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

July 2023

# 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 subjected 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 the institution's internal control activities during the past financial year and to describe its procedures for measuring, monitoring, managing and disclosing the risks to which it is exposed.

**The items listed below are given for illustrative purposes based on their relevance with regard to 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 should include the most recent internal management reports on the analysis and monitoring of risk exposure that have been provided by the effective managers in accordance with Article 253 of the *Arrêté du 3 novembre 2014*, as amended, to the institution's supervisory body and, when applicable, to its risk committee.

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, should 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 of Internal Control shall be, in accordance with the provisions of Articles 12 and 13 of amended Instruction No 2017-I-24, communicated to the SGACPR **by electronic transmission in a computerised format**, according to the technical arrangements defined by the ACPR, **and electronically signed** according to the arrangements defined by amended Instruction No 2015-I-19 and by Annex I of amended Instruction No 2017-I-24.

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 at the latest by 30 April 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.

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 for risk measurement, monitoring and management should be described for each supervised institution.*

[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.

# 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 carried out on 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 effective managers, 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 IFR regulation, identification and rationale behind the k-factors relevant for the institution's activities (cf. appended table describing k-factors);
- for investiment firms subjet to IFR regulation, 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 identifying, managing, monitoring and mitigating 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 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 data on risks at different levels within the institution, including for foreign business and outsourcing: *establishing, in a manner that is appropriate to the size, nature and complexity of the institution's business, a uniform or consistent data structure to unambiguously identify risk data and measures to ensure the accuracy, integrity, completeness and timeliness of risk data, and defining a governance process for the risk data aggregation system* (refer to article 104 of the *Arrêté du 3 novembre 2014*, as amended);
- for investments firms subject to IFR regulation, a brief presentation of the orderly closure mechanism: *description of the reasoning and general repercussions of an orderly closure of the institution.*

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

*If there has been no significant changes made 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 or provide a copy of the internal control charter in force.*

## 2.1. Changes to the permanent control system at the "1st and 2nd level of control" (including the organisation of the internal control of 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 and functional position of the person, or persons, in charge of permanent control and any other functions exercised by this person, or by these persons, in the institution or in other entities of the same group, specify which units are in charge of the 2nd 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 and functional position 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 person responsible for 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 (when 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 in the organisation of the risk management function: *specify in particular the identity, the hierarchical and functional position of the person in charge of the risk management function and any other functions exercised by this person in the institution or in other entities in the same group;*
- the identity of the effective manager in charge of the consistency and efficiency of 2nd level permanent control systems.

## 2.2. Changes in periodic control procedures for the "3rd level of control" carried out by the internal audit function (including the organisation of the internal control of 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 effective manager in charge of ensuring the consistency and efficiency of periodic control mechanisms;
- a description of significant changes made in 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 person in charge of the internal audit function (cf. Article 17 of the *Arrêté du 3 novembre 2014*, as amended);
- a description of the arrangements made, where appropriate, to ensure that the full cycle of investigations regarding the whole range of 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 arrangements made, where appropriate, to ensure that the audit cycle is determined according to 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 proper internal application, the process implemented in the event of a breach and modalities defined for the information of senior management…;
- a description of processes set up to identify, manage and prevent conflicts of interest (including in the context of credit granting procedures and the execution of other transactions) within the institution itself as well as concerning its staff, and a description of the terms set for the approval and review of these processes (refer to Article 38 of the *Arrêté du 3 novembre 2014*, as amended, and to EBA Guidelines No 2021/05);
- a description of the processes set up 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),
- a description of the processes set up 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).

## 3.2. Involvement of management bodies in internal control

### *3.2.1. Procedures for reporting to the supervisory body and, when applicable, to the risk committee:*

- the procedure 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 for reporting to the supervisory body, to the central body, and, when appropriate, to the risk committee, on significant incidents as defined in Article 98 (cf. Article 245 of the *Arrêté du 3 novembre 2014*, as amended);
- if necessary, the procedure for reporting by the risk manager 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 set for the reporting, by the person in charge of the internal audit function, to the supervisory body and (when appropriate) to the risk committee, of 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 applied by the person in charge of the compliance function when reporting on the exercise of his or her missions to the supervisory body (see Article 31 of the *Arrêté du 3 novembre 2014*, as amended);
- findings (resulting from the control checks) that have been brought to the attention of the supervisory body and, when appropriate, of the risk committee, and in particular any shortcomings identified, along with the corrective measures ordered (see Article 243 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedure for reporting to the supervisory body regarding the periodic review carried out by the Nomination Committee and pertaining to the knowledge, skills and experience of the members of the supervisory body, both individually and collectively (cf. Article L. 511-100 of the *Code monétaire et financier*). The conclusions of this review shall be sent to the SGACPR, as well as the details of the follow-up to the measures imposed by the prudential supervisor within the framework of the authorisation procedure for the appointment of directors and effective managers.

### *3.2.2. Procedures for reporting to the effective managers*

- procedures for reporting to the effective managers on significant incidents as defined in 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 effective managers on the exercise of his or her duties (see Article 77 of the *Arrêté du 3 novembre 2014*, as amended);
- procedures allowing the risk manager to warn the effective managers of any situation that could have significant repercussions on risk management (see Article 77 of the *Arrêté du 3 novembre 2014*, as amended).

