Annex to the letter from the Secretary General of the *Autorité de contrôle prudentiel et de résolution* sent to the Director General of the French Association of Credit Institutions and Investment Firms

July 2025

Report on Internal Control
Credit institutions, financing companies and investment firms

(Report prepared in accordance with Articles 258 to 266 of the amended *Arrêté du 3 novembre 2014* on the internal control of banking sector companies, payment services and investment services subject to the supervision of the *Autorité de contrôle prudentiel et de résolution)*

Contents

Introduction

The Report on Internal Control is intended to provide details on institutions' internal control activities during the past financial year and to record the procedures used by institutions to measure, monitor, manage and disclose the risks to which they are exposed.

The items listed below are provided for illustrative purposes insofar as they are relevant in light of the institution's activities and organisational structure[1]. The institution should also provide whatever information is needed to enable the reader of the report to understand how the internal control system operates and to assess the risks it actually bears.

This document is based on a "combined" version of the reports prepared in accordance with Articles 258 to 266 of the *Arrêté du 3 novembre 2014*, as amended. However, institutions that wish to do so may continue to submit separate reports, provided that these reports cover all the elements listed below.

The Report on Internal Control must include the most recent internal management reports on the assessment and monitoring of risk exposure (internal dashboards) that have been provided by the members of the management body in its executive function to the institution's supervisory body and, when applicable, to its risk committee, in accordance with Article 253 of the *Arrêté du 3 novembre 2014*, as amended.

Moreover, it is recalled that in accordance with the provisions of Article 4 of amended Instruction No 2017-I-24, the documents examined by the institution's supervisory body in the course of its review of the conduct and results of internal control, in accordance with Articles 252 and 253 of the *Arrêté du 3 novembre 2014*, as amended, as well as the extracts from the minutes of meetings at which they were reviewed, must be sent to the Secretary General of the *Autorité de contrôle prudentiel et de résolution* (SGACPR) on a quarterly basis.

These documents as well as the Report on Internal Control shall be, in accordance with the provisions of Articles 12 and 13 of amended Instruction No 2017-I-24, sent to the SGACPR **electronically in a computerised format**, according to the technical arrangements defined by the ACPR.

In this respect, it is recalled that the various annexes[2] to the Internal Control Report listed below form stand-alone office documents, which must be sent electronically separately from the main body of the Report on Internal Control:

- annex on the security of non-cash means of payment;
- annex on measures implemented in favour of financially vulnerable customers;
- annex listing transactions entered into with executive directors, members of the supervisory body and, where applicable, with major shareholders;
- annex specifying the methods used, including stress tests, to assess the risks arising from the use of recognised credit risk mitigation techniques for the application of the CRR Regulation;
- annex (for financing companies) on the identification, measurement, management and control of liquidity risk, including a description of the assumptions used to draw up the projected cash flow statement;
- annex describing the assumptions and methodological principles used for credit risk stress tests, as well as the results of these stress tests, in accordance with Article 177 of the CRR Regulation;
- annex describing the assumptions and methodological principles used fo market risk stress tests, as well as the results of these stress tests, in accordance with point (g) of Article 368(1) of the CRR Regulation;
- annex describing the assumptions and methodological principles used for counterparty credit risk stress tests, as well as the results of these stress tests, in accordance with Articles 286 and 290 of the CRR Regulation;

[1] It is recalled that investment firms belonging to classes 2 and 3 are required to describe their systems dedicated to monitoring and managing the risks to which they are exposed, especially with regard to credit and counterparty risk, residual risk, concentration risk, market risk, intermediation risk, settlement-delivery risk, liquidity risk, operational risk, security risk and risks to the customers, risks to the market and risks to the undertaking within the meaning of (EU) Regulation No 2019/2033 of the European Parliament and Countil of 27 November 1019.

[2] Expectations regarding the submission of these annexes depend on the nature, activities and risk incurred by the institution concerned.

- annex on information on the segregation of customer funds, in accordance with the *Arrêté du 6 septembre 2017*;
- annex on Information and Communication Technology (ICT) applicable to institutions subject to European Regulation 2022/2554 on digital operational resilience for the financial sector ("DORA" Regulation), for which the relevant framework template is appended to the letter from the Secretary General to the AFECEI.

The Report on Internal Control shall be sent to the SGACPR at the latest:

- by 31 March following the end of the financial year for groups and institutions subject to the ECB's direct supervision, excluding the section relating to the remuneration policy and practices which can be sent by 30 April at the latest following the end of the financial year;
- by 30 April following the end of the financial year for other supervised institutions, including the section relating to remuneration policy and practices for all insitutions that are required to submit that section.

The report should be drafted in French. By way of exception, for institutions subject to the ECB's direct supervision, the report may be written in English, except for the sections that remain the exclusive responsibility of the ACPR (sections 18, 19, 22 and annex 2).

N.B.: If the institution is supervised on a consolidated basis, or is subject to supplementary supervision applicable to financial conglomerates, the reports on internal control shall include information about how internal control is applied to the group as a whole or to the conglomerate. If the subsidiary's internal control system is fully integrated into the system of the group, it is not necessary to submit a report on the organisation of internal control within that subsidiary. However, the systems used for risk measurement, monitoring and management should be described for each supervised institution.

Please note: Pursuant to Articles L. 511-41-1-B, L. 533-2-2 and L. 533-2-3 of the French Monetary and Financial Code, and to the provisions of the *Arrêté du 3 novembre 2014*, as amended, and in view of the forthcoming entry into force of Directive (EU) 2024/1619 of the European Parliament and Council of 31 May 2024 amending Directive (EU) 2013/36 ("CRD6"), as well as of the Guidelines issued by the European Banking Authority on the management of environmental, social and governance (ESG[3]) risks, this report is expected to provide an account of the strategies, policies, and arrangements implemented to identify, measure, manage and monitor ESG risks to which the institution is exposed. These risk factors must be included in all sections of this report, as appropriate in light of the institution concerned.

[3] Guidelines EBA/GL/2025/01 on the management of environmental, social and governance (ESG) risks of 8 January 2025.

1. Overview of business conducted and risks incurred by the institution

1.1. Description of business conducted

- general description of business conducted;
- for new activities:
    - a detailed description of any new activities conducted by the institution in the past year (by business line, geographical region, and subsidiary);
    - an overview of the procedures established for these new activities;
    - a description of the internal control actions carried out for these new activities;
- a description of any major changes made in terms of organisation or human resources: integration of board members up-to-date (start and end dates of their mandates) and organisation of the executive board;
- a description of any significant projects launched or conducted during the past year.

1.2. Presentation of the main risks generated by the business conducted by the institution

- a description, formalised documentation of and updates to the institution's risk mapping;
- a description of the measures taken to manage the risks mapped;
- a presentation of quantitative and qualitative information on the risks described in the summary reports sent to the members of the management body in its executive function, the supervisory body, and (when appropriate) to the risk committee and the ad hoc committee, specifying the scope of the measures used to assess the level of risk incurred and to set risk limits (cf. Article 230 of the *Arrêté du 3 novembre 2014*, as amended);
- for investment firms subject to the IFR regulation, identification and rationale behind the k-factors relevant for the institution's activities, and identification of the institution's activities that are not captured by a k-factor.

1.3. Presentation of the risk strategy and the risk policy

- a description of the processes in place for the identification, management, monitoring and mitigation of every significant risk (cf. Articles L.511-55 or L. 533-29 of the French *Code monétaire et financier*);
- a detailed outline of the risk appetite framework and of the arrangements made for its definition and review (cf. Articles L.511-93 or L. 533-31-2 of the French *Code monétaire et financier*);
- a description of the policies governing the management, quality and aggregation of risk data at different levels within the institution, including for business conducted abroad and outsourcing: *implementation, in a way that is appropriate to the size, nature and complexity of the institution's business, of a uniform or consistent data structure that unambiguously identifies risk data, as well as of measures ensuring the accuracy, integrity, exhaustiveness and timely availability of risk data, and definition of a governance process for the risk data aggregation mechanism* (refer to article 104 of the *Arrêté du 3 novembre 2014*, as amended);
- for investments firms subject to the IFR regulation, a brief presentation of the orderly wind-down plan: *description of the rationale and main repercussions of an orderly wind-down of the institution.*

2. Significant changes made to the organisation of the internal control system

If there have been no significant changes to the organisation of the internal control system, which includes the three lines of defence corresponding to the levels of control described below, the institution may provide a general description in an annex (cf. framework template appended in Annex 1 of this document) or provide a copy of the internal control charter in force.

2.1. Changes to the permanent control system in the "1st and 2nd levels of control" (including the organisation of internal control for foreign business and outsourcing)

- a description of significant changes made to the organisation of permanent control, which corresponds to the first and second levels of control as defined in Article 12 of the *Arrêté du 3 novembre 2014*, as amended, (including the main actions planned in relation to internal control, cf. Articles 259 f) or 259 *bis* d) of the same Order): *specify in particular the identity, the hierarchical position and reporting line of the person(s) in charge of permanent control and any other functions performed by such person(s) in the institution or in other entities of the same group, indicate which units are in charge of second-level control and, for each of them, the identity of their manager;*
- a description of significant changes made to the organisation of the compliance function: *specify in particular the identity, the hierarchical position and reporting line of the person in charge of the compliance function and any other functions exercised by this person in the institution or in other entities of the same group;*
- a description of the internal procedures established as a framework for the appointment or removal of the head of the compliance function *(cf. Article 28 of the Arrêté du 3 novembre 2014*, as amended*);*
- a description of the significant changes made to the organisation of the risk, nomination and remuneration committees (as applicable): *specify in particular the date of establishment, composition, term of office, operating procedures and powers of each of these committees*;
- a description of significant changes made to the organisation of the risk management function: *specify in particular the identity, the hierarchical position and of the person in charge of the risk management function and any other functions performed by this person in the institution or in other entities of the same group;*
- the identity of the member of the management body in its executive function in charge of the consistency and efficiency of 2nd level permanent control.

2.2. Changes to periodic control procedures in the "3rd level of control" carried out by the internal audit function (including the organisation of internal control for foreign business and outsourced activities)

- the identity of the person in charge of the internal audit function for the 3rd level of control, as defined in Article 12 of the *Arrêté du 3 novembre 2014*, as amended;
- the identity of the member of the management body in its executing function in charge of ensuring the consistency and efficiency of periodic control mechanisms;
- a description of significant changes made to the organisation of the internal audit function;
- the main initiatives planned in the area of periodic controls (audit plan, etc.; cf. Articles 259 f) or 259 bis d) of the *Arrêté du 3 novembre 2014*, as amended);
- a description of the internal procedures in place for the appointment and dismissal of the head of the internal audit function (cf. Article 17 of the *Arrêté du 3 novembre 2014*, as amended);
- a description of the measures taken, where appropriate, to ensure that the full investigation cycle of all activities carried out by the institution does not exceed five years (cf. Article 25 of the *Arrêté du 3 novembre 2014*, as amended);
- a description of the measures taken, where appropriate, to ensure that the audit cycle is determined using an approach that is proportionate to the risks identified within the institution or, where appropriate, within the group.

3. Governance

3.1. General principles of governance

- a description of the "*risk culture*" policy applied within the institution: a summary of communication procedures and staff training programmes on risk profile and risk management accountability…;
- a presentation of the ethical and professional standards promoted by the institution (*indicating whether they are in-house standards or the result of the application of standards published by external associations/bodies*), a description of the mechanism implemented to ensure their proper internal implementation, the process implemented in the event of a breach and the procedures defined to inform governing bodies…;
- a description of the procedures in place to identify, manage and prevent conflicts of interest (including in the context of credit granting procedures and the execution of other transactions), both at the level of the institution and involving its staff, and a description of the procedures established for the approval and review of these procedures (refer to Article 38 of the *Arrêté du 3 novembre 2014*, as amended, and to EBA Guidelines No 2021/05 and No 2021/14);
- a description of the procedures in place to identify, manage and prevent discrimation of staff based on gender, race, ethnic or social origin, sexual orientation, ect. (cf. EBA Guidelines No 2021/05 and No 2021/14),
- a description of the procedures in place to ensure equal opportunities among staff members regardless of gender, and to improve representation of the under-represented gender in the governing body (cf. EBA Guidelines No 2021/05 and No 2021/14).

3.2. Involvement of management bodies in internal control

3.2.1. Procedures used to report to the supervisory body and, when applicable, to the risk committee:

- the procedure used for the approval of limits by the supervisory body and, when appropriate, by the risk committee (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedure used to report to the supervisory body, to the central body, and, when appropriate, to the risk committee, on significant incidents (excluding IT incidents) within the meaning of Article 98 (cf. Article 245 of the *Arrêté du 3 novembre 2014*, as amended);
- where necessary, the procedure used by the risk manager to report to the supervisory body and, when appropriate, to the risk committee, specifying the topics concerned (cf. Article 77 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedure used by the person in charge of the internal audit function to report to the supervisory body and (when appropriate) to the risk committee any failure to carry out corrective measures that have been ordered (cf. Article 26 b) of the *Arrêté du 3 novembre 2014*, as amended);
- the procedure used by the person in charge of the compliance function when reporting to the supervisory body on the performance of his or her missions (see Article 31 of the *Arrêté du 3 novembre 2014*, as amended);
- findings arising from conducted controls that have been brought to the attention of the supervisory body and, when applicable, to the risk committee, highlighting any shortcomings identified, along with the corrective measures decided to address them (see Article 243 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedure used to report to the supervisory body on the periodic assessment carried out by the Nomination Committee regarding the knowledge, skills and experience of the members of the supervisory body, both individually and collectively (pursuant to Article L. 511-100 of the *Code monétaire et financier*). The conclusions of this assessment shall be sent to the SGACPR, as well as details of the follow-up to any measures imposed by the prudential supervisor as part of the fit and proper authorisation

procedure for the appointment of board members and members of the management body in its executive function.

3.2.2. Procedures used to report to members of the management body in its executive function

- procedures used to report to the members of the management body in its executive function on significant incidents within the meaning of Article 98 of the *Arrêté du 3 novembre 2014*, as amended (see Article 245 of the *Arrêté du 3 novembre 2014*, as amended);
- procedures allowing the risk manager to report to the members of the management body in its executive function on the performance of his or her duties (see Article 77 of the *Arrêté du 3 novembre 2014*, as amended);
- procedures allowing the risk manager to alert the members of the management body in its executive function of any situation likely to have a material impact on risk management (see Article 77 of the *Arrêté du 3 novembre 2014*, as amended).

3.2.3. Verifications carried out by the members of the management body in its executive function and the supervisory body

- a description of the due diligence carried out by the members of the management body in its executive function and the supervisory body to verify the effectiveness of internal control systems and procedures (see Articles 241 to 243 of the *Arrêté du 3 novembre 2014*, as amended).

3.2.4. Processing of information by the supervisory body

- the procedure used to review the governance framework and periodically assess its efficiency (cf. Article L.511-59 of the French *Code monétaire et financier*);
- the procedure used to approve and review the risk strategies and policies on a regular basis (cf. Articles L. 511-60 or L. 533-29-1 of the French *Code monétaire et financier*);
- the procedure used to determine the guidelines and monitoring the implementation of the internal control mechanisms to ensure efficient and prudent management of the institution (cf. Article L. 511-67 of the French *Code monétaire et financier*);
- the procedure used to adopt and review the general principles underlying the remuneration policy and its implementation (see. Articles L. 511-72 or L. 533-29-1 of the French *Code monétaire et financier*);
- as part of the supervisory body's review of significant incidents identified through internal control procedures, the main shortcomings identified, the lessons learned from their analysis, and any corrective measures taken where necessary (see Article 252 of the *Arrêté du 3 novembre 2014*, as amended);
- the dates on which the supervisory body reviewed internal control activities and outcomes during the reporting period under review;
- the dates of approval of the aggregate exposure limits by the supervisory body, after consultation with the risk committee, where applicable (see Article 224 of the *Arrêté du 3 novembre 2014*, as amended).

3.3. Remuneration policies and practices (including those applied within foreign subsidiaries and branches)

This section may be treated in a separate report.

3.3.1. Governance of the remuneration policy

- the date of establishment, composition, term of office, operating procedures and powers of the Remuneration Committee referred to in Article L. 511-102 or Article L. 533-31-4 of the French *Code monétaire et financier* and in section 2.4.2 of EBA Guidelines No 2021/04 or in section 2.3.2 of EBA Guidelines No 2021/13;

- a description of the general principles underlying the remuneration policy established pursuant to article L. 511-72 or L. 533-30 of the French *Code monétaire et financier* (procedure and date of adoption, date of implementation, and review procedures) and, where applicable, the identity of any external consultants whose services have been used in the design of the remuneration policy (see Article 266 of the *Arrêté du 3 novembre 2014*, as amended);
- a description of the role of the risk, compliance and support functions in designing and implementing the remuneration policy (cf. paragraphs 36, 38 to 41, and 60 to 62 of EBA Guidelines No 2021/04 or paragraphs 35, 37 to 40, and 56 et 58 of EBA Guidelines No 2021/13);
- the date and results of the internal review intended to ensure compliance with the remuneration policies and procedures adopted by the supervisory body (see Article L. 511-74 or L. 533-30-2 of the French *Code monétaire et financier*).

