



HAITONG

**REGULATION No. COM03.R03
Third-Party Service Providers
- Outsourcing and ICT Services
of Haitong Bank, S.A.**

Approved by the Board of Directors
on the 25/06/2026

TABLE OF CONTENTS

1. OBJECTIVE.....	3
2. LEGAL FRAMEWORK	3
3. RECIPIENTS	4
4. RESPONSIBILITY	4
5. DEFINITIONS	4
6. OUTSOURCING.....	7
6.1 APPLICABLE PRINCIPLES.....	7
6.2 OUTSOURCING REQUIREMENTS	8
6.2.1 REGARDING THE THIRD-PARTY SERVICE PROVIDER	8
6.2.2 REGARDING THE BANK.....	9
6.2.3 WRITTEN AGREEMENT	11
6.3 OUTSOURCING OF OPERATIONAL TASKS OF INTERNAL CONTROL FUNCTIONS	12
6.4 OUTSOURCING SERVICES IN THIRD COUNTRIES.....	12
6.5 OUTSOURCING SERVICES TO INTRA-GROUP ENTITIES.....	13
6.6 OUTSOURCING MANAGEMENT.....	14
6.7 OUTSOURCING MONITORING	14
6.8 OUTSOURCING PROPOSALS.....	15
7. ICT SERVICES	15
7.1 ICT SERVICE PROVIDER.....	15
7.2 ICT SERVICES AGREEMENTS	16
7.3 WRITTEN AGREEMENT	17
7.4 ICT SERVICES MONITORING	19
7.5 ICT SERVICES PROPOSALS	19
8. CONFLICTS OF INTEREST	19
9. ARCHIVE	19
10. DISCLOSURE	19
11. CONTROL OF VERSIONS	20

1. OBJECTIVE

This document defines the Third-Party Service Providers Regulation (“**Regulation**”) adopted by Haitong Bank, S.A. (“**Bank**”).

This Regulation intends to establish the framework applicable to all Outsourcing and ICT Services agreements entered between the Bank and a Third-Party Service Provider, in order to properly mitigate and manage third-party risks, and to ensure compliance with the applicable framework.

The entering into a business relationship, either constituting Outsourcing, ICT Services or both, its terms and conditions, and its management, monitoring and termination shall comply with this Regulation.

2. LEGAL FRAMEWORK

This Regulation is based on the current national and European legal and regulatory framework, namely:

- Directive 2014/65/EU;
- Commission Delegated Regulation (EU) 2017/565;
- Regulation (EU) 2022/2554 (DORA);
- Commission Delegated Regulation (EU) 2024/1773;
- EBA/GL/2019/02 - Guidelines on outsourcing arrangements (February 2019);
- EBA/GL/2019/04 – Guidelines on ICT and security risk management (November 2019);
- ESMA Guidelines on outsourcing to cloud service providers;
- Bank of Portugal Notice no. 3/2020;
- Bank of Portugal Notice no. 8/2023;
- Commission Delegated Regulation (EU) 2025/532;
- Decree-Law no. 125/2025, of 4th December;
- Law no. 73/2025, of 23rd December.

Other applicable internal rules:

- RIS09.R39 – Operational Risk Regulation;
- RIS20.R64 – ICT Risk Management Regulation;
- COM02.R02 - Conflict of Interest Prevention and Management Regulation;
- COM12.PM030 - Prevention and Management of Conflicts of Interest (Procedure);
- COM38.PM333 - Third-Party Service Providers Procedure Outsourcing and ICT Services Procedure;

- FIN29.PM362 - Capex and OPEX Management;
- ITI02.PM210 – Management of Incidents and Cyber Incidents;
- RIS30. PM317 – ICT Risk Monitoring;
- CIS02.PM396 – Monitoring Procedures.

3. RECIPIENTS

- a. The content of this Regulation represents a minimum standard that shall apply to the Bank and its subsidiaries, branches and representative office (“**Haitong Bank Group**”).
- b. In case of conflict between any provision of this Regulation and the local laws and regulations applicable to any Bank's subsidiary or branch, the relevant local laws and regulations shall prevail.