#### *3.2.3. Verifications carried out by the effective managers and the supervisory body*

- a description of the due diligence carried out by the effective managers 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 for reviewing the governance system and the periodic assessment of its efficiency (cf. Article L.511-59 of the French *Code monétaire et financier*);
- the procedure for approving and reviewing 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 for determining the guidelines and monitoring the implementation of the oversight systems in order to ensure the efficient and prudent management of the institution (cf. Article L. 511-67 of the French *Code monétaire et financier*);
- the procedure for adopting and reviewing 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 revealed by internal control procedures, the main shortcomings noted, the conclusions drawn from their analysis, and the measures taken to remedy them (see Article 252 of the *Arrêté du 3 novembre 2014*, as amended);
- the dates on which the supervisory body reviewed the activities and results of the internal control system for the past financial year;
- the dates of approval of the aggregate exposure limits by the supervisory body, after consultation of 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 remuneration policies*

- the date of establishment, composition, term of office, operating modalities 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* (terms and date of adoption, implementation date, and review procedures) and, when necessary, the identity of external consultants whose services have been used to establish remuneration policies (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);
    - policies concerning deferred remuneration;
    - policies concerning guaranteed variable remuneration exceptionally paid under the conditions laid down in Articles L. 511-74 or L. 533-30-8 of the French *Code monétaire et financier*;
    - criteria for determining the ratio of cash remuneration to other forms of remuneration.
    - criteria for determining the amount of severance payments, subject to compliance with 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);
    - existing policy for preventing the circumvention of regulation 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 for monitoring pay gaps for the population concerned[2] (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 responsible for validating and checking operations (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 for taking all risks into account when establishing the basis for variable remuneration, including the liquidity risks inherent in the activities concerned and the capital needed to cover the risks incurred (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 communication to the ACPR or, as applicable, to the ECB, of the maximum limit proposed at the general meeting concerned for the variable component of remuneration (*as a reminder, the General Meeting that is competent regarding subsidiary staff is the one of the subsidiary and not that of the parent undertaking*) and the list of persons concerned by the limit on the variable component of remuneration,

[2] 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).

as well as the justification of these choices, 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 limit pursuant to paragraph 43 of the aforementioned EBA Guidelines.

### *3.3.3. Disclosures concerning the remuneration of the effective managers and of the persons whose professional activities have a significant impact on the institution's risk profile (cf. Article 202, or, when 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 overall amount and type of variable remuneration, with a beakdown distinguishing between cash, shares or equivalent ownership rights, and other instruments within the meaning of Article 52 or 63 of Regulation (EU) No 575/2013, or other instruments which can be fully converted to Common Equity Tier 1 instruments or written down. Please also indicate the vesting period 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 overall amount of deferred remuneration with a breakdown between vested and unvested portions of remuneration (cf. Articles R. 511-18 or R. 533-19 of the French *Code monétaire et financier*);
- the overall amount of deferred remuneration awarded during the year, paid or reduced, after adjustment for performance (cf. Article R. 511-18 or R. 533-19 of the French *Code monétaire et financier*);
- payments made for 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 largest 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 adjustment calculations (cf. Articles 203 to 210 of the *Arrêté du 3 novembre 2014*, as amended);
- the total remuneration of each effective manager 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 control of remuneration policies*

- the procedures for verifying that remuneration policies are consistent with risk management objectives, in particular having regard to the size, systemic importance, nature, scale and complexity of the activities

of the institution concerned 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 Regulation (EU) No 575/2013 (cf. Article 268 of the *Arrêté du 3 novembre 2014*, as amended, and Section 20 of EBA Guidelines No 2021/04);
- arrangements for the disclosure of information on 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 programme of assignments (risks and/or entities that have been to the subject of checks 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 observed;
- measures taken to remediate the shortcomings observed**,** 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 for following up on the recommendations generated 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 remediate any identified shortcomings.

## 5. Inventory of transactions with effective managers, 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 commitments for which a deduction has been made 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), type of commitment, gross amount, deductions (if any), risk weight, setup and expiry date;
- **the nature of commitments to principal shareholders, effective managers and members of the supervisory body for which a deduction has not been made from regulatory capital** due either to the date on which the commitment was made or to the rating or score assigned to the beneficiary of the commitment. However, it is not necessary to mention commitments the gross amount of which does not exceed 3% of the institution's capital.

Credit institutions and investment firms are required to append a document setting out **the characteristics of commitments to key shareholders, effective managers 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 commitments, gross amount, any deductions and weighting applied, date of establishment and maturity date.

## 6. Process for assessing the adequacy of internal capital

*This mechanism is not mandatory for institutions included in consolidation and consequently exempted from compliance with management ratios on an individual or sub-consolidated basis.*

- a description of the scope of activities relevant for the assessment of internal capital adequacy and the approach used to determine the materiality of risks;
- a description of methodologies used to measure, assess and aggregate risks in order to quantify internal capital (analysis horizons, economic value approach, description of models and calculation parameters…). This description shall include explanations of the limits or weaknesses of the calculation methodology 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 distribution 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 covered by Pillar 1* (cf. Article 96 of the *Arrêté du 3 novembre 2014*, as amended);
- a description of the establishment and update of a capitalisation plan to ensure that a sufficient level of internal and regulatory capital is maintained for at least 3 years, including in adverse circumstances (stress testing):
    - level and definition of the 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 to allocate capital within the institution;
    - projections of the internal capital level;
- stress testing carried out to assess the adequacy of internal capital:
    - 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 elaboration, implication of senior management in the validation process…*,
    - description of the assumptions and methodologies used, and summary of the results obtained,
    - description of the process used for taking stress tests into account in decision-making processes, especially with regard to risk appetite, capital planning and determination of limits;
- internal control procedures designed to verify that these systems and procedures remain adapted in the event of changes in the institution's risk profile;
- documentation formalising the process established for setting and validating internal capital adequacy, as well as the assumptions, capitalisation plan, stress tests and methodologies used in the process, including the distribution of roles and the information to 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 by integrating internal capital and risk appetite considerations into managerial decision-making processes through appropriate reports;
- 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 that justifies their capital adequacy. To that end, the "reader's guide" shall provide an overview of all the documents sent 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 connecting the specific pieces of 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 significant changes made to communicated information compared with what was submitted previously, elements possibly excluded from the scope of information provided 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 any information made public by the institution on its capital adequacy.