3.3.2. Main characteristics of the remuneration policy

- a description of the institution's remuneration policy (see Article 266 of the *Arrêté du 3 novembre 2014*, as amended), including:
    - (relative as well as absolute, quantitative and qualitative) criteria used to measure performance and to adjust remuneration according to risk (cf. paragraph 215 of EBA Guidelines No 2021/04 or paragraph 209 of EBA Guidelines No 2021/13);
    - (relative as well as absolute, quantitative and qualitative) criteria used to define the link between remuneration and performance (cf. paragraph 215 of EBA Guidelines No 2021/04 or paragraph 209 of EBA Guidelines No 2021/13) in the policy on variable remuneration deferral;
    - policy concerning guaranteed variable remuneration exceptionally granted under the conditions laid down in Articles L. 511-74 or L. 533-30-8 of the French *Code monétaire et financier*;
    - criteria used to determine the ratio of cash remuneration to other forms of remuneration.
    - criteria used to determine the amount of severance payments in the event of early termination of employment, subject to compliance with the applicable provisions of the French *Code du travail* (cf. paragraph 162 of EBA Guidelines No 2021/04 or paragraph 155 of EBA Guidelines No 2021/13);
    - policy in place to prevent circumvention of remuneration rules by staff through personal hedging strategies (cf. section 10.1 of EBA Guidelines No 2021/13).
    - pay gaps between women and men: specifics of the framework used to monitor pay gaps for the population concerned[4] (see Article 511-71 of the French *Code monétaire et financier*, Article 266 of the *Arrêté du 3 novembre 2014*, as amended, or paragraphs 59, 60 and 61 of EBA Guidelines No. 2021/13).
- when appropriate, a description of exemptions applied by the institution, as well as the justification and scope of these exemptions, as provided in Articles 198 and 199 of the *Arrêté du 3 novembre 2014*, as amended;
- for banking groups subject to supervision on a consolidated basis, a description of the mechanism in place, where applicable, within subsidiaries that are asset management companies or insurance or reinsurance undertakings, concerning their staff the missions of which may have a direct and material impact on the risk profile or business of credit institutions, investment firms and financing companies within the group (see Article 200 of the *Arrêté du 3 novembre 2014*, as amended);
- a description of remuneration policies applicable to the staff tasked with control and validation functions (cf. Article 15 of the *Arrêté du 3 novembre 2014*, as amended and Articles L. 511-71 and L. 511-75 or L. 533-30 and L. 533-30-3 of the French *Code monétaire et financier* and sections 12 and 14.1.3 of EBA Guidelines No 2021/04 or No 2021/13);
- the procedures used to incorporate risks into the determination of the variable remuneration base (including liquidity risks inherent in the activities concerned and the capital needed in light of incurred

[4] Meaning risk takers excluding members of the management body, members of the management body in its executive capacity, members of the supervisory body and other staff members (see paragraph 101 of EBA Guidelines No 2021/14).

risks) (cf. Articles L.511-76, L. 511-77, L. 511-82 and L. 511-83 or L. 533-30-5 and L. 533-30-8 and L. 533-30-12 of the French *Code monétaire et financier* and paragraphs 118 and 120 of EBA Guidelines No 2021/13) as well as the impact of the remuneration policy on capital and liquidity (cf. paragraphs 118 and 120 of EBA Guidelines No 2021/13);

- the date of disclosure to the ACPR or, as applicable, to the ECB, of the variable remuneration cap proposed at the competent general meeting for variable components of remuneration (*as a reminder, the competent General Meeting for staff employed in subsidiaries is that of the subsidiary and not that of the parent undertaking*) and the list of staff members subject to the variable remuneration cap, as well as the justification of these proposals, pursuant to Article L. 511-78 of the French *Code monétaire et financier* and to Section 2.3 of the EBA Guidelines, including the mention of any potential reduction of that cap pursuant to paragraph 43 of the aforementioned EBA Guidelines.

3.3.3. Disclosures concerning the remuneration of the members of the management body in its executive function and of the persons whose professional activities have a significant impact on the institution's risk profile (cf. Article 202, or, where applicable, Article 199 and Article 266, 5° of the Arrêté du 3 novembre 2014, as amended, and Article R. 511-18 or R. 533-19 of the French Code monétaire et financier)

Please specify:

- the categories of staff concerned;
- the total amount of remuneration for the year, broken down into fixed and variable components, and the number of beneficiaries. A breakdown by area of activity shall also be provided;
- the total amount and composition of variable remuneration, with a beakdown distinguishing between cash payments, shares or equivalent ownership instruments, and other instruments within the meaning of Article 52 or 63 of (EU) Regulation No 575/2013, or other instruments which can be fully converted into Common Equity Tier 1 instruments or written down. Please also indicate the vesting schedule or minimum holding period set for such shares (cf. Articles L. 511-81, L. 533-30-11, R. 511-22, R. 511-23, R. 533-21 and R. 533-21-2 of the French *Code monétaire et financier*);
- the total amount of deferred remuneration with a breakdown between vested and unvested components of remuneration (cf. Articles R. 511-18 or R. 533-19 of the French *Code monétaire et financier*);
- the total amount of deferred remuneration awarded during the year, paid out or reduced, after performance adjustment (cf. Article R. 511-18 or R. 533-19 of the French *Code monétaire et financier*);
- payments made to new hires, severance payments and number of beneficiaries (cf. Article R. 511-18 or R. 533-19 of the French *Code monétaire et financier*);
- redundancy benefits granted during the year, number of beneficiaries, and highest amount granted to a single beneficiary (cf. Article R. 511-18 or R. 533-19 of the French *Code monétaire et financier*);
- the methodology used for discounting calculations (cf. Articles 203 to 210 of the *Arrêté du 3 novembre 2014*, as amended);
- the total remuneration of each member of the management body in its executive function as well as that of the head of the risk management function and, when appropriate, that of the person in charge of the compliance function (cf. Article 266 of the *Arrêté du 3 novembre 2014*, as amended).

3.3.4. Transparency and oversight of remuneration policies

- the procedures used to verify that remuneration policies are aligned with risk management objectives, in particular having regard to the size and systemic importance of the institution, as well as the nature, scope

and complexity of its activities and taking into account the principle of proportionality (cf. Article 4 of the *Arrêté du 3 novembre 2014*, as amended);

- the procedures for disclosing information on remuneration policies and practices laid down in Article 450 of (EU) Regulation No 575/2013 (cf. Article 268 of the *Arrêté du 3 novembre 2014,* as amended, and Section 20 of EBA Guidelines No 2021/04);
- the arrangements in place for the disclosure of information on the remuneration policy and practices under Article 51 of Regulation No 2019/2033 of the European Parliament and of the Council of 27 November 2019 (see Section 20 of EBA Guidelines No 2021/13).

4. Results of periodic controls conducted during the last reporting period, including concerning foreign business (cf. Article 12 of the *Arrêté du 3 novembre 2014*, as amended)

- the internal audit mission programme (risks and/or entities that have been audited by the internal audit function during the last reporting period), their respective stage of completion and the resources allocated to them, expressed in man-days. If an external service provider is used: specify the frequency of its intervention and the size of the team;
- main shortcomings identified;
- measures taken to remediate the identified shortcomings**,** the expected date of implementation of these measures, and the state of progress of such implementation as at the date of drafting of this Report;
- the procedures used to follow up on the recommendations issued as a result of the periodic checks (*tools, persons in charge*) and the outcomes of that follow-up;
- the investigations conducted by the internal audit function of the parent entity and by external bodies (external agencies, etc.), the summary of their main conclusions, and the specifics of the decisions taken to remedy any identified shortcomings.

5. Inventory of transactions with members of the management body in its executive function, members of the supervisory body and principal shareholders (cf. Articles 113 and 259 g) or 259 bis e) of the *Arrêté du 3 novembre 2014,* as amended)

Financing companies are required to provide the following information in an appended document:

- **the characteristics of exposures deducted from regulatory capital** in accordance with Article 5 of the *Arrêté du 23 décembre 2013* on the prudential regime applicable to financing companies: the identity of the beneficiaries, the type of beneficiary (natural or legal person, shareholder, senior manager or member of the supervisory body), the type of exposure, gross amount, deductions (if any), risk weight, date of origination and maturity date;
- **the nature of exposures to principal shareholders, members of the management body in its executive function and members of the supervisory body for which no deduction has been made from regulatory capital** due either to the date on which the exposure was granted or to the credit rating or score assigned to the beneficiary of the exposure. However, mention of exposures the gross amount of which does not exceed 3% of the institution's capital is not required.

Credit institutions and investment firms are required to append a document setting out **the characteristics of exposures to key shareholders, members of the management body in its executive function and members of the supervisory body**: identity of the beneficiaries, type of beneficiaries -natural or legal person, shareholder, director or member of the supervisory body-, nature of the exposures, gross amount, any deductions and weighting applied, date of origination and maturity date.

6. Internal capital adequacy assessment process

This process is not mandatory for institutions that are part of a consolidated group and are exempted from compliance with own-fund requirements on an individual or sub-consolidated basis.

- a description of the scope of relevant activities for the assessment of internal capital adequacy and the approach used for the risk materiality assessment;
- a description of methodologies used to measure, assess and aggregate risks in order to determine internal capital needs (time horizons for risk analysis, economic value approach, description of models and calculation parameters…). This description shall include explanations of the limitations or weaknesses of the calculation method used, as well as the way these elements are managed or remediated when assessing internal capital adequacy;
- a description of the systems and procedures in place to ensure that the amount and allocation of internal capital are appropriate in view of the nature and level of risks to which the institution is exposed, *with particular emphasis on risks that are not captured by Pillar 1* (cf. Article 96 of the *Arrêté du 3 novembre 2014*, as amended);
- a description of the establishment and update of the capital planning framework used to ensure that internal and regulatory capital levels remain adequate over a three-ear horizon at a minimum, including in adverse scenarios (stress testing):
    - level and definition of internal capital allocated by type of risk for the last reporting period, detailing the main differences between internal capital and regulatory capital, as well as the methods and assumptions used for capital allocation within the institution;
    - forecasts of internal capital levels;
- stress testing carried out to assess internal capital adequacy:
    - description of the scope of stress tests and associated design process: *scope (entities and risks taken into account), frequency of testing, tools used, unit(s) in charge of their development, involvement of senior management in the validation process…,*
    - description of the assumptions and methodologies used, and summary of associated results,
    - description of the process used to integrate stress testing results in decision-making processes, especially with regard to risk appetite calibration, capital planning and determination of limits;
- internal control mechanisms designed to ensure that these systems and procedures remain appropriate in the event of changes to the institution's risk profile;
- formalised documentation of the process established for the development and validation of internal capital adequacy, as well as the assumptions, capital planning, stress tests and methods used in the process, including the allocation of responsibilities and the notification and involvement of management and/or supervisory bodies in the validation step;
- documentation formalising the integration of this process into the overall strategy of the institution, in particular inclusion of internal capital and risk appetite considerations into managerial decision-making processes through appropriate reporting;
- institutions subject to the CRR that are not under the ECB's direct supervision shall provide a "reader's guide", drawn up as a comprehensive document aimed at facilitating the assessment of the documentation supporting their capital adequacy. To that end, the "reader's guide" shall provide an overview of all the documents submitted to the competent authorities on that matter as well as the status of these documents (new, unchanged, amended with minor changes, etc.). The "reader's guide" shall esentially function as an index linking the specific information required for the report on internal control to the documents sent to the competent authority regarding the assessment of capital adequacy. The "reader's guide" shall also include information on material changes made to information compared to previous submissions, any elements excluded from the current submission and any other information that could be useful to the competent authority in the course of the assessment. Furthermore, the "reader's guide" shall provide references to all information publicly disclosed by the institution on its capital adequacy.

- institutions subject to the CRR that are not under the ECB's direct supervision shall formalise and submit the conclusions of their internal capital adequacy assessments, including the impact of ICAAP outcomes on risk management and on the overall governance of the institution.
- Class 2 investment firms are required to draw up a formal report in accordance with Article L533-2-2 of the French *Code Monétaire et Financier* in order to document the ICAAP framework set up by the investment firm and demonstrate the adequacy of internal capital in light of the risks to which it is exposed, with both a dynamic and a forward-looking assesment, covering both normal and stressed market conditions over time. A template outlining the list of key information to be included by the investment firm in that report is made available by the SGACPR on the ACPR's website[5].

7. Compliance risk (excluding the risk of money laundering and terrorist financing)

Reminder: *information on the risk of money laundering and terrorist financing shall be sent in the dedicated annual report on the organisation of AML-CFT and asset freeze internal control mechanisms provided for in Articles R. 561-38-6 and R. 561-38-7 of the French Code Monétaire et Financier, in accordance with the terms defined in the Arrêté du 21 décembre 2018.*

7.1. Training provided to staff on compliance control procedures, and prompt dissemination to staff of information on changes in the provisions that apply to the operations they carry out (cf. Articles 39 and 40 of the *Arrêté du 3 novembre 2014*, as amended);

7.2. Assessment and control of reputational risk

7.3. Other non-compliance risks (including compliance with banking and financial ethics codes)

7.4 Procedures used to report shortcomings, breaches and deficiencies

Please specify:

- the procedures set up to enable staff to report to the competent management bodies and committees of the institution, and to the ACPR (or, when applicable, to the ECB) on any actual or potential shortcomings or breaches of prudential regulations within the institution (cf. Article L. 511-41 of the French *Code monétaire et financier*);
- the procedures set up to enable senior managers and staff to raise concerns with the head of compliance of the entity or business line they belong to, or with the person referred to in Article 28 of the *Arrêté du 3 novembre 2014*, as amended, regarding potential deficiencies in the compliance control framework (cf. Article 37 of the *Arrêté du 3 novembre 2014*, as amended).
- the procedures set up to allow the staff to notify the ACPR of any failure to comply with the obligations defined by European regulations and by the French *Code monétaire et financier* (cf. Article L. 634-1 and L. 634-2 of the French *Code monétaire et financier*).

7.5 Procedures used for internal and external growth operations as well as operations relating to new products

- a presensation of compliance review procedures implemented when conducting operations relating to new products of services, or relating to material changes in existing products and services or material changes to the systems associated with such products, during internal or external growth operations or for exceptional transactions: *the opinion of the head of the compliance function shall systematically be provided in writing prior to the execution of these*

[5] Framework template available on the following webpage: Prudential reporting | ACPR (banque-france.fr)

operations (see Article 35 and first paragraph of Article 221 of the *Arrêté du 3 novembre 2014,* as amended).

7.6. Centralisation and implementation of remediation and follow-up measures

Please specify:

- the procedures set up to centralise information related to potential deficiencies in the implementation of compliance requirements (cf. Articles 36 and 37 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedures set up to monitor and assess the effective implementation of remedial actions aiming to remediate deficiencies in the implementation of compliance requirements (cf. Article 38 of the *Arrêté du 3 novembre 2014*, as amended).

7.7. Description of the main deficiencies identified during the reporting period

7.8. Results of 2nd level permanent control on compliance risk

- the main shortcomings identified;
- the measures taken to remediate the identified shortcomings**,** the expected implementation date of these measures, and the state of progress of such implementation as at the date of drafting of this Report;
- the procedure used to follow up on the recommendations issued as a result of permanent control actions (*tools, persons in charge, etc.*);
- the procedure used to verify that the remedial measures ordered by the institution have been carried out by the appropriate persons within a reasonable timeframe (cf. Articles 11 f) and 26 a) of the *Arrêté du 3 novembre 2014*).

8. Credit and counterparty risk (cf. Articles 106 to 121 of the *Arrêté du 3 novembre 2014*, as amended)

Nota bene*: for investment services providers (ISP), the specific case of* ***transactions using the deferred settlement service (SRD)*** *is covered in this section, including information on the selection of the set of customers for whom this type of order is authorised, the intervention limits set, and risk management (initial coverage, ongoing coverage, monitoring of extensions, provisioning for non-performing loans).*

8.1. Credit operations selection procedures

- predefined operation selection criteria;
- factors used in profitability forecasts for credit decisions: *methodology, variables considered (loss ratios, etc.);*
- a description of credit granting procedures, including where appropriate any delegation, escalation and/or limitation mechanism;
- credit granting procedure applied for housing loans granted to French customers, in particular criteria pertaining to the repayment burden as a percentage of borrowers' disposable income, loan-to-value ratios and total loan duration.

