectives established in the prior Review or in the course of normal business activities were achieved. The review includes the evaluation of improvement opportunities and any changes required to the quality management system, including quality policies and objectives.

#### **Input of the Quality Management Review**

The Quality Management Review is based on analysis of the following information, documented on paper or electronically and prepared by the Quality Manager:

- Results of internal inspections, including information regarding non-compliance, observations, and improvement opportunities.
- Information received from customers, with particular attention to complaints, compliments and results of Customer Satisfaction surveys
- Indicators that measure process and service performance, and the related analysis
- Status of corrective and preventive actions undertaken, in terms of efficiency and effectiveness
- Actions defined in the prior Review that will be evaluated during the current Review
- Any changes to be made to the Quality Management System
- System improvement proposals
- Any other information that the Department considers important for discussion and that has a direct or indirect impact on the Quality Management System.

#### **Output of the Quality Management Review**

Following the Review meeting, the following must be defined and documented:

- The decisions taken and actions agreed regarding process improvements and objectives
- The decisions taken and actions agreed regarding service performance improvement in relation to customer requirements
- Resources necessary to achieve the objectives and implement the decisions taken

The above will be formalised in appropriate Improvement Plans.

### **1.13.2 Information Security Management Review**

The Company Management, through the appropriate departments, performs an annual review of the Information Security Management System (ISMS) in order to verify the risk exposure of its services, based on the rules and requirements of the reference standards and regulation, with the aim of identifying specific countermeasures to safeguard the security of its information assets. The Company Management performs a Information Security Management Review on an annual basis in order to verify that the objectives established in the prior Review or in the course of normal business activities were achieved.

#### **Input of the Information Security Management Review**

The Information Security Management Review is based on analysis of the following information (“input review”, according to ISO27001 terminology), documented on paper or electronically:

- Actions defined during the prior Management Review
- Status of corrective actions undertaken in the current Risk Treatment Plan
- Results of internal inspections, including information regarding non-compliance, observations, and improvement opportunities.
- Results of internal and external security audits.
- The system of security indicators related to the processes in the Information Security Management System
- Results of Security Incidents in the business services.

#### **Output of the Information Security Management Review**

The output of the Information Security Management Review (“output review”, according to ISO27001 terminology), documented on paper or electronically, contains the results of business services risk exposure, indicated by the monitoring of:

- Analysis of infrastructure risks
- Results of internal and external audits
- Results of Internal/External Security Inspections
- Analysis of security incidents
- Comparison with national/international standards and regulation
- Comparison with corporate Security Policies and Guidelines

Risk exposure is managed through intervention actions formalised in the Risk Treatment Plan.

### **1.13.3 Business Continuity Management Review**

The Business Continuity Management System review aims at verifying its adequacy in the face of regulatory and standard requirements evolution and at identifying specific activities to ensure its maintaining.

Its adequacy is verified through the output's analysis and processing of the following activities:

- Risk Analysis
- Business Impact Analysis
- Internal and External Business Continuity Audit
- Internal and External Business Continuity Inspections
- Comparison with Company Business Continuity policy and guidelines.

#### **Input of the Business Continuity Management Review**

The input of the Business Continuity Management Review ( "Review input" in the BS 25999 terminology) is constituted by the Business Continuity objectives, defined in the previous Review of Management and in the other major activities carried out or planned in the course of the year and accompanied by the work-in-progress information. In particular, the following items are covered by the Review:

- Processes and procedures that have been reviewed during the year,
- The results of tests and exercises carried out during the year,
- The results of the Awareness and Training carried out in the year,
- The status of corrective and preventive actions,
- The possible adoption of new instruments / tools to improve the performance and effectiveness of the BCMS.

As for the Risk Analysis and all activities, they refer to activities carried out within the Information Security Management System.( As far it concerns the Risk Analysis and all the activities that support it are concerned, they refer to activities carried out within the perimeter of the ISMS).

#### **Output of the Business Continuity Management Review**

The output of the Review of Business Continuity Management ("Review output" in the BS 25999 terminology) is composed by the future BCMS objectives, which may include, for example:

- Updating of the Business Continuity Policy
- Maintaining of the BCMS
- Maintaining of the BS 25999 Certification
- Updating of the Business Impact Analysis
- Updating of the Business Continuity Plans
- Carrying out of the tests and exercises
- Organizing awareness sessions to embed and improve the BCM Knowledge in the organization's culture
- Valuation of the chance to increment the current perimeter of the application of Business Continuity.

---

## 2. THE PROCESSES SYSTEM

The company has defined its processes, differentiating between business, governance and support processes.

### 2.1 Business Processes

The general map of SIA-SSB business processes illustrates how the Company Management System is integrated and interacts with the primary processes that make up the business of SIA-SSB.

The business processes are connected across a lifecycle that generates value-added services for SIA-SSB customers.