4. RESPONSIBILITY

- a. This Regulation is sponsored by the Compliance Department.
- b. However, the responsibility arising hereunder on Outsourcing and ICT is distributed as follows:
 - Each Service Requester of Outsourcing and ICT Services is responsible for first-line control in the onboarding and ongoing monitoring of the relevant risks of the Third-Party Service Provider (including documentation maintenance).
 - IT Infrastructure is responsible for first-line control of ICT Services, together with the Service Requester in the onboarding and ongoing monitoring of the relevant risks of the Third-Party Service Provider.
 - Compliance is responsible as second-line control in monitoring the compliance of Outsourcing and ICT Services.
 - Risk is responsible for second-line control in the management of Outsourcing and ICT Services risks, taking in consideration, among others, risks reported by the Service Requester, IT Infrastructure and Compliance.
- c. This Regulation should be reviewed on an annual basis or whenever necessary to comply with applicable rules.

5. DEFINITIONS

Outsourcing

- a. Based on the Guidelines on Outsourcing issued by the European Banking Authority (“EBA/GL/2019/02”), outsourcing is considered “*an agreement, regardless of its form, entered into*

between an institution [...] and a service provider, under which the service provider carries out a process, provides a service, or develops an activity that would otherwise be performed by the institution itself [...].

- b. Operational tasks from internal control functions, including, but not limited to collaborative solutions, are considered outsourcing.
- c. The following situations are, nevertheless, excluded¹:
 - Functions that are legally required to be performed by a service provider (e.g. statutory auditor);
 - Market information services (e.g. provision of data by Bloomberg, Moody's, Standard & Poor's, Fitch);
 - Global network infrastructures (e.g. Visa, MasterCard);
 - Clearing and settlement arrangements between clearing houses, central counterparties and settlement institutions and their members;
 - Global financial messaging infrastructures that are subject to oversight by relevant authorities;
 - Correspondent banking services;
 - The acquisition of services that would otherwise not be undertaken by the Bank (e.g. advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, physical custody of documents, cleaning, gardening and maintenance of premises, medical services, servicing of company cars, insurance, security services, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators), of goods (e.g. plastic cards, card readers, office supplies, personal computers and all IT-related goods, furniture) or utilities (e.g. electricity, gas, water, fixed and mobile communications).

ICT Services

- d. As per Regulation (EU) 2022/2554 on digital operational resilience for the financial sector ("DORA Regulation"), ICT Services encompasses "[...] *digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services*".
- e. As this is quite a broad definition, one should also consider the following types of contractual arrangements, as identified by the European Supervisory Authorities:

¹ Please refer to paragraph 28 of EBA/GL/2019/02 and Bank of Portugal Letter CEX_2025_0000038773.

- software and application services (IT development; off the shelf software packages, licensing, and installation thereof etc);
 - network infrastructure services (excluding telecommunication services);
 - data centre (physical data centre space and basic utilities);
 - ICT consultancy and managed ICT services;
 - information security and cybersecurity services (including control and monitoring, penetration testing, security operations centre, etc.);
 - cloud computing (covering all service models and types);
 - data analysis and other data services (provision of data, data entry, data storage, data processing and reporting services, data monitoring as well as data-based business and decision support services).
- f. Situations where (i) the software is hosted in the Bank's servers, (ii) the software is exclusively operated by the Bank and (iii) the provider does not provide any ongoing service other than releasing updates and patches, are excluded from the definition of ICT Services.