8.2. Risk measurement and monitoring framework

- stress scenarios used to assess risk exposure, underlying assumptions, results and description of their operational integration;
- overview of credit risk exposure limits – by individual obligor, by connected debtors, by industry sector etc. (*specify the level of such limits in relation to own funds and in relation to earnings*);

- the procedure used to review credit risk limits and the frequency of such review (*specify the date of the most recent review*);
- any breach of credit risk limits identified during the last reporting period (*specify their causes, the counterparties involved, the total amount of exposure concerned, the number of breaches, and their respective amounts*);
- the procedure used to authorise credit risk limit breaches;
- the measures taken to rectify credit risk limit breaches;
- the identification, staffing levels, and hierarchical position and reporting line of the unit in charge of monitoring and managing credit risk;
- a description of the arrangements in place for the monitoring of early warning risk indicators (*specify the main criteria used to place counterparties under watch-list*);
- the procedures and frequency of credit exposure quality assessments; indication of any reclassification of exposures made within the internal risk assessment categories, as well as any changes in allocation to accounting items dedicated to doubtful or impaired exposures, indication of any adjustments made to provisioning levels, and the date on which this analysis was carried out for the last reporting period;
- the procedures and frequency of revaluation of guarantees and collateral, as well as the main fndings of any reviews carried out during the year;
- a presentation of the credit risk measurement and management system implemented to identify and manage problem loans, make the appropriate value adjustments and record adequate provisions or write-downs (cf. Article 115 of the *Arrêté du 3 novembre 2014*, as amended);
- for credit institutions and investment firms with a level of non-performing loans in excess of 5%: presentation of the strategy used to manage and reduce non-performing exposures (*action plan and schedule, assessment of operating environment, quantitative targets, short-term, medium-term and long-term targets, targets set for each of the main portfolios, targets by implementation options…*) and description of the operational implementation mechanism (*operational plan approved by the management body, units involved, tools used, frequency of reporting established, involvement of senior management…*);
- for credit institutions and investment firms: presentation of the exposure restructuring process *(criteria considered in the restructuring decision, applicable timeframes, control procedures implemented to ensure the viability of the restructuring measures taken…*) and procedures used to monitor restructured exposures including key performance indicators (*non-performing exposure parameters, renegociation activities, liquidation activities, promises to pay and cash collection…*);
- description of the accounting process used to assess expected credit losses (methods used, factors and assumptions taken into account in the internal models developed, frequency of review…);
- the procedure and frequency of provisioning decisions, including when appropriate any delegation and/or escalation measures;
- the procedure and frequency of back-testing exercises for collective and statistical provisioning models, as well as the main results for the year where applicable;
- the procedure and frequency of impairment risk analysis for leased assets (financial leasing);
- the procedure and frequency of impairment risk analysis for financed real estate assets (including assets financed through leasing agreements);
- the procedure, frequency and results of credit file reviews (at a minimum for counterparties with past-due, non-performing, impaired or otherwise significant exposures in terms of risk or volume);
- a breakdown of exposures by risk level (cf. Articles 106 and 253 a) of the *Arrêté du 3 novembre 2014*, as amended);
- the procedure used to report to the members of the management body in its executive function, the supervisory body and, where applicable, the risk committee on the level of credit risk, using summary statements (cf. Article 230 of the *Arrêté du 3 novembre 2014*, as amended);

- roles of the members of the management body in its executive function, the supervisory body and, when applicable, the risk committee, in identifying, overseeing and reviewing the institution's overall credit risk strategy and its current and future credit risk appetite (cf. Articles L. 511-92 and L. 511-93 or L. 533-31-1 and L. 533-31-2 of the French *Code monétaire et financier*), and in setting credit risk limits (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended);
- analysis of changes in credit margins, in particular on loan production over the past year: *methodology, data used for the analysis, results;*
    - provision of detailed information on the margin calculation method used: earnings and expenses included; whether refinancing needs are taken into account, indication of the net borrowing position and the refinancing rate used; if gains from the investment of allocated own funds are taken into account, indication of the amounts and remuneration rates;
    - identification of the various categories of exposure (such as loans to retail customers, with a focus on housing loans) or of the business lines for which margins are calculated;
    - highlighting of observed changes identified based on calculations using outstanding amounts (at year-end and at previous cut-off dates) and, where applicable, calculations based on new loans for the past year;
- the procedures used by the members of the management body in its executive function to analyse the profitability of credit operations, the frequency and results of such analysis (*including the date of the most recent analysis*);
- the procedures used to report to the supervisory body on the institution's credit risk exposure, and the frequency of these reports (attach the most recent management report issued for the supervisory body);
- the procedures used to monitor the credit granting criteria used for housing loans to French customers;
- a breakdown of housing loan exposures according to the type of colleral (credit bonding, mortgage, etc.);
- a presentation of the LTV ratio on housing loans by type of guarantee (at origination, on average and after revaluation of collateral);
- the procedures for approval by the supervisory body, assisted, where applicable, by the risk committee, of the limits proposed by the members of the management body in its executive function (cf. Article 253 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedures for approval and review by the supervisory body of the strategies and policies governing risk-taking and the management, monitoring and mitigation of credit risk (cf. Article L. 511-60 of the French *Code monétaire et financier*);
- when appropriate, the procedures used to analyse, assess and monitor the risks associated with intragroup transactions and the frequency of such analysis of (credit risk and counterparty credit risk).

<u>Elements specific to counterparty credit risk:</u>

- a description of the risk metrics used to assess counterparty credit risk;
- a description of the integration of counterparty credit risk monitoring into the overall credit risk monitoring mechanism.

8.3. Concentration risk

8.3.1. Counterparty concentration risk

- tool used to monitor counterparty concentration risk, including central counterparties and entities from the shadow banking system: any aggregate measures defined, description of the methodology used to measure exposures to a single beneficiary (including the prudential framework applicable to the counterparties concerned, the financial situation of the counterparty and the portfolio, vulnerability to asset price volatility, especially for entities from the shadow banking system, details on procedures used to identify connected beneficiaries (including any quantitative threshold above which such identification

measures are systematically implemented, etc.); use of the look-through approach, particularly for exposures to collective investment undertakings, securitisation or refinancing of trade receivables (factoring, etc.) and the inclusion of credit risk mitigation techniques), procedures used to report to the members of the management body in its executive function and the supervisory body;

- system used to set counterparty exposure limits: summary description of the system used to set counterparty limits (*specify their level in relation to own funds and earnings*), the procedures used to review limits and the frequency of these reviews, any breaches of limits identified, and the arrangements to involve the members of the management body in its executive function in the determination of limits and in reporting on their monitoring;
- amounts of exposures to main counterparties;
- conclusions on the institution's exposure to counterparty concentration risk, including central counterparties and entities from the shadow banking system.

8.3.2. Sectoral concentration risk

- tool used to monitor sectoral concentration risk (including for the shadow banking system): any aggregate measures defined, economic model and risk profile, description of the method used to measure exposures to a single business sector (including interconnectedness between counterparties), and procedures used to report to the members of the management body in its executive function and the supervisory body;
- sectoral exposure limit mechanism: summary description of the sectoral limit system in place (*exposure amounts*, *specify their level in relation to own funds and earnings*), the procedures used to review limits and the frequency of these reviews, any breaches of limits identified, and the procedures used to involve the members of the management body in its executive function in the setting of limits and reporting on their monitoring;
- breakdown of exposures by sector;
- conclusions on the institution's exposure to sectoral concentration risk (including exposure to the shadow banking system).

8.3.3. Geographical concentration risk

- the system used to monitor geographical concentration risk: any aggregate measures defined, description of the system used to measure exposures in the same geographical area, and procedures used to report to the members of the management body in its executive function and the supervisory body;
- the mechanism used to set exposure limits to the same geographical area: summary description of the system used to set limits on geographical concentration (*specify their level in relation to own funds and earnings*), the procedures used to review limits and the frequency of these reviews, any breaches of limits identified, and the procedures used to involve the members of the management body in its executive function in the setting of limits and reporting on their monitoring;
- breakdown of exposures by geographical area;
- conclusions on the institution's exposure to geographical concentration risk.

8.4. Requirements relating to the use of internal rating systems to calculate capital requirements for credit risk

- ex-post controls and benchmarking against external data to ensure the accuracy and consistency of internal rating systems, the processes and the parameters used;
- the content and frequency of review of rating systems within the framework of permanent control and internal audits conducted on internal rating systems;
- a description of the operational integration of rating systems ('use test'): effective use of the parameters derived from the internal rating systems in credit granting and pricing, in recovery management, in risk monitoring, in the provisioning policy, in the allocation of internal capital, and in corporate governance

(including the elaboration of management reports for use by the members of the management body in its executive function and the supervisory body);

- the procedures used to involve the members of the management body in its executive function in the design and ongoing update of internal rating systems: including the approval of methodological principles, verification of sound understanding and control over the design and functioning of the system(s), arrangements governing the way members of the management body in its executive function are kept informed of the performance of these systems;
- demonstration proving that the internal credit risk assessment methods do not rely exclusively or mechanistically on external credit rating systems (cf. Article 114 of the *Arrêté du 3 novembre 2014*, as amended).

8.5. Risks associated with securitisation transactions and securitisation schemes

- a presentation of the institution's securitisation and credit risk transfer strategy;
- a presentation of the internal policies and procedures in place to ensure, prior to any investment, that institutions acting as originators, sponsors or initial lenders have a thorough understanding of the relevant securitisation positions and that they comply with the requirement to retain 5% of net economic interest when acting as originator, sponsor or original lender;
- the procedures used to assess, monitor and manage the risks associated with securitisation transactions or schemes (including, in particular, an analysis of their economic substance) for institutions acting as originators, sponsors or investors, including by incorporating stress testing scenarios (assumptions, frequency, impact);
- for institutions acting as originators, a description of the internal process used for prudential deconsolidation assessment, supported by an audit trail and by the procedures for the ongoing monitoring of risk transfer over time through reviews carried out reguarly.

8.6. Intraday credit risk

Risk incurred in the context of custody activities, by institutions granting intraday credit to their clients, in cash and/or securities, to facilitate the settlement of securities transactions[6].

- a description of the policy applied by the institution to manage intraday credit risk; a description of limits (procedures used for their definition and monitoring);
- a presentation of the system used to measure exposures and monitor limits on an intraday basis (including the management of any instance of overshooting of such limits);
- the procedures used to grant intraday credit;
- the procedures used to assess the quality of collateral;
- a description of the procedures used to report to the members of the management body in its executive function and the supervisory body;
- conclusions on exposure to intra-day credit risk.

8.7. Results of 2nd level permanent control measures on credit activities

- main shortcomings identified;
- corrective measures taken to remedy the identified shortcomings**,** planned completion date for these measures, and state of progress of their implementation as at the date of drafting of this Report;
- the procedures used to follow up on the recommendations resulting from permanent control actions (*tools, persons in charge*, etc.);

6 Intraday credit risk also covers overnight credit risk for transactions settled overnight.

- the procedures used to verify that the corrective measures ordered by the institution have been carried out by the appropriate persons within a reasonable timeframe (cf. Articles 11 f) and 26 a) of the *Arrêté du 3 novembre 2014*, as amended).

8.8. Risks associated with the use of credit risk mitigation techniques

Attach an annex providing:

- a description of the system used to identify, measure and monitor the residual risk to which the institution is exposed when it uses credit risk mitigation techniques;
- a summary description of the procedures designed to ensure, when credit risk mitigation instruments are implemented, that they are legally valid, that their value is not correlated with that of the debtor, and that they are duly documented;
- a presentation of the procedures used to integrate the credit risk associated with the use of credit risk mitigation techniques in the overall credit risk management system;
- a description of the stress tests conducted on credit risk mitigation techniques (including the assumptions and methodological principles used and the results obtained);
- a summary of any incidents that occurred during the year (rejected collateral calls, non-enforcement of pledged collateral, etc.).

8.9. Stress testing for credit risk

Attach an annex describing the assumptions and methodological principles used (in particular the approach to incorporating contagion effects across markets and the integration of ESG risk factors, espescially those related to physical risk and transition risk arising from climate change) and summarising the results obtained.

8.10. Summary conclusion on credit risk exposure

9. Risks linked to OTC derivative contracts

9.1 Risk mitigation techniques used for OTC derivative contracts that are not cleared by a central counterparty:

- a description of the procedures and arrangements in place to ensure the timely confirmation of the terms of OTC derivative contracts not cleared by a central counterparty, to reconcile portfolios, to manage the associated risk and to allow for the early identification of disputes between parties and their resolution, as well as to monitor the value of outstanding contracts (cf. paragraph 1 of Article 11 of (EU) Regulation No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, as amended);
- a description of procedures used for the valuation of OTC derivative contracts not cleared by a central counterparty (cf. paragraph 2 of Article 11 of (EU) Regulation No 648/2012, as amended);
- a description of procedures used for counterparty risk management and for the exchange of collateral with respect to OTC derivative contracts not cleared by a central counterparty (cf. paragraph 3 of Article 11 of (EU) Regulation No 648/2012, as amended);
- a description of the procedures used for the calculation and collection of variation margins;
- a description of the procedures used for the calculation and collection of initial margins;
- a description of the models used for the calculation of initial margins;
- a description of the criteria used for the selection of collateral exchanged;
- a description of the methods used for the valuation of collateral;
- a description of the operational procedures and contractual documentation used for collateral exchange;

- a description of the number, volume and evolution of identified collateral disputes with counterparties with which collateral is exchanged, as well as resolution procedures for such disputes;
- a description of the methods applied and frequency of calculation of the amount of capital allocated to the management of risks not covered by appropriate collateral exchange (cf. paragraph 11 of Article 11 of (EU) Regulation No 648/2012, as amended).

9.2 Risk management and risk monitoring procedures for risks associated with intragroup transactions

- a description of the centralised procedures used for the valuation, assessment and monitoring of risks linked to the intragroup transactions referred to in paragraphs 2. a) and d) of Article 3 of (EU) Regulation No 648/2012, as amended;
- a description of the risk management procedures used to manage the risks associated with intragroup transactions that benefit from the exemptions provided for in paragraphs 6, 8 or 10 of Article 11 of (EU) Regulation No 648/2012, as amended;
- a description of any significant changes that may affect the smooth transfer of own funds or the prompt repayment of liabilities between counterparties that benefit from the exemptions provided for in paragraphs 6, 8 or 10 of Article 11 of (EU) Regulation No 648/2012, as amended. This description shall include detailed observations or forward-looking assessments regarding countries where conditions have materially changed in this respect;
- information on intragroup transactions carried out during the year and benefiting from the exemptions provided for in paragraphs 6, 8 or 10 of Article 11 of (EU) Regulation No 648/2012, as amended (cf. Article 20 of Commission Delegated (EU) Regulation No 148/2013 of 19 December 2012 supplementing (EU) Regulation No 648/2012).

10. Market risk

A description of the institution's policies on proprietary trading:

10.1. Market risk measurement system

- recording of market transactions; calculation of positions and results (*specifying frequency*);
- reconciliation between management results and accounting results (*specifying frequency*);
- reconciliation between prudent valuation, as defined in Commission Delegated (EU) Regulation No 2016/101 of 26 October 2015, and accounting valuation for portfolios recognised at fair value through profit and loss;
- risk assessment (including credit valuation adjustment risk) arising from trading book positions (*specifying frequency*);
- the procedures used to capture the various risk components (including basis risk and securitisation risk) (in particular for institutions with significant trading volumes applying aggregated risk assessment);
- the scope of risks covered (across various business lines and portfolios; including various geographical areas).

10.2. Market risk monitoring system

- roles of the members of the management body in its executive function, the supervisory body and, when applicable, the risk committee, in defining the institution's overall market risk strategy and current and forward-looking market risk appetite (cf. Articles L. 511-92 and L. 511-93 or L. 533-31-1 and L. 533-31-2 of the French *Code monétaire et financier*), and in setting risk limits (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended);
- the identification, staffing levels, and hierarchical position and reporting line of the unit tasked with market risk oversight and control;

- controls performed by this unit**,** and in particular regular assessment of the validity of comprehensive risk assessment tools (back-testing);
- a summary description of the market risk limits (specify the level of limits, broken down by type of risk incurred, in relation to own funds and earnings);
- the frequency with which market risk limits are reviewed (*indicating the date of the most recent review carried out during the past year*); the identity of the body responsible for setting such limits;
- the framework used to monitor compliance with procedures and limits;
- any breaches of limits identified during the past year (*specifying causes, number of breaches and amounts*);
- the procedures used to authorise such breaches and the measures taken to remedy them;
- the procedures used for reporting on compliance with limits (*frequency, recipients*);
- the procedures, frequency and conclusions of the analysis provided to the members of the management body in its executive function and the supervisory body on the results of market operations (*specify the date of the most recent analysis*) and on the level of risk incurred, in particular with regard to the amount of own funds allocated and the level of internal capital used to cover material market risks that are not subject to own funds requirements (cf. Articles 130 to 133 of the *Arrêté du 3 novembre 2014*, as amended):
    - attach a sample of the documents provided to the members of the management body in its executive function that enable them to assess the risk incurred by the institution, in particular in relation to its own funds and earnings.

10.3. Results of 2nd level permanent control actions for market risk

- main shortcomings identified;
- measures taken to remedy the identified shortcomings**,** the expected completion date of these measures, and the state of progress of their implementation as at the date of drafting of this Report;
- the procedures used to follow up on the recommendations issued following permanent control actions (*tools, persons in charge, etc.*);
- the procedures used to verify that the corrective measures ordered by the institution have been carried out by the appropriate persons within a reasonable timeframe (cf. Articles 11 f) and 26 a) of the *Arrêté du 3 novembre 2014*, as amended).

10.4. Stress testing for market risk

Institutions that use their internal models to calculate own funds requirements for market risk shall attach an annex detailing the assumptions and methodological principles used, and summarising the results obtained; this annex shall provide a comprehensive overview of any changes made to the model during the year under review, distinguishing between those identified as material and those identified as non-material, pursuant to the definitions of Commission Delegated (EU) Regulation No 2015/942 of 4 March 2015. Insitutions shall explain the extent to which such changes have originated from internal control processes.

10.5. Overall conclusion on exposure to market risk

11. Operational risk

11.1 Governance and organisation of operational risk

- summary description of the overall framework used to identify, manage, monitor and report on operational risk, in line with the complexity of the institution’s activities, its risk profile and its risk appetite;

- governance: description of the governance framework used to manage operational risk and, where applicable, model governance, role and responsibilities of the various committees set up, structuring decisions taken during the year regarding operational risk;
- organisation: presentation of the various teams in charge of permanent control for operational risk, by business line and geographical area (numbers of FTEs, both forecasted and actual, responsibilities, reporting lines), objectives of the various permanent control teams, actions undertaken during the year and state of progress of reorganisation projects at year-end, constraints faced and solutions considered/implemented during the execution phase of these reorganisation projects, targets to be achieved and expected timeline for full deployment of the target organisation;
- scope of entities: entities included and consolidation methods (expressed as numbers and as a proportion of total assets), treatment of entities included in the scope of prudential consolidation in the last two financial years, any entities excluded from consolidation and the reasons for such exclusion, transactions taken into account.

