



# Abstract of Security Policy

|               |                |                                |
|---------------|----------------|--------------------------------|
| Code<br>PY059 | Version<br>004 | Data of approval<br>10/02/2025 |
|---------------|----------------|--------------------------------|

The contents of this document are confidential and protected by copyright.

Any infringement shall be subject to legal action.

## Index

|  |           |
|--|-----------|
| <b>1 PREMISE</b> .....   | <b>3</b>  |
| <b>2 SCOPE OF APPLICATION</b> .....  | <b>4</b>  |
| 2.1 Roles and Responsibilities.....  | 4         |
| <b>3 MISSION AND SECURITY STRATEGY</b> .....   | <b>10</b> |
| <b>4 GOVERNANCE OF SECURITY</b> .....  | <b>11</b> |
| 4.1 Security Domains .....   | 11        |
| 4.2 Security Management Process .....  | 13        |
| 4.3 Annual report on the state of implementation of security initiatives and Summary report on the ICT and information security risk situation ..... | 16        |
| 4.4 Information Security Measuring and Reporting Performance .....   | 16        |

# 1 PREMISE

Banca Generali, within the competitive context and financial sector in which it operates, has the primary responsibility of protecting its tangible and intangible assets from any attack and unauthorized access.

The Security Policy (hereinafter also the “Policy”) describes the objectives, basic principles, and main responsibilities regarding security within Banca Generali and includes:

- IT Security, which involves protecting data and information systems from unauthorized access, use, disclosure, blockage, modification, or deletion to ensure data confidentiality, integrity, and availability.
- Cyber Security, which encompasses the ability to prevent security incidents or vulnerabilities in IT systems and to protect/defend the use of internet networks from cyberattacks.
- Physical Security, aimed at ensuring protection from unauthorized access to premises, equipment, and resources, as well as safeguarding Personnel during missions and business trips.
- Corporate Security, which pertains to managing security aspects in the most relevant corporate events (e.g., Shareholders’ Meeting) and, on the other hand, to activities such as brand abuse, social intelligence, and business intelligence, including the protection of intellectual property from attacks and damages (e.g., industrial espionage and data theft) also carried out in collaboration with external entities, as well as national and local public authorities to gather information related to specific cyber and physical threats affecting the monitored brands.
- Business Continuity, which includes the ability to ensure the maintenance of critical business functions at defined acceptable levels in case of events with High or Very High severity.
- Fraud Management, which covers the ability to prevent, detect, and mitigate risks arising from fraudulent activities perpetrated by external parties through remote banking channels, ensuring the implementation of advanced security measures, real-time monitoring technologies, and ongoing personnel training to promptly recognize and respond to fraud attempts.

The Policy aligns with and is consistent with the guidelines contained in the security policy of the Insurance Group, where not in contrast with sector regulations that the Bank is required to observe.

The Policy is based on international standards, frameworks, and best practices, and completes the body of normative Policies adopted by the Bank to determine the principles and guidelines for the security of IT applications and the integrated management of information data, aimed at supporting the Bank’s data-driven decisions and strategies. Matters relating to health and safety at work pursuant to Legislative Decree 9 April 2008, no. 81, are not included in this scope.

The principles and requirements regarding IT Security are further detailed within the Bank’s secondary-level regulations.

## 2 SCOPE OF APPLICATION

This Policy applies to all employees and collaborators of Banca Generali and the other companies in the Banking Group.

### 2.1 Roles and Responsibilities

The **Chief Security Officer (CSO)**, a role attributed to the Head of Security and BCP, the Bank's strategic vision for security, implementing programs to protect information assets and ensure the security of IT infrastructures, and for identifying, developing, and implementing processes to mitigate risks arising from the adoption of digital technologies.

