Guidelines on ICT and Security Risk Management

CONTENTS

KEY REGULATORY AND INFORMATION CONTENT 3
GENERAL ASPECTS 4
ICT AND SECURITY RISK MANAGEMENT MODEL 6
OBJECTIVES 6
ELEMENTS OF THE ICT AND SECURITY RISK MANAGEMENT MODEL (REFERENCE FRAMEWORK) 7
General Overview 7
Business Functions and Processes 7
Responsible Users 7
IT Resources 8
Risk Factors 8
Risk Scenarios 8
Impact of Risk Scenarios 8
Risk Mitigation Measures 8
Exposure and Vulnerability of Resources 9
Probability of Risk Events 9
Assessing the Level of Risk 9
Key Risk Indicators 10
ANALYSIS METHODOLOGY 10
General Overview 10
RISK MANAGEMENT AND ACCEPTANCE 11
REPORTING TO THE BOARD WITH STRATEGIC OVERSIGHT 11

KEY REGULATORY AND INFORMATION CONTENT

The Bank of Italy's Circular No. 285/2013, entitled "Supervisory provisions for banks", outlines in Part One (Implementation of CRD IV in Italy) - Title IV (Corporate governance, internal controls and risk management) - Chapter 4, the general requirements for the development and management of the **Information System** by financial intermediaries.

The Montepaschi Group assigns the responsibilities of the ICT Risk Control and Security Function, as defined in Circular 285/2013[1], to the **Chief Risk Officer** and the **Compliance Function**, in accordance with the roles, responsibilities and competencies specific to each function.

The Guidelines establish the organisational and methodological framework adopted by the Group for the execution of the "ICT Risk and Security Management" process, within the responsibilities and competencies of the **Risk Control** Function.

To this end, this Montepaschi Group document includes:

- The definition of the reference organisational model, identifying the roles and responsibilities involved in the ICT and Security Risk Management process, including the preparation of documentation to be submitted to the Corporate bodies;
- The establishment of a methodological framework for the identification, analysis, evaluation, monitoring and communication of ICT and security risks, ensuring that these risks remain within the limits of the Bank's defined risk appetite.

[1] Bank of Italy Circular no. 285, Title IV, Chapter 4 - Information System: Section II - Management, Organisation and Control of the Information System (point 4 - The ICT and Security Risk Control Function) and Section III - ICT and Security Risk Management.

GENERAL ASPECTS

Bank of Italy Circular No. 285, entitled " Supervisory Provisions for Banks ", sets out a series of general requirements for the development and management of information systems by financial intermediaries[2]. Among these, the Circular specifies the requirements for the implementation of a comprehensive organisational and methodological framework for the execution of the ICT and security risk management process, assigning management and control responsibilities to a second-level control Function[3].

The Montepaschi Group, in accordance with the Group Policy on Internal Control Systems, assigns the responsibilities of the **second-level control Function for ICT and security risks** to the **Risk Control** function and the **Compliance** function, in accordance with the roles, responsibilities and competencies specific to each of these functions.

The *ICT and Security Risk Management* Guidelines define the organisational and methodological framework for ICT and security risk management adopted by the Group.

As defined in the Group Policy on Internal Control Systems, the **first-level controls** over ICT and security risks are provided by the **Information Technology** and **Information Security** functions, which are responsible for establishing and implementing procedures, safeguards and controls appropriate to mitigate the risks. In all cases, all business Functions, Group employees and third-party suppliers share primary responsibility for the prevention of ICT and security risks through the proper application of the established procedures, safeguards and controls designed to mitigate these risks.

ICT and security risk is defined by Circular 285/2013 as the risk of incurring losses due to breaches of confidentiality, insufficient integrity of systems and data, inadequacy or unavailability of systems and data, or the inability to replace information technology (IT) within reasonable time and cost limits in response to changes in external requirements or business activities (agility). This includes security risks arising from inadequate or failed internal processes and external events, such as cyber-attacks or inadequate physical security measures. In the Internal Capital Adequacy Assessment Process (ICAAP), this type of risk is categorised into operational, reputational and strategic risks based on specific aspects.

[2] Bank of Italy Circular no. 285, Title IV, Chapter 4 - Information System.

[3] Bank of Italy Circular no. 285, Title IV, Chapter 4 - Information System: Section II - Management, organisation and control of the information system (point 4 - The *ICT and security risk control function*) and Section III - ICT and security risk management.

The ICT and security risk management process must be fully integrated and aligned with the Bank's overall risk management process. The objective of this process is to provide the decision-making bodies and individuals responsible for managing ICT and security risks with the necessary elements of judgement to manage these risks in accordance with the limits established in the Bank's **Risk Appetite Framework (RAF)**.

The ICT and security risk management methodology comprises a set of rules and procedures designed to:

- identify, analyse and assess the ICT and security risks to which the Bank is exposed;
- monitor the evolution of these risks and the effectiveness of risk mitigation measures.;
- communicate the risks to the relevant decision-making bodies and individuals authorised to manage them.