11.2. Identification and assessment of operational risk

- a description of the types of operational risk to which the institution is exposed;
- a description of the system used to identify; assess and monitor operational risk: the institution's framework for the identification of exposures to operational risk, mechanisms used to track relevant data -including data on significant losses- procedures used to verify data quality; definition of the processes the allow for the adoption of corrective measures;
- the monitoring framework implemented to ensure the comprehensive identification of all incidents that should be identified, including those related to legal and compliance risks; identification of risks that require improvements to be made to the current monitoring system and remedial action taken;
- presentation of the operational risk mapping, including identification of business lines/risks that are not (yet) covered by the risk mapping established as at year-end;
- a summary description of the reports used to measure and manage operational risk (*specifying in particular the frequency of reporting and recipients of those reports, the risk areas covered, and the existence or lack of early warning indicators highlighting potential future losses, and historical loss data*); documentation on and communication of the procedures used to monitor and manage operational risk;
- a description of the specific procedures used to manage internal and external fraud risk, as defined in Article 324 of (EU) Regulation No 575/2013 of the European Parliament and of the Council of 26 June 2013, as amended;
- a summary description of any insurance techniques used;
- a summary of ongoing discussions on changes that the institution has to anticipate concerning the methods used to calculate regulatory requirements for operational risk.

For institutions with a business indicator equal to or exceeding EUR 750 million:

- description of the sysems, processes, and mechanisms implemented to establish and continuously maintain a comprehensive dataset on losses, including the scope of entities and operational risk events covered, as well as te type of information recorded for each operational risk event;
- description of the framework in place to ensure the resilience, robustness, and performance of the IT systems and infrastructure required to maintain and update the loss dataset;
- description of the organisational structure and controls established to ensure the exhaustiveness, accuracy and quality of loss data, including the associated independent review procedures.

11.3. Integration of the operational risk measurement and management framework into the permanent control system

- a description of the procedures used to integrate operational risk monitoring into the permanent control system, including, inter alia, risks related to low-frequency high-severity events, internal and external

fraud risks as set out in Article 324 of (EU) Regulation No 575/2013, as amended, and risks related to model risk as defined in Article 4 of Delegated (EU) Regulation No 2018/959;

- a description of the main operational risks identified in the course of the year (settlement incidents, errors, fraud, etc.) and the lessons learned from them.

11.4. Results of 2nd level permanent controls carried out for operational risk

- main shortcomings identified;
- corrective measures taken to remedy the identified shortcomings**,** the expected date of completion of these measures, and the state of progress of their implementation as at the date of drafting of this Report;
- the procedures used to follow up on the recommendations issued as a result of permanent controls (*tools, persons in charge, etc.*);
- the procedures used to verify that the corrective measures ordered by the institution have been carried out by the appropriate persons within a reasonable timeframe (cf. Articles 11 f) and 26 a) of the *Arrêté du 3 novembre 2014*, as amended).

11.5. Overall conclusions on exposure to operational risk

12. Accounting risk

12.1. Significant changes made to the institution's accounting system

If no significant changes have been made to the accounting system of an institution, that institution may provide a summary description of the accounting system in an annex (cf. framework template appended in Annex 1 of this document).

- a presentation of changes made to the consolidation scope, if any (additions and exclusions).

12.2. Results of 2nd level permanents controls carried out for accounting risk

- main shortcomings identified;
- corrective measures taken to remedy identified shortcomings**,** expected date of completion of these measures, and state of progress of their implementation as at the date of drafting of this Report;
- the procedures used to follow up on the recommendations issued as a result of permanent controls (*tools, persons in charge, etc.*);
- the procedures used to verify that the corrective measures ordered by the institution have been carried out by the appropriate persons within a reasonable timeframe (cf. Articles 11 f) and 26 a) of the *Arrêté du 3 novembre 2014*, as amended);
- a presentation of the accouting risk prevention framework, covering the risk of IT system failure (fallback sites…).

13. Overall interest-rate risk (IRRBB)

- a summary description of the overall framework used to identify, assess and manage the overall interest-rate risk in the banking book (*specifying the scope of entities and operations covered, and justifying the role of the members of the management body in its executive function and the supervisory body as well as the allocation of responsabilities for the oversight and steering of overall interest-rate risk*);
- a description and justification of the potential use of the principle of proportionality in light of the volume, complexity, risk appetite and risk level of interest-rate sensitive positions as well as of the institution's size, strategy and business model, applicable to the following guideline requirements:

- calculation and allocation of internal capital for interest-rate risk (taking into account both the impact on economic value and on net interest income[7]);
- measurement and monitoring of interest-rate risk (including use of appropriate internal shock scenarios as referred to in paragraphs 89 to 102 of the EBA Guidelines and application of the proportionality measures set out in the "sophistication matrix" included in Annex II of the EBA Guidelines), and including consideration of interactions and cross-effects between different types of risks: interest rate, credit, liquidity, and market risk;
- risk monitoring arrangements (including the limits and sub-limits applied exclusively to the material components of interest-rate risk referred to in paragraphs 44(c) and 44(d) of the EBA Guidelines);
- governance arrangements (adaptation of reporting to the management body in line with the institution's activities, as outlined in paragraph 67 of the EBA Guidelines).

13.1. Overall interest-rate risk measurement and monitoring framework and methodological principles used

- a description of the tools and methodological principles used to manage overall interest-rate risk (*specifying the indicators used by the institution, such as static or dynamic gap analysis, net interest income sensitivity calculations, net present value assessments, assumptions and outcomes of internal stress testing scenarios including, where applicable, interactions and cross-effects between different types of risks (interest rate, credit, liquidity and market risks – paragraph 97 of the EBA Guidelines), assessment of the impact of overall interest-rate risk variations on the institution's business during the past year, the methodology used to aggregate exposures in the event of exposures in multiple currencies, consideration of the impact of fair value instruments*);
- a description of the runoff assumptions used by the institution [*specifying the scope covered, the main assumptions retained, the treatment applied to new production, treatment of non-interest-bearing products (such as own funds), treatment of automatic (explicit or implicit) and behavioural options, including the methodology used for non-maturity deposits (presentation of the methodology used for the segmentation of deposits by category, identification of stable deposits), run-off assumptions used for the various segments of non-maturity deposits, for early loan repayments, for early withdrawals from term deposit accounts, for off-balance sheet items (e.g. undrawn credit and liquidity facilities) and for regulated savings products]*;
- a presentation of hedging activities (*specifying the adopted strategy, the various instruments implemented and controls performed on these activities);*
- a description of the results of overall interest-rate risk measurement indicators used by the institution:
  - *specifying the levels of static or dynamic gaps, the results of net interest income sensitivity calculations, net present value assessments and stress-testing outcomes),*
  - *for the calculation of sensitivity in terms of economic value and net interest income, provide a justification for any deviations from the standardised assumptions described in the framework of the "Supervisory outlier test",*
  - *for the measurement of net interest income sensitivity based on the underlying internal assumptions retained by the institution for its internal risk management of the overall interest-rate risk, based on one- to five-year projections, including at least one baseline scenario and one shock or stress scenario as stated in paragraph 15 of the EBA Guidelines (also refer to the sophistication matrix included in Annex II of the EBA Guidelines). Include a presentation of the assumptions used and of the method used for the inclusion of fair value instruments.*

[7] As specified in paragraph 23 of the EBA Guidelines (EBA/GL/2022/14), both measures must be considered in the internal capital allocation process. However, institutions are not expected to double-count capital requirements for each measure (net interest income and economic value).

Annex 1 of EBA Guidelines EBA/GL/2022/14 provides an example of methods that can be used, for institutions that do not have their own methodology;

- sensitivity of shock outcomes to changes in the assumptions used (*specifying the impact of various (parallel and non-parallel) yield curve variations, the impact of mismatches between different rate references (basis risk) and changes to the retained assumptions and runoff conventions used);*
- presentation of the internal capital allocated in view of the overall interest-rate risk incurred by the institution, along with the chosen allocation methodology;
- presentation of the alternative interest-rate scenarios used by the institution (for example, curve flattening or steepening, curve inversion, short-term interest-rate shocks, etc.) and presentation of their impact on economic value and net interest income.

13.2. Monitoring system used for overall interest-rate risk

- for both net interest income and economic value measures, a summary description of the limits set with respect to overall interest-rate risk (*specifying the nature and level of the implemented limits, for example gap limits, sensitivity limits expressed as a percentage of capital or earnings, specifying the date on which such limits were reviewed in the course of the past financial year, and the procedure used to monitor breaches of limits*);
- a summary description of the reports used to manage overall interest-rate risk (*specifying in particular the frequency and recipients of these reports*);
- the roles of the members of the management body in its executive function, the supervisory body and, when applicable, the risk committee, in defining the institution's overall strategy and risk appetite (both current and forward-looking with respect to interest-rate risk in the banking book (cf. Articles L. 511-92 and L. 511-93 of the French *Code monétaire et financier*), and in setting up limits (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended).

13.3. Permanent control system used for overall interest-rate risk management

- specify whether a dedicated unit is responsible for monitoring and managing overall interest-rate risk, and more generally, how this oversight is integrated into the permanent control framework.

13.4. Results of 2nd level permanent controls on overall interest-rate risk

- main shortcomings identified;
- corrective measures taken to remedy the identified shortcomings**,** expected implementation date of these measures, and the state of progress of their implementation as at the date of drafting of this Report;
- the procedures used to follow up on the recommendations issued as a result of permanent controls (*tools, persons in charge, etc.*);
- the procedures used to verify that the corrective measures ordered by the institution have been carried out by the appropriate persons within a reasonable timeframe (cf. Articles 11 f) and 26 a) of the *Arrêté du 3 novembre 2014*, as amended).

13.5. Monitoring framework used for the credit spread risk in the banking book (CSRBB):

- a summary description of the general framework used to identify, assess and manage CSRBB risk: *specifying the scope of operations covered and any exclusion of instruments applied, stating the reasons for such exclusions, a description of the role of the members of the management body in its executive function and the supervisory bodies and the allocation of responsibilities for CSRBB risk oversight;*
- a description of the monitoring and assessment of positions exposed to credit spread risk outside the trading book, especially through economic value and net interest income metrics (see Article 84(2) of Directive No 2013/36/EU): *specify the indicators and tools used, the assumptions and methodological principles used, and the results obtained;*

- a summary description of the reports used for CSRBB risk management *(specifying in particular the frequency and recipients of these reports).*

13.6. Overall conclusion on exposure to overall interest-rate risk

- institutions must formalise and submit the conclusions of their IRRBB and CSRBB risk sensitivity assessments, and their impact on risk management and on the overall management of the institution.

14. Intermediation risk for investment services providers

- statements of the overall breakdown of exposures by set of counterparties and by principal (by internal rating, by financial instrument, by market, or by any other criteria that is relevant in the context of the business conducted by the institution);
- information on risk management practices (collateral arrangements, margin calls to cover positions, guarantees, etc.) and on the procedures followed in the event of default by an originator (insufficient hedging of positions, declined transaction);
- a brief description of the exposure limit framework for intermediation risk -by beneficiary, by connected debtors, etc. (specifying the level of these limits in relation to the volume of operations by beneficiaries and in relation to own funds);
- the procedures used to review intermediation risk limits and the frequency of such review (*specifying the date of the most recent review*);
- any breaches of limits identified during the past year (*specifying their causes, the counterparties involved, the total exposure amount, the number of breaches, their duration and amounts*);
- the procedures used to authorise such breaches and the measures taken to resolve them;
- the risk assessment criteria used to assess risk incurred through originators that is taken into account when marking decisions on exposures (*methodology, data used for the analysis*);
- a typology of errors identified during the past year in the processing and execution of orders (*methods and frequency of error analysis conducted by the head of internal control, threshold set by the members of the management body in its executive function to document such errors*);
- results of permanent controls conducted on intermediation risk;
- main conclusions derived from the risk analysis conducted.

15. Settlement/delivery risk

- a description of the system used to measure settlement/delivery risk (*highlighting the various phases of the settlement process, including the way new transactions are incorporated into ongoing transactions, etc.*);
- a summary description of the limits set for settlement/delivery risk (*specifying the level of limits by type of counterparty, in relation to the transaction volumes with these counterparties and to the institution's own funds*);
- the frequency with which settlement/delivery limits are reviewed (*specifying the date of the most recent review*);
- any breaches of limits identified during the past year (*specifying their causes and number of occurrences, their duration and the amounts involved*);
- the procedures used to authorise such breaches and the measures taken to remedy them;
- an analysis of outstanding unsettled items (*indicating their anteriority, their causes, and the action plan in place to clear them*);

- the results of permanent controls carried out in relation to settlement/delivery risk;
- the main conclusions of the risk analysis conducted.

For investment services providers offering settlement finality guarantees:

- a description of the various financial instruments processed and of each settlement system used, identifying the various phases of the settlement and delivery process;
- the procedures used to monitor cash and securities flows;
- the procedures used to monitor and resolve unsettled items;
- the procedures used to measure readily available resources, securities and cash to ensure the timely fulfilment of obligations to counterparties**.**

16. Liquidity risks

- a summary description of the general framework used to identify, measure, manage and monitor liquidity risks: *specifying the scope of entities and operations covered, taking into account off-balance sheet exposures, the role of the members of the management body in its executive function and the supervisory body, and the allocation of responsibilities pertaining to liquidity risk oversight, including the institution's risk profile and its risk tolerance* (cf. Articles 181 and 183 of the *Arrêté du 3 novembre 2014*, as amended).
- information on the diversification of the funding structure and the sources of funding: description of the institution's funding structure and of the funding sources used (*specifying the various funding channels and the intragroup financing links, amounts, maturities, main counterparties, and the use of liquidity risk mitigation instruments*), description of the indicators used to measure funding diversification (cf. Article 160 of the *Arrêté du 3 novembre 2014*, as amended).
- for credit institutions and branches of credit institutions the head office of which is located in a third country, specify how the internal methodology takes into account the potential systemic repercussions that may arise due to the significance of the institution in its market, especially in each Member State of the European Union where it operates (cf. Article 150 of the *Arrêté du 3 novembre 2014*, as amended).

16.1. Liquidity risk measurement framework (and methodology used)

- a description of the tools and methods used to manage liquidity risks: *specifying the assumptions retained and time horizons considered for the calculation of liquidity risk indicators used by the institution (cf. Article 156 of the* Arrêté du 3 novembre 2014, as amended*), in line with the complexity of its activities, risk profile and risk tolerance, including a breakdown of the information systems, tools and indicators used for each currency in which the institution conducts significant business and specifying the alternative scenarios considered, as provided for in Article 168 of the* Arrêté du 3 novembre 2014, as amended;
- financing companies shall provide an annex to their Internal Control Report which includes:
  - a description of the characteristics and assumptions used to prepare the projected cash-flow statement, and any changes to these characteristics and assumptions made during the year;
  - an analysis of any evolution of liquidity gaps calculated on the basis of cash flow statements prepared during the year under review.
- where applicable, a description and justification of scenarios specific to certain foreign branches, legal entities or business lines (cf. Article 171 of the *Arrêté du 3 novembre 2014*, as amended);
- information on deposits and their diversification (*expressed as a number of depositors*);
- a description of the assumptions used to determine the stock of liquid assets in relation to the liquidity risk limit framework;
- a description of the means implemented to ensure continuous monitoring of the required stock of liquid assets, and the assumptions used to adjust stock across the various time horizons considered;

- a description of the methodology used for the regular assessment, in accordance with Article 23 of Delegated (EU) Regulation No 2015/61, as amended, on liquidity coverage ratio requirements (LCR) for credit institutions, a description of the likelihood and potential volume of liquidity outflows over 30 calendar days related to products or services which are not referred to in Articles 27 to 31 of the LCR. Where applicable, information on actual cash outflows not provided for in ACPR Decision 2016-C-26;
- internal liquidity cost allocation framework and analysis of the evolution ofliquidity cost indicators over the past financial year;
- procedures used to taking account of, measure, monitor and control intra-day liquidity risk;
- a description of funding plans: methods used to assess the institution's ability to raise funds from its funding sources under both business-as-usual and stressed conditions, across all relevant maturities and broken down by currency (*underlying assumptions, test results*, etc.), procedures used to take account of reputational risk; procedures used to distinguish between encumbered and unencumbered assets available at all times, particularly in emergency situations, procedures used to take account of the legal, regulatory and operational constraints on the tranfer of liquidity and unencumbered assets between entities, procedures used to take account of potential haircuts in the event of the sale of assets within a short timeframe, etc.
- a description of the stress scenarios used to measure the risk incurred in the event of significant variations in market parameters (indicate the assumptions used, the frequency with which they are reviewed, and the validation process; summarise the results of the stress tests and the procedures used to report on them to the supervisory body), as well as the main conclusions of the analysis of the risk incurred in the event of a significant change in market parameters;
- a description of contingency plans implemented in order to withstand a liquidity crisis (this plan must consider both the institution-specific refinancing risk, broader market liquidity risk and the interactions between these two risks, while also, where applicable, integrating intra-day liquidity risk): *specify the procedures implemented (identity and hierarchic level of persons concerned, liquidity sources considered, public communication plan, regular testing of contingency plans…)*;
- a description of the liquidity recovery plans setting up the strategies and measures implemented in order to address potential liquidity shortfalls, which must be tested regularly: *specify the operational measures adopted to ensure immediate execution of the recovery plans (holding of readily available collateral…)*.