Critical or Important Functions

- g. Regardless of the nature of the contractual arrangement, the Bank shall assess whether the underlying service concerns critical or important functions.
- h. For Outsourcing purposes, and in line with points 29 to 31 of the EBA/GL/2019/02, a function should be considered critical or important where:
- A defect or failure in its performance would materially impair:
 - the institution's compliance with the conditions of its authorization or with its other obligations under Directive 2013/36/EU, Regulation (EU) No 575/2013, Directive 2014/65/EU, Directive (EU) 2015/2366, and Directive 2009/110/EC, as well as its regulatory obligations;
 - its financial performance; or
 - its soundness or continuity of its banking and payment services and activities.
 - Operational tasks relating to internal control functions are outsourced.
 - Functions related to banking or payment services are outsourced to an extent that would require authorization by a competent authority.
- i. Moreover, in the context of this assessment, it should be determined whether the service relates to functions associated with critical functions or critical business lines. If so, they must be considered critical or important.

- j. For ICT Services purposes, per DORA Regulation, a function is deemed critical or important whenever its disruption “[...] *would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law*”;
- k. DORA Regulation also refers to Directive 2014/59/EU, which defines critical functions and critical business lines as follows:
- Critical functions: “*activities, services or operations the discontinuance of which would be likely to lead to the disruption of services that are essential to the real economy or to disrupt financial stability, due to the institution’s or group’s size, market share, external and internal interconnectedness, complexity or cross-border activities, with particular regard to the substitutability of such activities, services or operations.*”
 - Critical business lines: “*business lines and associated services which represent material sources of revenue, profit or franchise value for an institution or for a group to which it belongs.*”

Sub-Outsourcing

- l. A situation where the Third-Party Service Provider under an Outsourcing and / or ICT Services arrangement further transfers the process, service or activity, or parts thereof, to another third-party service provider.

Third-Party Service Provider

- m. A third-party entity that is undertaking a process, service or activity, or parts thereof, under an Outsourcing and / or ICT Services arrangement.

Service Requester

- n. A business, support or control area that proposes an Outsourcing and / or ICT Services arrangement.

6. OUTSOURCING

6.1 Applicable Principles

When considering an arrangement with a Third-Party Service Provider the Bank shall ensure that the outsourcing:

- (i) Does not materially impair the internal control to be performed by the Bank;
- (ii) Does not materially impair the competent authority's ability to control the Bank's compliance with its legal or regulatory obligations;
- (iii) Does not result in the delegation of the Executive Committee responsibilities;
- (iv) Allows the Bank to maintain control of the outsourced activities and functions;
- (v) Does not empty the Bank's activity;
- (vi) Allows the Bank to maintain its relationship and obligations towards its clients under the applicable legislation, including its information duties, while also ensuring that:
 - The Bank defines the management policy/regulation and takes the main decisions in case the services, activities or functions in question involve any type of management powers;
 - The Bank maintains exclusive relationships with its clients, including payments to be made by or to the client;
- (vii) Allows compliance with all requirements of the Bank's authorisation and licence as a credit institution and financial intermediary;
- (viii) Does not remove or modify any condition subject to which the Bank's authorization and licence was granted.

6.2 Outsourcing Requirements

The Bank shall exercise due skill, care and diligence when entering into, renewing, managing or terminating any arrangement for the outsourcing to a Third-Party Service Provider and shall take the necessary steps to ensure that the below-mentioned conditions are satisfied.

6.2.1 Regarding the Third-Party Service Provider

The Bank shall ensure that the Third-Party Service Provider:

- (i) Has the ability, capacity, sufficient resources, appropriate organisational structure supporting the performance of the outsourced functions, and any authorisation required by law to perform the outsourced functions and to carry out the outsourced functions or activities in a reliable and professional manner;
- (ii) Effectively performs the outsourced functions or activities in compliance with the applicable law and regulatory requirements;