- institutions subject to the CRR that are not under the ECB's direct supervision shall formalise and provide the conclusions of internal capital adequacy assessments and their impact on the risk management and the overall management of the institution.
- Class 2 investment firms must draw up a report in accordance with Article L533-2-2 of the French *Code Monétaire et Financier* in order to document the ICAAP mechanism set up by the investment firm and to demonstrate that its available internal capital is effectively aligned to the risks to which it is exposed, both dynamically and over time, under normal and stressed market conditions. A template illustrating the list of key information to be provided by the investment firm in that report shall be made available by the SGACPR.

## 7. Non-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 transactions 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 for reporting shortcomings, breaches or deficiencies

Please specify:

- the procedures set up to enable staff to report to the competent managers and committees of the institution, and to the ACPR (or, when applicable, to the ECB) on shortcomings or breaches of prudential rules either committed or likely to be committed within the institution (cf. Article L. 511-41 of the French *Code monétaire et financier*);

- the procedures set up to enable managers and staff to report to the compliance officer of the institution or of their business line, or to the responsible person referred to in Article 28 of the *Arrêté du 3 novembre 2014*, as amended, on potential deficiencies regarding the compliance monitoring system (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 procedures implemented during the execution of operations relating to new products of services, or relating to material changes in such products and services or material changes to the systems associated with such products, during internal or external growth operations or for exceptional transactions: *the view of the head of the compliance function shall systematically be provided in writing prior to the execution of these*

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

### 7.6. Centralisation and setting up of remediation and monitoring 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 rectify 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 non-compliance risk

- the main shortcomings observed;
- the measures taken to remediate the shortcomings observed**,** 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 (service de règlement différé – SRD)*** *is covered in this section, with information on the set of customers for which this type of order is authorised, the set limits, and risk management (initial margin, maintenance of that margin, monitoring of time extensions, provisioning of non-performing loans).*

### 8.1. Loan approval procedures

- predefined loan approval criteria;
- factors used in analysing the expected profitability of loans that are taken into account in the granting process: *methodology, variables considered (loss ratios, etc.);*
- a description of the loan granting procedure, including where appropriate any delegation, escalation and/or limitation mechanism;
- policy for approving 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. Systems for measuring and monitoring risks

- stress scenarios used to measure incurred risk, retained assumptions, results and description of their operational integration;
- overview of exposure limits – by beneficiary, by associated debtors, by business lines etc. (*specify the level of such limits in relation to own funds and in relation to earnings*);

- the review procedure for credit risk limits and the frequency of conduction of such review (*specify the date of the most recent review*);
- any breach of credit risk limits observed during the last reporting period (*specify their causes, the counterparties involved, the total amount of the commitment concerned, the number of breaches, and their respective amount*);
- the procedure followed for authorising credit risk limit overshootings;
- the measures taken to rectify credit risk limit breaches;
- the identification, staffing levels, and hierarchical and functional position of the unit in charge of monitoring and managing credit risk;
- a description of the arrangements in place for the monitoring of advanced risk indicators (*specify the main criteria for placing counterparties under watch-list*);
- the methods and frequency of analysis of the quality of credit commitments; indication of any reclassification of commitments made under the internal risk assessment categories, as well as any changes in allocation to accounting items dedicated to doubtful or impaired loans, indication of any adjustments made to the level of provisioning, 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 results of any controls carried out during the year;
- a presentation of the credit risk measurement and management system put in place to identify and manage problem credits, make the appropriate value adjustments and record provisions or write-downs at the appropriate amounts (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 for managing and reducing 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 (*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 taken into account in the restructuring decision, deadlines applied, control procedures in place to ensure the viability of the restructuring measures taken…*) and procedures used for the monitoring of 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 applied to and frequency of provisioning decisions, including when appropriate any delegation and/or escalation measures;
- the procedure applied to 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 used for analysing the risk of loss of value incurred by leased assets (financial leasing) and the frequency of the analysis;
- the procedure used for analysing risks of impairment losses incurred by financed real estate assets (including assets financed through financial leasing) and its frequency;
- the procedure used for updating and reviewing loan files, the frequency of review, and the results of such analysis (at least for counterparties the receivables of which are unpaid, non-performing or impaired, or which present significant risks or exposure volumes);
- breakdown of exposures per level of risk (cf. Articles 106 and 253 a) of the *Arrêté du 3 novembre 2014*, as amended);

- the procedure used for reporting on the level of credit risk to the effective managers, the supervisory body and, where applicable, the risk committee, using summary statements (cf. Article 230 of the *Arrêté du 3 novembre 2014*, as amended);
- roles of the effective managers, the supervisory body and, when applicable, the risk committee, in identifying, monitoring and reviewing the institution's overall strategy regarding credit risk and 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 up the limits (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended);
- analysis of changes in margins, in particular for 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 taken into account; whether refinancing needs are taken into account, the amount of the net borrowing position and the retained refinancing rate; if gains stemming from the investment of own funds allocated to outstanding amounts, the amounts and return rates;
    - identification of the different outstanding loan categories (such as loans to retail customers, with housing loans highlighted) or the business lines for which margins are calculated;
    - highlighting trends identified through calculations based on 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 effective managers to analyse the profitability of lending activities, 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 granting criteria used for housing loans to French customers;
- a breakdown of housing loans 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 effective managers (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 used for taking, managing, monitoring and mitigating credit risks (cf. Article L. 511-60 of the French *Code monétaire et financier*);
- when appropriate, the procedures used for analysing, assessing and monitoring the risks associated with intragroup transactions and the frequency of such analysis of (credit risk and counterparty credit risk).