16.2. Liquidity risk monitoring framework

- a summary description of the liquidity risk limits and liquidity risk tolerance level (*specify and justify the limit levels for each type of business, currency and counterparty, in relation to the volume of operations with these counterparties and in relation to the institution's own funds*);
- the procedure and frequency with which liquidity risk limits are reviewed (*specify the date of the most recent review, contributors, method applied*);
- the frequency of review of the criteria used for asset identification, valuation, liquidity and availability, and recognition of liquidity risk mitigation instruments (*specify the date of the most recent review*);
- the frequency of review of the assumptions and alternative assumptions related to the funding conditions, liquidity positions and risk mitigation factors *(specify the date of the most recent review)*;
- any breaches of limits identified during the past year (*specify their causes, the number of occurrences, and the amounts involved*);
- the procedures used to authorise such breaches and the measures taken to address them;
- a summary description of the reports used to manage liquidity risk (*including their frequency and recipients*);
- a description of all incidents encountered during the past financial year;
- a description of the systems used to measure and manage the quality and composition of liquidity buffers and a description of the systems used to measure and monitor encumbered and unencumbered assets;
- the control procedures carried out by the risk management function on liquid assets;

- the procedures used for the approval and review by the supervisory body of the strategies and policies governing risk-taking, risk management, risk monitoring and mitigation for liquidity risks (cf. Article L. 511-60 of the French *Code monétaire et financier*);
- institutions subject to the CRR and not under the ECB's direct supervision shall provide a "reader's guide", drawn up as a comprehensive document to facilitate the assessment of documentation supporting their liquidity adequacy. To that end,, the "reader's guide" shall provide an overview of all documents submitted to the competent authorities on that matter, as well as their respective status (new, unchanged, amended with minor corrections, etc.). The "reader's guide" should essentially function as an index linking the specific items of information required for the internal control report to the documents provided to the competent authority concerning their liquidity adequacy assessment. The "reader's guide" shall also provide information on significant changes to the information compared to previously submitted infromation, any elements excluded from the submitted documents and any other information that may be useful to the competent authority for the purpose of the assessment. Furthermore, the "reader's guide" shall contain references to all information publicly disclosed by the institution on its liquidity adequacy.
- class 2 investment firms shall prepare a formal report pursuant to Article L533-2-2 of the French *Code Monétaire et Financier* to document the ILAAP framework implemented by the institution and to demonstrate the effectiveness of the adequacy between its available liquid assets and the risks to which it is exposed, both dynamically and over time, under normal and stressed market conditions. A template listing the key information to be provided by the investment firm in this report is made available by the SGACPR on the ACPR's website[8].

16.3. Liquidity risk and pro-cyclicality risk stemming from margin calls associated with central clearing by clearing members and exposures not subject to central clearing

- a presentation of the procedures in place to ensure that the provision of central clearing services to customers does not trigger sudden and significant changes in margin calls, margin collection or credit rating downgrades;
- a presentation of the procedures in place to ensure that, for over-the-counter derivative contracts and securities financing transactions not subject to central clearing, risk management procedures do not trigger sudden and significant changes in margin calls, margin collection and credit ratings downgrades;
- a presentation of the procedures in place to limit liquidity constraints related to margin collection (for instance, using excess initial margin collateral rather than requiring additional collateral, consideration of customers' operational constraints).

16.4. Permanent control framework for liquidity risk management

- a presentation of the control environment in place for the management of liquidity risks (*specifying the role of the permanent control function*).

16.5. Results of 2nd level permanent control actions carried out for liquidity risks

- main shortcomings identified;
- corrective measures taken to address the identified shortcomings**,** the date on which these measures are expected to be carried out, and the state of progress of their implementation as at the date of drafting of this Report;
- the procedures used to follow up on the recommendations issued as a result of permanent control actions (*tools, persons in charge, etc.*);
- the procedures used to verify that the corrective measures ordered by the supervised institutions have been carried out by the appropriate persons within a reasonable timeframe (cf. Articles 11 f) and 26 a) of the *Arrêté du 3 novembre 2014*, as amended).

[8] Framework template available on the following webpage: Prudential reporting | ACPR (banque-france.fr)

16.6. Overall conclusion on exposure to liquidity risks

- institutions subject to the CRR and not under the ECB's direct supervision shall formalise and submit the conclusions of their internal liquidity adequacy assessment and its impact on risk management and on the institution's overall governance.

17. Excessive leverage risk

This section does not apply to financing companies (*sociétés de financement*) (cf. Article 230 of the *Arrêté du 3 novembre 2014*, as amended).

- a description of the policies, processes and indicators (including leverage ratio and mismatches between assets and liabilities) used to identify, manage, and monitor excessive leverage risk in a conservative manner (cf. Article 211 of the *Arrêté du 3 novembre 2014*, as amended);

- the leverage ratio target set by the institution;

- the stress scenarios used to assess the institution's resilience in the event of a reduction of its own funds levels due to expected or realised losses (cf. Article 212 of the *Arrêté du 3 novembre 2014*, as amended), including capital strengthening plans under stressed conditions.

18. Internal control framework for the safeguarding of customer funds by investment firms

- the organisational arrangements made for the management of customer cash accounts and alignement (allowing for the various cash flows to be traced chronologically) with the execution of investment or clearing services;
- a presentation of the method implemented to ensure the safeguarding of client funds in accordance with applicable regulations (i.e. *Arrêté du 6 septembre 2017*, as amended, on the segregation of client funds held by investment firms) and a description of the tool used to calculate the amount of client funds received that need to be segregated;
- for institutions safeguarding client funds by placing them in one or more account(s), opened specifically for that purpose with a credit institution: submission of the segregated account agreement(s) and of any amendments to previously submitted segregation agreements, description of the procedures in place to ensure the investment of funds;
- for institutions safeguarding client funds through a guarantee mechanism: submission of any amendments to the guarantee mechanism or surety agreement and of any information on the adjustment of the coverage amount in line with changes in business volume;
- for institutions safeguarding client funds through deposits with a credit institution, bank or qualifying money market fund belonging to the same group: disclosure of the amount deposited with one or more intra-group entities as a share of the total amount of segregated client funds, including a rationale for the proportion of intra-group segregated funds;
- a presentation of the procedures in place to ensure compliance with client fund safeguarding requirements, presentation of the associated checks and disclosure of any incidents or shortcomings identified as a result of such auditing measures;
- disclosure of the identity of the single individual with sufficient skills and authority that is specifically responsible for ensuring the institution's compliance with its obligations as regards the safeguarding of client financial instruments and funds, in accordance with Article 9 of the *Arrêté du 6 septembre 2017*, as amended, on the segregation of client funds held byinvestment firms;

- submission of the report issued by statutory auditors on compliance with the regulatory requirements on client fund segregation.

19. Provisions on the separation of banking activities

***Nota bene**:* This section concerns the application of Title I of the Law on the Separation and Regulation of Banking Activities (*Loi de séparation et de régulation bancaire n° 2013-672 du 26 juillet 2013*, also referred to as *Loi SRAB*). Institutions are reminded that the mandates of the internal units mentioned in the mapping must be sent to the SGACPR along with the report on internal control. This submission, which may be made electronically, must specify (i) the list of internal units the activity of which has substantially changed since the last report sent to the SGACPR (ii) at a minimum, the updated mandates of those internal units. Institutions may also submit all mandates, highlighting any substantial changes compared to the last submission to the SGACPR.

19.1. Mapping of trading activities in financial instruments

- submission of the updated mapping of internal units in charge of trading in financial instruments as referred to in Article 1 of *Arrêté du 9 septembre 2014*, at the most granular organisational level within the institution, identifying any groupings made. The mapping must include at least the following elements:
    - the literal name of the lowest organisational level,
    - a summary description of the activities carried out,
    - the relevant category(ies) of exemptions from separation as provided for in Article L.511-47 of the French *Code monétaire et financier*,
    - the number of traders,
    - NBI generated over the year,
    - the main risk limits (VaR, other internal measures), including average and maximum use over the course of the year,
- a description of any changes in that mapping,
- a description of major new activities and discontinued activities.

19.2. Monitoring indicators

- a description of the indicators in place to monitor compliance with the provisions of Title I of Law No 2013-672 of 26 July 2013 on the Separation and Regulation of Banking Activities (*Loi SRAB*), in particular those related to market-making activities (cf. Article 6 of the *Arrêté du 9 septembre 2014* implementing Title I of the Law on the Separation and Regulation of Banking Activities);
- a summary description of the results derived from the indicators in place and the analyses carried out over the course of the past year (identifying atypical desks).

19.3. Assessment of activities with leveraged funds within the meaning of the *Loi SRAB*

- description of activities, including detailed information on the business lines used by the institution to classify transactions conducted with Collective Investment Undertakings (CIUs) and other similar vehicles that make substantial use of leverage;
- inventory of leveraged funds:

	Number of funds
A. CIUs or similar foreign vehicles through which the institution is exposed to credit or counterparty risk	
A.1. which directly or indirectly make substantial use of leverage and which are not explicitly excluded	
A.1.a. which make substantial use of leverage[9]	

[9] Within the meaning of Article 111 of Delegated Regulation No 231/2013 of the Commission of 19 December 2012

A.1.b. which are significantly invested in or exposed to[10] CIUs or other similar vehicles that make substantial use of leverage	
A.2. not making substantial use of leverage or explicitly excluded	
including: explicitely excluded under Article 7, paragraph I, sections 1 to 4 of the Arrêté du 9 septembre 2014	

- specify how often CIUs and similar vehicles are inventoried and categorised within the abovementionned classes;

- conclusions on the results and risks generated (credit and counterparty risks):

***Nota bene*: The tables and questions below, preceding section 19.4 refer only to transactions that expose the entity to credit or counterparty risk in relation to CIUs or other similar foreign vehicles that directly or indirectly make substantial use of leverage and that are not explicitely excluded under Article 7, paragraph 1, sections 1 to 4 of the *Arrêté du 9 septembre 2014*.**

- summary of exposures broken down by transaction type:

Expressed in thousands of EUR	Gross carrying amount under IFRS	Nominal amount under IFRS	Notional amount under IFRS	Exposure value before recognition of collateral	Risk-weighted assets for credit and counterparty risks
A. Transactions that have CIUs or other similar vehicles as a counterparty					
A.1. Financing activities excluding market transactions					
A.1.a. Accounts receivable and advances					
A.1.b. Loans excluding reverse repurchase agreements					
A.1.c. Undrawn credit lines					
A.1.d. Guarantee commitments					
A.2. Market transactions					
A.2.a. Securities repurchase agreements and securities lending and borrowing					
A.2.b. Derivatives					
A.2.b.i. Derivatives aimed at financing positions					
A.2.b.ii. Other derivatives					
A.3. Other					

[10] Beyond the threshold mentioned in Article 7 of the *Arrêté du 9 septembre 2014*

B. Investments in CIUs or similar vehicles					
B.1. Holdings in units of CIUs or similar vehicles held					
B.2. Other					
Total (A+B)					

- for institutions meeting one of the following conditions as at the reporting date:
    - the gross carrying amount under IFRS of the "Total (A+B)" line item exceeds EUR 300 million
    - the exposure value before recognition of collateral of the "Total (A+B)" line item exceeds EUR 300 million
    - the exposure value before recognition of collateral of the "Total (A+B)" line item exceeds 5% of prudential own funds:
        - fill out the table below:

Expressed in thousands of EUR	Net banking income
A. Transactions with CIUs or similar vehicles as a counterparty	
A.1. Financing activities other than market transactions	
A.2. Market transactions	
A.3. Other	
B. Investment in CIUs or similar vehicles	
B.1. Holdings in units of CIUs or similar vehicles	
B.2. Other	
C. Other activities that do not generate credit or counterparty risks	
Total (A+B+C)	

        - specify the indicators used to measure the risk/return profile of the various activities;
        - indicate the level of granularity and frequency at which those indicators are calculated and monitored;
        - specify any quantitative targets or limits associated with these indicators;
- description of the risk management frameworks used for the aforementioned risks, and description of the associated controls:
- specify which internal business lines, as presented in the general description of activities, are governed by a collateralisation policy;
- for each business line with a collateralisation policy:
    - summarise its principles;
    - set out the eligibility, availability and quantity criteria applicable to collateral that ensure that such collateral covers the exposures generated by such transactions, in accordance with the provisions of Article 7 of the *Loi SRAB*;

  - specify how the quantity and availability criteria applied to collateral are adjusted according to the quality of collateral and the level of risks involved in the transactions secured by such collateral;
  - where the quality and availability criteria are not met, indicate whether an increased collateral requirement is provided for and if so, to what extent;
  - indicate whether the policy provides for any exemptions. If so, describe the governance framework that applies to them;
  - specify whether indicators are used to measure the degree of collateralisation of transactions. If so, define them and comment on their operational use;
- provide a summary of the principles applied to manage the concentration level of (i) individual exposures to a CIU or other similar vehicles making substantial use of leverage, and (ii) collateral received from such counterparties.

19.4. Control results

- results of ongoing control actions carried out pursuant to the requirements set out in Article 2 of the *Arrêté du 9 septembre 2014* implementing Title I of the Law No 2013-672 of 26 July 2013 on the Separation and Regulation of Banking Activities; corrective actions and measures taken to address the identified shortcomings;
- results of the periodic control actions carried out on compliance with Title I of Law No 2013-672 of 26 July 2013 on the Separation and Regulation of Banking Activities, corrective actions and measures implemented to address identified shortcomings.

20. Outsourcing policy

***Reminder**: outsourced ICT activities must be addressed in the dedicated ICT annex.*

- presentation of the institution's or group's outsourcing strategy, including in particular a description of existing arrangements to inform outsourcing decisions (*prior analysis of the criticality of the activity to be outsourced and assessment of associated risks*) before outsourcing decisions become effective;
- description of outsourced activities (as defined in q) and r) of Article 10 of the *Arrêté du 3 novembre 2014*, as amended) and expressed as a proportion of the institution's total activities *(both aggregated and broken down by business area)*;
- description of the conditions underlying the use of outsourcing: name of the service provider, country of establishment, licensing status and prudential supervision of external providers, procedures implemented to ensure that a written agreement exists and that it complies with the requirements set out in Article 239 of the *Arrêté du 3 novembre 2014*, as amended, including those allowing the ACPR, or the ECB, when appropriate, to conduct on-site inspections at the premises of the external service provider, etc.;
- description of permanent and periodic control framework for outsourced activities;
- description of the methodology used for the assessment of service quality and frequency of review;
- description of the procedures used for the identification, management and monitoring of risks associated with outsourced activities;
- description of procedures implemented by the institution to retain the necessary expertise in order to effectively control outsourced activities and manage the risks associated with outsourcing;
- description of the procedures used for the identification, assessment and management of conflicts of interest related to the outsourcing mechanism of the institution, including between entities within the same group;
- description of the business continuity plans and exit strategies defined for critical or important outsourced activities: formalised retained scenarii and objectives as well as alternative measures considered, presentation of the tests carried out (frequency, results…), reporting to senior management (on test outcomes and updates to the defined plans or exit strategies);

- procedures to inform the supervisory body and, when appropriate, the risk committee on measures taken to ensure control over outsourced activities and the resulting risks (cf. Article 253 c) of the *Arrêté du 3 novembre 2014*, as amended);
- description of due diligence carried out by the members of the management body in its executive function to verify the efficiency of the internal control mechanisms and procedures used for outsourced activities (cf. Article 242 of the *Arrêté du 3 novembre 2014*, as amended);
- description, formalisation and date(s) of update of the procedures supporting the permanent and periodic control of outsourced activities (including compliance review procedures);
- results of 2nd level permanent control actions carried out on outsourced activities: main shortcomings identified and corrective measures implemented to address them (provisional date of implementation and state of progress of their implementation at the time of drafting of this report), procedures used to follow-up on recommendations resulting from permanent control actions (*tools, persons in charge*);
- results of periodic control actions carried out on outsourced activities: main shortcomings identified and corrective measures implemented to address them (provisional date of implementation and state of progress of their implementation at the time of drafting of this report), procedure used to follow-up on recommendations resulting from periodic control actions.

21. Specific information required from financial conglomerates

- Group balance sheet total and respective balance sheet totals for the banking, insurance and non-financial sectors.

21.1. Internal control and risk assessment framework applied to all the entities belonging to the financial conglomerate

- a presentation of the conditions under which the activities of insurance entities are covered by the conglomerate's internal control framework;
- a presentation of the procedures used to assess the impact of growth strategies on the risk profile of the conglomerate and the additional capital requirements;
- a presentation of the procedures used to identify, measure, monitor and carry out controls on intra-group transactions between the various entities of the conglomerate, as well as risk concentration;
- the results of 2nd level permanent control actions conducted on insurance entities.

21.2. Information on risks associated with entities in the insurance sector

- a description of the risks borne by insurance entities that are of the same nature as the risks associated with banking and finance activities;
- a description of the risks specific to insurance activities (*specifying which risks are managed centrally, with reference to the relevant procedures, and which ones remain decentralised*).

22. Annex on the security of non-cash means of payment provided or managed by the institution, the security of payment account access and information

CONTENTS

IV. Audit report on the implementation of security measures provided in the RTS (Regulatory Technical Standards)

V. Annexes

1. Fraud risk rating matrix of the institution
2. Glossary

INTRODUCTION

Reminder on the legal framework

This annex is dedicated to the security of **non-cash means of payment** (as defined in Article L. 311-3 of the French *Code monétaire et financier*) issued or managed by the institution, and to **the security of accesses to payment accounts and payment account information** within the framework of the provision of payment initiation and payment account information services. Any instrument enabling a person to transfer funds, regardless of the medium or technical process used, is deemed to be a payment instrument.

The annex is sent by the General Secretariat of the *Autorité de contrôle prudentiel et de résolution* to the Banque de France for the performance of its tasks as defined in Article L. 141-4 and Article L-521-8 of the aforementioned French *Code Monétaire et Financier* and, for the annexes drawn up by institutions having their registered office in the French territorial communities of the Pacific region, to the *Institut d'Émission d'Outre-Mer* (IEOM) for the performance of its duties as defined in Article L. 721-20 of the same Code[11].

The annex, which is mainly aimed at the Banque de France, is a document independent from the rest of the reports established pursuant to Articles 258 to 266 of the *Arrêté du 3 novembre 2014*, as amended. Additionally, insofar as the Banque de France's competence is limited to the French territory, this annex solely applies to payment instruments offered in France (or to payment accounts opened in France), thereby excluding services provided by institutions through their branches established abroad.

