Company Management System

SIA – Processes and Management Systems

INDEX

EXECUTIVE SUMMARY

This document describes the System of Processes, the ISO certified Management Systems and other company management systems.

1. THE COMPANY CONTEXT

SIA designs, creates and manages technology infrastructures and services for Financial Institutions, Central Banks, Businesses and Public Administration Bodies, in the areas of payment systems, e-money, network services and capital markets in Italy and Europe.

Every three years, SIA draws up a business plan which has as its objective organic growth with particular reference to the European market and the Italian Public Administration market. The company has assigned to the Strategies, Planning and Control department responsibility for monitoring the progress of the plan.

The evolutions of the macroeconomic context are documented in the supplementary notes to the financial statement.

1.1 Interested Parties

The interested parties, identified by SIA according to their relevance for the company and to the Sustainable Value Report [5] are:

- the community since it is the beneficiary of SIA's social initiatives and of the effects of the company procedures concerning reduction of the environmental impact;
- the domestic and European financial system intended as the totality of direct and indirect users of the SIA services, who express requirements in terms of quality, security and continuity of services;
- the people of SIA, who express requirements in terms of protection of personal safety, safeguarding jobs, professional development, personal motivation, balance between working life and private life;
- customers and users of the services, who express requirements in terms of service quality, security and availability of the service, respect of delivery times, respect of contractual requirements, pricing, ability to understand the customer and propose innovative solutions;
- group companies, who express requirements in terms of protection of the relevant business;
- shareholders, who express requirements in terms of company profitability and market positioning;
- suppliers and partners, who can play a crucial role in the SIA value chain and who express requirements in terms of continuation of the supply relationship;
- regulatory bodies, which issue industry regulations applicable to the SIA context (e.g. Bank of Italy, payment schemes, etc.).

2. LEADERSHIP AND RESPONSIBILITY

The management of SIA has drawn up the Quality Policy, the Business Continuity Policy, the Information Security Policy (par. 4.2.2) and the Risk Policy [9] and distributes them to all staff.

SIA has granted to all heads of corporate functions the authority necessary for the performance of the duties assigned to them.

SIA has described the structure and the responsibilities of the Organizational Units [7] which make it up, and has drawn up its own system of roles [8] and the methods to ensure that the various roles are covered by the persons who possess the necessary competences. The specific competences are set out in the system of roles for all the professional profiles, including those which directly influence the quality of the services and products.

SIA has identified the roles and the information flows relating to the management systems for Business Continuity, Information Security, Compliance and Risks. [10]

Responsibility for the certification of the management systems is assigned to the Risk Governance department.

In the strong belief that ethical behavior in the conduct of business affairs is a necessary condition for the company's success and in the application of the provisions of Legislative Decree 231/2001, SIA:

- has set out its **Organizational Model** which describes the effective application of the principles of legality, transparency, correctness and loyalty which have always characterized the company's relations with its stakeholders [68]
- has approved its own **Code of Ethics** which is binding, without exceptions, on all representatives of the company and on all external consultants. Conduct in line with the principles contained in the Code of Ethics is also required from suppliers, business partners, in addition to all parties who, directly or indirectly, have business, professional or work relations with SIA [6]
- has set out **anti-corruption guidelines** aimed at promoting compliance with the ethical standards and full conformity with national and international laws concerning prevention of corruption, in all its direct and indirect forms, as well as integrity, transparency and correctness in the performance of the company's activities [16].

The task of supervising the correct functioning and effectiveness of and compliance with the Organizational Model and of overseeing its updating is assigned to the **Supervisory Body**.

In the **Code of Ethics** SIA underlines its commitment also to eliminating every form of conflict of interests of a personal or corporate nature.

3. THE SYSTEM OF PROCESSES

The **System of Processes** at SIA describes the activities, responsibilities and interactions between the Organizational Units. The processes are drawn up by the Human Resources & Organization department, in collaboration with all the corporate functions involved with the exception of the specific processes for the Business Continuity, Compliance, Risks, Data Protection and Safety Management systems which are drawn up by the Risk Governance department. The processes relating to Information Security are drawn up by the Risk Governance department in collaboration with the Technology & Infrastructures department.

The company has:

- identified the governance, business and support processes;
- established the sequences and the interactions between the processes;
- defined the measurement criteria to evaluate the effectiveness of the processes;
- ensured that the necessary resources exist to guarantee the correct working of the processes;
- arranged checkpoints to evaluate whether the processes achieve the expected results and if they are liable to improve;
- identified the risks connected to the company processes.

The company organization and the System of Processes were set out also taking into account the indications on the governance and control of the processes and the regulations on business continuity of Bank of Italy.

3.1 Governance Processes

The process of drawing up the **strategic plan** describes the activities and responsibilities for the definition, approval and subsequent monitoring of the three-year Strategic Plan of the group. The process for the management of the **merger and acquisition** operations defines the responsibilities, activities and decisions concerning all mergers and acquisitions. Responsibility for these processes is assigned to the Strategies, Planning and Control department. [11][12]

In order to attain a more effective representation of the economic dimensions of each service/ product, SIA has drawn up the **industrial accounting** system. [13]

SIA has set out rules for the drawing up of the **financial budget of the company and the group** in addition to the relative revisions; these activities are assigned to the Strategies, Planning and Control department. [14]

The process for the management of the **inter-group contracts** defines the criteria governing the transfer of products and services between the companies in the SIA Group; responsibility for the process is assigned to the company departments. [15]

The **anti-corruption** guidelines were drawn up with the aim of promoting compliance with ethical standards and full conformity with national and international laws concerning prevention of corruption, in all its forms, as well as integrity, transparency and correctness in the performance of the company's activities. [16]