Specific elements on counterparty credit risk:

- a description of the risk metrics used to assess the 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. Concentration risk by counterparty*

- tool used to monitor concentration risk by counterparty, including central counterparties and entities from the shadow banking system: any aggregate measures defined, description of the system for measuring exposures to the same beneficiary (including prudential framework applicable to counterparties the

considered, the financial situation of the counterparty and portfolio, vulnerability to the volatility of asset prices, especially for entities from the shadow banking system, details on procedures used to identify associated beneficiaries (establishment of a quantitative threshold above which such measures are systematically implemented, etc.); use of the transparency approach notably for exposures to collective investment undertakings, securitisations or refinancing of trade receivables (factoring, etc.) and the inclusion of credit risk mitigation techniques), procedures for reporting to the effective managers and the supervisory body;

- system used to limit exposure by counterparty: general description of the system for setting limits on counterparties (*specify their level in relation to own funds and earnings*), the procedures for reviewing limits and the frequency of these reviews, any breaches of limits reported, and the procedures for involving the effective managers in the setting and monitoring of limits;
- amounts of exposures to main counterparties;
- conclusions on the institution's exposure to concentration risk by counterparty, including central counterparties and entities from the shadow banking system.

#### *8.3.2. Sectorial concentration risk*

- tool used for monitoring sectorial concentration risk (especially for the shadow banking system): any aggregate measures defined, economic model and risk profile, description of the system used for measuring exposures in the same business sector (especially interconnectedness between counterparties), and procedures for reporting to the effective managers and the supervisory body;
- sectoral exposure limit system: summary description of the secoral limit system in place (*amount of exposures, specify their level in relation to own funds and earnings*), the procedures for reviewing limits and the frequency of these reviews, any breaches of limits reported, and the procedures for involving the effective managers in the setting and providing information on the monitoring of limits;
- breakdown of exposures by sector;
- conclusions on the institution's exposure to sectorial concentration risk (especially for 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 for reporting to the effective managers and the supervisory body;
- the system used to set exposure limits within 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 for reviewing limits and the frequency of these reviews, any breaches of limits reported, and the procedures for involving the effective managers in the setting and monitoring of limits;
- 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 comparisons with external data to ensure the accuracy and consistency of internal rating systems, including the methodologies and parameters used;
- the nature and frequency of checks on rating systems as part of ongoing and periodic controls conducted on internal rating systems;
- a description of the operational integration of the rating systems ('use test'): effective use of the parameters derived from the internal rating systems in credit granting and pricing, in debt collection management, in risk monitoring, in the provisioning policy, allocation of internal capital, and corporate

governance (including the elaboration of management reports for use by the effective managers and the supervisory body);

- the procedures for involving the effective managers in the design and updating of internal rating systems: including approval of the methodological principles, verifying that the design and operation of the system(s) are properly controlled, arrangements governing the way effective managers are informed of the performance of these systems;
- demonstration proving that the internal credit risk assessment methods do not rely exclusively or mechanistically on on an external credit rating system (cf. Article 114 of the *Arrêté du 3 novembre 2014*, as amended);
- a description of the measures implemented by the institution to comply with, on the one hand, the EBA Guidelines on probability of default (PD) estmation, loss given default (LGD) estimation, and the treatment of defaulted exposures (EBA/GL/2017/16), and, on the other hand, the EBA Guidelines on the estimation of LGD appropriate for an economic downturn (EBA/GL/2019/03);
- a description of the measures implemented by the institution to comply with the EBA Guidelines on credit risk mitigation for institutions applying the IRB approach with own estimates of LGDs (EBA/GL/2020/05).

### 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 put in place to check, prior to any investment, that institutions acting as originator, sponsor or initial lender have in-depth knowledge of the securitisation positions concerned 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 control the risks associated with securitisation transactions or schemes (including, in particular, an analysis of their economic substance) for institutions that act as originators, sponsors or investors, including by means stressed scenarios (assumptions, frequency, consequences);
- for banks acting as originators, a description of the internal process used to assess transactions that are deconsolidating for prudential purposes, supported by an audit trail and by the procedures for monitoring risk transfer through reviews carried out reguarly.

### 8.6. Intraday credit risk

*In the context of custody activities, risk incurred by institutions that grant their customers intraday credit, in cash or securities, to facilitate the execution of securities transactions*[3].

- 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 exceeding of such limits);
- the procedures for granting intraday credit;
- the procedures for assessing the quality of collateral;
- a description of the procedures used to report to the effective managers 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 observed;

[3] Intraday credit risk also covers overnight credit risk for transactions settled overnight.

- corrective measures taken to remedy the shortcomings identified**,** planned completion date for these measures, and state of progress of their implementation as at the date of drafting of this Report;
- the procedures for following up on the recommendations resulting from 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).

### 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 technics;
- 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 (guarantee calls refused, unfulfilled pledges, etc.).

### 8.9. Stress testing for credit risk

Attach an annex describing the assumptions and methodological principles used (in particular how contagion effects to other markets are taken into account) 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 early and their resolution, as well as to monitor the value of outstanding contracts (cf. paragraph 1 of Article 11 of the Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories);
- a description of procedures used for the valuation of OTC derivative contracts not cleared by a CCP (cf. paragraph 2 of Article 11 of the Regulation (EU) No 648/2012);
- 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 CCP (cf. paragraph 3 of Article 11 of the Regulation (EU) No 648/2012);
- a description of procedures used for the calculation and collection of variation margins;
- a description of procedures used for the calculation and collection of initial margins;
- a description of models used for the calculation of initial margins;

- a description of criteria used for the selection of the collateral exchanged;
- a description of methods used for the valuation of collateral;
- a description of 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 these disputes;
- a description of the methods and frequencies of calculation of the amount of capital allocated to manage the risk not covered by the appropriate exchange of collateral (cf. paragraph 11 of Article 11 of the Regulation (EU) No 648/2012).