Institutions managing payment instruments, without issuing them, shall fill in this annex. Institutions that neither issue nor manage cashless payment instruments must include the following statement: "Institution that neither issues nor manages cashless payment instruments as part of its business".

Features and contents of this annex

This annex aims at assessing the level of security reached by all the non-cash means of payment issued or managed by the institution, as well as that of access to payment accounts held by the institution.

This annex is divided into five sections:

- a section dedicated to the presentation of each payment method and service, the associated fraud risks and risk management mechanisms in place (I);
- a section dedicated to the results of periodic control procedures applied to the scope of non-cash means of payment and account access (II);
- a section dedicated to collecting the the institution's self-assessment of compliance with the recommendations issued by external bodies as regards the security of non-cash means of payment and account access (III);
- a section on the audit report on the implementation of security measures provided for in the RTS (Regulatory Technical Standards)[12] (IV);
- an annex including the fraud risk rating matrix and a glossary of definitions for the technical terms/acronyms used by the institution in the annex (V).

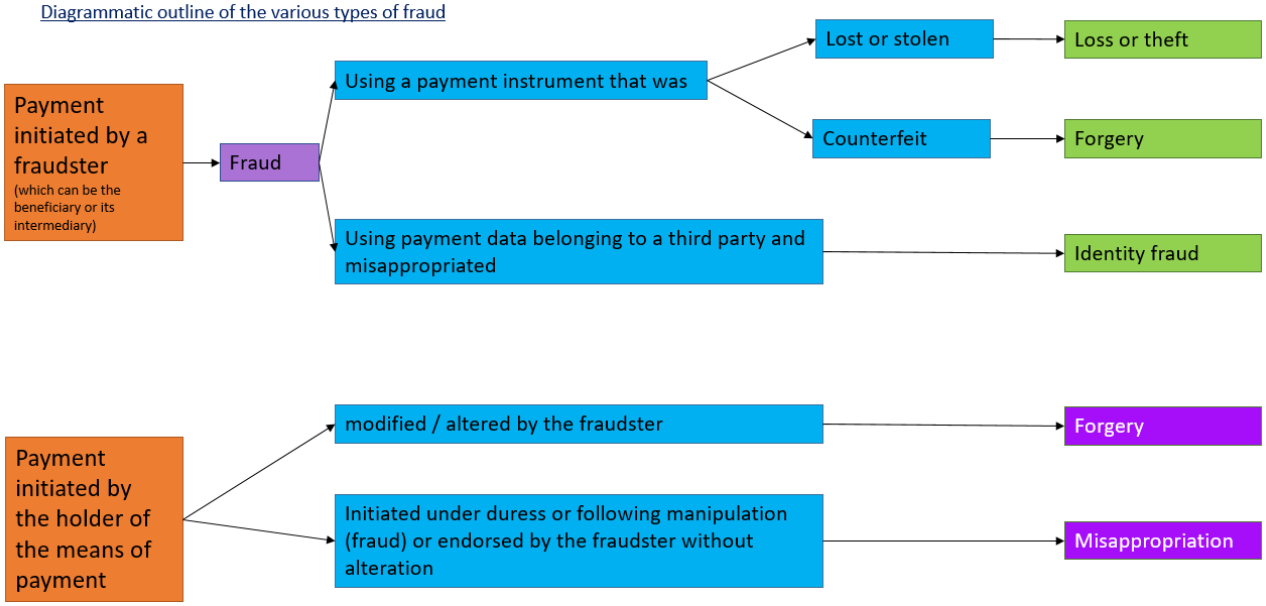
[11] For payment service providers having their head office registered in one of the French territorial communities of the Pacific region (New Caledonia, French Polynesia, Wallis and Futuna Islands), reference to the "Banque de France" should be replaced with one to "IEOM" in this Annex, and references to the "French territory" should be replaced with one to the "French territorial communities of the Pacific region".

[12] Delegated Regulation No. 2018/389/EU issued by the European Commission on 17 November 2017 supplementing Directive 2015/2366/EU of the European Parliament and Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

Regarding section I, the analysis of fraud risks for each means of payment is carried out using fraud data as submitted by the institution to the Banque de France within the framework of the collection of statistics on the "Inventory of fraud on non-cash means of payment"[13]. As a consequence, this analysis is carried out:

- on gross fraud and covers both internal and external fraud, and
- based on the definitions and typology of payment instrument fraud retained for the purposes of statistical reporting to the Banque de France.

Diagrammatic outline of the various types of fraud



NB: this diagram should be considered in conjunction with the official guides issued by the Banque de France and pertaining to statistical data collected on payment instrument fraud.

To this end, the fraud risk analysis grids dedicated to each non-cash means of payment, that are presented in the annex, are to be filled in according to the specific offerings of each institution. **Since the 2023 annual report on the 2022 financial year, institutions have also been required to fill in the section dedicated to cheques**. As far as the cheque section is concerned, yearly internal control reporting to the Banque de France allows institutions to escalate information on their offer of products and services related to cheques, on the operational organisation of their cheque business, on changes in fraud trends over the year under review, and on the risk control mechanisms they have in place, which the annual self-assessment exercise using the *Référentiel de Sécurité du Chèque* (the French cheque security reference framework, also referred to as RSC) of the Banque de France does not allow.

The list of recommendations on the security of means of payment issued by external bodies, presented in section III of this annex, takes account of the entry into force, on 13 January 2018, of the 2nd European Payment Services Directive. Institutions are expected to provide explanatory comments for any recommendation they are not fully compliant with.

Section IV is dedicated to the collection of the results of the audit report which has to be established by the institution pursuant to Article 3 of Commission Delegated (EU) Regulation 2018/389 of 27 November 2017 supplementing (EU) Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication or RTS (Regulatory Technical Standards). These technical standards are fundamental requirements for the security of non-cash means of payment, accesses to payment accounts and payment account information. The purpose of this report is to assess the institution's compliance with security requirements provided for in the RTS. It takes the form of a questionnaire covering the security measures provided for in the RTS and for which the institution must provide reasoned answers on their implementation

[13] See the guide to the completion of fraud statistics (in French): https://www.banque-france.fr/stabilite-financiere/securite-des-moyens-de-paiement-scripturaux/oscamps/documentation-des-collectes

or, where applicable, on the action plan envisaged to comply with them. Pursuant to Article 3 of the RTS, it is reminded that this audit report has to be drawn up annually by the periodic control teams of the institution. However, regarding the assessment of the institution's compliance with Article 18 of the RTS in the event the exemption set out therein is used, it has to be performed by an external independent and qualified auditor on the first year of its implementation, and then every three years. The purpose of this assessment is to check compliance with the conditions for implementing the exemption based on risk analysis and in particular, with the fraud rate measured by the institution for the type of payment transaction concerned (i.e. with regard to the payment instrument used and the amount of the payment transaction); this assessment carried out by an external auditor shall be annexed to section IV on the conclusions of the audit report.

Important note concerning banking institutions affiliated to a group, network or central body: the latter is responsible for the internal control and risk management framework at central level for the security of means of payment and access to accounts.

- for the section on the presentation of each means of payment (I), the affiliated institution is required to present its offer of products and services as well as the operational organisation of its activities. However, it is exempted from providing the risk analysis matrix and main fraud incidents and it must instead state that "*it refers to the information provided by the institution in charge of the risk control and risk management framework in its own annex*".
- concerning the section dedicated to the presentation of periodic control results (II), if this function is carried out under the responsibility of the group, nework or central body and described by the latter in its own annex, only the controls specific to the affiliated institution must be provided by the latter.
- concerning the section dedicated to the self-assessment of compliance with recommendations issued by external bodies as regards the security of non-cash means of payment (III), the affiliated institution is exempted and must state that "*it refers to the information provided by the institution in charge of the internal control and risk management framework in its own annex*".
- concerning the audit report on the implementation of security measures provided for in the RTS (IV), the affiliated institution is exempted from providing it and must state that "*it refers to the information provided by the institution in charge of the internal control and risk management framework in its own annex*".

When an institution refers the reader to the annex drawn up by the institution in charge of the internal control and risk management framework for the security of means of payment and account access, it shall specify the exact identity and interbank code of the institution concerned.

Definition of the main concepts used in the annex

Terms	Definitions
Initiation channel	Depending on which of the various services and means of payment is meant, the concept of initiation channel refers: - for cards, to the channel of use of the card: payment at point-of-sale, withdrawal, remote payment, contactless payment, enrolment in e-wallets or mobile payment solutions; - for transfers, to the reception channel of the transfer order: desk, online banking, teletransmission solution…; - for direct debit, to the reception channel of the direct debit order; - for cheques, to the channel of cheque deposit: mail, machine… - for information on accounts and payment initiation services, to the connection means used: website, mobile application, dedicated protocol…

External fraud	In the field of means of payment, misappropriation of the latter, through the acts of third parties, for the benefit of an illegitimate beneficiary.
Internal fraud	In the field of means of payment, misappropriation of the latter, through the acts of third parties involving at least one member of the company, for the benefit of a illegitimate beneficiary.
Gross fraud	Within the meaning of the Banque de France's statistical collection "Inventory of fraud on non-cash means of payment", gross fraud corresponds to the nominal amount of authorised payment transactions which are subject to an *ex post* rejection due to fraud. Therefore, it does not take into account the funds which have been recovered after the relevant litigation process is through.
Gross risk	Risks likely to affect the proper functioning and security of means of payment, before the institution takes into account the procedures and measures used to mitigate them.
Residual risk	Risk remaining after risk coverage measures are taken into account.
Coverage measures	All actions undertaken by the institution in order to improve risk control, by mitigating both the impact of risks and their frequency of occurrence.

I – PRESENTATION OF MEANS AND SERVICES OF PAYMENT AND RISKS OF FRAUD THE INSTITUTION IS EXPOSED TO

1. Card and equivalent

1.1. Presentation of the offer

a. Description of products and services

Product and/or service	Characteristics, age and functionalities offered	Target clients	Initiation channel	Comments on the evolution of business volume	Comments on technology, functional or security-related developments
As an issuing institution					
*Ex: **payment card**: international card*	*Ex: - Maturity - Date of first commercial release - Equipped with the contactless function by default - Enrolment in an authentication device - Virtual card service*	*Ex: Individuals*	*Ex: at the point-of-sale or at the cash machine, remote payment,…*	*Specify the explanatory factors behind significant fluctuations of business (volume and amount)*	*Report any development that occurred during the period under review Ex: pilot testing, implementation of SMS alerts for international transactions on high-end cards…*
*Ex: **Withdrawal card***					
*Ex: **Enrolment in wallets***					
As an acquiring institution					
Ex: proximity card payment acceptance offer					
Ex: Remote card payment acceptance offer					

b. Planned projects for products and services

Describe short- and medium-term projects for the marketing of new products/services or the upgrade of existing ones, in terms of technology, features and security.

1.2. Operational organisation of activities

Provide an overview of the process associated with the payment instrument/service from issuance/reception to remittance to exchange/charge to account systems, specifying in particular outsourced processes (including those outsourced to other entities of the group) and those shared with other institutions. An organisational diagram can be added as necessary.

Actors	Roles
Issuing and management activity	
Directorates, departments, service providers	
Acquisition activity	

Describe changes and/or organisational projects launched or conducted during the financial year under review or planned in the short- and medium- term.

1.3. Risk analysis matrix and main fraud incidents

a. Reminder of applicable fraud typology

The analysis is conducted based on the categories and definitions of payment card fraud retained for statistical reporting to the Banque de France, which are available on the survey declarant webpage of the Banque de France's website : Data collection "Inventory of fraud on means of payment".

b. Overall rating for fraud on payment cards and equivalent instruments

The rating matrix used by the institution to assess fraud risk must be communicated in Section IV of this annex.

Gross risk (*Inherent risk before coverage measures*)	
Residual risk *(Risk remaining after coverage measures)*	

c. Coverage measures for fraud risk

Describe coverage measures by specifying, on the one hand, in bold type, those implemented during the financial year under review and, on the other hand, those that are planned, in which case mention their implementation deadline.

As an issuing institution:

Category of fraud		Initiation channel	Coverage measures
Forgery	Lost or stolen card	*Ex: at the point-of-sale*	
	Card not received		
	Counterfeit card		
	Misappropriated card number		
	Other cases		
Counterfeiting			
Misappropriation			

As an acquiring institution:

Category of fraud		Initiation channel	Coverage measures
Forgery	Lost or stolen card	*Ex: at the point-of-sale*	
	Card not received		
	Counterfeit card		
	Misappropriated card number		
	Other cases		
Counterfeiting			
Misappropriation			

d. Evolution of gross fraud over the period under review

As an issuing institution:

Category of fraud	Initiation channels	Description of the main cases of fraud encountered (as regards their amount and/or frequency)
Ex: stolen card number	*Ex: remote payment*	*Ex: skimming attacks, SIM card swap fraud*

As an acquiring institution:

Category of fraud	Initiation channel	Description of the main cases of fraud encountered (as regards their amount and/or frequency)

e. Presentation of emerging fraud risks

Describe new scenarios of fraud encountered during the financial year under review

2. Transfer

2.1. Presentation of the offer

a. Description of products and services

Product and/or service	Characteristics, age and funcationalities offered	Clients targeted	Initiation channel	Comments on the evolution of business volume	Comments on developments concerning technology, fonctionality and security
As an institution of the originator					

b. Planned projects for products and services

Describe the projects concerning the marketing of new products/services or pertaining to changes to an existing technology, functionality or security offer planned in the short- and medium-term.

2.2. Operational organisation of transfer activities

Provide an overview of the processing of payment means/services, from issuance/reception to remittance to exchange/charge to account systems, specifying in particular outsourced processes (including those outsourced to entities of the same group) and those shared with other institutions. An organisational diagram can be added as necessary.

Actors	Roles
Issuing and management activity	

Describe organisational changes and/or projects launched or conducted during the financial year under review or planned in the short- or medium-term.

2.3. Risks analysis matrix and main fraud incidents

a. Reminder of applicable fraud typology

The analysis is conducted based on the categories and definitions of transfer fraud retained for statistical reporting to the Banque de France, which are available on the survey declarant webpage of the Banque de France's website : Data collection "Inventory of fraud on means of payment".

b. Overall risk rating for transfer fraud

The rating matrix used by the institution to assess fraud risk must be provided in section IV of this annex.

Gross risk *(Inherent risk before coverage measures)*	
Residual risk *(Risk remaining after coverage measures)*	

c. Coverage measures for fraud risk

Describe coverage measures by specifying on the one hand, in bold type, those implemented over the financial year under review and, on the other hand, those that are planned, in which case include their implementation deadline.

Category of fraud	Initiation channel	Coverage measures
Forgery		
Counterfeiting		
Misappropriation		

d. Evolution of gross fraud over the period under review

Category of fraud	Initiation channel	Description of the main cases of fraud encountered (as regards their amount and/or frequency)

e. Presentation of emerging fraud risks

Describe new scenarios of fraud encountered during the financial year under review

3. Direct debit

3.1. Presentation of the offer

a. Description of products and services

Product and/or service	Characteristics, age and features offered	Clients targeted	Initiation channel	Comments on the evolution of business volume	Comments on developments concerning technology, functionality and security
As the institution of the debtor					
As the institution of the creditor					

b. Planned projects for products and services

Describe short- and medium-term plans for the marketing of new products/services or technological upgrades to existing ones in terms of technology, functionality and security.

3.2. Operational organisation of direct debit activities

Summarise the processing of payment means/services from issuance/reception to remittance to exchange/charge to account systems, specifying in particular outsourced ones (including those outsourced to other entities of the group) and those shared with other institutions. An organisational diagram can be added as necessary.

Actors	Roles
Issuing and management activity	

Describe organisational changes and/or projects launched or conducted during the financial year under review or planned in the short- or medium-term.

3.3. Risks analysis matrix and main fraud incidents

a. Reminder of applicable fraud typology

The analysis is conducted based on the categories and definitions of direct debit fraud retained for statistical reporting to the Banque de France, which are available on the survey declarant webpage of the Banque de France's website : Data collection "Inventory of fraud on means of payment".

b. Overall risk rating for direct debit fraud

The rating matrix used by the institution to assess the fraud risk shall be provided in section IV of this annex.

Gross risk *(Inherent risk before coverage measures)*	
Residual risk *(Risk remaining after coverage measures)*	

c. Fraud risk coverage measures

Describe coverage measures by specifying, on the one hand, in bold type, those implemented over the financial year under review and, on the other hand, those that are planned, in which case indicate their implementation deadline.

As the institution of the debtor

Category of fraud	Initiation channel	Coverage measures
Forgery		
Misappropriation		

As the institution of the creditor

Category of fraud	Initiation channel	Coverage measures
Forgery		
Misappropriation		

d. Evolution of gross fraud over the period under review

As the institution of the debtor:

Typology of fraud	Initiation channel	Description of the main cases of fraud encountered (as regards their amount and/or frequency)

As the institution of the creditor:

Typology of fraud	Initiation channel	Description of the main cases of fraud encountered (as regards their amount and/or frequency)

e. Presentation of emerging fraud risks

Describe new scenarios of fraud encountered during the financial year under review.

4. Bill of exchange and promissory note

4.1. Presentation of the offer

a. Description of products and services

Product and/or service	Characteristics, age and functionalities offered	Customers targeted	Initiation channel	Comments on the evolution of business volume	Comments on developments concerning technology, functionalities and security

b. Planned projects for products and services

Describe short- and medium-term plans for the marketing of new products/services or technological upgrades to existing ones in terms of technology, functionality and security.

