

# Company Management System

## SIA-SSB Information Security Management System



Document Code: 1-CMS-2010-021-01  
*Company-Project/Service-Year-Document No.-Version*

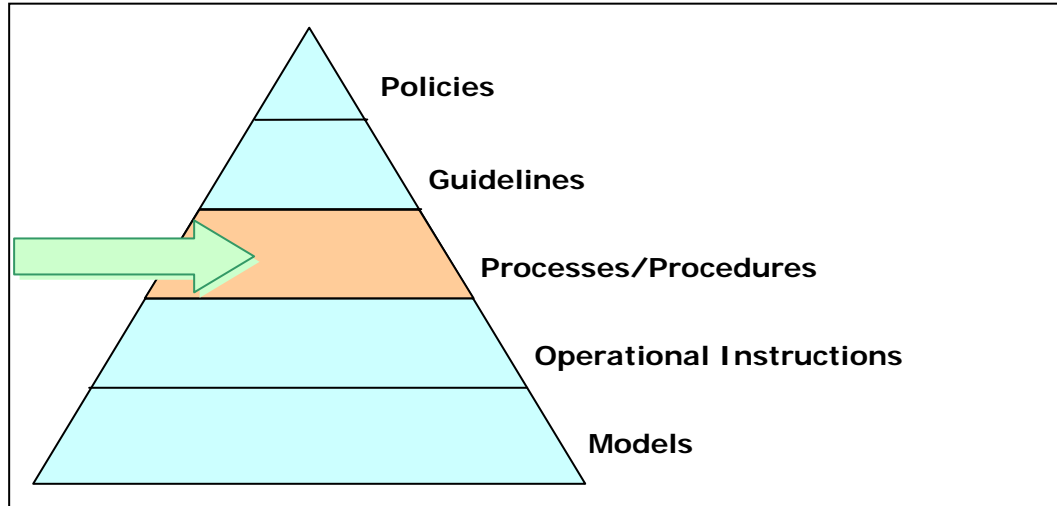
Classification: Public



---

## POSITIONING OF THIS DOCUMENT

SIA-SSB has created a positioning chart for all the security documentation it produces which forms an integral part of its Information Security Management System. The chart organizes the documents according to their typology (security policies, procedures, etc.). This deliverable falls into the *Processes/Procedures* level of the security document structure shown below:



---

## SUMMARY

<b>1. INTRODUCTION</b> .....	<b>4</b>
1.1 Aim of the document .....	4
1.2 Validity.....	4
1.3 Definitions.....	4
1.4 References .....	4
<b>2. SIA-SSB INFORMATION SECURITY MANAGEMENT SYSTEM</b> .....	<b>5</b>
2.1 Description of the SIA-SSB Information Security Management System.....	5
2.2 Security Roles and Responsibilities .....	6
2.3 Security Guidelines .....	6
2.4 Security Risks Analysis and Management .....	6
2.5 Safety Risks Analysis .....	6
2.6 Security Awareness .....	7
2.7 Security incidents .....	7
2.8 Security indicators.....	7
2.9 Security Compliance .....	7
2.10 Technical Security .....	7

---

## 1. INTRODUCTION

### 1.1 Aim of the document

This document describes the Information Security Management System of SIA-SSB.

### 1.2 Validity

The instructions contained in this document are valid for all SIA-SSB corporate divisions.

### 1.3 Definitions

Acronym/Term	Definition
CO.BAN.	Consorzio Bancomat
DNV	Det Norske Veritas
IEC	International Electrotechnical Commission
ISO	International Standards of Organization
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry – Data Security Standard
ISMS	Information Security Management System

### 1.4 References

- [01] ISO/IEC 27001:2005 – Information technology. Security techniques. Information security management systems. Requirements.
- [02] ISO/IEC 27002:2009 – Information technology. Security techniques. Code of practice for information security techniques.

---

## 2. SIA-SSB INFORMATION SECURITY MANAGEMENT SYSTEM

### 2.1 Description of the SIA-SSB Information Security Management System

In general, the objective of an Information Security Management System (hereinafter referred to as ISMS) is to guarantee an adequate level of security with regard to processes and infrastructures involved in the provision of corporate business services through the identification, assessment and management of security risks.

In particular, each ISMS defines a series of organizational, technical and procedural measures aimed at guaranteeing that basic security requirements are satisfied, namely:

- Confidentiality, or rather the characteristic of a given piece of information to be known only to those entitled to it;
- Integrity, or rather the characteristic of a given piece of information to be amended exclusively by those who are entitled to do so;
- Availability, or rather the characteristic of a given piece of information to be accessible and used when requested by processes and users entitled to it;
- Compliance, or rather the characteristic of a given piece of information to be processed according to the industry laws and regulations on security.