The Chief Security Officer is therefore responsible for:

- supporting the definition of the Bank's security strategy, integrating the strategic security guidelines defined at the Generali Group level and considering the risk appetite set in the Risk Appetite Framework, outsourcing policies, the current and future structure of business sectors, processes, and the Bank's organization;
- preparing the Report on the status of implementation of security initiatives, including the Operational Plan of security initiatives and the Information Security training and awareness plan to be submitted for approval to the Chief Executive Officer/General Manager;
- defining, usually on an annual basis, the Operational Plan of security initiatives to achieve the objectives set in the strategy;
- assessing the specific needs of the Bank in terms of budget, investment planning, and resources (financial, human, technological, etc.), in order to ensure the correct implementation of the Operational Plan of security initiatives;
- defining, usually annually and in conjunction with the Chief People Office, the Information Security training and awareness plan to be submitted for approval to the Chief Executive Officer/General Manager;
- ensuring the monitoring of the implementation status of the Operational Plan of security initiatives and informing, usually annually, the Head of C.O.O. & Innovation and the Chief Executive Officer/General Manager;
- promoting, on a quarterly basis (or upon request by the Chief Risk Officer), a roundtable for a holistic examination of the various security components. Participants in the roundtable include: the Head of C.O.O. & Innovation, Chief Risk Officer, Chief Compliance Officer, Chief Audit Officer, Head of IT & Operations and, as needed, the Head of Territorial Network Assistance and Bank Branches, the Head of Logistics, the Head of Chief People Office, and the Head of Marketing, Training, and Communication. These meetings cover, among other things: a) the progress status of major ICT and security initiatives, b) any remedial actions planned and/or in progress on improvement areas identified by second-level control functions, and c) monitoring of first-level controls on security issues;
- implementing security governance within the Bank, in line with the Security Management

The contents of this document are confidential and protected by copyright.

Any infringement shall be subject to legal action.

process (as outlined in Chapter 5) and with the support of the organizational structures involved in the various processes;

- in agreement with the Chief Risk Office and in compliance with the security and reputational risk management methodology, identifying specific risks, collecting the necessary information for their assessment and verification, ensuring the adoption of appropriate mitigation measures across the various security domains (as described in Chapter 5);
- promoting, in the field of security, the adoption of measures to ensure the protection of personal data, liaising in this regard with the Data Protection Officer;
- defining the procedures for implementing a third-party security management process, in accordance with the ICT outsourcing and third-party management policy and considering the guidelines of the Generali Group;
- defining the procedures for implementing security measures and ensuring that such measures are implemented on systems managed by third parties;
- defining the procedures for implementing access control measures to the Bank's information systems, including privileged user access, and ensuring that such measures are implemented on systems managed by third parties;
- defining the procedures for carrying out an annual security test plan on the information systems managed by the Bank and ensuring that such checks are carried out on systems managed by third parties;
- defining the procedures for implementing a Security by Design process that allows for the implementation of appropriate security and protection measures during the acquisition phase of new technology, the design of a new IT system, or in the case of significant changes to existing systems (change management);
- in the event of a request from the Supervisory Authority for the execution of a Threat Led Penetration Test (TLPT), defining the scope specification document for the TLPT and informing the Bank's Board of Directors. The document includes: (i) the list and related information of Critical or Important Functions to be involved and (ii) a high-level description of the objectives of the testing activities;
- defining an incident management process for the Bank and promptly informing the Chief Executive Officer, the Board of Directors, and the Generali Group's security function in the event of Major incidents (incidents with High or Very High severity) and/or serious security threats;
- ensuring that procedures and technologies are activated, including services provided by the Generali Group (e.g., Security Operation Center, Group Cyber Threat Intelligence, Brand Abuse), to guarantee the identification of security events and the detection of security incidents;
- ensuring the adoption of a physical security framework and the security of events, supporting in this aspect Institutional Events, Corporate Communication, and Image in the management of the most relevant corporate events;

The contents of this document are confidential and protected by copyright.

Any infringement shall be subject to legal action.

- defining the procedures for implementing access control measures at the Bank's premises, and ensuring that such measures are implemented for the protection of data centers managed by third parties;
- ensuring the adoption of prevention measures and monitoring from an anti-fraud perspective of direct channels (Home Banking and Mobile Banking), collaborating with the relevant structures to provide information on losses incurred to the Chief Risk Office;
- ensuring reporting to the Chief Security Officer of the Generali Group regarding the status of security services according to the methods shared by the Group's security function;
- with the support of the Legal and Regulatory Hub, ensuring the updating of this Policy and the drafting/updating of the operational security Policies and regulations stemming from it.

The Chief Security Officer must be provided with adequate resources for their responsibilities and must not be involved in business activities to avoid conflicts of interest, and must report directly to the Head of the C.O.O. & Innovation Area.