4.2. Operational organisation of bill of exchange and promissory note activities

Summarise the processes associated with payment means/services from issuance/reception to remittance to exchange/charge to account systems, specifying in particular outsourced ones (including those outsourced to another entitiy of the group) and those shared with other institutions. An organisational diagram can be added as necessary.

Actors	Roles
Drawee's activity	
Remitter's activity	

Describe the organisational changes and/or projects launched or carried out during the year under review or planned for the short- and medium- term.

4.3. Risk analysis matrix and main fraud incidents

a. Reminder of applicable fraud typology

The analysis is conducted based on the categories and definitions of bill of exchange and promissory note fraud retained for statistical reporting to the Banque de France, which are available on the survey declarant webpage of the Banque de France's website : Data collection "Inventory of fraud on means of payment".

b. Overall risk rating for fraud risk on bills of exchange and promissory notes

The rating matrix used by the institution to assess the fraud risk shall be attached in Section IV of this Annex.

Gross risk *(Risk inherent before coverage measures)*	
Residual risk *(Risk remaining after coverage measures)*	

c. Fraud risk coverage measures

Describe the coverage measures specifying, on the one hand, in bold type, those implemented during the financial year under review and, on the other hand, those planned, in which case include their implementation deadline.

Category of fraud	Initiation channel	Risk mitigation measures
Theft, loss		
Counterfeiting		
Forgery		
Misappropriation, double presentment		

d. Evolution of gross fraud during the period under review

As institution of the drawee:

Category of fraud	Initiation channels	Description of the main cases of fraud encountered (having regard to their amount and/or frequency)

As institution of the remitter:

Category of fraud	Initiation channels	Description of the main cases of fraud encountered (having regard to their amount and/or frequency)

e. Presentation of emerging risks

Describe the new scenarios of fraud encountered during the financial year under review.

5. Cheque

5.1. Presentation of the offer

a. Description of products and services

Product and/or service	Characteristics, age and functionalities offered	Clients targeted	Delivery/remittance channel	Comments on the evolution of business volume	Comments on developments regarding technology, functions and security

b. Planned projects for products and services

Describe plans for the marketing of new products/services or changes to existing ones in terms of technology, functionality and security over the short- and medium-term.

5.2. Operational organisation of cheque activities

Summarise the processes associated with payment means/services from issuance/receipt to remittance to exchange/charge to account systems, specifying in particular outsourced ones (including those outsourced to another entity of the group) and those shared with other institutions. An organisational diagram can be added as necessary.

Actors	Roles
Issuer activity	
Remitter activity	

Describe changes and/or organisational projects launched or conducted during the financial year under review or planned in the short- and medium-term.

5.3. Risk analysis matrix and main fraud incidents

a. Reminder of applicable fraud typology

The analysis is conducted based on the categories and definitions of cheque fraud retained for statistical reporting to the Banque de France, which are available on the survey declarant webpage of the Banque de France's website : Data collection "Inventory of fraud on means of payment".

b. Overall risk rating for cheque fraud

With reference to the scoring matrix used by the institution to assess the fraud risk, to be disclosed in Section V of this Annex.

Gross risk *(Risk inherent before coverage measures)*	
Residual risk *(Risk remaining after coverage measures)*	

c. Risk coverage measures in place for fraud risk

Description of coverage measures indicating on the one hand, in bold type, measures taken during the financial year under review, and, on the other hand, measures that are under consideration, including the associated implementation deadline.

As the institution of the drawee:

Category of fraud	Delivery channel used for cheque forms	Coverage measures
Theft, loss		
Counterfeiting		
Forgery		
Misappropriation, double presentment		

As the institution of the remitter (including measures to prevent fraudulent remittances made through the remitting customer):

Category of fraud	Remittance channel	Coverage measures
Theft, loss		
Counterfeiting		
Forgery		
Misappropriation, double presentment		

d. Evolution of gross fraud during the period under review

As the institution of the drawee:

Category of fraud	Delivery channel used for cheque forms	Description of the main cases of fraud uncountered (in terms of amount and/or frequency)
Theft, loss		
Counterfeiting		
Forgery		
Misappropriation, double presentment		

As the institution of the remitter:

Category of fraud	Remittance channel	Description of the main cases of fraud uncountered (in terms of amount and/or frequency)
Theft, loss		
Counterfeiting		
Forgery		
Misappropriation, double presentment		

e. Presentation of emerging risks

Describe the new fraud scenarios encountered during the financial year under review.

6. Electronic money

6.1. Presentation of the offer

a. Description of products and services

Product and/or service	Characteristics, age and functions offered	Customers targeted	Initiation channel	Comments on the evolution of business volume	Comments on evolutions regarding technology, functions and security

b. Planned projects for products and services

Describe plans for the marketing of new products/services or changes to existing ones in terms of technology, functionality and security over the short- and medium-term.

6.2. Operational organisation of electronic money activities

Summarise the processes associated with the payment means/service, specifying in particular outsourced ones (including those outsourced to other entities of the group) and those shared with other institutions. An organisational diagram can be added as necessary.

Actors	Roles

Describe changes and/or organisational projects launched or conducted during the financial year under review or planned in the short- and medium-term.

6.3. Description of main fraud incidents

Main fraud incidents encountered:

Category of fraud	Initiation channel	Description of the main cases encountered (having regard to their amount and/or frequency)

7. Account information and payment initiation services

7.1 Presentation of the offer

a. Description of the service offer

Service	Scope of activity	Customers targeted	Initiation channel	Comments on the evolution of business volume	Comments on evolutions regarding technology, functions and security

b. Planned projects for the service offering

Describe the technological, functional and security changes to the existing offer planned in the short- and medium-term.

7.2 Operational organisation of the offer

Summarise the processes associated with the provision of account information services and payment initiation services, specifying in particular the methods used to access information on accounts along with the associated security measures as well as outsourced processes (including those outsourced to another entity of the group) and those shared with other institutions. An organisational diagram can be added as necessary.

Participants	Roles

Describe changes and/or organisational projects launched or conducted during the financial year under review or planned in the short- and medium-term.

7.3. Description of protection measures for sensitive payment data

Describe measures in place to ensure the confidentiality and integrity of sensitive payment data.

II - PRESENTATION OF THE RESULTS OF PERIODIC CONTROL ACTIONS CARRIED OUT ON THE SCOPE OF NON-CASH MEANS OF PAYMENT AND ACCESS TO ACCOUNTS

Describe the results of periodic control actions carried out over the year under review in the scope of non-cash means of payment (including inter general inspection missions carried out on the providers of outsourced core services).

Mission statement	Scope and goals of the mission	Main findings and recommendations in terms of security for non-cash means of payment and implementation deadline

III – ASSESSMENT OF COMPLIANCE WITH RECOMMENDATIONS ISSUED BY EXTERNAL ENTITIES ON THE SECURITY OF NON-CASH MEANS OF PAYMENT AND ACCOUNT ACCESS

The recommendations set out below, issued over the past few years by the Observatory for the Security of Payment Means (OSMP), are systematically included in each edition of the OSMP's annual report. They serve as a basis for the collection of self-assessments carried out by PSPs concerning the recommendations that are applicable to them.

Recommendations	Issuing body	Answer provided by the institution	
		Assessment of compliance (yes / partial / no / N.A.)	**Comments on the assessment (in the event of non-compliance or partial compliance)**
Studies derived from the technological watch carried out by the Observatory for the Security of Payment Means (OSMP)			
Quantum computing and the security of bank card payment systems (annual report 2023)	OSMP		
Payment acceptance solutions for smartphones or tablets (annual report 2022)	OSMP		
Digital identity and payment security (annual report 2021)	OSMP		
Real-time payment security (annual report 2020)	OSMP		
Payment data security (annual report 2019)	OSMP		
Mobile payment security (annual report 2018)	OSMP		
Occasional papers by the Observatory for the Security of Payment Means (OSMP)	OSMP		
Non-authenticated remote card payments issued without using the 3-D Secure protocol (annual report 2023)	OSMP		
SEPA payment security (annual report 2023)	OSMP		
Reimbursement of fraudulent payment transactions (annual report 2022)	OSMP		
Security of cheque payment transactions (annual report 2020)	OSMP		

IV – AUDIT REPORT ON THE IMPLEMENTATION OF SECURITY MEASURES PROVIDED FOR IN RTS (REGULATORY TECHNICAL STANDARDS)

For the section dedicated to common and secure communication standards, institution should fill in the questionnaire depending on the access interface solution implemented for third-party PSPs.

Ref. Articles (EU) Regulation 2018/389	**Questions asked to PSP**	**Assessment of compliance**	
		Yes / partially / No / N/A	**For each security measure, specify the conditions for implementation. In the event of non-compliance or partial compliance, present the remedial action plan envisaged along with its implementation deadlines. If the security measure does not apply to the PSP (N/A), provide a justification.**
Security measures for the application of strong customer authentication procedures			
Authentication code			
4	When the PSP applies the strong customer authentication procedure, is it effectively based on two or several items categorised as "knowledge", "possession" and "inherence", and does it generate an authentication code?		
	Is the authentication code accepted only once by the PSP when the payer uses this		

	code in the following situations? - To access its online payment account; - To initiate an electronic payment transaction; - To perform an action, using a remote communication channel likely to involve a risk of payment fraud or any other misuse.		
	Does the PSP have security measures in place to ensure compliance with each requirement listed below? - No information on one of the items categorised as “knowledge”, “possession” and “inherence” can be inferred from the disclosure of an authentication code; - It is not possible to generate a new authentication code based on another previously generated authentication code; - The authentication code cannot be forged.		

	Does the PSP ensure that authentication carried out through the generation of an authentication code integrate each of the measures listed below? - When the authentication for remote access, remote electronic payment and every other action through a remote communication channel that may involve a risk of payment fraud or any other misuse does not result in the generation of an authentication code, it is not possible to determine which authentication factor (knowledge, possession and inherence) was incorrect; - The number of consecutive unsuccessful authentication attempts after which the actions referred to in Article 97(1) of (EU) Directive No 2015/2366 are temporarily or		

	permanently blocked does not exceed five within a specified period; - Communication sessions are secured against interception of authentication data transmitted during the authentication process and against manipulation by unauthorised third parties; - The payer's maximum period of inactivity before session timeout, following successful authentication to that payer's online payment account, does not exceed five minutes.		
	In the event of a temporary lockout following unsuccessful authentication attempts, are the account lockout duration and the number of additional retries determined based on the features of the service provided to the payer and the associated risks, taking into account, at a minimum,		

	the factors set out in Article 2 (2) of the RTS? Is the payer duly notified before the lockout becomes permanent?		
	In the event of a permanent lockout, is a secure procedure in place to allow the payer to regain access to the locked electronic payment instruments?		
Dynamic links			
5	When applying the strong customer authentication procedure (in accordance with Article 97 (2) of (EU) Directive 2015/2366), does the PSP ensure compliance with the requirements listed below? - The payer is informed of the amount of the payment transaction and the identity of the payee. - The generated authentication code is specific to the payment transaction amount and to the payee approved by the payer when		

	initiating the transaction. - The authentication code accepted by the payment service provider matches the specific original amount of the payment transaction and the identity of the payee approved by the payer. - Any changes to the amount or beneficiary renders the generated authentication code invalid.		
	Does the PSP implement security measures that ensure the confidentiality, authenticity and integrity of each of the elements listed below? - The amount of the transaction and the identity of the payee during all stages of authentication; - the information displayed to the payer during all stages of theauthentication, including during the generation,		

	transmission and use of the authentication code.		
	When the PSP applies strong customer authentication (in accordance with Article 97(2) of (EU) Directive 2015/2366) does the PSP meet the requirements listed below? - for card-based payment transactions for which the payer has approved the exact amount of funds to be blocked under Article 75 (1) of that Directive, the authentication code is specific to the amount for which the payer gave consent and that the payer approved when initiating the transaction; - for payment transactions where the payer has approved the execution of a series of remote electronic payment transactions for the benefit of one or more beneficiaries, the authentication code is		

	specific to the total amount of the series of payment transactions and to the designated beneficiaries.		
Requirements for items categorised as "knowledge"			
6	Has the PSP implemented measures to mitigate the risk that strong customer authentication items categorised as "knowledge" be uncovered by or disclosed to unauthorised third parties?		
	Is the payer's use of strong authentication items categorised as "knowledge" subject to risk mitigation measures to prevent their disclosure to unauthorised third parties?		
Requirements for items categorised as "possession"			
7	Has the PSP implemented measures to mitigate the risk that the strong customer authentication items categorised as "possession" be used by unauthorised third parties?		
	Is the payer's use of the strong authentication items categorised as "possession"		

	subject to measures to prevent their duplication?		
Requirements for devices and software associated to items categorised as "inherence"			
8	Has the PSP implemented measures to mitigate the risk that authentication items categorised as "inherence" be exposed to unauthorised third parties when read using access devices and software provided to the payer? At a minimum, does the PSP ensure that it is highly unlikely that an unauthorised third party could be authenticated as the payer through such access devices and software?		
	Is the payer's use of strong customer authentication items categorised as "inherence" subject to measures ensuring that such devices and software prevent any unauthorised use of those items through access to such devices and software?		
Independence of items			
9	Does the PSP ensure that the use of strong customer		

	authentication items categorised as “possession”, “knowledge” and “inherence” is designed with safeguards, in terms of technology, algorithms and parameters, that ensure, should one item become compromised, that the others remain reliable?		
	When one of the strong customer authentication items or the authentication code itself is used through a multifunctional device, has the PSP implemented security measures to mitigate the risks arising from that multifunctional device being tampered with, and do these mitigation measures include all of the elements listed below? - the use of separate secure execution environments enabled by the software installed on the multifunctional device; - mechanisms to ensure that the software or device has not been		

	altered by the payer or by a third party; - in the event of tampering, mechanisms to mitigate impact.		
EXCEPTIONS TO THE STRONG CUSTOMER AUTHENTICATION OBLIGATION			
Analysis of transaction risks			
18	For the implementation of Articles 18 to 20, institutions may refer to the note issued by the Observatory for the Security of Payment Means (*Observatoire pour la Sécurité des Moyens de Paiement*, OSMP) in its annual report for 2020 on exemptions based on transaction risk analysis, which is available on its website. In the event of use of an exemption based on risk analysis, does the PSP meet the requirements listed below? - the fraud rate for this type of transaction is equivalent to or lower than the reference fraud rates set out in the Annex to Delegated Regulation 2018/389		

	for “remote electronic card-based payments” and “remote electronic credit transfers” respectively; - the amount of the transaction does not exceed the corresponding exemption threshold value set out in the Annex to Delegated Regulation 2018/389; - the PSP has not detected any of the following elements after real-time risk analysis: (i) unusual expenses or unusual behaviour of the payer; (ii) unusual information on the use of the payer's device or software access; (iii) signs of malware infection during a session of the authentication procedure (iv) a known fraud scenario in the context of providing payment services;		

	(v) unusual location of the payer; (vi) location of the beneficiary identified as high-risk. - At a minimum, the risk factors listed below are taken into account: (i) the past spending patterns of the individual payment service user; (ii) the payment transaction history of each payment service user of the payment service provider; (iii) the location of the payer and the beneficiary at the time of the payment transaction when the access device or software is provided by the payment service provider; (iv) the identification of unusual payment behaviour of the payment service user compared to the aforementioned user's payment transaction history.		
Calculation of fraud rates			
19	For each type of transaction ("remote electronic card-based payments" and "remote electronic credit		

	transfers"), does the PSP ensure that the overall fraud rates are equivalent to or below the maximum reference rates set out in the Annex to the RTS?		
	For each type of transaction ("remote electronic card-based payments" and "remote electronic credit transfers"), does the PSP duly calculate the fraud rates: - based on the initial amount of fraudulent payment transactions ("gross fraud approach") divided by the total value of all payment transactions with or without strong authentication; - and on a rolling quarterly basis (90 days).		
Suspension of exemptions based on the analysis of transaction risks			
20	If the PSP makes use of the exemption based on risk analysis (Article 18), does the PSP have a procedure in place to immediately notify the Banque de France of any overshooting of the		

	maximum permissible fraud rate (as set out in the Annex to the RTS), and to provide a description of the measures envisaged to return to compliance?		
	Does the PSP have procedures in place to immediately suspend the application of the exemption based on risk analysis (Article 18) if the maximum permissible fraud rate is exceeded for two consecutive quarters?		
	After the suspension, does the PSP only plan on resuming its use of the exemption based on risk analysis (Article 18) once the calculated fraud rate has remained equal to or below the maximum permissible rate for one full quarter, and is there a procedure in place to notify the Banque de France accordingly, with evidence that the fraud rate has returned to compliance?		
Monitoring			
21	Should exemptions from strong authentication be used (Articles 10 to 18), has		

	the PSP implemented a mechanism to record and monitor the data listed below, for each type of payment transaction and on a quarterly basis? - the total value of unauthorised or fraudulent payment transactions, the total value of all payment transactions and the resulting fraud rate, including a breakdown of payment transactions initiated using strong customer authentication and initiated under each exemption type; - the average transaction value, including a breakdown of payment transactions initiated using strong customer authentication and under each of the exemptions; - the number and percentage of payment transactions processed under each exemption relative to the total		

	number of payment transactions.		
CONFIDENTIALITY AND INTEGRITY OF THE PERSONALISED SECURITY CREDENTIALS OF PAYMENT SERVICE USERS			
General requirements			
22	Does the PSP ensure the confidentiality and integrity of the user's personalised security credentials, including authentication codes, throughout all stages of authentication in line with the following requirements? - personalised security credentials are masked when displayed and are not fully readable when entered by the payment service user during authentication; - personalised security credentials in data format and associated cryptographic material are never stored in plain text; - secret cryptographic material is protected against unauthorised disclosure.		
	Does the PSP fully document the cryptographic material management process used		