### 9.2 Risk management and risk monitoring procedures for the risks linked to intragroup transactions

- a description of the centralised procedures used for the valuation, assessment and monitoring of risks linked to intragroup transactions referred to in paragraphs 2. a) and d) of Article 3 of the Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories;
- a description of the risk management procedures used to manage the risks linked to intragroup transactions benefiting from the exemptions provided for in paragraphs 6, 8 or 10 of Article 11 of the Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories;
- 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 the Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories. This description shall include detailed observations or expectations regarding countries the situation of which has changed significantly 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 the Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (cf. Article 20 of Commission Delegated Regulation (EU) No 148/2013 of 19 December 2012 supplementing Regulation (EU) 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 the frequency*);
- reconciliation between management results and accounting results (*specifying the frequency*);
- reconciliation between the prudent valuation, as defined in the Commission Delegated Regulation (EU) No 2016/101 of 26 October 2015, and the accounting valuation of the banking book, recorded at fair value through profit and loss;
- assessment of the risks (including credit valuation adjustment risk) arising from positions in the trading book (*specify the frequency*);
- the procedures used to capture the various components of risk, including basis risk and securitisation risk (in particular for institutions with high trading volumes that carry out risk assessment in an aggregated manner);
- the scope of risks covered (various business lines and portfolios; within institutions located in different geographical areas).

## 10.2. Market risk monitoring system

- roles of the effective managers, the supervisory body and, when applicable, the risk committee, in defining the institution's overall strategy regarding market risk and current and future 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 up limits (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended);
- the identification, staffing levels, and hierarchical and functional position of the unit charged with monitoring and managing market risk;
- controls conducted by that unit**,** and in particular regular assessment of the validity of the tools used to measure aggregate risk (back-testing);
- a summary description of the limits set for market risk (specify the level of limits, broken down by type of risk incurred, in relation to own funds and earnings);
- the frequency with which limits on market risk are reviewed (*indicating the date of the most recent review carried out during the past year*); identity of the body responsible for setting limits;
- the system used to monitor procedures and limits;
- any breaches of limits identified during the past year (*specifying causes, number of breaches and amounts*);
- the procedures used to authorise limit overruns and the measures taken to resolve them;
- the procedures used to report on compliance with limits (*frequency, recipients*);
- the procedures, frequency and conclusions of the analysis provided to the effective managers 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 internal capital allocated and the level of internal capital that is appropriate to cover material market risks that are not subject to an own funds requirement (cf. Articles 130 to 133 of the *Arrêté du 3 novembre 2014*, as amended):
- attach a copy of the documents provided to the effective managers that enable them to assess the risk incurred by the institution, in particular in relation to its own funds and earnings;
- a description of measures implemented by the institution to comply with the EBA Guidelines on the treatment of structural FX positions (EBA/GL/2020/09).

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

- main shortcomings observed;
- measures taken to remedy the shortcomings observed**,** 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 capital requirements for market risk shall attach an annex describing the assumptions and methodological principles used, and summarising the results obtained; this annex shall provide a comprehensive description 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 Regulation (EU) No 2015/942 of 4 March 2015. Insitutions shall explain the extent to which internal control has or has not been at the root of such changes.

## 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, taking into account the complexity of the activities and the risk tolerance of the institution;
- governance: description of the governance system deployed to manage operational risk and of the governance of the model where applicable, role and mission of the various committees established, structuring decisions taken regarding operational risk during the year;
- organisation: presentation of the various teams in charge of permanent control for operational risk by business lines and by geographical areas (numbers of FTEs, both forecasted and effective, missions, staff and line of reporting of teams), objectives of the various permanent control teams, actions carried out during the year and progress of reorganisation projects at the end of the year, constraints faced and solutions planned/implemented during the implementation phase of these reorganisation projects, targets to be achieved and planned schedule for the full deployment within the target organisation;
- scope of entities: entities included and methods (in numbers and as a proportion of assets), treatment of entities included in the scope of prudential consolidation during the last two financial years, any entities excluded 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 measure and monitor operational risk (*specifying the method used to calculate capital requirements*);
- the monitoring system deployed to ensure that capital requirement calculations take into account all incidents that should be identified, especially as regards legal and non-compliance risks; identification of risks that require for improvements to be made to the current monitoring system and remedial actions taken;
- presentation of the risk mapping detailing business/risks that are not (yet) covered by the risk mapping established at the end of the financial year;
- 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 areas of risk covered, and the existence or absence of warning indicators signalling potential future losses*);
- documentation and communication of the procedures used to monitor and manage operational risk;
- a description of the specific procedures used to manage the risk of internal and external fraud, as defined in Article 324 of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013;
- for institutions using a standardised approach, the procedures and criteria used to match the relevant indicators to business lines, and the review procedures used should a new business line be set up, or should an existing one be modified;
- for institutions using an advanced measurement approach, a description of the methodology used (*including factors relating to internal control and the environment in which they operate*) and any changes in methodology made in the course of the financial year, as well as a description of the procedures used to verify the quality of historical data;
- 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.

## 11.3. Integration of the operational risk measurement and operational risk management system 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 Regulation (EU) No 575/2013 and risks related to model risk as defined in Article 4 of delegated Regulation (EU) No 2018/959;
- a description of the main operational risks identified in the course of the year (settlement incidents, errors, fraud, cybersecurity etc.) and the lessons learned from them.

## 11.4. Contingency and business continuity plans

- objectives and definitions retained for the contingency and business continuity plans, scenarios used, overall architecture (a single, comprehensive plan versus one seperate plan for each business line, overall consistency in the case of multiple plans), responsibilities (*name and position of the officers responsible for managing and triggering contingency and business continuity plans and for managing incidents, name, contact details and positioning of the person(s) in charge of crisis management if different from the one responsible for managing and triggering contingency and business continuity plans*), scope of business covered by the plans, activities assigned a high level of priority in the event of an incident, residual risks not covered by the plans, timetable for implementing them;
- formalised procedures, summary description of fall-back and backup IT facilities;
- tests of contingency and business continuity plans (objectives, scope, frequency, results), procedures for updating those plans (frequency, criteria), tools used to manage continuity plans (software and IT development), reporting to senior management (on tests, and on any changes made to systems and procedures);
- audit of contingency and business continuity plans and results of permanent control actions;
- activation of the contingency and business continuity plan(s) and management of incidents occurring in the course of the year (for example, the H1N1 pandemic, the Covid pandemic).