- (iii) Controls the execution of the outsourced functions or activities, manages the risks involved in outsourcing and defines an individual as responsible for the outsourcing agreement;
- (iv) Has all the information needed for carrying out the outsourcing agreement;
- (v) Informs the Bank of any facts that may have a material impact in its ability to carry out the outsourced functions or activities in compliance with applicable legal and regulatory requirements;
- (vi) Adopts appropriate measures in order to transfer the outsourced functions or services to another third party or to reintegrate them at the Bank, ensuring a proper support during the transition;
- (vii) Informs the Bank of any changes regarding an outsourcing arrangement or the service provider (e.g. to its financial position, organizational or ownership structures, sub-outsourcing);
- (viii) In the case of sub-outsourcing of critical or important functions, the Third-Party Service Provider shall request prior authorization from the Bank (by written agreement) indicating the specific functions to be sub-outsourced. The Third-Party Service Provider is obliged to oversee the sub-outsourced functions that it has sub-contracted to ensure that all contractual obligations between the Third-Party Service Provider and the Bank are continuously met;
- (ix) Cooperates with supervisory authorities with regard to the outsourced functions or activities;
- (x) Provides the Bank, its auditors and supervisory authorities with access to information, where necessary for the purpose of effective oversight, on the outsourced functions or activities, as well as to its relevant business premises;
- (xi) Protects any confidential information involving the outsourcing of financial intermediation activities or its customers, including by means of confidentiality clauses which remain effective after the termination of the agreement.
- (xii) Ensures that personal data processed by service providers located in the EU and/or third countries are in accordance with Regulation (EU) 2016/679 ("GDPR").

Third-party outsourcing is not allowed in case it impairs the internal control to be performed by the Bank and/or the competent authority's ability to control the Bank's compliance with its legal or regulatory obligations.

6.2.2 Regarding the Bank

The Bank shall:

- (i) Supervise the carrying out of the outsourced functions or activities and manage outsourcing risks;

- (ii) Establish methods and procedures for assessing the standard of performance of the outsourcing Third-Party Service Provider and for reviewing periodically, or whenever any change so justifies, the provided services;
- (iii) Maintains and updates at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual outsourcing arrangements;
- (iv) Comply with the regulatory reporting duties, namely by disclosing to the Supervisor, on a timely manner, the critical or important outsourcing arrangements before their signing or whenever an ongoing agreement has become critical or important, following the templates provided by Bank of Portugal, in accordance with Bank of Portugal Notice no. 8/2023;
- (v) Assess the performance of the outsourcing arrangements, in accordance with the defined periodicity, or whenever any change so justifies;
- (vi) Assess the concentration risk regarding their Third-Party Service Providers;
- (vii) Identify, assess and manage the potential impact of outsourcing arrangements on the risk management framework, taking into consideration the assessment results when deciding if the proposed function should be outsourced to a Third-Party Service Provider, and should take appropriate steps to avoid undue additional risks before entering/renewing outsourcing arrangements;
- (viii) Take appropriate measures if it believes that the outsourcing Third-Party Service Provider may not be performing the outsourced functions or activities effectively and in compliance with applicable legal and regulatory requirements;
- (ix) Have the ability to terminate the outsourcing agreement, whenever necessary, without detriment to the continuity and quality of the services provided to its clients;
- (x) Whenever necessary, in view of the outsourced functions or activities, make a contingency plan for disaster recovery and periodic testing on backup systems (business continuity plan);
- (xi) Ensure that the continuity and quality of the outsourced functions or services are maintained also in the event of termination of the outsourcing arrangement (preparation of exit strategies and termination processes, including an exit strategy plan for each critical or important function), identifying the main measures to be taken by the Third-Party Service Provider, either by transferring the outsourced functions or services to another third party or by performing them itself.
- (xii) Ensure that the outsourced service providers accept the rules of HB's Code of Conduct, pursuant to Articles 2 (3 and 4) of Bank of Portugal Notice no. 3/2020, as further defined in COM38.PM333 – Third-Party Service Providers Procedure.

If the Bank and the Third-Party Service Provider belong to the same business group, the Bank may, for the purposes of the above paragraphs and the applicable legal and regulatory regime, take into account

the extent to which it controls the outsourcing service provider or influences its actions, and to which the outsourcing service provider is included in the group's consolidated supervision.