ICT and security risks are identified by considering events or a series of related events that may have a negative impact on the integrity, performance, availability, continuity, confidentiality and authenticity of the data managed by the information system, the business processes or the services provided to customers, as well as on the ability of ICT systems to evolve. Homogeneous risk events, grouped by type of threat and impact on IT systems and processed information, are organised into 'risk scenarios'. ICT and security risk is assessed by combining the estimated probability of occurrence of these risk events/scenarios with the potential negative impact on the Group, measured in terms of economic, reputational and market share loss.
The ICT and security risk management process applies to significant development and change initiatives within the information system, as well as to existing IT resources.

The organisational model established for ICT and security risk management formalises the role of the **Responsible User**, a corporate figure identified for each ICT system, who formally assumes responsibility on behalf of the users and in interaction with the relevant Functions responsible for technical development and management[4]. The Responsible User participates in the ICT and security risk analysis process and formally accepts the risk mitigation measures and residual risk.

[4] The definition is provided in Circular 285/2013 Title IV - Chapter 4 - Section I - Point 3 - *Definitions*.

The analysis of ICT and security risks is carried out with the support of the **Responsible User**, the **Information Technology** Function, the **ICT and Security Operational Risk Control** Function, **the Information Security** Function and, where appropriate, the **Compliance** and **Internal Audit** Functions, according to the methodology and responsibilities outlined in this document, taking into account the respective organisational roles and competencies. In cases where IT resources are managed by external providers through outsourcing or cloud services, the provider and the **Outsourced Activity Representative (OAR)** are also involved in the analysis.

As part of the management of ICT and security risks, the **Compliance** Function monitors the risk of non-compliance within the information system. It carries out assessments of compliance with external and internal regulations, performing second-level controls (Part One, Title IV, Chapter 4 of Bank of Italy Circular no. 285) in accordance with the responsibilities assigned by the internal policy for the management of non-compliance risks.

Specifically, the Compliance function is responsible for defining and updating the overall process for managing the risk of non-compliance in relation to the information system, in particular in the ICT and security areas. Within Banca MPS, the activities of the Compliance function are divided into the following components:

- **Advisory**, which:
  - continuously identifies regulations applicable to the Group and the associated risks of non-compliance affecting business processes, assessing their implications in terms of potential penalties and reputational damage;
  - validates internal regulatory documents related to the information system, cyber security, business continuity, payment systems, outsourcing and third-party ICT services; verifies compliance profiles for third party ICT service contracts and outsourcing arrangements.
- **Compliance controls**, which conduct second-level controls on processes or operational functions where ICT and security compliance risks are significant, including on-site compliance checks at operational facilities.

ICT AND SECURITY RISK MANAGEMENT MODEL

OBJECTIVES

The Montepaschi Group recognises the value of ICT and security risk management in achieving the objectives set out in its Strategic Plan. This management serves as a tool to ensure the effectiveness

and efficiency of measures that protect ICT resources and the services provided to both internal and external users. Consequently, the Group promotes a methodology based on a holistic view of business functions, the business processes supported by the information system, the threats to ICT resources, their vulnerabilities and the associated risk mitigation measures.

The mitigation measures are calibrated according to the criticality classification of ICT resources and the level of risk appetite for ICT and security established within the Group's Risk Appetite Framework (RAF).

ELEMENTS OF THE ICT AND SECURITY RISK MANAGEMENT MODEL (REFERENCE FRAMEWORK)

General Overview

The following paragraphs provide a brief description of the elements that make up the ICT risk management and security model adopted by the **Risk Control** function, as well as the relevant relationships between them.

These elements are defined in accordance with internationally established standards and frameworks, as well as industry best practices.

Business Functions and Processes

Business functions and processes are components of the ICT and security risk management model in that they guide the assessment of the impact of risk scenarios on the supporting ICT resources, based on their level of criticality.

Responsible Users

The heads of the corporate functions are the key figures for assessing the impact of ICT and security risk scenarios and for making risk management decisions. The role of Responsible User is formalised within the Organisational Structure of Banca MPS.

IT Resources

IT resources are all the technological hardware and software components that support the Bank's operations and provide ICT services to internal or external users.

IT resources are under the management and control of the **Information Technology** and **Information Security** Functions. All IT resources are recorded in a specific **inventory**.

Risk Factors

The analysis of risk factors is based on the definition of a taxonomy of **threats**, which are the potential causes of ICT and security risk events. Threats can be internal or external and can vary in terms of whether they are intentional or not. Furthermore, threats can be grouped into different categories, such as external cyber-attacks, malicious insider actions, physical attacks, system failures, human error, negligence, process failures, natural events, etc.

Risk Scenarios

An **ICT and security risk scenario** is a description of the potential occurrence of risk events that are homogeneous in terms of the type of threat that causes them. These events could have a negative impact on normal operations, the security of IT resources and information processed, and the ability to meet business objectives or regulatory requirements.