In planning these processes, the company defined:

- 1 the product/service quality objectives
- 2 the product/service requirements
- 3 the resources and documents needed to realise the product/service
- 4 the verification, validation and monitoring activities for the product/service and the related acceptance criteria including the review points
- 5 the records needed to provide evidence that the product/service meets the requirements

#### 2.1.1 Sales Process

The objective of this process is the description of the methodology for preparation, approval and delivery of product and service offers to SIA-SSB Customers so that:

- 1 the offers contain all information the customer needs to evaluate whether to accept, as well as the essential elements that will govern any future contractual relationship with the Customer
- 2 the review of the requirements and the offer was performed, or the contents of the offer were previously reviewed and accepted by all of the business areas involved in providing the service/product to the Customer
- 3 the company is able to guarantee the offer made to the customer is consistent with the expressed requirements

#### 2.1.2 Contract Management Process

The objective of this process is the description of the methodology for defining, drafting, approving, delivering to customers, and archiving the contractual documentation related to SIA-SSB's products/services, so that:

- 1 all necessary contractual documents were prepared, signed and sent, and acceptance signatures were obtained from customers, for all products/services sold to customers by SIA-SSB
- 2 the contractual documents contain all information related to delivering the products/services and the conditions protecting SIA-SSB and the customer
- 3 the contents of the contractual documents were previously checked and accepted by all the SIA-SSB's entities involved in providing the products/services to the customer and the contents are also compliant to the technical, organisational and economic requirements previously agreed

### 2.1.3 Feasibility Process

The Feasibility Process is intended to:

- 1 analyse customer, reference market or internal needs, translate them into requirements and propose high-level solutions that implement said requirements
- 2 support and assist company management to identify and evaluate the major risk exposures (operational, financial, legal, contractual, informational, or other) in order to frame them to evaluate the opportunity to develop an initiative
- 3 perform technical and economic/financial studies to allow company management to evaluate opportunities to develop an initiative
- 4 provide the sales process with the necessary information to formalise offers to customers.

The process applies to all business activities, including:

- ⇒ developing new products or services
- ⇒ system integration activities
- ⇒ developmental maintenance
- ⇒ technology developments
- ⇒ responses to calls for tender
- ⇒ putting new customers into production
- ⇒ etc.

#### 2.1.3.1 Requirements Review

The Department Managers involved in identifying the requirements conduct the feasibility phase review or the requirements review from the feasibility study and the business plan to ensure the accuracy of the offer issued and the order received, in particular that:

- 1 the contents of the offer correspond to the Customer requirements
- 2 the contents of the offer correspond to the contents of the order
- 3 the competent and necessary resources are available to provide the service

If inconsistencies are discovered, they are clarified internally and with the Customer.

In the event of changes to the offers or orders, the reviews are repeated until the Customer accepts the agreed conditions.

### 2.1.4 Service & Product Development Process

The objective of the Service & Product Development Process is to perform detailed analyses of requirements (functional and non-functional), design solutions to be implemented and realised that are consistent with the initial requirements, and within time and budget constraints.

#### 2.1.4.1 Processes Related to the Customer

##### Determining the product/service requirements

With the aim of understanding the needs and expectations of the customer and in order to correctly define the product/service requirements, the organisation carries out and updates processes related to the customer, initially defined in the feasibility process.

In the design phase, requirements analysis is performed in a more detailed and precise manner as compared to the feasibility phase. In this phase the security requirements are also defined, which directly involves the security department.

### **Customer Communications**

Communications with the Customer are normally carried out via telephone, email, or through the institution of joint Steering Committees.

In the event the communications have particular contractual significance, they must be formalised as provided for in the sales, feasibility, and service & product development processes.

Of particular importance are communications regarding Customer complaints, which are duly registered, analysed and resolved, while keeping the Customer informed of the process.

#### **2.1.4.2 Design and Development Planning**

For each project, a Project Quality Plan is developed that defines the rules, methodologies and controls that will be applied to ensure the results, the achievement of quality objectives and customer satisfaction.

In addition, the following are established in the Plan:

- a) the design and development phases
- b) the review, verification and validation activities adapted for each phase of design and development
- c) the responsibilities and authorities for design and development

The planning output is updated throughout design and development.

If the project involves a service, a service management plan is also developed that defines the environments, the measurement and control tools and the necessary support personnel for service delivering.

For each project, the security risks relative to the project solutions are addressed as well as appropriate countermeasures.

Each project is planned by identifying the defined process phases, with the related review, verification, and design validation points, and detail for each activity involving specific skills and responsibilities.

#### **2.1.4.3 Input of Design and Development**

The input of design and development is the output of the feasibility process:

- 1 Feasibility Studies that contain the requirements definition, high-level technical characteristics and project objectives
- 2 any documentation provided by the customer
- 3 the Business Plan, which contains the details of timeframes and costs for project development and the business risk analysis
- 4 requirements review

Among the input of design, the mandatory requirements issued by trade unions, supervisory authorities or by customers are of particular importance.

This input is reviewed to verify its adequacy and completeness and to clarify any ambiguities.

