SIA Information Security Management System

Aim of the document:
Provide a presentation of SIA's Information Security Management System.

1-CMS-2010-005-05
13th October 2017

SUMMARY

1. INFORMATION SECURITY POLICY

1.1 Introduction

SIA considers information security a primary aspect for the protection of its business and clients.

The reputation of the company is based on its physical, information and personnel assets, so a security framework to protect business processes and information from a wide range of threats and to minimize the impact of any threats on the continuity of operations is fundamental to its preservation.

SIA Security posture also contributes to wider security objectives, including the cyber resilience improvement of whole financial eco-system meeting authorities, regulators and customers' expectations.

1.2 Policy statement

The Board and Management promote effective Information Security Governance by doing the following:

- Establishing an information security culture that promotes an effective information security program and the role of all employees in protecting the services and company's information, systems and infrastructure;
- Clearly defining and communicating information security responsibilities and accountability throughout the company;
- Providing adequate resources to effectively support the information security program;
- Choosing ISO/IEC 27001 as reference standard for its Information Security Management System.

This policy and related procedures that provide details on instructions to be followed apply to all SIA functions, employees and third-parties who use corporate ICT facilities, equipment and systems, or have access to, or custody of, corporate information.

The Information Security Policy is regularly reviewed or in case significant changes occur, in order to ensure its continue suitability, adequacy, and effectiveness.

1.3 Objectives

The main objectives of SIA Information Security Management System are:

- guaranteeing a proper protection of information in terms of confidentiality, integrity and availability;
- protecting the interest of clients, employees and third-parties;
- ensuring compliance with applicable laws and regulations concerning information processing and protection;
- ensuring a standard framework for information protection and the management of related risks;
- responding effectively to the growing threats to the information system in the cyber space.

They serve as foundation for the establishment, implementation, operation, monitoring, review, maintenance and continuous improvement of an effective information security management system, designed in line with ISO/IEC 27001 standard.

1.4 Roles and Responsibilities

SIA promotes a digital culture aware of security and privacy risks.

A security culture contributes to the effectiveness of the information security program. The information security program is more effective when security processes are deeply embedded in the SIA's culture.

To build a security culture, information security management system is organized as follows:

- Individual

  SIA Security Policy applies to all employees and third-parties who use corporate ICT facilities, equipment and systems, or have access to, or custody of, corporate information. They are responsible for adopting behavioral measures in line with the code of conduct, with the security guidelines, with the legislation and the contracts in force, with specific reference to the confidentiality clauses and to personal data protection according to the applicable laws.

- Management

  Management, in accordance with their area of competence, business or technical, are responsible and committed for integrating security policies and program into the SIA's lines of business, operations, support functions, and third-party management program.

  They are also required to inform suppliers and consultants that perform activities on behalf of the company, of the information protection guidelines and procedures required for information processing.

- Cybersecurity team

  A dedicated cyber security management team has been established for a dynamic, intelligence-driven approach to security into Operations Department.

  Cybersecurity function is in charge of managing directly the most critical security solutions, producing technical procedures concerning cybersecurity topics, ensuring the cyber-attacks identification, prevention and reaction by means of security analysis and control, tools and information sources both internal and external, ensuring security monitoring and the execution of security testing, designing the security of projects and initiatives, performing security risk assessments.

  Within Cybersecurity, SIA CERT plays a relevant role in managing cyber-security related events and in establishing info-sharing practices among recognized parties of the financial ecosystem.

- Security Representatives

  For each main Department (i.e. Divisions, Service Lines, etc) Security Representative
  - acts as reference for security matters
  - support for the central function of cybersecurity in identifying, evaluating and addressing the remediation of security risks and vulnerabilities
  - support in defining access criteria related to CIA levels with communication to the functions involved for their implementation
  - are members of Risk and Security Team where a status concerning security risks, emerging threats, treatment plan and compliance on security matters is shared and discussed.

- Risk Governance

  A Cybersecurity Governance organizational unit has been established into the Risk Governance, that is within Strategies, Risk, Finance & Control Department that reports to the CEO.

  This organization ensures that Cybersecurity Governance is separated from the IT and Business Service Lines and that Security Risks are managed in an integrated manner with other risk and control frameworks, i.e. Risk Management, Compliance, Business Continuity.

- Risk Committee

  Risk Committee is made up of SIA's main apical and management functions.

  Regular updates on cyber risks, the threat landscape changes and relevant mitigation activities are presented in this context in order to let the Board evaluating any discrepancy with Company objectives.