Impact of Risk Scenarios

Impact refers to the negative consequences for the Montepaschi Group, in terms of economic losses, reputational damage and loss of market share, caused by the occurrence of risk scenarios affecting IT resources. The impact is assessed in terms of potential, following a worst-case approach.

Risk Mitigation Measures

Risk mitigation measures refer to the technological, organisational, procedural, directive or training-based controls and safeguards implemented to reduce the level of exposure and/or vulnerability of IT resources to threats (inherent risk), thereby limiting the probability of risk events occurring or the possibility that they will have a negative impact.

The **ICT and Security Operational Risk Control** function ensures the existence and ongoing effectiveness of controls to mitigate inherent risks. It also identifies the level of residual risk based on controls defined by international standards, frameworks and industry best practice.

Exposure and Vulnerability of Resources

The **exposure** of an IT resource to a threat means that the resource is potentially accessible to that threat based on its characteristics and its position within the information system architecture. In such cases, the threat and potential risk events or scenarios associated with it are considered 'applicable'.

The **vulnerability** of an IT resource refers to any weakness, deficiency or flaw in its design, implementation, configuration, protection or operational management. This includes its obsolescence and failure to update in line with vendor recommendations. Such vulnerabilities can be exploited by threats, leading to risk events that have a negative impact on the Group.

Probability of Risk Events

The **probability of occurrence** of an ICT and security risk event is the estimated annual frequency with which the event could impact the IT resources under analysis and negatively affect the Group.

The assessment of probability is an expert judgement made by people with extensive knowledge of the IT resources being analysed and the threats to which they are exposed. An accurate assessment of the likelihood of risk events occurring requires specific expertise to assess the effectiveness of the mitigation measures in place and the level of exposure and vulnerability of each resource to various threats. It also relies on the availability of information and statistics on operational and cyber security incidents that have occurred within the Bank and those observed in the wider system.

Assessing the Level of Risk

'Inherent' (or 'intrinsic') risk is defined as the risk to which the Bank is exposed in the absence of any mitigating measures.
On the other hand, **'residual'** risk is defined as the risk to which the Bank is exposed after applying the mitigating measures identified by the risk analysis process.

Based on specific rules (risk matrix), ICT and security risk is assessed on the basis of the combination of the likelihood of risk events occurring and their estimated impact.

Key Risk Indicators

Key Risk Indicators (KRIs) are quantitative indicators that detect the occurrence of incidents, the emergence of technological, process or security anomalies and vulnerabilities, as well as the evolving threats to which the information system is exposed. KRIs are measured at the level of individual resources or, more broadly, across the application and infrastructure areas that make up the information and IT security system.

KRIs enable continuous monitoring of the evolution of ICT and security risks against pre-defined thresholds. They provide critical insight to identify threats and vulnerabilities that require more in-depth risk analysis.

KRIs can also be used within the Risk Appetite Framework to set the ICT and security risk appetite limits at Group level.

ANALYSIS METHODOLOGY

General Overview

The **ICT and Security Risk Analysis** methodology outlines the rules adopted by the Risk Control function to identify, assess and monitor risks, based on the elements of the model described in the previous section.

The **evaluation methodology** involves carrying out two types of analysis in parallel, which operate at different but complementary levels:

1. A **detailed risk analysis** carried out at the level of individual ICT resources.
2. A **high-level risk analysis**, carried out at a more general and cross-functional level than that of individual IT resources, which aims to identify and assess ICT and security risks across the following key areas in the management of the information system.

In addition, the evolution of ICT and security risks and the effectiveness of mitigation measures are continuously **monitored** through a set of Key Risk Indicators (KRIs). These KRIs are used to identify risk trends in the application and infrastructure areas that make up the information system and cyber security framework. At least once a year, the results of the high-level analysis are appropriately integrated with the results of the detailed analysis of individual resources to provide a comprehensive and consistent representation of the Group's ICT and security risk situation.

RISK MANAGEMENT AND ACCEPTANCE

The analysis of the ICT and security risks to which the IT resources are exposed determines the residual risk to be submitted for formal acceptance by the Responsible User.

If the residual risk exceeds the risk appetite defined in the Risk Appetite Framework (RAF), the Responsible User defines additional mitigation measures to bring the risks back within acceptable limits, or alternatives (e.g. risk transfer).

As part of the Internal Control System, ICT and security risks that exceed the risk appetite limits defined in the RAF are flagged as 'mandatory mitigation actions' by the **ICT and Security Operational Risk Control** function. Once the mitigation action is declared complete, the risk analysis is updated to verify the effectiveness of the mitigation implemented and the resulting reduction in the residual risk level. The Risk Reporting System ensures the monitoring of ongoing actions.

REPORTING TO THE BOARD WITH STRATEGIC OVERSIGHT

The Board of Directors is informed promptly, and at least annually, of the ICT and security risk situation in relation to the risk appetite, including the results of the risk assessment, and approves the summary Report.