#### **2.1.4.4 Output of Design and Development**

The output of design and development must be provided in a manner that allows it to be verified against the input and must be approved prior to being released.

The output of design and development must:

- a) satisfy the design and development input requirements
- b) provide adequate information for service supply, production and delivering
- c) contain or refer to product acceptance criteria
- d) specify the product characteristics that are essential for their secure and adequate use

The design process output is the developed software (product or service to be delivered) that responds to the defined requirements and to the acceptance criteria described in the documents related to the verification and validation phases.

#### **2.1.4.5 Design and Development Review**

The end of each phase of the process includes a review point that is appropriately planned in order to verify that:

- 1 what has been developed up to that point is consistent with the initial project requirements
- 2 any problems, changes and risks are noted, managed and delegated to a person responsible for resolution
- 3 if it is deemed appropriate, the customer or any other interested parties (e.g., suppliers) are present to confirm the results obtained, the delivery timeframe and any other necessary information

The review documentation, appropriately documented, is archived in the project folder of the document management system.

#### **2.1.4.6 Design and Development Testing**

The design and development verification points, planned by the Project Manager based on project complexity, are aimed at verifying that the design output is consistent with and satisfies the input requirements.

Project documentation verification and product/service verification are performed, in particular by controlling test results, by comparing the results obtained with the expected results and repeating until the test is a success.

The verification point documentation is a fundamental part of the project and results are documented and archived in the project folder of the document management system.

#### **2.1.4.7 Design and Development Validation**

Validation points, planned by the Project Manager based on project complexity, are used to verify that the design results are able to satisfy the functional and security requirements initially specified. Consequently, it is important to validate the project results in an environment that resembles the production environment to the extent possible.

The documentation of validation is a fundamental part of the project and results of validations are documented and archived in the project folder of the document management system.

#### **2.1.4.8 Design and Development Change Control**

Changes that emerge over the course of the project must be documented and an analysis of the impact on activities underway must be performed to determine if they would result in changes to the planning or requirements of the project as a whole, and consequently the project objectives.

In the event the changes introduce requirements that were not included in the initial feasibility studies or in their subsequent versions, it may be necessary to initiate the sales and feasibility process to define new contractual requirements and new planning.

Changes must be reviewed, tested, validated and approved before they are implemented. Design and development change review includes evaluating the effects the changes have on the component parts and on products already delivered.

Planning changes are tracked in the progress reports.

#### **2.1.5 Service Management Processes**

The objective of the Service Management Processes is to manage the service lifecycle, guaranteeing the Service Level Agreement (SLA) standards contractually agreed with customers.

Security risks related to service delivering are evaluated in terms of levels of Confidentiality, Integrity, Availability and Compliance for the information under examination.

The Service Management Plan guarantees the definition and coordination of responsibilities and execution methods for each activity, including management of incidents, problems, progress, and monitoring of the SLAs.

The service management processes as a whole guarantee to follow the service lifecycle and to monitor all aspects:

Incident Management defines all the necessary aspects and activities to manage incidents noted internally or by the client starting from notice of the incident to closure. In the event that closure of the incident is not definitive, but requires further investigation, a problem is opened and the related activities are described in Problem Management.

In addition to incidents, the service may be changed for development requests from the customer or for new mandatory laws. All changes are managed as defined in the Change Management process, and bundled into releases which are then issued into production as described in Release Management and the updated configuration items (Configuration Management).

The service is monitored and controlled to verify that it complies with the defined SLAs (SLA Management), which guarantees the appropriate levels of capacity, continuity and availability.

##### **2.1.5.1 Control of Activities for Service Production and Delivery**

Each service is characterised by a Service Management Plan that includes:

- the necessary information for service delivery
- working instructions for service delivery, where necessary
- identification and utilisation of appropriate equipment for service delivery
- the availability of performance measurement and monitoring tools, in accordance with contractual requirements
- the resources necessary for service delivery, both human and structural
- the security risks connected with the information managed

- the implementation of release, delivery and post-delivery activities

### **2.1.5.2 Validation of the Delivery Process**

Within the delivery process the following sub-processes have been identified:

- Definition of delivery requirements, related costs, in terms of feasibility – The scope of this activity is the delivery requirements definition requested by the customer, investigation of the preliminary solution, analysis and the determination of costs. These phases are carried out during the feasibility process.
- Organisation of the delivery, in planning - In this instance, the operating scenario is characterised in terms both of work organisation and technology infrastructure and operating environments (Test and Production), simultaneously defining the appropriate procedures for production release (divided into specific activities of testing, control and release), set in the third and final sub-process.
- Delivery management – This activity begins at the point in which the application becomes operational and includes a specific service monitoring action in production, in order to provide the necessary measurements to manage the service.
- The service performance is described and analysed in the monthly and quarterly reports that include the performance of the SLAs contractually defined with the customer.

### **2.1.5.3 Identification and Traceability**

The identification and traceability criteria regarding documentation is managed through the document management system.