## 11.5 IT risk

### *11.5.1. IT strategy and adequacy of IT resources*

- a presentation of the institution's IT strategy, defined pursuant to Article 270-1 of the *Arrêté du 3 novembre 2014*, as amended (organisation, coordination with the overall strategy, priority objectives and action plans set up, risk appetite framework…) and resources dedicated to its implementation (procedures in place to ensure its compliance, dedicated budget and steering procedure, number and nature of staff dedicated to the management of IT operations, to the security of the IT system and to business continuity;
- a presentation of the governance process (roles of effective managers, supervisory body and where appropriate, risks committee in the definition, monitoring and review of the IT strategy).

### *11.5.2. IT risk management (cf. Article 270-2 of the* **Arrêté du 3 novembre 2014***, as amended)*

- a presentation of the risk mitigation techniques used for major IT risks, a presentation of control measures used to monitor the efficiency of these techniques and a description of the process followed to inform effective managers and the supervisory body;
- a presentation of the organisation of the management of IT risk (definition of the roles and responsibilities of players[4], assessment framework used to define the IT risk profile and its results, risk tolerance threshold, auditing process, methods and frequency of reporting to senior management and the supervisory body on the entity's exposure to IT risks[5]…);
- a description of the periodic and permanent control mechanisms used for IT systems and summary of the observations derived from the controls carried out (cf. 11.6);

[4] Especially those in the IT function.

[5] Attach the latest dashboard issued dedicated to informing them.

- a presentation of the IT risk map, including in particular risks to availability and continuity, data security and data integrity as well as risks associated with changes made to IT systems (identifying in particular what systems and services are essential to the smooth running, availability, continuity and security of the institution's activities)[6].

#### *11.5.3. Security of the IT system*

- a presentation of the objectives of the information system security policy (protection of confidentiality, integrity and availability of information, assets, IT services and customer data) and name of the person responsible for the security of IT systems;
- a description of the procedures set up to prevent and address incidents (i.e. one or more adverse or unexpected events likely to seriously compromise the safety of information and to affect the business of the institution), in particular for major incidents[7] (mechanisms for physical and logical security, for the safeguarding of data integrity and confidentiality, specific measures in place for online banking activities, description of penetration testing carried out during the financial year, IT recovery plan…);
- a presentation of the process used to inform the relevant supervisor in the event of a major incident;
- a presentation of the IT security awareness programme (raising awareness among both employees and service providers) and of the regular training sessions offered (cf. last subparagraph of Article 270-3 of the *Arrêté du 3 novembre 2014*, as amended).

#### *11.5.4. Management of IT operations*

- a description of the IT operation management processes: presentation of the processes covering the operation, monitoring and control of IT services and systems;
- a description of the process used to detect and manage operational or security incidents (cf. Article 270-4 of the *Arrêté du 3 novembre 2014,* as amended).

#### *11.5.5. Change management and project management*

- a description of the framework used to conduct IT projects and manage IT software;
- a description of the management process dedicated to the acquisition, development and maintenance of IT systems, a description of the process used to manage changes to IT software: *specifying the method used to record, test, assess, approve and implement changes made to IT systems* (cf. Article 270-5 of the *Arrêté du 3 novembre 2014*, as amended).

### 11.6. Results of 2nd level permanent controls carried out for operational risk including IT risk

- main shortcomings observed;
- corrective measures taken to remedy the shortcomings observed**,** 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).

### 11.7. Overall conclusions on exposure to operational risk

[6] In particular, specify whether the institution is exposed to specific risks and the specific measures taken to manage these risks.

[7] Incidents with a financial impact exceeding EUR 25 million or 0.5% of the CET1. For instance, a cyber attack.

## 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.*

- 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 observed;
- corrective measures taken to remedy the shortcomings observed**,** 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);
- a presentation of the accouting risk prevention system, covering the risk of disruptions of IT systems (fallback site…).

## 13. Overall interest-rate risk

***Nota bene**: for the financial year 2023, this section should include a description of the adjustments the institution has made to comply with the new provisions introduced by the EBA Guidelines specifying criteria used to identify, assess, manage and mitigate the risks arising from potential interest rate fluctuations and to comply with the provisions on the assessment and monitoring of the credit spread risk of institutions' non-trading book activities (EBA/GL/2022/14), in force as of 30 June 2023*[8].

- a summary description of the overall framework used to identify, assess and manage the overall interest-rate risk (*specifying the entities and transactions covered, justifying the role of the effective managers and supervisory body as well as the distribution of powers regarding control of the overall interest-rate risk*);
- a description of and justification for the potential use of the principle of proportionality in light of the volume, complexity, risk appetite and risk level of their positions sensitive to interest rate risk as well as of the size, strategy and business model of the institution, 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[9]);
    - measurement and monitoring of the interest rate risk (especially using internal and appropriate shock scenarios as referred to in paragraphs 89 to 102 of the EBA Guidelines and using the proportionality measures set out in the "sophistication matrix" included in Annex II to the EBA Guidelines) including the recognition of interactions and cross effects between different types of risks: interest rate, credit, liquidity, market;
    - supervisory arrangements (including the application of limits and sub-limits reserved to the material components of interest rate risk referred to in paragraphs 44 (c) and 44 (d) of the EBA Guidelines);

[8] Excluding Sections 4.5 and 4.6 of the guidelines which apply as of 31 December 2023.

[9] As specified in paragraph 23 of the EBA Guidelines (EBA/GL/2022/14), the two measures must be taken into account in the internal capital allocation process, however institutions are not expected to capitalise twice - in respect of each measure (net interest income and economic value).