3.2 Business Processes

3.2.1 Management of offers and contracts with customers

Marketing & sales aims to define the activities, rules, roles and responsibilities relating to the marketing & sales process, developing a common language in the company and a knowledge sharing system about market and customers and a monitoring of the activities. [17]

The **offer management** process aims to draw up, approve and send offers to customers or renegotiate the conditions for services already activated, in order that the offers contain all the information necessary for the customers for their acceptance, as well as the essential information which governs the future contractual relationship with the customer. It applies to the divisions and departments that play a role within the sales cycle of SIA services/products. [18]

The aim of the process for the **management of contracts with customers** is to describe the methods to follow for the definition, drawing up, approval, forwarding to customers, and filing of the SIA contractual documentation. The process is activated with the signing of the Offer by the customer, followed by the preparation, negotiation and internal approval of the Contract, and signature by the customer; responsibility for the management of the process is assigned to the LAW department. [19]

The aim of the process for **management of orders** with Public Administration Bodies is to define the activities, rules, roles and responsibilities relating to the sales process which applies to the management of orders with the Public Sector, Special Corporations (Municipalized), State-owned companies (e.g. Poste Italiane), with respect to what is set out in the procedure for the management of relations with the Public Sector. [20] [21]

3.2.2 Feasibility and Design

The **Feasibility and Design** process is articulated in two phases.

The *feasibility* process is activated on the specific request of customers, for business or internal requirements, such as evolutionary/corrective maintenance, compliance; it involves preliminary analysis of requirements, identification of solutions to be implemented, planning of activities and analysis of risks. The persons responsible for monitoring the correct application of the process regulated by this procedure are the feasibility officers.

The aim of the *design* process is the correct management of projects and includes detailed analysis of requirements, design of the solution, realization of what is designed and execution of the test and trial activities, up to the release into production of what is realized.

The process applies to all the activities of software development, system integration, infrastructural realization, migration or evolutionary/corrective maintenance.

The design process describes the detailed analysis of requirements (functional and non-functional), design of solutions, realization of what is designed in compliance with the initial requirements and respecting the timescales and costs planned, including the performance of the tests, training of the personnel concerned in the new solutions, the release of the new product/service and all the activities necessary for the organization of the management and supply.

The project includes the analysis of security and business continuity requirements and the definition of the solutions related to them.

The person responsible for the correct application of the design process is the Project Manager appointed by the Director of the department responsible. [22]

3.2.3 Service Management

SIA has defined its processes relating to the management of the services based on the best practices defined by ITIL 3.0.

The aim of the SIA **ICT incident management** process is to manage incidents in the services, in order to restore, in the shortest possible time, normal operations, minimizing the effects on the security, quality and availability levels required for the normal running of services.

The following are the Incident and Problem definitions adopted by SIA consistent with the definitions of ITIL 3.0:

- Incident: unplanned interruption of an IT service or reduction in the quality of the IT service,
- Problem: unknown cause of one or more Incidents (already happened or potential).

During the normal running of services, all the parties involved in the supply of the services monitor its trend to detect any incidents.

In the case where incidents are detected, the incident management process begins with the report of the incident and consequent opening of the ticket, followed by the analysis phase and the information, decisional and operative phases, up to the solution and closure of the ticket. Responsibility for the process is assigned to the Business Divisions or the Technology & Infrastructures department [23].

Cyber security incident management process: the aim of this process is to govern the management of incidents or threats to information security in terms of detection, response and restoration in order to minimize impacts on the company. The process applies to security incidents, namely violations, (current or imminent) due to deliberate actions, of the confidentiality, integrity and availability of the information and support assets during their entire lifecycle. Responsibility for the process falls within the perimeter of the Technology & Infrastructures department. [24]

SIA has also defined the **NO ICT incident management process** aimed at managing events under the following categories: physical, logistical, plant & equipment, organizational. [25]

In the case in which the incident report has a high level of gravity, the **emergency and crisis management process** is activated with the aim of defining the steps to activate the staff involved in the management of emergency and crisis situations, underlining the methods to activate the Teams, the related responsibilities and the general flow of information inside and outside the company; this process is part of the **Business Continuity Management System**. [26]

The aim of the SIA **problem management** process is to eliminate the causes of the incidents and/or anomalies and to prevent the occurrence of events which negatively impact the trend of the service, namely the levels of availability, quality and security of the service itself. Responsibility for the process is assigned to the Technology & Infrastructures department. [27]

The aim of the **RFC** (Request For Change) **management** process is to manage amendments to the systems, guaranteeing timely responses to customers and ensuring respect for priorities, avoiding process inefficiencies, tracking each phase of the process from the managerial and accounting viewpoints, applying them to the configurations and systems of Disaster Recovery (DR). Every RFC must have an owner, the person responsible for the operative management of the entire lifecycle of the RFC. [28]

The aim of the SIA **release management process** is to manage in a controlled, secure manner all the releases into production, according to a shared calendar of all interventions in the production and Disaster Recovery environment. The objective is to avoid the introduction, in the production environment, of unauthorized releases which could give rise to disservices and/or interruptions to business continuity. The Release Management Process applies to the

management of every release into production concerning the administration and supply of IT services; responsibility for the process is assigned to the Technology & Infrastructures department. [29]

The aim of the SIA **service level management** process is to define, negotiate and manage all service levels, in order to ensure that all service management activities, Operating Level agreements and Subcontracting Contracts meet the service level objectives agreed. The process provides for definition and negotiation aimed at formally establishing the service levels agreed with the customer, as well as monitoring and regular reporting on the service levels in order to control and continually improve the service; responsibility for the process is assigned to the departments and divisions involved in supplying the services. [30]

The **capacity planning** process describes the activities of estimation, planning, management and analysis of the production capacity and of the load levels necessary to guarantee the performance requirements requested by customers, keeping under control the costs of the production systems and the expected timescales; responsibility for this process is assigned to the Technology & Infrastructures department. [31]

