The SIA Compliance Management System

SOMMARY

1. INTRODUCTION

The compliance function arises in the context of the supervisory activities in the banking system that have developed since the 90's as a result of the increased complexity of the system, the wide variety of products offered and the increasing internationalization of operations.

The growing awareness of the risks that may invest the entire system has prompted the regulatory authorities, national and international, to promote internal control activities at the organizational and regulatory, as well as the more traditional side sheet.

On the basis of observations of the Basel Committee, the organizations operating within the banking and financial system have provided for the adoption of the compliance function as an integral part of the system of internal controls in order to prevent the risk of non-compliance.

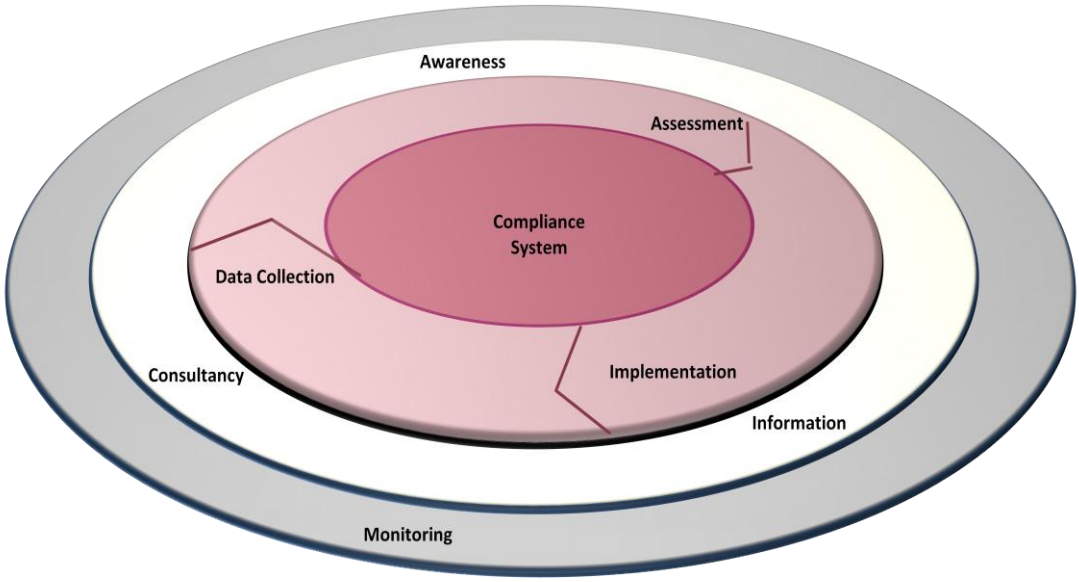
2. THE SIA COMPLIANCE FUNCTION

The Compliance department in collaboration with each SIA Department works to define and manage the corporate compliance management system.

In detail, the SIA Compliance function:
• leads the program for a government of systematic compliance with laws/regulations and standards subject to certification
• performs, in accordance with the SIA Departments, the collection of laws/regulations/standards applicable, identifies the applicable rules and monitors compliance with the main business obligations and deadlines
• maintains the SIA certifications for ISO27001 (Information Security), ISO22301 (Business Continuity), ISO9001 (Quality) and for PCI-DSS (Payment Card Industry – Data Security Standard)
• coordinates the activities for the preparation of the report ISAE3402
• maintains updated the SIA 231 organizational model, operating in contact with the Supervisory Board
• informs the Company Management and the SIA Departments on the compliance issues.

3. THE SIA COMPLIANCE SYSTEM

The SIA compliance system is structured in a part of program, in progressive development, and a part of operation, which is carried out continuously during the time, and ensures that, consistent with what has been implemented, the actualization of the program itself.



The complete picture of the SIA compliance system includes a series of cyclical phases and a series of supporting activities. The cyclicla phases are:

3.1 Data Collection

The data collection phase is aimed at:
·identify the laws/regulations applicable by the Company
·define the correlation between laws/regulations and basic elements (services)
·create/manage a system for monitoring the deadlines of the obligations that apply to the Company and provide an internal alerting service
·create a dashboard of certifications, accreditations and approvals of business and professional certifications, working groups and associations involving SIA.

3.2 Assessment

The assessment phase is aimed at:
·detect the status of implementation of laws/regulations and identification of any uncovered issues
·produce the Security and Compliance Risk Treatment Plan
·guarantee the alignment with the corporate Risk Treatment Plan, highlighting the risk of compliance that may arise.

3.3 Implementation

The implementation phase is aimed at:
- the application in the company of the laws / regulations of the industry, compliance issues in contracts, corporate regulations.

The supporting activities are:

3.4 Awareness

The awareness activity includes:
- the preparation and execution of the compliance awareness plan for the current year
- the maintenance and monitoring of its dashboard.

3.5 Consultancy

The activity of consultancy includes:
- responses to national and international compliance consultations (eg, the Bank of Italy and the European Central Bank)
- the progressive integration of issues of compliance into business processes.

3.6 Information

The activity of information includes:
- preparation of the annual information report on the activities of the SIA compliance management system
- periodic reporting of compliance to the Compliance Team and Risk Governance Committee
- preparation of the statement of compliance for the Annual Report.

Apart of the cyclical phases and support activities, the compliance management system includes the monitoring and certification phase, which is a series of activities that allow the operational management of the compliance system itself, and in particular:
- updating the document of compliance terminology
- maintaining the Quality (ISO9001), Information Security (ISO 27001), Business Continuity (ISO22301) and PCI-DSS certifications
- coordinating the preparation of the report ISAE3402
- developing the issues related to the Organisational Model 231, on the instructions of the SIA Supervisory Board.

APPENDIX A – GENERAL INFORMATION

A.1 Definitions

Acronyms / Terms	Descriptions
ISAE 3402	International Standard on Assurance Engagements 3402
PCI-DSS	Payment Card Industry – Data Security Standard
RGO	Risk Governance