2. INFORMATION SECURITY MANAGEMENT SYSTEM

The effectiveness of SIA information security program is based upon:

- Applying systematic risk assessment practices;
- Performing situational awareness activities as threat intelligence and info-sharing, since they are adaptive risk management practices;
- Selecting, designing and implementing measures to mitigate security risks;
- Providing assurance and verification of security controls effectiveness;
- Reviewing the adequacy of the controls and effectiveness of the information protection system to ensure its continuous maintenance and improvement in the light of evolving threat, business, technological or normative context.

2.1 Risk identification, assessment and evaluation

In order to provide proper protection, requirements selection, controls implementation, maintenance, verification and enhancement are performed following a risk based approach and ensuring the adoption of best practices currently available to ensure compliance to relevant legislation on information processing.

Risk based approach is defined by means of methodologies and tools suitable to identify, assess and treat Information Security and Cyber Security risks.

Treatment activities are monitored within Security Risk Treatment Plan and Statement of Applicability provides the list of applicable controls to SIA context.

A systematic approach to information security risk management contributes to the Enterprise Risk Management Framework, giving an integrated view of all operational risks affecting business and internal services and determining a security posture that suits the needs of SIA business and risk objectives. Information and Cyber Security risk are categorized within Operational risk, defined as the risk of failure or loss resulting from inadequate or failed processes, people, or systems.

2.2 Threat Intelligence

In addition to risk based approach, the relevance and frequency of changes occurring in the business scenarios, technical ones and in the sophistication of criminal practices impose an adaptive security posture by means of detection and reaction capabilities to imminent threats.

Threat intelligence provides such benefits and contributes to update risk scenarios included in risk based approach.

The SIA CERT is interested in the issue of collecting and analyzing threat intelligence from the cyber domain under the context of situational awareness and how it can assist the organization to proactively defend its own information environment.

2.3 Information Security Training and Awareness

The Information Security culture is deemed by SIA to be a key value for the Company and is promoted through a continuous training and information process.
SIA realizes its awareness program through multimedia training sessions, tests and drills, participation in specific training courses as well as any other initiative that may be useful in spreading knowledge and awareness concerning security within the company.

All staff receive periodic information security awareness training, appropriate for their daily tasks and their function within information security.

2.4 Information Security and Business Continuity Guidelines

SIA has defined a set of documents relating to security issues that covers Security Policy, Security and Business Continuity Guidelines and Procedures.
The formalization of Security requisites and the articulation of the relative documentation on several levels permit the definition and the indication of governance and controls for the individual work activities.

Security and Business Continuity Guidelines are designed in line with ISO/IEC 27001 Annex A controls, PCI DSS requirements, Data Protection Regulations and other applicable industry best practices. These Guidelines are regularly reviewed, at the light of risk assessments results, laws and standard updates, the evolution of technological and threat landscape.

In addition specific controls are embedded into SIA internal processes and procedures such as identity and access management, service development lifecycle, change management, service management, vulnerability management, incident management.

Security and Business Continuity Guidelines provide criteria, requirements and controls that are designed to provide effectiveness to Information Security Policy objectives.

2.4.1 Organizational Security

People are a success factor to build effective information security within the company.

Criteria and controls are specified to address the risk introduced by people lack of knowledge and awareness regarding issues of security and business continuity and by innovative working methods (e.g. remote work), and to prevent fraudulent behavior.

Corporate functions responsible for managing the human resources must apply these criteria establishing the working methods, roles, training, working tools and personnel performance assessments during their entire working cycle.

The Guidelines include general rules on:

- Personnel selection and recruitment
- Security and business continuity roles and responsibilities
- Security and business continuity training and awareness
- Identity and Access Management system
- Disciplinary system

2.4.2 Information System Development

Security is the result of a process oriented towards continuous improvement and as such must be considered and pursued during the entire lifecycle of the information systems.

Appropriate security controls must be put in place to integrate information security and business continuity topics during requirements collection for new initiatives and in their feasibility evaluation, in order to guarantee that the related risks are identified and dealt with from the initial phases and not only after the creation of the solutions.

For any third-parties involved in the Information System acquisition, development and maintenance process, information security requirements must be included in any contract or service level agreement.

The document includes guidelines on:

- Security and business continuity requirements definition
- Secure development and engineering principles
- Outsourced development of information systems

2.4.3 Information System Management

Effective security levels can be achieved through diligent ordinary management of the information systems.

Appropriate security controls must be put in place to guarantee the secure operation of the information systems, mitigating the risks related to intentional and accidental threats such as data loss, changes to systems, networks and applications, depletion of system resources, introduction of malevolent codes, the detection and management of exploitable vulnerabilities.

These guidelines must be applied by the corporate functions that are responsible for managing and checking the correct development and maintenance of systems, networks and applications.