The aim of the **claims, reimbursements and penalties management** process is to describe the methods to follow to manage claims, requests for reimbursement and the application of penalties by customers on the basis of the provisions of the Contracts in force. The process refers to written communications not necessarily connected to requests for reimbursements or penalties. The claims management process is activated upon receipt at SIA of claims from customers, which are recorded upon receipt and subsequently registered in the appropriate company tool. They are then managed through the definition of corrective and preventive actions. Responsibility for the process is assigned to the Business Divisions. [32]

The aim of the **asset management** process is to manage and protect the integrity of the information relating to company assets, to minimize the risks connected to them, to optimize their performance, through a "central" control system, and to permit possible analysis in case of incidents or crisis situations. This objective takes the form of identification of the assets (IT and non-IT) and of the information connected to them and their collection and entry in one or more "peripheral" repositories (which feed the central system), at the same time guaranteeing constant updating, starting from the acquisition phase up to the definitive decommissioning; the information relating to the assets is correlated among them and with the business, in order to have available the widest and most detailed representation of the assets present and used in the company. The ownership is assigned to the Organizational Unit which creates or acquires a company asset, or which is responsible for managing a proprietary third party. [33]

3.3 Support Processes

3.3.1 Suppliers and Purchases

The aim of the **supplier qualification and evaluation** process is to describe the activities to manage the preliminary (qualification) and final (assessment) evaluation of suppliers and to meet the company's requirement to have a complete picture of its set of suppliers; what is described in the process applies to all the suppliers used and to potential suppliers. Responsibility for managing the process is assigned to the Technology & Infrastructures department. [34]

The **supplier risk** process describes the methodology for monitoring risks related to suppliers. Responsibility for the process falls within the perimeter of the Risk Governance department and the Technology & Infrastructures department. [35]

The aim of the **procurement management** process is to regulate the purchasing cycle of goods and services necessary for the performance of the company activities, guaranteeing the

maximum efficiency of the process, rationalizing the procurements, in order to support the realization of the corporate strategy and optimize use of the company's financial resources, guaranteeing the utmost sharing of choices among all the divisions concerned by the procurement. Responsibility for the process falls within the perimeter of the Technology & Infrastructures department. [36]

3.3.2 Human Resources Processes

SIA has assigned to the Human Resources and Organization department responsibility for the personnel processes. A process was defined which describes the **personnel search, selection and recruitment** methods of SIA. [37] SIA has implemented a **performance evaluation** system aimed at assessing the performance level of the staff, evaluating the level of consistency of behaviors with the corporate values, giving value to distinctive professional competences by role; responsibility for the evaluation is assigned to each Head of Organizational Unit. [38] SIA has defined and applies a **training management** process aimed at planning and guaranteeing the adequate competence of the personnel in terms of study, training and experience, identifying any training needs and providing to meet them, assessing and recording the effectiveness of the training activities. [39]

3.3.3 Administration and Finance

SIA has assigned, to the **Finance and Administration** department, responsibility for the activities of an administrative, accounting and financial nature. Processes have been defined for **invoicing management**, which has the aim of defining the methods applied in the company and the responsibilities for invoicing [40], for **authorization of invoices payable** which has the aim of defining activities for receipt of goods and services and authorization for payment of invoices payable [41], for **credit and treasury management** which has the aim of defining the rules for recovery of credits and for management of incoming and outgoing financial flows [42][43], for definition of the **consolidated financial statement** which has the aim of defining the activities and information necessary for the correct and timely drawing up of the monthly statements and the annual financial statement, in fulfillment of the obligations of law. [44]

3.3.4 Communication

SIA, through the Communication department, manage communication activities implemented by the company to relate with external audiences. These activities are an important and delicate element for the development, consolidation and protection of the corporate image. [45]

SIA, in addition to the External Relations Policy, has defined the guidelines for **communication during emergencies and crises** to outline the guiding principles for communication during these situations, to identify the persons responsible and the addressees of the communication, the contents and roles of the communication. [46]

3.4 SIA Group: policies and quick guides

Following the international growth of SIA Group, 2018 saw the birth of a system of policies and processes issued by the parent company, aimed to be the guidelines and the direction for all the subsidiary companies. Among the policies prepared from a Group perspective, which can always be supplemented locally with specific regulations for the various countries, have been issued:

- Employee Attendance Policy
- Staff selection and recruitment process
- Training process
- Group Anti-corruption guidelines

- Guidelines for the definition of transfer price among Group companies
- Procurement management policy
- International mobility policy

As far as it concerns the business processes, in order to facilitate the understanding and the communication of shared rules, have been created the "Quick guides", synthetic documents aimed at the description of main processes and service models. These documents follow an innovative graphic standard with respect to traditional documents, full of graphics, flow charts, tables:

- Service model – Feasibility & Project Management – Quick guide
- Service model – Global Incident management process – Quick guide
- Service model – Global Problem management process – Quick guide
- Service model – Global Service Level management process – Quick guide
- Service model – Fast close – Quick guide
- Service model – Global Top Management Reporting – Quick guide
- Service model – Global Release management process – Quick guide
- Service model – Claim and Compensation management – Quick guide
- Service model – Client Audit management – Quick guide

4. MANAGEMENT SYSTEMS

SIA has defined its management systems for Risks, Quality, Information Security, Business Continuity, Compliance, Safety, Physical Security, Personal Data Protection and for Legislative Decree 231/2001.

Figure 1: Management systems

4.1 Risk Management System

SIA is aware of its exposure to risks, which are heterogeneous and dynamic. It is also aware of the impact these risks may have on its operations, on customer's operations, on payment systems, on financial community and citizens.