By entering into an outsourcing arrangement, the Bank shall ensure that the entity to which the activity is outsourced maintains a record of personal transactions entered into by any relevant person and provides that information to the Bank promptly on request.

6.2.3 Written agreement

Outsourcing arrangements shall be formalised by a written agreement stating the rights and obligations that, in line with the above paragraphs and the applicable legal regime, arise for the Bank and the Third-Party Service Provider.

The Bank shall ensure that the Third-Party Service Provider, responsible for the outsourcing arrangement, is authorized and registered by a competent authority (when applicable). When drafting the written agreement, the Bank shall ensure that:

- (i) The principles and rules above mentioned in sections 6.1 and 6.2 of this Regulation are generally followed;
- (ii) In addition, the agreement shall clearly state:
 - The purpose of the agreement;
 - That the Bank keeps, in any event, its instruction and termination rights, its rights of information and its right to inspections and access to documentation and premises of the Third-Party Service Provider;
 - The duration of the agreement, termination and exit management clause, terms of contractual renewal and the Bank's ability to terminate the agreement;
 - The amounts, methods and deadlines for the payments to be made;
 - The rights and obligations of the parties, including the outsourcing Third-Party Service Provider's obligation to comply with all applicable legal and regulatory requirements;
 - Compensation clauses to be applied in the event of default of the outsourcing agreement and/or applicable legal and regulatory requirements;
 - The proper metrics and measures to be implemented by the Bank in order to evaluate the service level of the outsourcing arrangement;
 - In case of contract termination, a guarantee by the Third-Party Service Provider that the appropriate support will be granted to the Bank regarding a suitable transition of

the outsourced services either to the Bank or to another Third-Party Service Provider designated by it;

- The Third-Party Service Providers will cooperate with the supervisory authorities and auditors with regard to the outsourced functions or activities, providing all the information requested by the supervisory authorities and auditors in due time;
- The identification of the agreement management team, including at least one individual designated by the Bank and another by the other party;
- Governing law and means of settling disputes (arbitration or jurisdiction);
- Other specific clauses that may be considered essential for the Bank depending on the agreement's nature.

6.3 Outsourcing of operational tasks of internal control functions

The Bank may, subject to prior approval of the management and supervisory bodies, outsource specific operational tasks of internal control functions, provided that such outsourcing enhances the efficiency of the internal control system.

In addition to the communication referred to in section 6.2.2 (iv) above, which applies to all critical or important outsourcing arrangements, the Bank shall also notify Bank of Portugal of its intention to adopt collaborative solutions for the performance of operational tasks related to internal control functions, at least 60 days prior to the intended implementation date. This notification shall include the following information:

- (i) A description of the envisaged solution;
- (ii) The underlying rationale, provided by the management and supervisory bodies, for outsourcing those tasks, taking into account the nature, scope, and complexity of the Bank's activities and an internal control and risk management system that ensures the sound and prudent conduct of its business.

The Bank shall ensure that it maintains full access to all relevant information, documentation, and data necessary to fulfil its oversight responsibilities, to conduct audits and to comply with its reporting obligations towards the competent authorities.

6.4 Outsourcing services in third countries

In addition to meeting the requirements described in the previous sections, whenever the Bank wishes to outsource services to an entity located outside of the European Union, the Bank shall ensure that:

- (i) The Third-Party Service Provider is authorised to provide this service in its country of origin and is effectively supervised by a competent authority in that third country;
- (i) A cooperation agreement exists between regulators and the outsourcing Third-Party service provider's supervisory authority that shall secure that regulators are able, at least, to:
 - obtain on request the information necessary to carry out their supervisory tasks pursuant to Directive 2014/65/EU and Regulation (EU) No. 600/2014;
 - obtain access to the documents relevant to the performance of their supervisory duties maintained in the third country;
 - receive information from the supervisory authority in the third country as soon as possible for the purpose of investigating apparent breaches of the requirements of Directive 2014/65/EU and its implementing measures and Regulation (EU) No. 600/2014;
 - cooperate with regard to enforcement, in accordance with the national and international law applicable to the supervisory authority of the third country and the competent authorities in the Union in cases of breach of the requirements of Directive 2014/65/EU and its implementing measures and relevant national law.