In line with Banca Generali's HR processes and regulatory requirements, the Security Governance Model is defined as follows:

- Sourcing: the hiring and dismissal of the Chief Security Officer are the responsibility of the Head of C.O.O. & Innovation (in coordination with the Chief People Office) and in line with the Chief Executive Officer/General Manager.
- Performance evaluation: the definition and evaluation of the Chief Security Officer's objectives are the responsibility of the Head of C.O.O. & Innovation in agreement with the Chief Executive Officer/General Manager, according to the Group's procedures and processes in force from time to time.

The **Chief People Office**, with regard to physical security, is responsible, in coordination with the Chief Security Officer, for the operational aspects of staff security concerning business trips and assignments. Furthermore, the Chief People Office supports the Chief Security Officer in implementing training and awareness initiatives on security topics.

The **Deputy General Manager for Distribution**, through the Territorial Assistance for Networks and Bank Branches and Logistics, is responsible for:

- implementing the operational aspects of physical security, based on the Security Plan and in coordination with the Chief Security Officer;
- managing, for matters within their competence, the Group's Facility Management outsourcers;
- ensuring, based on the physical security risks identified by the Chief Security Officer, appropriate mitigation measures;
- verifying compliance with physical security requirements for all substantial changes to the Bank's offices, branches, and premises;
- promptly informing the Chief Security Officer of any threats to security or critical incidents (e.g., robberies) that have occurred.

In the context of staff security (e.g., robberies), *Territorial Assistance for Networks and Bank Branches*

The contents of this document are confidential and protected by copyright.

Any infringement shall be subject to legal action.

receives support and collaboration from the *Chief People Office*.

The **Chief Communication Office & External Relations**, in relation to Corporate Security and in coordination with the Chief Security Officer, is responsible for managing operational security aspects within the organization of corporate events.

The Head of C.O.O. & Innovation is responsible for:

- overseeing the implementation of the Security Plan and the Bank's security initiatives;
- supervising the proper implementation of Security Measures and periodically informing the Risk Committee on the security strategy within their areas of competence, the definition and execution of the operational security plan, and any security threats or critical incidents that occurred in the relevant period;
- approving and submitting, through the Chief Executive Officer, to the Board of Directors guidelines, directives, and management standards for IT Security regarding the evolution of the field, the products provided, and the technologies;
- taking the highest level of responsibility in managing highly critical situations, supporting the preparation of possible communications to supervisory authorities and/or to the corresponding role at the Group level.

These responsibilities apply to IT Security (infrastructure and data protection), Cyber Security (incident prevention and response), Corporate Security (IP protection, events, and intelligence), Physical Security (protection of offices and personnel), and Business Continuity (resilience and crisis response).

In line with HR processes and the regulatory requirements of Banca Generali, the Security Governance Model is structured as follows:

- Sourcing: the hiring and dismissal of the CSO are the responsibility of the Head of the C.O.O. & Innovation Area (following consultation with the Human Resources Department) in agreement with the CEO/General Manager.
- Performance evaluation: the definition of objectives and the evaluation of the CSO's objectives are the responsibility of the Head of the C.O.O. & Innovation Area in agreement with the CEO/General Manager, according to the procedures and Group processes in force from time to time.

The **Chief Risk Office**, in its control role, liaises with the Chief Security Officer to identify, assess, and verify the measures to be adopted for mitigating security risks, based on the risk propensity defined in the Bank's Risk Appetite Framework. Within the scope of managing security and reputational risks, the Chief Risk Office:

- promotes regular alignment with the Chief Security Officer and reviews the Bank's security risks;
- cooperates with the Chief Security Officer to collect the information necessary to quantify exposure to security risks;
- is promptly informed by the Chief Security Officer in the event of serious security or business continuity incidents and in the event of any occurrence that may significantly alter the level of

The contents of this document are confidential and protected by copyright.

Any infringement shall be subject to legal action.

security risks identified within the Bank's perimeter;

- is periodically updated by the Chief Security Officer on the status of implementation of security measures within its area of responsibility, specifically regarding the implementation of the security strategy;
- is periodically informed about the main Key Performance Indicators (KPIs) related to security within the Bank's scope.

The **Chief Compliance Office**, as part of its control role, periodically verifies the adequacy of security controls in relation to legal and regulatory requirements.

The **Chief Audit Office**, in its control function, periodically checks the effectiveness and efficiency of the defined standards, controls, policies, and procedures.