SIA - as the infrastructure for the payment systems and financial markets - is under the surveillance of Bank of Italy and has implemented a risk governance system and an internal control system through which it fights threats and vulnerabilities that may arise and jeopardize the delivery of its services.

SIA, taking inspiration from the international standard ISO 31000:2018 and taking into account the relevant provisions of the Bank of Italy, has defined its risk management process, which is represented as follows:

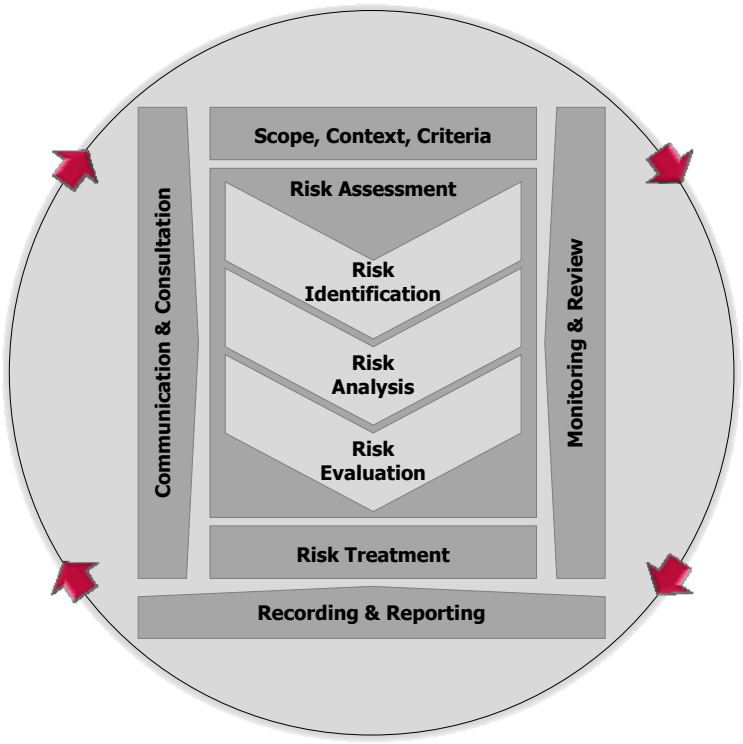

Figure 2: the Risk Management Process

SIA's risk management process:

- protects the value of the Company and pursues the corporate objectives;
- is integrated with the corporate organization and the processes, the initiatives being defined and the services supplied;
- addresses uncertainties with the best available information and is a component of the decision-making processes;
- is carried out in a systematic, structured, dynamic and documented manner;
- takes into account the human, perceptive and cultural factors that may facilitate the notifications of risks and evaluations of impact;
- is continually improved through learning and experience;
- is regularly assessed in order to guarantee that the process in its entirety is consistent with the corporate objectives.

SIA is aware that human behaviour and culture significantly influence risk management. For this reason an awareness program is in place to increase the risk culture in the Group, in particular to increase awareness of corporate risks, accelerate the taking of responsibility, validate and implement the Risk Policy.

SIA manages risk throughout the organizational structure. A Risk Team composed of representatives of company functions meets regularly. A Risk Committee is also in operation (with company management and the first levels). Specific information flows are provided to the top management.

4.2 ISO Certified Management Systems

SIA has achieved certifications for the management systems relating to Quality, Information Security and Business Continuity. These systems comply with the standards ISO 9001:2015, ISO/IEC 27001:2013 and ISO 22301:2012.

The Business Continuity and Information Security management systems are described in the documents: *Business Continuity in SIA* [49] and *SIA Information Security Management System*. [50]

In particular, for the management of information security, SIA has defined a Cyber Security department with the main aim of guaranteeing an adequate level of protection to the processes, the infrastructures, the services and the applications.

The department is responsible for protecting or addressing following Cybersecurity subjects and controls:

Cybersecurity governance and risk:

- ISMS management
- Security risk management
- Security awareness
- Security indicators

Cybersecurity operations:

- Security Engineering / architectures
- Identity and Access Management,
- Data Encryption, Key & Certificates Management,
- Security Infrastructure,
- Testing & Assurance,
- Security Monitoring,
- Threat and Incident Management.

The company has also defined a document system relating to security issues which consists of the Security Policy [67], and Security and Business Continuity Guidelines. [53]

The ISO certifications are managed by the Compliance System (par. 4.3.1), which also includes the PCI DSS certifications and the activities for the preparation of the ISAE 3402 reports.

4.2.1 Field of Application

Concept, design, development, marketing of infrastructure management services, professional services and IT solutions to Financial and Central Institutions, Corporates and Public Administration in the areas of payments and collections, e-money, services for retention of digital documents, network services, capital markets and large databases.

4.2.2 The Certified Management Systems Policy

SIA pays great attention to **Quality, Business Continuity**, and **Information Security**, as crucial elements in the supply of its services in full compliance with what is defined in the contracts with customers, in the Bank of Italy Guidelines and in the requirements of the other national and international industry regulatory bodies.

SIA has drawn up the Management systems of Quality, Business Continuity and Information

Security in compliance with the relevant standards at international level.

The Management Systems Policy indicates the principles adopted by SIA in order to operate in compliance with the requirements expressed by the relevant standards; it is regularly reviewed and updated if necessary to guarantee the constant meeting of the requirements by the parties concerned.

The Management Systems Policy defined by the Company management and distributed to all the staff expresses the following guiding principles:

- orientation towards customer satisfaction;
- attention to issues concerning the company's reputation;
- collaboration with the parties concerned;
- evaluation and management of the risks connected to the company processes;
- evaluation and management of security risks;
- guarantee of satisfaction of the customer's requirements;
- guarantee of respect of the applicable regulatory requirements;
- continual improvement of company processes through measurement and monitoring systems;
- behavioral and technical training aimed at guaranteeing the professionalism able to ensure customer satisfaction;
- adoption of a business continuity model which is recognized as a model of reference at international level and which enables the pursuit of continual improvement of the BCMS;
- regular review of the policy itself, implementation and maintenance of Management Systems compliant with the international standards ISO 9001:2015; ISO 22031:2012; ISO/IEC 27001:2013.