- governance arrangements (adaptation of reports to the management body according to the institution's activities, referred to in paragraph 67 of the EBA Guidelines).

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

- a description of the tools and methodological principles used to manage the overall interest-rate risk (*specifying the methods used by the institution, such as static or dynamic gap analysis, sensitivity in terms of net interest income, calculation of net discounted value, the assumptions and results of stress tests including, where appropriate, interactions and cross effects between types of risks (interest rate, credit, liquidity, market – paragraph 97 of the EBA Guidelines), the impact of changes in overall interest-rate risk on the institution's business during the past year, the methodology used to aggregate exposures, the impact of fair value instruments*);
- a description of the run-off assumptions used by the institution [*specifying the scope covered, the main assumptions retained, the treatment applied to production, non-interest-bearing products (such as own funds), automatic (explicit or implicit) and behavioural options, in particular the treatment of deposits with no maturity date (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 deposits with no maturity date, for the early repayment of loans, for early withdrawals from term deposit accounts, for off-balance sheet draws (e.g. liquidity facilities) and for regulated savings products]*;
- a presentation of hedging activities (*specify the strategy adopted, the different tools implemented and controls carried out on these activities);*
- a presentation of the results of the "*Supervisory outlier test*" on the economic value of equity under six standardised interest-rate shock scenarios as well as on net interest income under two standardised interest-rate shock scenarios as laid out in the EBA technical standard (EBA/RTS/2022/10) pending publication by the European Commission as a Delegated Regulation (publication expected by Q3 2023) - *main assumptions*:
    - shocks applied with integration of a post-shock floor starting with -150 bps (in accordance with paragraph (k) of Article 4 of the aforementioned technical standard),
    - exclusion of own funds from liability items (CET1 instruments and other perpetual own funds without a call date);
    - refer to Article 4 of the abovementioned technical standard for the exhaustive list of assumptions used to calculate the economic value sensitivity of equity for the *"Supervisory outlier test"*;
    - refer to Article 5 of the abovementioned technical standard for the exhaustive list of assumptions used to calculate net interest income sensitivity for the *"Supervisory outlier test"*;
- a presentation of the economic value results of the *"Supervisory outlier test"* under 6 differentiated shocks detailed in the abovementioned technical standard, for each currency and applied to 15% of the institution's TIER 1 capital;
- a presentation of the net interest income results of the *"Supervisory outlier test"* under 2 differentiated supervisory shocks detailed in the technical standard referred to above, applied to 5% of the institution's TIER 1 capital;
- a description of the results derived from overall interest-rate risk measuring indicators used by the institution:
    - *specifying the static or dynamic gap levels, the results of the sensitivity calculations carried out on net interest income, the results of net present value calculations and the results of stressed scenarios),*
    - *for the sensitivity calculations in economic value and net interest income, provide a justification for any differences with the standardised assumptions described in the framework of the "Supervisory outlier test",*

- *for the calculation of net interest income measures, according to 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, using at least one baseline scenario and one shocked or stressed 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 instruments at fair value.*

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

- sensitivity of shock outcomes to a change in the assumptions used (*specifying the impact of the various (parallel and non-parallel) movements of the yield curve, the impact of mismatches between different rate benchmarks (basis risk) and that of changes to the retained assumptions and run-off practices);*
- presentation of the internal capital allocated in view of the overall interest-rate risk incurred by the institution and 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 effects on economic value and net interest income.

### 13.2. Monitoring system used for overall interest-rate risk

- for net interest income measures 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 in terms of gap, in terms of sensitivity in relation to capital or earnings, specify the date on which such limits were reviewed in the course of the last 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 effective managers, the supervisory body and, when applicable, the risk committee, in defining a global strategy regarding the overall interest-rate risk and the current and future interest-rate risk appetite of the institution (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 there is a unit responsible for monitoring and managing the overall interest-rate risk, and more generally how this oversight is integrated into the permanent control system.

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

- main shortcomings observed;
- corrective measures taken to remedy the shortcomings observed**,** 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)[10]:

[10] The sections of Guidelines EBA/GL/2022/14 on the CSRBB only apply from 31 December 2023.

- a summary description of the general framework used to identify, assess and manage CSRBB risk: *specify the scope of transactions covered and any exclusion of instruments applied, stating the reasons for such exclusions, a description of the role of the effective managers and supervisory bodies and the allocation of responsibilities in terms of managing CSRBB risk;*
- a description of the monitoring and assessment of positions affected by credit spread risk in the banking book, via, in particular, economic value metrics and net interest income metrics (see Article 84(2) of Directive No 2013/36/EU): *specify the indicators and tools used, describe 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 should formalise and deliver 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 commitments by set of counterparties and by principal (by internal rating, by financial instrument, by market, or by any other criteria that is significant in the context of the business conducted by the institution);
- information on risk management (guarantees obtained, margin calls to cover positions, collateral, etc.) and on the procedures followed in the event of default by an originator (insufficient coverage of positions, refusal of the transaction);
- an overview of the exposure limits set for intermediation risk- by beneficiary, by related debtors, etc. (specify the level of limits in relation to the volume of transactions by beneficiaries and in relation to own funds);
- the procedures used and frequency with which the limits set for intermediation risk are reviewed (*specify the date of the most recent review*);
- any breaches of limits observed during the past year (*specify their causes, the counterparties involved, the size of the total exposure, the number of breaches, their duration and amounts*);
- the procedures used to authorise such breaches and the measures taken to resolve them;
- the analytical factors used to assess the risk associated with the principal when making a commitment (*methodology, data used for the analysis*);
- a typology of the errors that have occurred during the past year in the acceptance and execution of orders (*methods and frequency of analysis conducted by the head of internal control, threshold set by the effective managers to document such errors*);
- results of permanent controls on intermediation risk;
- main conclusions of 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 and the treatment of new transactions in addition to pending transactions, etc.*);
- a summary description of the settlement/delivery risk limits (*specify the level of limits, by type of counterparty, in relation to the counterparties' transaction volumes and in relation to own funds*);
- the frequency with which settlement/delivery limits are reviewed (*specify the date of the most recent review*);

- any breaches of limits identified during the past year (*specify their causes and their number, duration and the associated amounts*);
- the procedures used to authorise such breaches and the measures taken to resolve them;
- an analysis of outstanding items (*indicate their anteriority, their causes, and the action plan for clearing them*);
- the results of permanent controls carried out for settlement/delivery risk;
- main conclusions of the risk analysis conducted.