These guidelines include general rules on:

- Change management
- Logging and monitoring
- Data Backup
- IT resources separation
- Malware protection
- Technical vulnerabilities management and security testing
- Configuration management
- IT devices disposal
- Encryption, digital certificate management and control

2.4.4 Access Control

One of the security objectives is to guarantee confidentiality, that is the property of the information to be known only to authorized users.

Dedicated guidelines indicate controls to address the risks related to unauthorized access to information; these risks can lead to IT fraud caused by data theft.

Access to corporate information and information systems must be controlled through authentication and authorization process, based on principles to assigns correctly the access privileges, security rules to identify and authenticate user profiles and systems which access the information, and methods to define access privileges and rights.

All the personnel and external collaborators are accountable for guaranteeing the protection of their own authorization credentials.

The Guidelines include general rules on:

- User and system access in terms of identification, authentication and authorization
- User Responsibilities in ensuring proper protection

- Access to network services and networking controls
- Remote access

2.4.5 Information Classification

Information is a critical asset for the company; this requires that information must be protected in an appropriate manner respect to the value that the company itself directly or indirectly attributes to it (evaluation of customers, regulators or third parties). Corporate information must always be classified based on their sensitivity and relevance.

Criteria are defined for the information classification in order to prevent and address the risks related to non-observance of the regulatory obligations concerning failure to comply with the applicable provisions, points of criticality with respect to unauthorized disclosure or change of the same.

Classification is a mandatory requirement to perform Risk Assessment process.

Ownership must be assigned to information in order to ensure accountability in the information classification process. Information retention requirements must be identified as needed. Information classification must be periodically reviewed.

The document includes guidelines on:

- Information classification criteria
- Document classification and management

2.4.6 Physical Security

The information security is achieved by guaranteeing the protection of all the physical infrastructures (e.g. data centers, plants, IT equipment) which are necessary for the functioning of the information systems.

Guidelines are in place to guarantee the information systems protection against unauthorized physical accesses, damages and interferences to processing rooms and devices, in order to prevent loss, alteration, theft or compromise of the information assets, the business interruption and health and safety in the working environments.

There are dedicated corporate functions responsible for the management of the data-centers, the company premises and the related equipment in full collaboration with the security and business continuity function.

The Guidelines include general rules on:

- Physical area classification and responsibility assignment
- Physical access and perimeter security
- Sites protection from natural disasters and external threats
- Protection of work environments

2.4.7 Security Incident Management

A valid and effective approach to security is achieved by developing capabilities and tools designed to acknowledge and manage events threatening systems and information security.

A structured incident management process must be in place, defining all needed safeguards that guarantee a rapid, effective and systematic response to any actual or suspected information security incidents.

Figures involved in the process are: owner of the Incident Management process, technical structures involved in the Incident and Problem Management process, Points of contact towards customers and the Authorities, functions responsible for the management of Security and Business Continuity, each employee as a reporter of possible security incidents.

Moreover, all employees and contractual third parties have the duty to promptly report any actual or suspected information security incident.

The document includes guidelines on:

- Cyber Security incident management process
- Employee responsibilities in the incident management process
- Cyber intelligence capabilities

2.4.8 Supplier management

Typically, to attack larger and more structured companies, efforts are focused on weakest components which in this case might be the suppliers.

Dedicated guidelines suggest the definition of activities and agreements with the suppliers in order not to invalidate the overall level of security and business continuity and therefore to permit suppliers to be an enabling factor for business objectives achievement.

These guidelines apply to all corporate functions having responsibility in the selection and management of relations with suppliers.

2.4.9 Business Continuity

The growing complexity of financial services and of their supporting infrastructures, the intense use of information technology and the Customers and Supervisory Authorities expectations require that organizations like SIA consolidate their commitment to guaranteeing adequate business continuity levels.

The implementation of a business continuity management system and the related activities (e.g. drawing up of continuity plans, the performance of testing and awareness activities) permit the definition of roles, tools, procedures and skills to tackle the risk scenarios which have as a consequence the unavailability of offices and/or equipment rooms at the service supply sites resulting from natural events or human activities, and the personnel unavailability.

These guidelines must be applied by the personnel of Departments/Divisions with a role in the business continuity management system, and by the corporate functions involved in the definition and management of Disaster Recovery infrastructures, in the management of external communication and in the procurement of goods and services.

2.4.10 Security Compliance

In a framework of integration with the company's Compliance Governance, the Information Security Governance System takes into account the requirements of laws and industry regulations (for example the Privacy Code [4], PCI-DSS [6]) for the protection and processing of information.

Dedicated guidelines aim to avoid the occurrence of infractions of law, rules, regulations or contractual terms obligations for all concerning information and security requirements.