Relating to Information Security, the objectives of SIA's management system are shown in Group Information Security Policy. [72]

The Company management undertakes to pursue the objectives of this Policy with adequate resources and means, in order to reduce to a minimum the possibility of running into events that impact negatively on the achievement of the company objectives.

4.2.3 Objectives and planning for their achievement

The company objectives are defined in the Business Plan; in the long term, the plan lays the foundations for SIA to become a leading operator at international level, in particular in payment services.

Monitoring of progress in the activities defined in the Business Plan is done by the Strategies, Planning and Control department.

The specific objectives of the certified management systems are defined in the department reviews and monitored by the Risk Governance department. (4.2.10)

4.2.4 Addressing Risks and Opportunities

The following paragraphs illustrate the methods which SIA adopts to deal with risks and opportunities within the framework of the Quality, Business Continuity and Information Security management systems.

4.2.4.1 Process Risks

SIA has identified and documented the risks related to the **company processes** [Attach. 01]; these risks are dealt with through the **Risk Management System** in compliance with the risk management process. In addition, SIA has defined the risk objectives and alerts. [47][48]

4.2.4.2 Business Impact Analysis

Business Impact Analysis (BIA) is the evaluation of the impact on business in the case of significant events which could compromise the company activities and the supply of services. In order to direct the appropriate Business Continuity solutions, the requirements to restore the services are identified. SIA produces the Business Impact Analysis with the aim of assessing the services which are significant for the company business, identifying the impacts connected to the unavailability of the service, identifying the restoration times at contractual/regulatory level, identifying the most critical services, and identifying which activities need to be restored at a later time. SIA's Business Impact Analysis mainly involves analysis of the business services and identification of the critical activities using evaluation parameters which take into account constraints at regulatory level, contractual constraints with customers, significance of the service/activity for the company business, and strategic significance of the service/activity for the company. The BIA is updated with the information provided by the company structures involved and made available to the company for the preparation of the Disaster Recovery plans. [49]

4.2.4.3 Statement of Applicability

The SIA ISMS - Information Security Management System – is based on the **Security Risks Analysis**. The Analysis and Management of Information Security Risks is the process by which the Company identifies and adopts the type and level of security countermeasures to be applied, based on the riskiness and on adequacy respect to the value of the Information to be protected; the abovementioned process is aligned with the cyclical paradigm PDCA (Plan – Do – Check – Act, the Deming cycle). The process is based on a methodology which ensures and guarantees the identification, evaluation and treatment of Information Security Risks. In a manner compliant with the provisions of ISO/IEC 27001, the set of security checks applicable and applied constitutes the SoA document (Statement of Applicability). The Information Security risks treatment actions are collected and monitored in the PTRs-cs (Security and Security Compliance Risks Treatment Plan). [50]

4.2.5 Resources

The organization determines and provides the necessary resources for the establishment, implementation, maintenance and continuous improvement of the processes and business activities and the management systems.

4.2.6 Competence, Awareness and Communication

SIA has identified the competences necessary for coverage of the company roles included in the various professional categories.

The Human Resources and Organization department manages internal mobility through a job rotation system designed to provide adequate coverage of the needs of the various Organizational Units and to offer staff opportunities for professional development or change.

Within the Management Systems, regular awareness initiatives are carried out designed to spread, throughout the company, awareness of the issues relating to risk management, quality, information security and business continuity.

The Communication department has responsibility for the definition and management of internal and external communication plans and responsibility for management of relations with the

media; in addition the line Organizational Units are assigned responsibility for specific communications to customers.

SIA also draws up a Value Report which represents the evolution towards transparent and well-structured communication with its stakeholders and constitutes an important tool to illustrate what the Group has achieved in terms of sustainability, integrating the economic-financial information with that of a non-financial nature. [5]

4.2.7 Documented Information

SIA has defined a procedure for the Management of Documented Information which describes the operating methods used to manage the company documentation.

In particular, the management methods are defined which aim to guarantee:

- identification of the current version (approved) of documents;
- identification of the amendments made between different document versions;
- distribution and availability of the documents in the places where it is used;
- storage and identification of obsolete documentation;
- storage of documented information;
- management of documents with external origin/destination.

SIA has organized a document management system, which permits implementation of what defined by the procedure and structured into libraries. [56]

4.2.8 Monitoring, Measurement, Analysis and Evaluation

SIA has defined a monitoring system to keep the main company processes and compliance with service levels under control; the departments charged with collecting and monitoring the indicators are: Strategies, Planning and Control, Human Resources and Organization, Technology & Infrastructures and Risk Governance.

4.2.9 Internal Inspections

The Risk Governance department plans and carries out internal inspections of the Quality, Business Continuity and Information Security Management systems; these activities are designed to keep under control the correct application of the management systems and to identify areas for improvement. [69]

On the basis of the outcomes of the inspection activities, specific corrective actions are defined and planned.

Responsibility for implementation of the corrective actions falls on the owners identified; the Risk Governance department is responsible for keeping progress in the recovery plan under control.

The Internal Audit department is responsible for providing assurances on the overall adequacy of the Governance, Internal Control and Risk Management processes.

4.2.10 Department Review

The company management defines the objectives compliant with the policies of the management systems which are monitored and reviewed at preset intervals according to their level of criticality.

Control of progress in the objectives of the Quality, Information Security and Business Continuity Management Systems is regularly carried out in the Risk Governance department.