The service, in terms of software and technical applications, is managed with configuration management tools.

Requests for corrective changes (incidents and problems) and development changes (sales, feasibility, service and product software development) are managed through defined processes and information tools set up within the company.

### **2.1.5.4 Customer Property**

The organisation will exercise care with customer property while it is under the organisation's control or being used by the organisation.

SIA-SSB identifies, verifies, protects and safeguards client property (generally software products) made available to be utilised and incorporated in the products.

If any customer property is lost, damaged or otherwise found to be unsuitable for use, this shall be immediately reported to the customer and related records will be kept.

### **2.1.5.5 Products Maintenance**

The company commits to set up appropriate security measures so that its equipment, used in service delivering, is adequately protected, data are saved at established intervals and customer outputs (e.g., executable code/source code/technical manuals/specific technical documents) are protected from unauthorised access.

### **2.1.5.6 Management of Monitoring and Measuring Devices**

The company has set up monitoring devices that consist primarily of software applications to gather information on consumption, performance, alarms and any events connected with the delivery of services, including incidents/security events.

## 2.2 Governance Processes

The governance processes, fundamental to defining business objectives and verifying their achievement, are identified as follows:

### 2.2.1 Quality

The Quality process is responsible for defining the system of business processes, identifying interactions among these processes, carrying out education and giving support to all business departments in its application.

The SIA-SSB Company Management System represents and governs the business processes system with the following objectives:

- Establishing a unique system of processes/procedures, for the individual companies and the Group
- Defining, for all business departments, the same reference processes/procedures
- Ensuring that controls and regulations/methodologies required by the SIA-SSB's business and by the Supervisory Authorities are included

The specific system governance processes are described in detailed in the following section and are related to internal inspection management, documentation and quality and security records management, and management of non-compliance, corrective actions, preventive action and improvements.

### 2.2.2 Security

The Security Department is responsible for the Information Security Management System. This includes:

- Defining relevant policies and guidelines
- Defining and managing the governance system for risk control
- Identifying the risk areas for insurance purposes
- Managing security compliances
- Developing and maintaining the Information Security Management System in terms of policy, guidelines, documents and procedures
- Developing and maintaining the Privacy Management System.

### 2.2.3 Business Continuity

The Business Continuity function is responsible for the Business Continuity Management. This includes:

- Defining the relevant policies and guidelines
- Defining and managing the Business Continuity Management System
- Managing the Business Continuity compliances towards to Bank of Italy
- Developing and maintaining Business Continuity Management in terms of strategy, Business Impact Analysis, Business Continuity Plan, Test programmes, Awareness programmes, etc.

### 2.2.4 Project Control Methodology

The company considers it important to define the project monitoring and control process in which the following main activities are described:

- method of definition, in the budget phase of business projects and their strategic priorities

- method of opening projects based on an approved budget and a business plan that respects the financial criteria defined by the company
- performance control criteria and methodologies over the project lifecycle
- method of preparing reports to the management committee and Board of Directors and its contents.

## 2.3 Support Processes

The support processes, essential to the functioning of the business processes, are identified as follows:

### 2.3.1 Legal

The legal processes are primarily related to defining customer contracts, the contract management process, the resolution of any claims brought by the customer, and the process of reimbursement and penalty management.

### 2.3.2 Human Resource Management

Processes and the related tools for human resource management have been prepared that reflect the following fundamental principles:

#### Resource availability

Company management has identified and assigned the necessary resources to implement the Quality and Security Management System consistent with the Quality, Security and Business Continuity policies and objectives for the achievement of customer satisfaction.

These resources are competent and adequately trained in information and information support systems, infrastructure, work environments and technologies utilized.

The personnel that perform roles in the Quality and Security areas are identified and their skills and knowledge are monitored.

#### Skills, knowledge, and training

Management considers the skills and training of personnel as critical success factors in that they directly contribute to customer satisfaction.

Specific skills are defined in the roles system for all the professional profiles, including profiles that directly impact service and product quality.

In addition, each year the education and training needs are defined, consistent with the business approach, and are clarified in an education plan that is implemented and verified for effectiveness through appropriate checks, if provided for, or in the evaluation report.

Two months following the end of each education or training event, the effectiveness of the course is evaluated directly by the Manager of the Organisational Unit.

All data relative to human resource management in each process (Promotions; Wage and organisational changes; Performance evaluations; Training) are recorded and maintained in specific applications.

Human resource management, in adherence with the principles described above, is detailed in the human resource management processes indicated below:

- Education and training management process
- Personnel recruitment, selection and hiring process

### 2.3.3 Supply

The following processes, and related tools, have been defined:

- supply process
- vendor management process

### **2.3.3.1 Supply Process**

The supply process has the scope of guaranteeing that all purchased components are compliant with specified requirements.

The requirements are defined by management based on needs that become apparent during feasibility or during delivery of services and are then sent to the Purchasing Office.

In order to guarantee that products and services are compliant with specified requirements, the company controls the supply process. This process is coordinated by the Purchasing Office with the support of the individual departments.