The **Risk Committee** supports the Chief Executive Officer in supervising the implementation and development of the Bank's security strategy.

Within the activities of the Risk Committee, security-related issues are addressed semi-annually for a holistic examination of the various components to ensure an integrated view of the different specialized and competent areas, under the responsibility of the Chief Security Officer, with the participation of the Head of C.O.O. & Innovation, the Deputy General Manager for Distribution, the Head of Chief People Office, as well as the Head of Chief Communication Office & External Relations.

The **Chief Executive Officer/General Manager**, as the management body:

- upon proposal from the Head of the C.O.O. & Innovation structure, appoints the Chief Security Officer;
- defines roles and responsibilities for managing security risk, as well as related business continuity activities;
- annually approves the Report on the state of implementation of security initiatives, including the Operational Plan of security initiatives and the Training and Awareness Plan on information security;
- ensures that all personnel, including those in key roles, receive adequate training on ICT and security risks;
- makes timely decisions regarding serious cybersecurity incidents and, with the support of the Company Control Functions, provides information to the Board of Directors in case of major business issues arising from incidents and malfunctions.

The **Board of Directors**, as the body responsible for strategic supervision, is promptly informed of any critical incidents or significant events related to security. Furthermore, the Board:

- approves the Bank's ICT strategy, including the strategic security guidelines, upon proposal by the Chief Executive Officer / General Manager;
- approves, with the support of the Control and Risk Committee, the organizational and governance structure of the Bank with reference to the information system and the management of corporate security risk;

The contents of this document are confidential and protected by copyright.

Any infringement shall be subject to legal action.

- ensures that the governance and control system for security risks is constantly adequate, also in terms of the qualitative and quantitative sizing of staff and available financial resources, to meet operational needs and to implement the security strategy;
- is informed by the Chief Executive Officer / General Manager regarding the Report on the state of implementation of security initiatives, including the Operational Plan for security initiatives and the Training and Awareness Plan on information security;
- is promptly informed by the Chief Executive Officer and/or the involved company control functions in the event of serious security incidents and malfunctions of the information system with an impact on the Bank's operational continuity.

### 3 MISSION AND SECURITY STRATEGY

The Bank's security strategy is based on an integrated One-Security model, which synergistically combines the areas of IT Security, Cyber Security, Physical Security, and Corporate Security, in line with the latest national and European regulatory trends.

This approach is rooted in regulations such as Regulation (EU) 2016/679 (GDPR) for the protection of personal data, the NIS 2 Directive (Directive (EU) 2022/2555) for the security of networks and information systems, and Legislative Decree 231/2001 on the administrative liability of entities, integrating the principles established by these regulations within the company's security policies and procedures.

Among the most significant strategic drivers are:

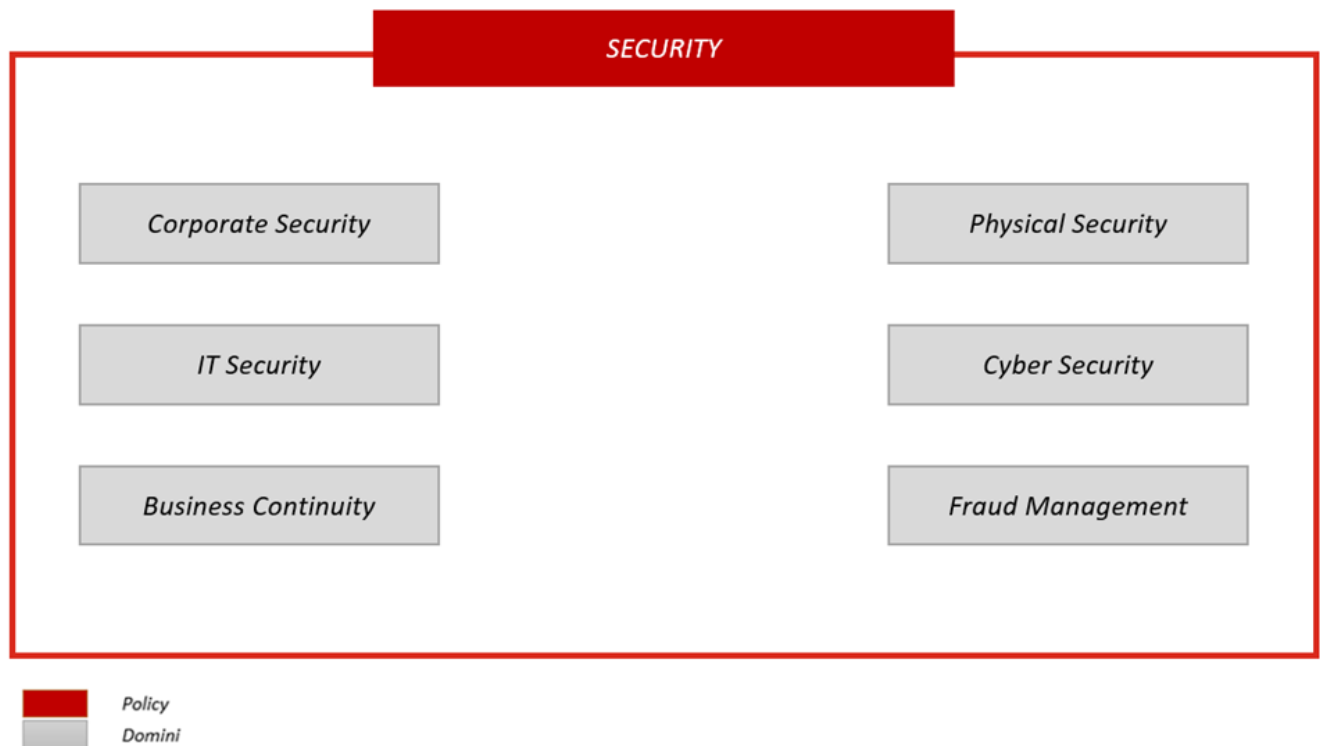
- **Prevention of incidents and protection from threats:** The Bank adopts appropriate technical and organizational measures to prevent harmful events and protect information, physical assets, and people, in accordance with Article 32 of the GDPR and the guidelines of ENISA (European Union Agency for Cybersecurity). Regular risk assessments and vulnerability assessments are carried out, also in compliance with the requirements set by the Bank of Italy regarding IT security.
- **Risk management, with a particular focus on third-party suppliers:** In accordance with Article 28 of the GDPR and the guidelines of the EBA (European Banking Authority) on outsourcing, the Bank conducts a thorough assessment of third-party service providers, regarding both data security and operational resilience. Every contractual relationship includes specific clauses on security, auditability, and regulatory compliance.
- **Corporate alignment and resilience of digital services:** The adoption of new technologies and innovative services takes place in compliance with applicable security requirements, as provided for by regulations in the banking and financial sector (for example, the Supervisory Provisions of the Bank of Italy and PSD2 for digital payment services). Operational resilience is ensured by business continuity and disaster recovery plans, also defined in accordance with international best practices (such as ISO/IEC 27001).
- **Regulatory and legal compliance:** All activities are constantly monitored and updated to ensure adherence to the requirements of sector regulations, such as GDPR, NIS 2, Legislative Decree 196/2003, and the guidelines issued by the relevant supervisory authorities. Ongoing staff training on security and privacy issues is also provided, as required by law.

In this way, the Bank's security strategy is structured as a dynamic and proactive system, capable of responding promptly to regulatory changes and new threats, ensuring the protection of corporate assets and the trust of customers and stakeholders.

## 4 GOVERNANCE OF SECURITY

### 4.1 Security Domains

This Policy includes the following security domains, as described below.



**IT Security's** primary objective is to protect the company's data belonging to customers, employees, and business partners, including implementing measures to safeguard infrastructures, applications, endpoints, mobile devices, and data.

**Cyber Security's** main goal is to ensure the prevention, identification, and response to security incidents and vulnerabilities in the information system, also considering the growing relevance of global cyber threats.

**Corporate Security's** primary aim is to preserve assets and intellectual property and includes principles and requirements to prevent, deter, delay, and mitigate possible threats, minimize related consequences, and properly and promptly manage security aspects in the most significant company events (such as the Shareholders' Meeting). It also covers business intelligence activities carried out in cooperation with local and national public authorities to gather information on specific economic, political, and financial situations concerning countries and/or competitors and partners. Corporate Security also pertains to security intelligence activities for the protection of the Bank's brands and products, monitoring digital media conversations and harmful online activities.

**Physical Security's** main objective is to prevent, deter, delay, and mitigate possible threats,

The contents of this document are confidential and protected by copyright.