The Company management performs and documents the Review of the ISO management systems with the aim of checking the degree of adequacy of the Management systems.

The department Review is based on the analysis of the following document information:

- the results of the internal audit activities, with indication of Non-conformities, Observations and opportunities for improvement;
- feedback information from customers, with particular attention to claims and to the results of Customer Satisfaction surveys;
- indicators which measure the performances of processes, of the company and the related analysis;
- the working status of corrective actions undertaken;
- actions defined in prior Reviews and which are evaluated in the current Review;
- any amendments to make to the management systems and proposals to improve the System.

The outgoing elements from the department Review include the decisions and related actions:

- for improvement of the management systems and Processes;
- for improvement in the performance of services in relation to customers' requirements;
- The need for resources necessary to achieve the objectives and implementation of the decisions taken.

On a quarterly basis, the Risk Governance department performs review activities in order to keep under control the activities planned for the maintenance and evolution of the Management systems.

4.2.11 Non-compliance and corrective actions

For Certified Management Systems, the Risk Governance department manages the necessary corrective actions deriving from the outcomes of internal inspections or those by the Certification Body.

For each non-compliance, an owner and a recovery plan are identified; Risk Governance is responsible for identifying the owners and monitoring the working status and the effectiveness of the corrective actions defined.

4.2.12 Continual Improvement

SIA undertakes continually to improve its management systems using as a guide the policies, the objectives, and the results of the inspections, the analysis of the data and the department Review.

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

4.2.13 Planning of Amendments

The SIA Management Systems and System of processes provide for phases of planning, execution, control, review; they are continually updated and improved in relation to the customers' needs and the organizational needs of the company.

4.3 Other Management systems

4.3.1 Compliance Management System

In order to guarantee compliance with the regulatory requirements, SIA has defined a Compliance System, responsibility for which is assigned to a specific function of the Risk Governance department.

The Compliance System essentially comprises the following activities and cyclical phases:

- recognition, assessment and implementation of laws and sector regulations;
- support, training, information and internal consulting;
- monitoring (maintenance of certifications; preparation of ISAE 3402 reports, reconciliation with the Corporate Risk Management Plan).

During the recognition phase, the laws and sector regulations applicable to the company are identified and collected in a company database. In addition to the key information referring to said regulations, the obligations to which the company is subject and to which compliance is constantly monitored are identified as well. Moreover, there is an internal "alert" system to ensure widespread and extensive reporting on the new regulatory trends. Lastly, in the event of compliance risk, evidence is provided to the risk system for tracking within the Risk Management Plan and subsequent monitoring and management.

A specific "compliance team" has been established that meets periodically. [10][54]

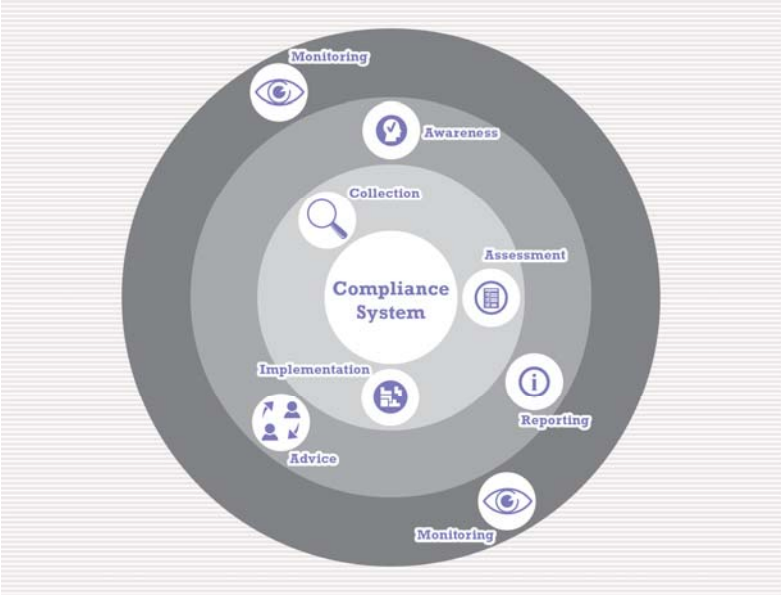

Figure 3: The Compliance Management System

4.3.2 The Personal Data Protection Management System

In order to comply fully with the law on Personal Data Protection and minimize risks deriving from the processing of personal data carried out by the Company, SIA has set up a specific Personal Data Protection Management System and, in accordance with new European regulatory (GDPR 679/2016) appointed a *Data Protection Officer* (DPO) with the task of:

- ensure compliance with the GDPR and continual improvement of the company regulations;

- interfacing the Supervisory Authority, the Data Protection Officer of customers and suppliers, the 'data subjects' and the organizational units of SIA and group companies for all topics related to privacy.

The organizational unit Data Protection Officer & Privacy Support (DPO) is under the authority of Board of Directors and is located within the Risk Governance department.

The fulfillments, coordinated by the DPO organizational unit, are carried out by all departments/divisions, each for their own area of competence. Responsibility for implementing the fulfillments falls on all staff, according to their role and competences, also with regard to the application by third parties involved in the performance of the activities.

The principal reference for the activities is the internal regulation set out in specific documents. [55] [56]

4.3.3 The Safety Management System

Safety at SIA is managed through a structured system which permits company results regarding safety and health at work to be kept under control and guarantees compliance with Legislative Decree 81/08. The system defines the methods to identify, within the company organizational structure, the responsibilities, procedures, processes and resources to realize the company prevention policy, in compliance with the law in force on health and safety, in order to make them more efficient and more integrated with general company operations, in a cycle of continual improvement. **Safety** is governed by the Risk Governance department through a system of processes and procedures in line with the law in force and with the international *best practices* and through a program of infrastructural, organizational, and training activities which involve all the staff and parties concerned. [59][60][61][62][63][64][65] [66] [71]

4.3.4 Physical Security

In compliance with the rules defined by the Cyber Security Management Organizational Unit to safeguard the company's information assets and the security of its premises, functions have been defined relating to active and passive anti-intruder systems, control of physical accesses, detection of irregular situations, fire-detection and fire-fighting systems, flood protection systems, video surveillance, power supply continuity and constructive technical security systems; responsibility for the security of the premises and control of accesses are assigned to the Technology & Infrastructures department.

