



## ICT Policy Abstract

Code PY076	Version 001	Date of approval 24/01/2025
---------------	----------------	--------------------------------

The contents of this document are confidential and protected by copyright.  
Any infringement shall be subject to legal action.

**CONTENTS**

<b>1 INTRODUCTION.....</b>	<b>3</b>
<b>2 ROLES AND RESPONSIBILITIES.....</b>	<b>3</b>
<b>3 ICT MANAGEMENT AREAS.....</b>	<b>3</b>
3.1 DEFINITION AND APPLICATION OF THE ICT STRATEGY .....	3
3.2 ICT OPERATIONS MANAGEMENT .....	3
3.3 ICT INCIDENT AND PROBLEM MANAGEMENT .....	4
3.4 THIRD PARTY MANAGEMENT.....	4
<b>4 OTHER INFORMATION .....</b>	<b>4</b>

## **1 INTRODUCTION**

Banca Generali's ICT Policy is a strategic document that defines the vision, mission, and strategy in the field of Information and Communication Technology (ICT). Its purpose is to guide the organization's technological evolution while ensuring security, efficiency, and alignment with corporate objectives.

The ICT vision considers technology services as a key business driver, while the mission focuses on supporting the company's strategy through cost optimization, revenue growth, and risk mitigation.

The ICT strategy is based on a full outsourcing model and aims to provide simple, secure, and resilient tools. It rests on two fundamental pillars: a structured governance model with clearly defined roles and responsibilities, and effective management of ICT processes.

## **2 ROLES AND RESPONSIBILITIES**

ICT governance is structured across multiple levels. The Board of Directors is responsible for defining and approving the ICT strategy, overseeing digital operational resilience, and monitoring incidents and projects. The Chief Executive Officer and General Manager is accountable for implementing the strategy, evaluating ICT performance, and training staff on cyber risk awareness.

The COO & Innovation supports the definition and monitoring of the strategy, promoting ICT culture and awareness. The IT function serves as the reference point for managing infrastructure, applications, and vendors, while the Security and BCP (Business Continuity Planning) functions handle physical and cyber protection.

Finally, the Chief Risk Office performs second-level control over ICT and cybersecurity risks.

After outlining the key roles in ICT governance, the Policy delves into the management areas, detailing the core activities required to implement the strategy.

## **3 ICT MANAGEMENT AREAS**

### **3.1 Definition and application of the ICT strategy**

The ICT strategy is updated every three years by the IT function, in alignment with the corporate strategy and with the support of the COO & Innovation. It is translated into an action plan structured around objectives, timelines, and projects, with a particular focus on security, architectural evolution, and vendor dependency management.

The strategy also includes the definition of ICT capabilities, convergence towards common operating models, and continuous monitoring of results. A central element is the integration with the security strategy, with specific controls to protect assets, processes, and third-party relationships.

The COO & Innovation is responsible for reporting annually to the Board of Directors on the implementation status of the strategy, while the Chief Executive Officer evaluates ICT performance and approves reports on costs and services.

Once the strategy is defined, it is essential to ensure its implementation through effective operational management. The next section describes the activities related to Operations Management.

### **3.2 ICT Operations Management**

ICT operational management covers the full lifecycle of assets, from traceability to maintenance and disposal. The Bank ensures detailed mapping of assets and supported processes, with classification based on confidentiality, integrity, and availability. Activities include patch management, backup and restore, performance and capacity management, also for outsourced services.

ICT operations must comply with regulations and ensure security, sustainability, and business continuity.

Another crucial aspect of ICT management is the ability to respond promptly to incidents and problems. The following section outlines the Incident and Problem Management process.

### **3.3 ICT Incident and Problem Management**

The Bank has established a structured process for managing ICT incidents and problems, including classification, tracking, root cause analysis, and corrective actions. Escalation procedures are in place, allowing employees to report incidents, vulnerabilities, and suspicious activities, with both internal and external communications to stakeholders. The IT function is the focal point for managing incidents and problems, using dedicated tools to track service requests. The process also includes crisis management and information sharing with the security function to ensure operational resilience. Finally, the Policy addresses Third-Party Management, a fundamental element in an ICT model based on outsourcing.

### **3.4 Third Party Management**

The Bank periodically monitors ICT suppliers through SLA, KPI, and KRI, proportionate to the criticality of the service. Specific cybersecurity requirements are defined for third parties, in line with the Group Policy. This approach ensures that outsourced services also comply with the Bank's defined security and quality standards.

## **4 OTHER INFORMATION**

The ICT Policy highlights additional management areas that complete the strategic and operational framework outlined in the document:

- It is emphasized that the IT function defines technological standards, ensuring uniformity, interoperability, and security among corporate systems.
- The adopted ICT architecture is described, it is structured into front-end, workflow, back-end, and core services, with the involvement of the outsourcer CSE.
- ICT project management is addressed, with a structured framework for planning and monitoring, coordinated by IT and Project Governance.
- The acquisition and development of ICT systems are discussed, with security requirements from the early stages, separate environments, and thorough testing.
- ICT Change Management is referenced, with a formal process to minimize risks and ensure traceability and security.
- ICT Risk Management is mentioned, integrated into the Bank's Risk Appetite Framework.
- ICT human resources and budget management are mentioned, with attention to continuous training and economic planning.