6.5 Outsourcing services to intra-group entities

The Bank considers an intragroup outsourcing any outsourcing arrangements with entities of the same economic group.

The Bank shall comply with the following duties when entering an intra-group outsourcing arrangement:

- (ii) Suitable due diligence must be conducted on the potential Third-Party Service Provider;
- (iii) A clear definition of the scope of services, stating the main responsibilities and powers which should be clearly divided between the Bank and Third-Party Service Provider;
- (iv) The Bank shall conduct proper oversight and control of the outsourced activities; and
- (v) Ensure that intra-group outsourcing arrangements are properly documented to reflect the commercial terms, responsibilities and reporting lines between the Bank and the Third-Party Service Provider.

The operational tasks of the internal control functions may be subcontracted to the parent company or to another entity of the group if prior consent by the management and supervisory bodies of all entities involved has been obtained.

6.6 Outsourcing management

The outsourcing process can involve relevant risks that must be considered in the selection, decision-making and formalisation process.

The Service Requester is responsible for effectively managing these risks.

In this context, the Bank ensures that:

- (i) The assessment methods are established for the service level to be provided by the outsourcing Third-Party Service Provider, in particular:
 - Methods for comparing costs against service quality;
 - Quality levels reflecting quantifiable goals, including their updating;
 - Frequency of monitoring to be performed.
- (ii) The appropriate measures are taken if there is a suspicion that the outsourcing Third-Party Service Provider may not be carrying out the outsourced functions or activities effectively and in compliance with applicable legal and regulatory requirements.

6.7 Outsourcing Monitoring

The Bank continuously monitors the performance of Third-Party Service Providers in relation to all outsourcing agreements on a risk-based approach, paying particular attention to the outsourcing of essential or important functions, including ensuring the availability, integrity and security of data and information.

To this extent, the Bank shall ensure that:

- (i) The outsourcing arrangements comply, at all times, with all applicable performance and quality standards;
- (ii) Independent assessments and audits of compliance with legal and regulatory requirements and the Bank's or the outsourced Third-Party Service Provider's internal policies are conducted;
- (iii) Evaluation on the performance of outsourced Third-Party Service Providers is carried out by the relevant areas, using tools such as key performance indicators, key control indicators, service delivery reports, etc.
- (iv) Takes appropriate measures if it identifies deficiencies in the provision of the outsourced function, which may include termination of the outsourcing agreement with immediate effect

- (v) Takes the necessary precautions in case of renewal processes.

Specifically, based on a periodicity to be defined by the Bank, the Service Requester shall conduct a reassessment of the Third-Party Service Provider and underlying services, leveraging on independent assessments and audits or, in their absence, conducting specific controls and diligences.

Should the outcome of such reassessment identifies new risks or any other material finding that was not initially accepted by the Bank, the Service Requester shall report it to the appropriate stakeholders, including, the Risk Department and the Executive Committee.

6.8 Outsourcing Proposals

All outsourcing proposals (either initial or renewals) shall be submitted to the Bank's Executive Committee by the Service Requester, which will be solely responsible for preparing a project file. Said file, aside from coping with the rules laid down in COM38.PM333 – Third-Party Service Providers Procedure Outsourcing and ICT Services Procedure, shall include (i) a description of pre- and post-outsourcing ("as is" and "to be") process(es), service(s) and activity(ies), including the required conditions of the agreement to be signed and a (ii) business case study identifying the investment to be made vis-à-vis the future cost reduction / revenue increase and past performances (if applicable).

If, following the Bank's Executive Committee approval, it is determined that the specific negotiated contractual conditions do not comply with the provisions required under this Regulation or any other material finding is identified, the process will be resubmitted to the Executive Committee so that it can decide on the outsourcing in view of the existing risks.