4.4 Organizational Model 231

SIA has identified the type of offences applicable to its company context and defined its own Organizational Model 231 designed to prevent these offences from being committed. [68]

The Organizational Model 231 is a document consisting of a series of regulations which clarify the contents of the law and address the company activities in line with these regulations to prevent the committing of the types of offences considered in Legislative Decree 231/2001. In addition, it provides instructions on the methods by which to monitor the working and compliance with the law and the Organizational Model itself; this document is available on the company intranet and is accessible to all company staff.

SIA has chosen to entrust the functions of the Supervisory Body to the Board of Statutory Auditors granted autonomous powers of initiative and of control.

4.5 Sustainability

In 2015, SIA Group embarked on a journey towards corporate social responsibility, laying the

foundations for a structured and organic path aimed at creating sustainable value for the company and for all its stakeholders - customers, employees, shareholders, suppliers, the community and the environment - in compliance with the organization's objectives and according to an ethical and socially responsible business model.

Despite the specific nature of its sector of operation, in recent years the Group has placed a growing focus on social issues across a wide range of SIA's activities. These include:

- the accessibility of SIA services, ensuring that there is no discrimination based on financial literacy or geographical provenance;
- efforts to develop cutting-edge solutions designed to strengthen the economy for the benefit of not only direct customers, but also end users, and - therefore - the entire community through investment in innovative infrastructure and projects,
- a comprehensive policy to ensure equal opportunities for employees and realize initiatives for employees and their families with regard to work-life balance, welfare, health and safety, corporate environment and training;
- the promotion of social initiatives in favor of the local community, by supporting scientific research in the health field, as well as initiatives for disadvantaged categories of people;
- the protection of the environment and energy resources, becoming actively involved in initiatives such as the purchase of green energy and the production of energy from renewable sources.

In order to continue the journey undertaken some time ago towards excellence, innovation and the adoption of international best practices, the SIA Group has decided to combine the following documents for its 2018 reporting:

› the "Management Report and Financial Statements as at December 31, 2018" document, approved by the Shareholders' Meeting and submitted for financial auditing;

› the "Non financial disclosure 2018" document, voluntarily produced according to GRI Standards and submitted to the Board of Directors.

By combining our non-financial and financial reporting, the SIA Group aims to provide readers with a more comprehensive, organic and exhaustive view of the trend and performance of the SIA Group, not only from the economic-financial viewpoint but also in terms of ethics, social issues and the environment. [5]

GENERAL INFORMATION

Attachments

[Attach. 01] 1-CMS-2013-039-08-ALL01 v1 Processi e Rischi.

History of amendments

General changes across the entire document.

References

[1] ISO 9001:2015 Quality Management Systems – Requirements
[2] ISO/IEC 27001:2013 Information technology – Security techniques - Information security management systems – Requirements
[3] ISO 22301:2012 Societal security – Business continuity management systems – Requirements
[4] ISO 31000:2018 Risk management –Guidelines
[5] Management Report and Financial Statements as at December 31, 2018 and Non-Financial Disclosure 2018
[6] Code of Ethics
[7] Organigramma e funzionigramma aziendale (disponibili sulla intranet aziendale)
[8] Mansionario di SIA (allegato al Contratto Integrativo Aziendale)
[9] Risk Policy 1-RISK-2014-005
[10] Incarichi e flussi informativi per la Risk Governance 1-CMS-2011-021
[11] Processo di definizione del Piano Strategico 1-CMS-2012-039
[12] Processo di gestione delle Operazioni di Merger e Acquisition 1-CMS-2010-068
[13] La contabilità industriale di SIA 1-CMS-2011-049
[14] Procedura di gestione del budget infragruppo 1-CMS-2011-070
[15] Processo di Gestione delle Forniture Infragruppo 1-CMS-2011-060
[16] Linee guida Anti-Corruzione 1-CMS-2014-006
[17] Marketing & sales process 1-CMS-2016-013
[18] Processo di Gestione delle Offerte 1-CMS-2007-011
[19] Processo per la Gestione dei Contratti con i Clienti 1-CMS-2007-010
[20] Processo di gestione commesse con la Pubblica Amministrazione 1-CMS-2016-012
[21] Procedura di gestione dei rapporti con la Pubblica Amministrazione 1-CMS-2011-062
[22] Processo di Fattibilità e Project Management 1-CMS-2007-002
[23] ICT Incident Management Process 1-CMS-2007-003