Any infringement shall be subject to legal action.

minimize related consequences, and manage potential security incidents concerning workplaces and personnel in an appropriate and timely manner. Physical Security refers to the definition, implementation, and monitoring of physical security measures necessary to ensure a minimum level of safety for company buildings and internal workspaces, adopting a risk-based approach. It includes defining and implementing actions and measures to guarantee Personnel safety during business trips.

**Business Continuity** primarily aims to ensure the Bank's operational continuity, identify priorities, and prepare solutions to address disruptive threats, providing a framework for effective response that safeguards its key stakeholders' interests, reputation, and value-creating activities. The business continuity domain includes identifying critical operations and risks, preparing plans to maintain or restore critical operations during a crisis, and developing plans for communicating with key personnel during emergencies.

**Fraud Management's** chief goal is to protect the integrity of banking operations, safeguarding the Bank and its customers from fraudulent activities. This objective is achieved through security actions that prevent potential vulnerabilities in banking processes and transactions, by adopting technologies for continuous detection of suspicious activities, and by implementing effective measures to limit the damages from fraudulent attacks, protecting bank assets and customer interests.

## 4.2 Security Management Process

The Chief Security Officer, in collaboration with Risk Management and with the support of the IT & Operations Department, keeps the inventory of ICT third parties up to date and subjects them to security assessments within the scope of the Third Party Security (TPS) process.

The Chief Security Officer, a central figure in the company's security structure, works closely with the Risk Management function and the active support of the IT & Operations Department. This synergy allows for constantly updated mapping of ICT third parties, ensuring an accurate census of suppliers, partners, and collaborators who access the Bank's sensitive resources and data.

Within the Third Party Security (TPS) process, regular security assessments are conducted on third parties, both during onboarding and throughout the contractual relationship. These assessments include risk analysis related to outsourcing services and the use of third-party technologies, verification of compliance with regulatory requirements and company security standards, and, where necessary, the introduction of specific mitigation measures.

The Chief Security Officer also oversees the definition and updating of procedures related to third-party management, promoting a shared security culture not only within the organization but also among all external entities involved. Through periodic audits, controls, and targeted training sessions, it is ensured that all parties comply with the required standards and that any critical issues are promptly identified and addressed.

These activities, integrated into business processes, strengthen the Bank's overall security posture, reducing the risk of exposure arising from relationships with external suppliers and partners and contributing to a proactive management of threats in today's increasingly complex digital landscape.

To correctly and effectively apply the above principles, the Bank adopts a security management process consisting of the following sub-processes:

- A. identification,
- B. protection,
- C. detection,
- D. response,
- E. recovery.

These sub-processes should be carried out continuously to foster a security-focused operational culture.



### **A) Identification**

This phase aims to identify security risks and assess their exposure, taking into account the evolution of threats, the business impacts in the event of incidents or security breaches, and regulatory requirements. The Chief Security Officer collaborates with the Chief Risk Office in identifying security risks, as well as in evaluating all security measures and the specific needs of the Bank necessary to mitigate such risks.

When assessing security risks, the following must be considered:

- The business context, based on the Bank's mission and strategy, objectives related to digital operational resilience, stakeholders, and core activities;
- The inventory of company assets, which includes data, personnel, IT devices, IT systems, and infrastructures that enable the Bank to implement its security strategy and ensure the management of security aspects;
- The management of third-party security, based on every security risk connected with such parties. In this regard, proper classification of the involved third parties must be ensured, their compliance with the security requirements set by the Bank must be verified, appropriate monitoring activities must be defined, and any security risk due to possible service or agreement interruptions must be identified;
- Security regulations, based on external supervisory provisions and the Bank's internal regulatory framework on security, as well as the specific activities put in place to manage and monitor the Bank's compliance with security requirements; to this end, the Chief Compliance Office provides guidance to the Chief Security Officer in defining processes, internal

The contents of this document are confidential and protected by copyright.

Any infringement shall be subject to legal action.

procedures, and organizational safeguards in accordance with internal regulations and external security provisions.

In addition, the Chief Security Officer must:

- Coordinate and support the security structures of the Subsidiaries within their area of responsibility, ensuring alignment with the methodology in place to properly identify exposure to security risk;
- Share identified common risks with the security structures of the Subsidiaries within their area of responsibility;
- Inform the Chief Risk Office and the Generali Group security function of any significant risks identified within the scope of the Subsidiaries.