7. ICT SERVICES

7.1 ICT Service Provider

Before entering in a contractual arrangement with a Third-Party Service Provider, on the use of ICT Services, the Bank shall, in particular:

- (i) Undertake all due diligence on prospective ICT Third-Party Service Providers and ensure throughout the selection and assessment processes that the ICT Third-Party Service Provider is suitable;
- (ii) Identify and assess conflicts of interest that the contractual arrangement may cause;

- (iii) Ensure that it only engages with Third-Party Service Providers that comply with appropriate information security standards.

For the purpose of this Regulation and aiming to comply with current framework on the matter, the Bank shall also indicate whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting service provider.

7.2 ICT Services agreements

When entering into ICT services agreements and during its execution, the Bank shall manage the risks that may arise from those agreements, in light of the principle of proportionality, namely by taking into account the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities. To this extent, the Bank:

- (i) Assesses whether the contractual arrangement covers the use of ICT services supporting a critical or important function, as above defined in section 5.;
- (ii) Assesses if supervisory conditions for contracting are met;
- (iii) Identifies and assesses all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT concentration risk;
- (iv) Maintains and updates at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers, which may be reported to the competent authorities upon request;
- (v) Pre-determine the frequency of audits and inspections as well as the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards.

The Bank shall also ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances:

- (i) Significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms;
- (ii) Circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement;

- (iii) ICT third-party service provider's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality, of data, whether personal or otherwise sensitive data, or non-personal data.

Whenever the ICT service supports critical or important functions, the Bank should also put in place exit strategies, taking into account the risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service.

Additionally, where the contractual arrangements on the use of ICT services supporting critical or important functions include the possibility that an ICT third-party service provider further subcontracts ICT services supporting a critical or important function to other ICT third-party service providers, the Bank shall weigh benefits and risks that may arise in connection with such subcontracting. To this extent, the Bank shall, in particular, before entering into a contractual arrangement with an ICT third-party service provider, decide whether that ICT third-party service provider may subcontract an ICT service that supports critical or important functions and, in that case, specify the scope of such subcontracting.

Whenever an ICT third-party service provider subcontracts ICT services that support critical or important functions or a material part thereof, it shall inform the Bank about any intended material changes to its subcontracting arrangements. Failure to provide this information, or the lack of approval of such material changes, shall entitle the Bank to terminate the contract concluded with the ICT third-party service provider.

7.3 Written agreement

The rights and obligations arising from the contractual arrangement on ICT Services must be set out in writing, including the service level agreements. The written document should be made available to the involved parties on paper, or in a document with another downloadable, durable and accessible format, and shall include the following information:

- (i) A clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting;

- (ii) The locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location;
- (iii) Provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;
- (iv) Provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the Bank in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements;
- (v) Service level descriptions, including updates and revisions thereof;
- (vi) The obligation of the ICT third-party service provider to provide assistance to the Bank at no additional cost, or at a cost that is determined ex-ante, when an ICT incident occurs;
- (vii) The obligation of the ICT third-party service provider to fully cooperate with the competent authorities;
- (viii) Termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities;
- (ix) The conditions for the participation of ICT third-party service providers in the Bank's ICT security awareness programmes and digital operational resilience training.

In addition to the elements above, whenever the functions supported by an ICT services agreement are deemed critical or important, the contractual arrangement shall also include:

- (i) Full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow effective monitoring of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met;
- (ii) Notice periods and reporting obligations of the ICT third-party service provider to the Bank, including notification of any development that might have a material impact on the ICT third-party service provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels;
- (iii) Requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security;

- (iv) The obligation of the ICT third-party service provider to participate and fully cooperate in the Bank's Threat-Led Penetration Tests (TLPT);
- (v) The right to monitor, on an ongoing basis, the ICT third-party service provider's performance;
- (vi) Exit strategies, in particular the establishment of a mandatory adequate transition period.