[24] Cybersecurity Incident Management Process 1-CMS-2015-005
[25] NO ICT Incident Management Process 1-CMS-2008-004
[26] Processo di Gestione delle Emergenze e dello Stato di Crisi 1-CMS-2008-041
[27] Problem Management Process 1-CMS-2007-005
[28] RFC Management Process 1-CMS-2008-130
[29] Release Management Process 1-CMS-2008-131
[30] Service Level Management Process 1-CMS-2008-198
[31] Processo di ICT Capacity planning 1-CMS-2013-013
[32] Processo di gestione dei reclami, rimborsi e penali 1-CMS-2008-030
[33] Asset Management 1-CMS-2015-018
[34] Processo di qualificazione e valutazione dei fornitori 1-CMS-2008-072
[35] Supplier Risk Management 1-CMS-2015-020
[36] Processo di Gestione degli Acquisti 1-CMS-2008-014
[37] Processo di Ricerca, selezione e assunzione del Personale 1-CMS-2008-015
[38] Politica Gestione delle valutazioni 1-CMS-2013-003
[39] Processo di Gestione della Formazione 1-CMS-2008-017
[40] Processo di gestione della fatturazione 1-CMS-2013-018
[41] Autorizzazione delle fatture passive 1-CMS-2010-002
[42] Gestione del credito 1-CMS-2010-049
[43] Processo di gestione della tesoreria 1-CMS-2010-035
[44] Procedura per la preparazione del Bilancio Consolidato 1-CMS-2011-026
[45] External relations policy 1-CMS-2008-036
[46] Linee guida di comunicazione durante l'Emergenza o lo Stato di Crisi 1-CMS-2008-086
[47] Processo di gestione dei rischi 1-RISK-2014-006
[48] Obiettivi di rischio e segnali di allerta 1-RISK-2014-007
[49] La Business Continuity in SIA 1-BC-2014-001
[50] Il Sistema di Governo della Scurezza delle Informazioni di SIA 1-CMS-2010-005
[51] Visa-MC-Amex & CUP card processing compliance process 1-CMS-2014-015
[52] Identity and Access Management Process 1-CMS-2010-080
[53] Linee Guida di Scurezza e Continuità Operativa 1-CMS-2013-040
[54] Il Sistema di Compliance di SIA 1-COMPLIANCE-2014-013
[55] Privacy - Privacy Policy - 1-CMS-2008-004
[56] Privacy – Procedura Privacy – "How to do in SIA" 1-CMS-2018-015
[57] Gestione della Documentazione 1-CMS-2007-006
[58] Piano di Trattamento dei Rischi PTRs-cs
[59] Cruscotto adempimenti d.lgs. 81/08 1-SAFETY-2016-010

[60] La formazione obbligatoria ai sensi del d.lgs. 81/08 1-SAFETY-2018-004

[61] Check list del contesto di rischio negli ambienti di lavoro 1-SAFETY-2016-004

[62] I flussi informativi ai sensi del d.lgs. 81/08 1-SAFETY-2016-011

[63] Prove di evacuazione 2019 sedi Italia 1-SAFETY-2019-010

[64] Sopralluoghi di valutazione dei rischi safety sedi Italia 1-SAFETY-2016-002

[65] Documento di valutazione dei rischi 1-SAFETY-2016-003

[66] Piani di emergenza per le diverse sedi aziendali 1-SAFETY-2018-010, 1-SAFETY-2019-004, 006, 007, 008

[67] Information Security Management System 1-CMS-2010-021-02

[68] Modello organizzativo 231 SIA 1-CMS-2018-011

[69] Procedura per le Verifiche Interne dei Sistemi di Gestione certificati ISO 1-COMPLIANCE-2018-016-01

[70] Riesame della Direzione - Sistemi di Gestione Qualità, Business Continuity e Sicurezza delle Informazioni - Avanzamento obiettivi e attività a ottobre 2019 - 1-COMPLIANCE-2019-015

[71] Calcolo degli oneri di sicurezza ai sensi del d.lgs. 81/08 1-SAFETY-2018-002

[72] Group Information Security Policy 1-SECURITY-2018-016

[73] SIA Security Standards [1-SECURITY-2019-002 up to 1-SECURITY-2019-022]

APPENDIX A: REQUIREMENTS OF STANDARDS ISO 9001, ISO 27001 AND ISO 22301

The following paragraphs underline the mapping between the binding requirements of the law on the basis of which SIA is certified with the processes and elements of management systems.

	ISO 9001	**ISO 22301**	**ISO/IEC 27001**
4 Context of the organization	[11]	[10][53]	[10][53]
5 Leadership	[1][7][8]	[1][7][8][10]	[1][7][8][10]
6 Planning	[11][47][48]	[40][48][49]	[40][48][50]
7 Support	[34][35][36][37][38] [39][40][41][45][56]	[34][35][36][30][46][56]	[34][35][36][37][56]
8 Operation	[18][19][14][22] [23] [19][27][28][29][30][32] [31][33]	[18][19][14][22] [23] [19][27][28][29][30][32] [31][33][49]	[18][19][14][22] [23][19][27][28][29] [30][32][31][33][52]
9 Performance Evaluation	[11][48][69]	[11][48][69]	[11][48] [69]
10 Improvement	[69][70]	[49] [69]	[58] [69]

COVER KEY

Document status

The signatures on the cover of this document or entered electronically via the document system, refer to the internal standards of SIA for the management of the documentation: Their aim is to permit configuration control and to indicate their working status.

Please note that the 'approval' signature authorizes circulation of the document only to the distribution list and in no way implies that the document has been revised and/or accepted by any external bodies.

More specifically, the document shall be deemed to be **DRAWN UP** if it bears the signature/s of the person/s responsible for its preparation; **VERIFIED** if it has successfully passed the internal verification and therefore bears the verification signature/s; **APPROVED** if it bears the approval signature.

An unsigned document has an undefined status, and cannot be circulated.

Classification

The classification of a document may be:

- **PUBLIC**, if the document may be circulated without restrictions;
- **INTERNAL**, if the document may be circulated only within SIA;
- **CONFIDENTIAL**, if the document may only be distributed to a limited number of addressees;
- **STRICTLY CONFIDENTIAL**, if the document may only be distributed to a limited number of addressees and each copy is controlled.

Application domain

Companies in the SIA Group to which the document applies:

SIA Group if the document is valid for all the Group subsidiaries

SIA SPA, if the document is valid only for SIA

LIST OF SUBSIDIARY COMPANIES FOR WHICH THE DOCUMENT IS VALID.

…**list of names of the Group companies**…**,** if the document is valid for several group companies.