### **B) Protection**

This phase aims to define the security measures to be implemented in order to protect the Bank's assets, based on the risk assessments carried out in the previous phase, updating the Bank's Operational Security Plan and the Information Security Training and Awareness Plan.

Security measures, also with a view to ensuring effective digital operational resilience, may cover at least the following areas:

- Identity management, authentication, and control of logical and physical access
- Data security
- Secure development of information services
- Secure management of operational activities on information systems
- Management of logs and IT traces
- Measures to protect against cyber fraud on direct channels
- Training and awareness of staff on security topics

### **C) Detection**

This phase aims to ensure continuous monitoring of potential security threats and the identification of security incidents, through the timely detection of anomalous activities, allowing for the evaluation of potential associated impacts.

### **D) Response**

This phase aims to implement appropriate activities to contain the impacts resulting from security incidents, enabling the definition of suitable strategies and timely mitigation actions.

### **E) Recovery**

This phase aims to develop and implement appropriate activities to maintain resilience plans and restore all capabilities or services affected by a security incident.

### **4.3 Annual report on the state of implementation of security initiatives and Summary report on the ICT and information security risk situation**

The Chief Security Officer prepares, within the first half of the year following the analysis period, the Annual Report on the state of implementation of security initiatives, on critical incidents that have occurred, and on training initiatives carried out. With particular regard to the latter aspect, the Report also includes the Operational Security Plan and the Information Security Awareness and Training Plan. In order to ensure an integrated view of the various security areas, the Chief Security Officer will be supported by the structures involved in the operational aspects of security.

The Operational Security Plan is defined by the Head of C.O.O. & Innovation, through the Chief Security Officer and with the support of the relevant structures, each for their area of expertise, and is submitted in a joint document for the opinion of the Risk Committee, in order to outline a summary with the key elements.

The Plan is annual and is reviewed whenever a significant change occurs (such as changes in the organizational model, legislation, market, regulations, the cyber threat landscape, etc.).

The Report on the state of implementation of security initiatives is first validated by the Head of C.O.O. & Innovation, who presents it to the Risk Committee for an opinion, and then submits it—together with the Operational Security Plan and the Information Security Awareness and Training Plan—for approval by the Chief Executive Officer.

The Report is then submitted to the Board of Directors by the Chief Executive Officer.

The Chief Risk Office, on the other hand, prepares the Summary Report on the ICT and Information Security Risk Situation and the Report on the Results of the Operational and Security Risk Analysis related to payment systems, with the support of the Chief Security Officer and C.O.O. & Innovation, as indicated in the ICT and Information Security Risk Analysis and Management Policy.

### **4.4 Information Security Measuring and Reporting Performance**

The area of information security performance measurement and reporting is essential for enabling the Bank, thanks to data provided by both external partners and internal resources, to continuously monitor the effectiveness of its security management model over time.

Through specific key performance indicators (KPIs), the Bank can promptly identify areas for improvement and strengthen processes, procedures, services, and technological tools supporting its activities.

The identification and collection of KPIs are entrusted to the Security and BCP Service, which on a quarterly basis shares the “Cyber Risk” KPI with the Risk Management Department, integrating it into the company RAF.

Within the security management system framework, the Bank adopts an integrated and coherent set of measures designed to protect information and ensure operational resilience against external threats.

A key element concerns security in human resource management (OdS3). In this context, security requirements in onboarding, ongoing employment, and offboarding are formalized, clarifying roles and responsibilities, regulating onboarding and offboarding, ensuring the return of devices and revocation of credentials, promoting ongoing periodic training, and applying, when necessary, disciplinary measures for policy violations.

As for supplier relationship management (OdS12), the Bank includes specific security requirements in contracts and agreements. In this way, it ensures that the services provided comply with internal standards and regulations, supports the monitoring of partner security performance, periodic verification through audits, as well as the definition of incident response plans involving outsourced services.

The management of ICT third parties also requires maintaining an up-to-date inventory, in collaboration with IT and Operations, and periodic supplier assessments according to information security and risk criteria (TPS), so as to promptly detect any issues and plan corrective actions.

Overall, these measures, organically integrated into the Bank's security framework, not only ensure regulatory compliance but also strengthen the protection of infrastructures and shared information. That consolidating the organization's ability to respond effectively and dynamically to potential threats.