SIA-SSB has developed its own ISMS as it deems this to be fundamental in relations with its stakeholders, such as customers, suppliers, partners, group companies, and in order to satisfy the regulatory and market requirements appropriately.

As far as its ISMS is concerned, SIA-SSB:

- issues the necessary security regulations to allow the company organization to carry out its activities in a secure manner;
- integrates security regulations and solutions in the processes of design and supply of corporate services;
- carries out the analysis of security risks with regard to the processes and infrastructures involved in the provision of corporate business services and the analysis of risks concerning the safety;
- monitors the security risks identified using the Security Risks Treatment Plan;
- pursues operational continuity objectives through a specific Business Continuity Management System, logistics solutions and Disaster Recovery;
- promotes a security culture;
- guarantees the compliance with the regulatory framework;
- manages security compliance (VISA, MasterCard, CO.BAN, etc.);
- defines security roles and responsibilities;
- manages a Security Committee to address and coordinate security issues;
- monitors its systems through specific Vulnerability Assessment plans;
- carries out monitoring and auditing activities relating to security;
- manages and administers the operational aspects of security according to a split knowledge and dual control logic.

For the development of its ISMS, SIA-SSB chose to adopt the ISO27001 standard.

SIA-SSB obtained the ISO27001 certificate with the company DNV.

## 2.2 Security Roles and Responsibilities

As part of its ISMS, SIA-SSB has defined a series of specific security roles for its staff within the corporate organization chart.

In addition, it has identified a series of specific responsibilities of organizational type relating to security, namely:

- Security Committee, made up of the main SIA-SSB top-level and executive staff, whose aim is to assess security risks, decide how to deal with them and monitor the progress of the Security Risks Treatment Plan,
- The Departmental Security Representative, who acts as the point of reference for the activities relating to the ISMS within his/her Division

and of operational type, such as the Local Security Administrator, who, within his/her organizational unit, carries out decentralized operational activities, and the System Administrators, as also defined according to the Italian Law Decree 196/03.

## 2.3 Security Guidelines

As part of its ISMS system, SIA-SSB has defined a series of security guidelines in order to guarantee the respect of security requirements, security regulations and the laws in force with regard to individual professional roles.

SIA-SSB's security guidelines cover organizational issues (Information Security Management System, Operational Continuity, Management of Human Resources, Definition of Contractual Clauses with suppliers in terms of security, Classification and Management of Company Documents, and the Management of Security Incidents) and operational issues (Physical and Logical Access Control, Vulnerability Assessment, Change Management, Audit and Logging, Data Backup, Use of IT and Electronic Tools, Use of e-mail and internet).

## 2.4 Security Risks Analysis and Management

SIA-SSB periodically carries out analysis of security risks in order to address and manage security risks relating to processes and infrastructures (applications, technologies, data, human resources, networks, and offices) involved in the provision of corporate business services.

The process, subdivided into three stages,

1. Analysis of Security Risks
2. Management of Security Risks
3. Monitoring of the Security Risks Treatment Plan

is a corporate process in which the organizational components participate, each one according to their specific responsibility/competence.

## 2.5 Safety Risks Analysis

In compliance with Italian Law 81/08, SIA-SSB periodically carries out an analysis of safety risks. The process involves the global assessment and documentation of all risks to the health and safety of the company staff with the aim of identifying adequate prevention and protection measures and of designing the measures necessary to guarantee the improvement of health and safety levels over time.

## **2.6 Security Awareness**

SIA-SSB considers the security culture to be a key value for the company and this is supported through a continuous training and information process.

SIA-SSB carries out its awareness program using multi-media training, tests and drills, participation in specific training courses, as well as any other initiative that may be helpful in spreading knowledge and awareness on security within the company.

## **2.7 Security incidents**

SIA-SSB manages security incidents as part of a wider framework of incident management at corporate level in order to highlight the possible security risks for business services and manage any action plans and related corrective measures.

## **2.8 Security indicators**

In order to achieve a continuous monitoring of its security system, SIA-SSB has adopted a system of security indicators (both procedural and technical) consistent with the NIST methodology. The SIA-SSB security indicators are subdivided into organizational, behavioral, operational and technical indicators.

## **2.9 Security Compliance**

Due to the types of services it provides, SIA-SSB must comply with security regulations and standards issued by national and international bodies (CO.BAN., Visa, MasterCard, etc.).

To date, security compliance includes CO.BAN. Validation, PCI-DSS, PCI PIN Security Programme and the Payment Technology Standard Manual.

## **2.10 Technical Security**

SIA-SSB supports the design, development, and provision of its services through the identification of security requirements, administration of security profiling and quantities, monitoring of events relating to security, vulnerability assessment activities and, more generally, addressing the ICT security.