The Purchasing Office is responsible for selecting suppliers, managing the financial negotiations and managing any non-compliance issues with suppliers.

#### **Supply information**

The supply process is managed by the Purchasing Office and is responsible for optimising process quality, obtaining advantageous purchase prices compared to that which could be obtained by individual departments, and proposing qualified suppliers.

The Purchasing Office's involvement in the supply process varies based on the different categories of products/services to be purchased, for example professional resources and consultancy or hardware and software products.

The supply management process is initiated directly by the requesting department, as described in the "Procedure for Supply Management".

#### **Supply verification**

SIA-SSB has defined and performs controls and tests or other necessary activities to ensure that the purchased products meet the specified supply requirements.

If SIA-SSB or its customer chooses to perform verifications at the supplier, SIA-SSB will clarify the methods for said verification and product release in the purchasing documents

This process and related acceptance controls are defined in the "Procedure for supply management".

### **2.3.3.2 Vendor Management Process**

The vendor management process defines the method of managing suppliers from qualification of new suppliers, to precise supplier verification and subsequent global supplier evaluation.

The objective of supplier evaluation is to:

- control the performance of qualified suppliers, verify conformance to qualitative standards and performance in various supply situations.
- create a useful database to support supplier qualification renewal
- define standard measurement criteria shared at a corporate level, which allow the most objective evaluation possible and that are applicable to multiple supply situations.

The principle player in the vendor management process is the Purchasing Office that performs its activities with the participation of other company players that may be involved from time to time in the process (e.g., direct beneficiaries of the supplied good, those with skills that are useful for evaluation, etc.)

## 2.3.4 Facilities

### 2.3.4.1 Infrastructure

The Facilities Department guarantees the suitability and security of the work environment and the protection of company assets.

Specifically, the Department:

- 1 ensures the maintenance of a suitable lay-out for the building and work spaces, consistent with applicable provisions, laws and regulations, and identifies maintenance needs for the building, systems, and other company assets;
- 2 manages the services inherent in physical security (access control, fire prevention, intrusion security, TVCC systems) ensuring compliance with legal and internally established standards, performing risk evaluations, identifying health and safety measures for the work environments as well as emergency management and access control.

Infrastructure management is described in detail in the physical and logistical access management process, which conforms to the principles described above.

Group ICT Operations manages the technical hardware and software infrastructures, guaranteeing that the business has all the necessary environments for development, testing, control, and service delivery.

Technical and environmental infrastructure management is described in the processes:

- 1 Feasibility
- 2 Service & Product Development
- 3 Service Management (Incident, Problem, Change, Release, SLA, Capacity, Continuity, Availability...)

### 2.3.4.2 Work Environment

Company management regards the work environment as a factor that influences the motivation, development and satisfaction of personnel.

SIA-SSB has measures for security, prevention, worker protection and workplace health in place in adherence with guiding principles introduced by Legislative Decree 81/08.

The Legislative Decrees identify the general measures for worker health and safety protection that are in turn subject to:

- 1 risk evaluation
- 2 adoption of necessary measures for worker protection
- 3 constant maintenance of prevention and protection measures

The evaluation performed by the employer, in collaboration with the manager of the prevention and protection service and the competent medical professional, are found in the "Corporate Security Plan" a document that states both the criteria and the methods adhered to for said evaluation, including the prevention and protection measures that have been or will be adopted.

### **2.3.5 Communication and Image**

The purpose of the communication and image processes is to control all activities of development, consolidation and protection of the corporate image.

Specifically, the process of managing activities with media and external relations is to provide guidelines adopted by the company for relations with the external public, with particular reference to press organisations.

### **2.3.6 Administration**

The administrative processes include all administrative and accounting management of the company. The primary administrative processes identified are:

- management and control reporting
- preparation of the annual budget and its revisions
- customer accounting
- supplier accounting
- preparation of the annual budget and its revisions

## 2.4 Relationship between Business Processes and Security Guidelines

The table below highlights the correlation between the security guidelines and the business processes described above:

| BUSINESS PROCESSES                             | SECURITY GUIDELINES   |
|--|---|
| Sales Process                                  | Not applicable  |
| Contract Management Process                    | Security Guideline on definition of contractual clauses with suppliers associated with operational or regulatory risks                        |
| Feasibility Process                            | Not applicable  |
| Service & Product Development Process          | Security Guideline on transaction logging<br>Security Guideline on data information back-up<br>Security Guideline on managing intrusion tests |
| Incident Management Process                    | Security Guideline on monitoring and managing security incidents  |
| Problem Management Process                     |   |
| Change Management Process                      | Security Guideline on managing application and technical changes  |
| Release Management Process                     | Security Guideline on separation of processing environments   |
| Configuration Management Process               | Security Guideline on managing application and technical changes<br>Security Guideline on separation of processing environments               |
| SLA Management Process                         | Not applicable  |
| Availability and Continuity Management Process | Security Guideline on business continuity   |
| Capacity Management Process                    | Not applicable  |
| Financial Management Process                   | Not applicable  |