All relevant statutory, regulatory, contractual, business requirements and standards applicable to SIA's information and information systems, that have an impact on information confidentiality, integrity,

availability must be identified, documented and communicated to ICT.

The Guidelines must be applied by personnel responsible for identifying requirements connected to laws, regulations and standards, respect of the obligations resulting from the same and to controls and compliance level maintenance.

2.5 Information Security Management effectiveness

The information security program is subject to periodic review to ensure continual improvement in the program's effectiveness.

The review address the changes in the context of the environment in which the program operates, in terms of evolution in the threat, technological, regulatory or business landscape, as well as in stakeholders expectation on SIA Security posture. Lessons learned from experience, audit findings, and other indicators of opportunities for improvement are identified and the program is then changed as appropriate.

2.5.1 Security testing

Security testing is embedded into the application and systems development lifecycle. This, together with upskilling developers, ensures that security is made the personal responsibility for all teams involved into the information systems lifecycle.

A comprehensive security testing includes:

- vulnerability assessment;
- penetration testing;
- static and dynamic application security testing;
- simulations and exercises;

covering both two parts of the process: a) the IT system's design and b) the IT system's operation.

All the security testing activities are checkpoints where cyber preparedness is measured against known cyber vulnerabilities and attacks scenarios.

2.5.2 Metrics

Metrics that demonstrate the extent to which the security program is implemented and whether the program is effective, are designed. Metrics are used to measure security policy implementation, conformance with the information security program, the adequacy of security services delivery, and the impact of security events on business processes.

2.5.3 Audits and verifications

Internal audits and verifications are conducted to provide information on how information security management system is implemented and maintained.

2.6 Relationship with external stakeholders

SIA maintains strong relationship on security matters with Customers, relevant Authorities, security expert groups both at National and European scale, suppliers and other SIA Group companies and subsidiaries.

- Collaboration is the key in managing relationship with Customers and relevant Authorities.

  Indeed, information flows are maintained with Customers concerning security incident or imminent threats.

  In addition, leveraging on SIA CERT, trusted channels with relevant peers and counterparties have been established, performing info-sharing practices within financial market ecosystem.

  SIA is actively collaborating with institutions as ENISA, CNAIPIC (eg. the Italian national computer crime center for critical infrastructure protection) and CERTs; thus, contributing to enhance collective cyber defensive capabilities of a broader community.

- Control and monitor are the key in managing suppliers and third parties. SIA operates following two main directives:
  - ruling security requirements and obligations within agreements with third parties and suppliers;
  - extending risk management practices also on the most critical suppliers.

- SIA Security Governance and Cybersecurity department maintain coordination on security topics among SIA Group companies and subsidiaries in order to harmonize and make effectiveness in managing security risks mitigation.

GENERAL INFORMATION

Definitions

Acronym /Term	Definition
Availability	property of being accessible and usable upon demand by an authorized entity
Confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Effectiveness	extent to which planned activities are realized and planned results achieved
Information Security	preservation of confidentiality, integrity and availability of information
Integrity	property of accuracy and completeness
ISMS	Information Security Management System
Management System	set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives
Risk	effect of uncertainty on objectives. In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.
SoA	Statement of Applicability
Threat	potential cause of an unwanted incident, which may result in harm to a system or organization

References

[1] ISO/IEC 27000:2016 - Information technology. Security techniques. Information security management systems. Overview and vocabulary

[2] ISO/IEC 27001:2013 - Information technology. Security techniques. Information security management systems. Requirements

[3] ISO/IEC 27002:2013 - Information technology. Security techniques. Code of practice for information security techniques

[4] ISO 22301:2012 Societal security - Business continuity management systems --- Requirements

[5] Legislative Decree 196/2003 - Personal Data Protection Code

[6] Legislative Decree 81/2008 - Consolidated Law on safety in the workplace

[7] Payment Card Industry - Data Security Standard (version in force)

[8] 1-CMS-2013-039: SIA - Processes and Management Systems (version in force)

COVER KEY

Status of the document

The signatures on the cover of this document refer to the internal standards of SIA for the management of documentation in the Company Management System. 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 does not, in any way, imply that the document has been reviewed and/or accepted by external bodies.

More specifically, the document shall be considered **DRAWN UP** if it bears the signature/s of the person/s responsible for its preparation; **VERIFIED** if it has successfully passed internal verification and it bears the verification signature/s authorizing its release to CONFIGURATION MANAGEMENT. In the case where the review has a negative outcome, the document is amended and verified and shall bear a new version number and issue date. The document is considered **APPROVED** if it bears the approval signature, which shall be added to the others.

The status of an unsigned document is undefined, and the document 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 names of Group companies**…**,** if the document is valid for several group companies