7.4 ICT Services Monitoring

Section 6.7 *Outsourcing Monitoring* above is applicable to ICT Services with the necessary adjustments.

7.5 ICT Services Proposals

ICT Services proposals (either initial or renewals), depending on the rules defined on CAPEX and OPEX Management Procedure No. FIN29.PM362, may be submitted to the Bank's Executive Committee by the Service Requester.

Regardless of being or not submitted to the Executive Committee, the Service Requester will be solely responsible for preparing a project file. Said file shall cope with the rules laid down in COM38.PM333 – Third-Party Service Providers Procedure Outsourcing and ICT Services Procedure.

If it is determined that if the specific negotiated contractual conditions do not comply with the provisions required under this Regulation or any other material finding is identified, the process will be submitted (either initially or a second time) to the Executive Committee, so that it can decide on the ICT Service in view of the existing risks.

8. CONFLICTS OF INTEREST

The Bank shall ensure that any outsourcing process complies with conflicts of interest rules.

9. ARCHIVE

This Regulation, and all the documents associated, are subject to the general archiving rules laid down in the procedure LEG12.PM220 – Archive Management.

10. DISCLOSURE

The Board of Directors ensures that the Regulation referred to in the preceding paragraph is properly implemented in the institution, which is subject to periodic reviews and is disclosed internally to all employees.

This Regulation is available on the Bank’s intranet and website and any change to the same should be duly communicated by e-mail to all the Bank’s employees.

11. CONTROL OF VERSIONS

Table 1: Information about the Document

Name of the Document	Outsourcing Regulation
Version	Version 11.0
Prepared by (Name/Department)	Compliance Department
Appreciated on (Committee name)	Audit Committee on 25/06//2026 and endorsed by the CGC on 24/06/2026
Approved by (Committee name)	Board of Directors (BoD)

Table 2: Versions’ update

Update and Approval Date	Main Changes
Version 1.0. - Approved By ExCOM on 11 August 2015	Original Version
Version 2.0 – Approved by ExCOM on 18 December 2017	New Logo and other updates.
Version 3.0 – Approved by ExCOM on 26 November 2019	Updated according with EBA guidelines on outsourcing arrangements.
Version 3.1 – Ratified by the BoD on 15 September 2020	According with BoP recommendation.
Version 4.0 – Approved by BoD on 25 February 2021	Updated according with Notice no 3/2020.
Version 5.0 – Approved by BoD on 19 December 2022	Development of the monitoring procedures and inclusion of the independent assessment of the regulation.
Version 6.0 – Approved by BoD on 27/12/2023	Annual Update; Clarification regarding acceptance the rules of its Code of Conduct, pursuant to Articles 2(3 and 4) of Bank of Portugal Notice no. 3/2020, other minor changes and clarifications.
Version 7.0 – Approved by BoD on 17/12/2024	Annual Update; Clarification on the responsibilities introduced by Bank of Portugal Notice No. 8/2023, namely with regard to the Responsible of Outsourcing function, and other minor changes.
Version 8.0 – Approved by BoD on 23/06/2025	Enlargement of the scope of the Regulation as to include as well certain ICT service providers that will need to be subject to a due diligence process similar to the outsourcing; adjustments arising from DORA Regulation; other minor changes.
Version 9.0 – Approved by BoD on 10/09/2025	Inclusion of the outsourcing of operational tasks of internal control functions, per regulatory framework introduced by Bank of Portugal Notice no. 2/2025 and other minor changes.
Version 10.0 – Approved by BoD on 12/03/2026	Clarification of responsibilities on outsourcing and ICT services. Further detail in terms of definitions and rules applicable to ICT Services.

Version 11.0 – Approved by BoD on 25/06/2026

Further clarification on the responsibilities on outsourcing and ICT services.

Exclusion of certain arrangements of the concept of ICT Services.