| <b>GOVERNANCE PROCESSES</b>      | <b>SECURITY GUIDELINES</b>  |
|----------------------------------|---|
| Quality                          | Security Guideline on classification and management of business documents |
| Security and Business Continuity | The Security and Business Continuity Management System (par. 1.14)        |
| Project Control Methodology      | Not applicable  |

| <b>SUPPORT PROCESSES</b>  | <b>SECURITY GUIDELINES</b>  |
|---------------------------|---|
| Legal                     | Security Guideline on definition of contractual clauses with suppliers associated with operational or regulatory risks  |
| Human Resource Management | Security Guideline on personnel duties<br>Security Guideline on human resource selection<br>Security Guideline on teleworking<br>Security Guideline on security education and awareness<br>Security Guideline on use of information and electronic tools<br>Security Guideline on use of electronic mail and the internet |
| Purchasing                | Security Guideline on definition of contractual clauses with suppliers associated with operational or regulatory risks  |
| Facilities                | Security Guideline on physical access<br>Security Guideline on logical access control   |
| Communications and Image  | Not applicable  |
| Administration            | Not applicable  |

---

### **3. MONITORING AND CONTROL**

The Company performs monitoring, measurement, analysis and improvement of its processes and services in order to guarantee the compliance of its own Quality Management System, Information Security Management System and Business Continuity Management System.

#### **3.1 The Quality Management System**

##### **3.1.1 Customer Satisfaction**

In recognition of the fundamental importance of customer satisfaction and the ability to develop “objective” measures to effectively direct our actions, a Customer Satisfaction survey system was defined.

The Customer Satisfaction results are analysed and submitted for management review to identify improvement opportunities.

##### **3.1.2 Internal Quality Inspections**

To certify that the provisions of the CMS have been effectively applied, internal quality inspections are conducted at least once a year.

The aim is to identify strengths and weaknesses in CMS, improvement opportunities, effective and efficient resource management, and relations with interested parties.

The internal inspections are performed against an inspection plan, defined at least annually. Inspections are conducted by evaluators chosen based on their skills and impartiality.

Any non-compliance issue is noted and analysed in order to agree upon and define the actions necessary to eliminate the causes that generated the issue. The managers of the area under inspection ensure that the actions necessary to eliminate the non-compliance and its causes will be adopted without undue delays.

The findings of the internal inspections and any defined corrective actions constitute part of the input of the Quality Management Review and for defining of the respective Improvement Plans.

##### **3.1.3 Monitoring and Measuring Processes, Products and Services**

The company has defined appropriate indicators to measure the capacity of processes, products and services to produce the expected results against defined objectives.

These measurement results are analysed and discussed in the management review.

###### **3.1.3.1 Monitoring and Measurement**

In order to guarantee that products, processes and services conform to the expected requirements, the company has identified appropriate indicators for monitoring.

These indicators, together with the Service Level Agreement (SLA) data on delivery of services, are analysed in the provision reports.

These measurement results are analysed and discussed in the management review.

###### **3.1.3.2 Data Analysis**

The effectiveness and efficiency data from the Quality Management System is submitted and analysed by the

various managers and summary data is discussed during the management review.

The aim of the data analysis is to identify strengths and weaknesses of the system and prepare any corrective or preventive actions in order to guarantee constant improvement of the Quality Management System.

The primary data analysed are:

- 1 customer satisfaction
- 2 product/service compliance
- 3 process performance
- 4 supplier performance
- 5 management data.

All the data are gathered and presented by the Quality Management Representative to be discussed during the management review.

### **3.1.3.3 Non-Compliance Management**

"Non-Compliance" is defined as not meeting a requirement, which therefore creates dissatisfaction in the customer (external or internal).

The sources of "Non-Compliance" may be manifold. Anyone that notes or receives indications of "Non-Compliance" must initiate the specific Non-Compliance management procedure, as described in the appropriate business procedure, that provides for root cause analysis, identification of solution(s) and verification of solution effectiveness.

SIA-SSB handles non-compliant products in one of the following manners:

- a) adopting actions aimed to eliminate the non-compliance detected
- b) authorising the use, release or acceptance with concessions by the relevant authorities, and when applicable, the customer
- c) adopting actions aimed at precluding the product's original use or application

When the non-compliant products are corrected, they may be re-verified to demonstrate their compliance with requirements.

When a non-compliant product is discovered after its delivery or after it has been used, the organisation must adopt appropriate actions for any consequences, real or potential, resulting from non-compliance.

## **3.2 The Information Security Management System**

### **3.2.1 ISMS Monitoring**

As regards the monitoring/management of its ISMS, the corporate organisation must:

a) *plan and conduct security controls* at regular intervals within the ISMS to determine if the objectives of the security measures, the security measures, the processes and the procedures of the ISMS are:

- conform to legal and regulatory requirements;
- conform to the identified information security requirements;
- effectively introduced and maintained;

- operating as expected.