	to encrypt or otherwise obfuscate the personalised security credentials?		
	Does the PSP ensure that the processing and routing of personalised security credentials and authentication codes takes place in secure environments that comply with strict and widely recognised industry standards?		
Data creation and transmission			
23	Does the PSP ensure that the creation of personalised security credentials takes place in a secure environment?		
	Are the risks of unauthorised use of personalised security credentials, authentication devices and software, following their loss, theft or duplication prior to delivery to the payer adequately mitigated?		
Association with the payment service user			
24	Does the PSP ensure that the payment service user is the only person securely associated with the personalised security		

	credentials, authentication devices and software, in line with the requirements listed below? - the association of the payment service user's identity with the personalised security credentials and the authentication devices and software takes place in secure environments under the responsibility of the payment service provider, such as the premises of the payment service provider and the Internet environment provided by the payment service provider, or other similar secure websites used by the PSP and by its withdrawal services at automated teller machines, and takes into account the risks associated with third-party devices and components involved in the association process		

	that are not under the responsibility of the PSP; - when the association of the payment service user's identity with their personalised security credentials and authentication devices or software is carried out remotely, strong customer authentication is used.		
Delivery of authentication data, devices and software			
25	Does the PSP ensure that the delivery of payment service users' personalised security credentials, devices and software is carried out in a secure manner designed to prevent the risks associated with their unauthorised use following their loss, theft or duplication, by implementing at least each of the measures listed below? - efficient and secure delivery mechanisms ensure that personalised security credentials and authentication devices		

	and software are delivered to the legitimate payment service user; - mechanisms are in place that enable the payment service provider to verify the authenticity of the authentication software delivered to the payment service user via the Internet; - arrangements are in place that ensure that, when the delivery of the personalised security credentials takes place outside the premises of the payment service provider or through remote communication channels: (i) no unauthorised third party may obtain more than one element of the personalised security credentials or devices or authentication software when		

	delivery is made through the same communication channel; (ii) the personalised security credentials or authentication devices or software must be activated before they can be used; - arrangements ensure that, where the activation of the personalised security credentials or authentication devices or software is required prior to first use, such activation is carried out in a secure environment in accordance with the association procedures referred to in Article 24.		
Renewal of personalised security credentials			
26	Does the PSP ensure that the renewal or reactivation of personalised security credentials complies with the procedures applicable to the creation, association and delivery of such credentials		

	and authentication devices in accordance with Articles 23, 24 and 25 of the RTS?		
Destruction, deactivation and revocation			
27	Does the PSP have effective procedures in place to apply each of the security measures listed below? - the secure destruction, deactivation or revocation of personalised security credentials and authentication devices and software; - when the payment service provider distributes reusable authentication devices and software, secure reuse of a device or software is established, documented in writing and implemented before it is made available to another payment service user; - the deactivation or revocation of information related to personalised security credentials is recorded in the payment service		

	provider's systems and databases and, where applicable, in public registers.		

Common open and secure communication standards			
To be applied by the account servicing PSP in the event no dedicated access interface has been implemented: access via the online banking website with third-party authentication			
29	Does the PSP ensure that all operations involving the payment service user (authentication, access to account information and payment initiation), including with merchants, other PSPs and other entities, are duly logged with unique, non-predictable identifiers and are time-stamped?		
30-1	Has the PSP made available to third-party PSPs an access interface that complies with the requirements listed below? - third-party PSPs are able to identify themselves to the PSP; - third-party PSPs are able to communicate securely with the PSP to perform their payment services.		
30-2	Does the PSP ensure that all authentication procedures offered to payment service users are also made available to third-party PSPs		

	for the purpose of authenticating such payment service users?		
30-2-a-b	Does the access interface provided by the PSP comply with the requirements listed below? - the PSP is able to initiate the strong authentication process at the request of a third-party PSP that has previously obtained the users' consent; - communication sessions between the PSP and third-party PSPs are established and maintained throughout the authentication process.		
34-1	Is access to the PSP's online banking website by third-party PSPs secured using qualified certificates for electronic seals or qualified website authentication certificates?		
35-1	Does the PSP ensure the integrity and confidentiality of personalised security credentials and authentication codes both during transit through communication channels and when stored in the PSP's information systems?		
35-5	Does the PSP ensure that the personalised security credentials and authentication codes communicated to users can never directly or indirectly be read by a staff member?		

36-1	Does the PSP comply with the requirements listed below? - it provides third-party PSPs with the same information from the designated payment accounts and associated payment transactions that is made available to the payment service user when accessing account information directly, provided that such information does not include sensitive payment data; - immediately upon receipt of the payment order, the PSP provides third-party PSPs with the same information on the initiation and execution of the payment transaction as is provided or made available to the payment service user when the payment service user initiates the transaction directly; - upon request, the PSP immediately provides third-party PSPs with a simple “yes” or “no” answer as to whether or not the amount necessary for the execution of a payment transaction is available on the payer's payment account.		

36-2	In the event of an error or unexpected event during the identification or authentication process or when exchanging information elements, do the PSP's procedures provide for the sending of a notification message to third-party PSPs, indicating the reasons for the error or unexpected event?		
To be applied by the account servicing PSP in the event of implementation of a dedicated access interface with a fallback mechanism (online banking access with third-party authentication)			
29	Does the PSP ensure that all operations involving the payment service user (authentication, access to account information and payment initiation), including with merchants, other PSPs and other entities, are duly logged using unique, non-predictable identifiers and are time-stamped?		
30-1	Has the PSP made an access interface available to third-party PSPs that complies with the requirements listed below? - third-party PSPs are able to identify themselves to the account servicing PSP; - third-party PSPs are able to communicate securely with the PSP in order to perform their payment services.		
30-2	Does the PSP ensure that all authentication procedures offered		

	to payment service users are also made available by third-party PSPs for the purpose of authenticating payment service users?		
30-2-a-b	Does the access interface provided by the PSP comply with the requirements listed below? - the PSP is able to initiate the strong authentication process at the request of a third-party PSP that has previously obtained the user's consent; - communication sessions between the PSP and third-party PSPs are established and maintained throughout the authentication process.		
30-3	Does the PSP ensure that its access interface complies with the communication standards issued by European or international standardisation organisations? Are the technical specifications of the access interface documentated, including a set of routines, protocols and tools that third-party PSPs need in order to ensure interoperability of their software and applications with the PSP's systems?		
30-4	In the event of changes to the technical specifications of the access interface, does the PSP ensure, excluding in case of emergency, that		

	such changes are made available to third party PSPs at least three months prior to their implementation? Do the PSP's procedures provide for emergency situations during which changes have been made to be documented in writing, and for such documentation to be made available to the ACPR and the Banque de France?		
32-1	Does the PSP ensure that its dedicated access interface offers, at all times, the same level of availability and performance, including support, as the interface(s) made available to the payment service user for direct access to its online payment account?		
32-2	Has the PSP defined transparent key performance indicators and service level targets for its access interface that are at least as stringent as those set for the interface used by its payment service users, both in terms of availability and data provided?		
32-4	Does the PSP monitor the availability and performance of its access interface and publish the corresponding statistics on its website on a quarterly basis?		

33-1	Has the PSP implemented a fallback mechanism that is triggered after five consecutive access requests to the third-party PSP's dedicated interface, where no response is received within 30 seconds?		
33-2	Does the PSP have communication plans in place to inform third-party PSPs that use the dedicated interface of measures taken to restore the system, and do the plans include a description of the other readily available options that they may use in the meantime?		
33-3	Do the PSP's procedures provide for the immediate notification to the ACPR of issues encountered with the dedicated interface?		
33-5	Regarding access to the fallback interface, does the PSP ensure that third-party PSPs are identified and authenticated using the same authentication procedures as those applied for its own customers?		
34-1	Is access by third-party PSPs to the PSP's dedicated access interface secured using qualified certificates for electronic seals or qualified website authentication certificates?		
35-1	Does the PSP ensure the integrity and confidentiality of personalised security credentials and authentication codes, both during		

	transit through communication channels and when stored in the PSP's information systems?		
35-5	Does the PSP ensure that the personalised security credentials and authentication codes communicated to users are never directly or indirectly readable by a staff member?		
36-1	Does the PSP meet the requirements listed below? -it provides third-party PSPs with the same information from the designated payment accounts and associated payment transactions that is made available to the payment service user when directly accessing account information, provided that such information does not include sensitive payment data; -immediately upon receipt of the payment order, the PSP provides third-party PSPs with the same information on the initiation and execution of the payment transaction as that provided or made available to the payment service user when the payment service user initiates the transaction directly; -upon request, the PSP immediately provides third-party PSPs with a simple "yes" or "no" answer, as to		

	whether or not the amount necessary for the execution of a payment transaction is available on the payer's payment account.		
36-2	In the event of an error or an unexpected event during the identification or authentication process or when exchanging information, do the PSP's procedures provide for the sending of a notification message to third party PSPs, indicating the reasons for the error or unexpected event?		
To be applied by the account servicing PSP in the event of implementation of a dedicated access interface without a fallback mechanism			
29	Does the PSP ensure that all operations (authentication, access to account information and payment initiation) involving the payment service user, including with merchants, other PSPs and other entities, are duly logged using unique, non-predictable identifiers and time-stamped?		
30-1	Has the PSP made an access interface available to third-party PSPs that complies with the requirements listed below? -third-party PSPs are able to identify themselves to the account servicing PSP; -third-party PSPs are able to communicate securely with the PSP to perform their payment services.		

30-2	Does the PSP make all authentication procedures offered to payment service users available for use by third-party PSPs for the purpose of authenticating payment service users?		
30-2-a-b	Does the PSP's access interface comply with the requirements listed below? -the PSP is able to initiate the strong authentication process at the request of a third-party PSP that has previously obtained the user's consent; - communication sessions between the PSP and third-party PSPs are established and maintained throughout the authentication process.		
30-3	Does the PSP ensure that its access interface complies with communication standards issued by European or international standardisation organisations? Are the technical specifications of the access interface documented, including a set of routines, protocols and tools that third-party PSPs need to ensure interoperability of their software and applications with the PSP's systems?		
30-4	In the event the technical specifications of the access interface		

	are changed, has the PSP ensured that, excluding in an emergency, thay are made available to third-party PSPs at least three months prior to their implementation? Do the PSP's procedures for a description provide in writing of the emergency situations in which the changes have been implemented and for making this documentation available to the ACPR and the Banque de France?		
32-1	Does the PSP ensure that its dedicated access interface offers, at all times, the same level of availability and performance, including support services, than the interface(s) made available to the payment service user for direct access its online payment account?		
32-2	Has the PSP defined transparent key performance indicators and service level targets for its access interface that are transparent and at least as stringent as those set for the interface used by their payment service users, both in terms of availability and data provided?		
32-4	Are the availability and performance of the access interface monitored by the PSP and are the associated statistics published on its website on a quarterly basis?		

33-6	Has the PSP submitted an application for exemption from the implementation of a contingency mechanism to the ACPR?		
34-1	Is the access of third-party PSPs to the PSP's dedicated access interface secured using qualified certificates for electronic seals or qualified website authentication certificates?		
35-1	Are the integrity and confidentiality of personalised security credentials and authentication codes ensured, both when transiting through communication channels and when stored in the PSP's information systems?		
35-5	Does the PSP ensure that the personalised security credentials and authentication codes communicated to users are never directly or indirectly readable by a staff member?		
36-1	Does the PSP comply with the requirements listed below? -it provides third-party PSPs with the same information from the designated payment accounts and associated payment transactions that is made available to the payment service user when directly accessing account information, provided that such information does not include sensitive payment data;		

	-immediately upon receipt of the payment order, the PSP provides third-party PSPs with the same information on the initiation and execution of the payment transaction as that provided or made available to the payment service user when the payment service user initiates the transaction directly; -upon request, the PSP immediately provides third-party PSPs with a simple “yes” or “no” answer as to whether or not the amount necessary for the execution of a payment transaction is available on the payer's payment account.		
36-2	In the event of an error or an unexpected event during the identification or authentication process or when exchanging information, do the PSP’s procedures provide for the sending of a notification message to third-party PSPs, indicating the reasons for the error or unexpected event?		

V- ANNEXES

1. Rating matrix for fraud risks

Present the methodology used for fraud risk rating, indicating in particular the rating grid used for the likelihood/frequency of occurrence and impact (financial, non-financial, especially media impact) and the overall rating matrix highlighting the criticality levels.

2. Glossary

Define technical terms and acronyms used in the annex.

Annex 1

Information expected in the annex on the organisation of the internal control framework and accounting arrangements

1. Overview of the internal control framework[14]

1.1. Overall internal control framework:

- attach an organisational chart showing the units dedicated to permanent control(s) (including monitoring of compliance) and periodic control, and including the hierarchical positioning of their respective managers;
- planned coordination between the various persons involved in internal audit;
- measures taken in the event of operations in a country where local regulations hinder the application of the rules stipulated in the *Arrêté du 3 novembre 2014*, as amended;
- measures taken in the event of data transfers to entities (where applicable, to external service providers) to a country that does not provide appropriate data protection;
- arrangements made for the monitoring and control of operations carried out under the freedom to provide services.

1.2. Permanent control framework (including monitoring of compliance):

- description of the organisation of the various levels involved in permanent control and monitoring of compliance;
- scope of intervention of permanent control and monitoring of compliance, including for foreign operations (*activities, processes and entities*);
- number of employees assigned to permanent control and compliance monitoring functions (Article 13, first indent of the *Arrêté du 3 novembre 2014*, as amended) (expressed in full-time equivalent relative to the total headcount of the institution);
- description, formalised documentation and update history of procedures underpinning ongoing internal control, including for foreign operations (including compliance assessment procedures);
- procedures used to report to the head(s) of permanent control and to the members of the management body in its executive function on the activities and results of compliance assessments.

1.3. Risk management function:

- description of the organisation of the risk management function (*scope of intervention, staffing levels of the units responsible for risk measurement, monitoring and control, and the technical resources at their disposal*);
- for groups, organisation of the risk management function;
- description of the procedures and systems implemented to monitor risks associated with operations involving new products and services, significant changes to existing products, services or processes, from

[14] Institutions may adapt this section in line with their size, their organisational structure, the nature and volume of their activities and their geographical presence, as well as the types of risk they are exposed to (especially when ongoing and periodic control duties are entrusted either to a single individual, or to members of the management body in its executive function).

internal and external growth operations, and exceptional transactions (see Article 221 of the *Arrêté du 3 novembre 2014*, as amended);

- summary description of the risk assessment carried out by the risk management function based on scenarios that are appropriate in view of the level of risks arising from these new products and activities.

1.4. Periodic control framework:

- description of the organisation of the internal audit function and a description of its scope of action, including for business conducted abroad (*activities, processes and entities*);
- human resources allocated to the internal audit function (cf. Article 25 of the *Arrêté du 3 novembre 2014*, as amended) (expressed in full-time equivalent relative to the total workforce of the institution);
- in the event external service providers are used: frequency of intervention and size of the team involved;
- description, formalised documentation and update history of procedures underpinning the internal audit function, including those applicable to business conducted abroad (including compliance assessment procedures), highlighting significant changes made during the year under review;
- methods used to determine the frequency and priorities of audit cycles, particularly with reference to risks identified within the institution.

2. Overview of accounting arrangements

- description, formalised documentation and update history of procedures relating to the audit trail for information included in accounting documents, as well as information included in statements submitted to the Autorité de contrôle prudentiel et de résolution (ACPR) or to the ECB, as appropriate, and information required for the calculation of regulatory ratios;
- organisational arrangements adopted to ensure the quality and reliability of the audit trail;
- procedures used for the segregation and monitoring of assets held on behalf of third parties (see Article 92 of the *Arrêté du 3 novembre 2014*, as amended);
- procedures used to monitor and address discrepancies between the accounting information system and the management information system.

Annex 2

Measures implemented for financially vulnerable customers (*Arrêté du 16 septembre 2020* approving the Charter for banking inclusion and over-indebtedness prevention)

I. Training:

1.1 Percentage of customer advisors that have, in the past year, completed appropriate training on the specific offer, its target customer segment and the monitoring of customers who receive basic banking services: %

1.2 Systematic refresher training scheduled for trained customer advisors: Yes/No

1.3 Percentage of customer-facing employees who have, in the past year, completed training on the arrangements in place for financially vulnerable customers within the institution: %

1.4 Systematic refresher training scheduled for individuals referred to in 1.3 who have already completed initial training: Yes/No

1.5 Percentage of individuals acting on behalf of the institution (excluding employees) who have, in the past year, completed appropriate training on the specific arrangements in place for financially vulnerable customers: %

1.6 Systematic refresher training scheduled for individuals referred to in 1.5 who already completed initial training: Yes/No

II. Internal control[15]

2.1. Does the permanent control framework (1st and 2nd level) cover all measures relating to:

2.1.1. - improving access to banking and payment services and facilitating their use? Yes/No

2.1.2. - preventing and detecting over-indebtedness? Yes/ No

2.1.3. - preventing overindebtedness/providing assistance? Yes / No

2.1.4. - staff training, in particular as referred to in points 1.1 to 1.6 above? Yes / No

2.2. Are all items listed under sections 2.1.1 to 2.1.4 covered within the periodic control cycle? Yes / No

2.3. Have any significant deficiencies been identified in the course of permanent control actions and, where applicable, periodic control actions in the past year? Yes / No.

Institutions that have answered "No" are exempted from answering questions 2.4 and 2.5

2.4. If your answer is yes, please specify the main deficiencies (maximum 3)

2.5. Have corrective actions been implemented? Yes/ No

III. Comments or remarks on the implementation of financial inclusion and overindebtedness prevention (optional)

[15] Explanatory comments to be provided in section III for institutions who answered "No" to either of the questions below.