- 

b) *revise the business processes risk level* periodically and regularly (at least once a year), to reflect:

- organisational changes;
- technology changes;
- business objectives and processes;
- identified threats;
- external events, such as legal or regulatory changes

or based on specific events resulting from:

- security controls (e.g., Vulnerability Assessment, Penetration Test).
- security incidents
- security key indicators.

c) *update the key roles* for Information Security in each B.U./Department to meet new regulations.

d) *revise the security incident control process* using outside experiences and new techniques, products or procedures that may be useful to improve effectiveness.

e) *update the Security Key Indicators (SKI) system* based on the risk analysis results.

f) *update the awareness and training programmes* for the key security roles within the Company, in the light of the results of the evaluation of the effectiveness of the training sessions undertaken.

### 3.2.2 Security Inspections

In order to pursue continuous improvement of ISMS, security inspections are periodically performed.

The security inspections aim at:

- certifying the application, suitability and effectiveness of ISMS;
- defining ISMS improvement actions;
- adopting the necessary corrective and preventive actions.

Achievement of the above objectives is subject to compliance with the requirements defined below:

- the RISM Department is responsible for the proper execution of all phases provided for by the performance of an inspection (planning, preparation, execution, etc.);
- the Security Inspections are planned at least annually in accordance with the RISM Manager's priorities and directions and are planned with the aim of verifying all processes and business areas involved in ISMS;
- the Security Inspections are divided into External Inspections and Internal Inspections:

- 1) External Inspections are conducted by a Manager (external evaluator) that has followed a specific course for ISMS evaluators and has participated as an auditor in at least three External Inspections;
  - 2) Internal Inspections are conducted by RISM staff that have performed at least one Internal Security Inspection at SIA-SSB (internal evaluator), or by a Manager (external evaluator) that has followed a specific course for ISMS evaluators and has participated as an auditor in at least three External Inspections.
- the results of the Security Inspections are documented and reviewed with the managers of the business unit under inspection, in order to agree on a Corrective Actions Plan and the management of any detected Non-Compliance;
  - at the deadlines agreed in the plan described above, the correct introduction of the actions developed to manage any Non-Compliance are verified by the SIA-SSB ISMS evaluator.

### **3.3 The Business Continuity Management System**

#### **3.3.1 BCMS Monitoring**

The monitoring and management of the BCMS is carried out through the implementation of the following three activities:

- exercises
- maintaining
- review

#### **Exercises**

SIA-SSB prepares annual plans to test/verify Business Continuity and Disaster Recovery arrangements.

The Business Continuity tests are carried out to verify the effectiveness and efficiency of the Emergency and Crisis Management Process that allows critical activities will be recovered as required.

The Disaster Recovery tests are important to verify the functionality and efficiency of back-up activities of the technological infrastructure and to update the skill of the involved human resources.

About Disaster Recovery tests, their frequency is due to several factors such as contractual obligations, the critical status of services and processes, the interdependence between those and other services and/or processes, any legal constraints, the importance of the customer, etc. . In the absence of contractual obligations the Disaster Recovery tests of the platform and the connection must be carried out at least once a year.

#### **Maintaining**

SIA-SSB has a process for updating the documentation by which any change, internal or external, that has an impact on the company, is incorporated within the management of the Business Continuity/Disaster Recovery. Any internal or external change which has an impact on the Company's activities is reflected (acknowledged) in the Company's documentation updating process.

#### **Review**

SIA-SSB carries out every two years, or for significant changes, a review of all the BCMS (Business Continuity

Management System) to ensure its adequacy and suitability in the face of regulatory, organizational, policy and legislation changes.

### 3.3.2 Business Continuity Inspections

In order to pursue continuous improvement of BCMS, BC inspections are periodically performed.

The BC inspections aim at:

- certifying the application, suitability and effectiveness of BCMS;
- defining BCMS improvement actions;
- adopting the necessary corrective and preventive actions.

Achievement of the above objectives is subject to compliance with the requirements defined below:

- the RISM Department is responsible for the proper execution of all phases provided (expected?) for an inspection performance (planning, preparation, execution, etc.);
- the BC Inspections are planned in accordance with the RISM dept. manager's priorities and directions and are planned with the aim of verifying all processes and business areas involved in BCMS at least annually;
- the BC Inspections are divided into External Inspections and Internal Inspections:
  - 1) External Inspections are conducted by a Manager (external evaluator) that has followed a specific course for BCMS evaluators and has participated as an auditor in at least three External Inspections;
  - 2) Internal Inspections are conducted by RISM staff that have performed at least one Internal Security Inspection at SIA-SSB (internal evaluator), or by a Manager (external evaluator) that has followed a specific course for BCMS evaluators and has participated as an auditor in at least three External Inspections.
- the results of the BC Inspections are documented and reviewed with the managers of the business unit under inspection, in order to agree on a Corrective Actions Plan and the management of any detected Non-Compliance;
- at the deadlines agreed in the plan described above, the correct introduction of the actions developed to manage any Non-Compliance are verified by the SIA-SSB BCMS evaluator.

### 3.4 Continuous Improvement

SIA-SSB commits to continuously improve CMS effectiveness, using the quality, security and business continuity policies, the quality, security and business continuity objectives, the results of quality, security and business continuity inspections, data analysis, quality, security and business continuity corrective and preventive actions and management reviews.

This objective is pursued by:

- 1 systematically analysing defined indicators and objectives
- 2 performing the management Review with particular attention to:
  - results of data analyses
  - inspection results
  - process and service performance

- achievement status of each Organisational Unit's objectives
- prior management Reviews
- Improvement Plans underway

A "Corrective Action" is an action defined to eliminate the cause of detected "Non-Compliance" or other critical situations.

When "Non-Compliance" repeats itself, it means that it was handled in such a way as to temporarily resolve the problem, but the true cause of the problem was not eliminated.

In this case, we refer to "Corrective Actions" to resolve the "Non-Compliance".

Based on data gathered and the causes identified "Corrective Actions" are agreed, identifying the person responsible, the timeframes and necessary resources. At the end of defined action, its effectiveness is evaluated.

The Preventive Actions are those measures put in place to avoid the occurrence of "Non-Compliance".

These are agreed based on data gathered and potential causes and identify the person responsible, the timeframes and necessary resources.

The requirements are defined for:

- a) identifying potential non-compliance and its causes
- b) evaluating the need of take actions to prevent that non-compliance occurs
- c) identifying and implementing the necessary actions
- d) recording the results of the actions taken
- e) reviewing the preventive actions taken.

---

## **4. THE DOCUMENT SYSTEM (CMS) AND DOCUMENTATION MANAGEMENT**

### **4.1 General Requirements**

The Company Management System (CMS) describes the processes, activities, methodologies, procedures and responsibilities of all company activities.

The CMS system integrates all of the business processes and is in compliance with the reference standards (ISO9001, ISO27001, Legislative Decree 196, 81, 231, etc.).

The company adopts a process management model that, in accordance with company rules, is based on the following phases:

- planning
- implementation
- monitoring
- reviewing.

These phases are carried out according to the following primary methods:

- planning of each phase
- recording all activities that make up the phases
- identifying the responsibilities of each phase
- monitoring each phase

### **4.2 Documentation Requirements**

#### **4.2.1 General Information**

The document system is based on the integration and evolution of all company processes and its documentation is articulated across various levels:

- 1 Company Governance and Guidelines
- 2 Quality policies and objectives-
- 3 Security policy and objectives
- 4 Business Continuity policy and objectives
- 5 Processes, procedures and guidelines
- 6 Templates
- 7 Quality records
- 8 Security records
- 9 Business Continuity records

The process that governs documentation management is described in the "Documentation Management and Quality and Security Records" procedure.

The company documentation is managed by a document system whose primary libraries are:

- 1 **Company Management System Library**, which includes the methodologies, processes, guidelines and business models
- 2 **Services and Projects Library**, where all documentation relative to individual projects/services are published after the related verification and approval (known as "Quality records")
- 3 **Department Library** dedicated to all activities related to the Departments
- 4 **Quality Library** dedicated to all activities specific to Quality, such as improvement plans, reporting to company management, plans and results of internal inspections, etc.
- 5 **Security Library** dedicated to all activities specific to Security, such as risk treatment plans, reporting to company management, plans and results of internal inspections, etc.
- 6 **Business Continuity Library** dedicated to all activities specific to Business Continuity, such as the Business Continuity Plan, emergency plans, reporting to company Management, etc.

#### 4.2.2 Company Governance and Guidelines

Company Governance and Guidelines is the document that describes the processes and methodologies adopted by the company to ensure customer satisfaction consistent with corporate regulations and adopted reference standards.

#### 4.2.3 Documents Control

Documents are managed according to the specific "Documentation Management and Quality and Security Records" procedure.

- 1 Each document is identified, classified, verified and approved before being issued and subsequently archived.
- 2 A change to the document is highlighted and is verified and approved before being issued.
- 3 Obsolete versions of documents should not be circulated and the latest valid version of document should be identifiable.
- 4 External documents, documents from Customers (e.g. terms) or documents from other sources (e.g. laws, directives, institutional communications, etc.) must be correctly identified and archived in such a manner as to be easily accessed by interested parties.

All documentation is managed by a document management system that guarantees that the approval cycle is adhered to and that all employees are able to access the latest approved version of each document.

#### 4.2.4 Records Control

Records related to data necessary for Company management that influence the performance of the Company Management System and provide objective evidence are identified and traceables accordingly to the "Documentation Management and Quality and Security Records" procedure and the "Company Governance and Guidelines" document, which also include the methods for identification and storing, protection, availability, duration of storing, and elimination methods. All Quality, Security and Business Continuity recorded documents are managed through the company document management system.