For investment services providers supplying performance bonds:

- a description of the various instruments traded and of each settlement system used, identifying the various phases of the settlement process;
- the procedures used to monitor cash and securities flows;
- the procedures used to monitor and handle outstanding items;
- the procedures used to measure resources, securities and cash that can easily be transferred to ensure that commitments to counterparties can be covered**.**

## 16. Liquidity risks

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

### 16.1. Tools and methodological principles used to measure liquidity risks

- a description of the tools and methods used to manage liquidity risks: *specify the assumptions retained and the maturities included in the calculation of indicators used by the institution (cf. Article 156 of the* Arrêté du 3 novembre 2014, as amended*) taking into account the complexity of activities, the risk profile and risk tolerance level of the institution, listing the information systems, tools and indicators used for each currency in which the institution conducts significant business and specifying the alternative scenarios 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 construct a projected cash-flow statement, and any changes in these characteristics and assumptions made during the year;
  - an analysis of any changes in liquidity gaps calculated on the basis of cash flow statements drawn up during the year under review.
- where applicable, a description and justification of scenarios that are specific to given foreign locations, 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 form the stock of liquid assets in relation to the liquidity risk limit system;
- a description of the means used to continuously monitor the required stock of liquid assets, and the adjustment assumptions used for the various time horizons considered;
- a description of the methodology used for the regular assessment, in accordance with Article 23 of Delegated Regulation (EU) No 2015/61, as amended, on liquidity coverage ratio requirements (LCR) for credit institutions, a description of the probability and potential volume of liquidity outflows over 30 calendar days for products or services which are not referred to in Articles 27 to 31. Where applicable, information on the existence of actual cash outflows not provided for in ACPR Decision 2016-C-26;
- the method used to take into account the internal cost of liquidity and analysis of any changes to liquidity cost indicators during the past financial year;
- procedures used to taking account of, assess, monitor and supervise intra-day liquidity risk;
- a description of financing plans (methods used to assess the institution's ability to raise funds from its funding sources under normal conditions and stressed environments, over all maturities considered and broken down by currency (*underlying assumptions, test results,* etc.), procedures used to take account of reputation risk; procedures used to distinguish between encumbered and unencumbered assets available at all times, especially in emergency situations, procedures used to take account of the legal, regulatory and operational constraints on any tranfers of liquidity and unencumbered assets between entities, procedures used to take account of potential discounts 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 a significant change in market parameters (indicate the assumptions used, the frequency with which they are reviewed, and the process used for their validation; 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 has to take into account both the institution's own funding liquidity risk, the risk of markets drying up and the interactions between these two risks, while also incorporating the intra-day liquidity risk dimension when appropriate): *specify the procedures implemented (identity and hierarchic level of persons concerned, solutions considered for access to liquidity, communication to the public, regular testing of contingency plans…)*;
- a description of the liquidity recovery plans setting up the strategies and measures implemented in order to remedy any potential liquidity shortfall, which should be tested regularly: *specify the operational measures adopted to ensure immediate implementation of these recovery plans (holding immediately available collateral…)*.

### 16.2. Liquidity risk monitoring system

- a summary description of liquidity risk limits and liquidity risk tolerance level (*specify and justify these levels by type of business, by currency and by type of counterparty, in relation to the counterparties' transaction volume and in relation to 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 the identification, valuation, liquidity, assets availability and consideration 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 situation, the liquidity positions and the 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 breaches, and the amounts*);

- the procedures used to authorise such breaches and the measures taken to remedy them;
- a summary description of the reports used to manage liquidity risk (*including their frequency and recipients*);
- a description of all incidents that occurred during the last 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 implemented 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 mitigating for liquidity risks (cf. Article L. 511-60 of the French *Code monétaire et financier*);
- institutions subject to the CRR and that are not under the ECB's direct supervision shall provide a "reader's guide", drawn up as a comprehensive document to facilitate the inspection of documentation justifying of their capital adequacy. In this regard, the "reader's guide" shall provide an overview of all the documents sent 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" should essentially function as an index linking the specific items of information required for in the internal control report to the documents provided to the competent authority concerning their capital adequacy assessment. The "reader's guide" shall also include information about significant changes to the information compared to that which was previously sent, any items excluded from information provided and any other information that could be useful to the competent authority in the course of the assessment. Furthermore, the "reader's guide" shall contain references to any information made public by the institution on its liquidity adequacy.
- class 2 investment firms shall submit a formal report pursuant to Article L533-2-2 of the French *Code Monétaire et Financier* to document their ILAAP framework and to justify the effectiveness of the match between its available liquid assets and the risks to which it is exposed, both dynamically and over time, under normal and stressed market conditions. An indicative list of key information to be provided by the investment firm in that report shall be made available by the SGACPR.

### 16.3. Liquidity risk and pro-cyclicality risk resulting from margin calls arising from central clearing by clearing members and non-centrally cleared exposures

- 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 OTC 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 linked to margin collection (for instance, using the excess initial margin collateral rather than collecting additional collateral, taking account of customers' operational constraints).

### 16.4. Permanent control system for liquidity risk management

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

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

- main shortcomings identified;
- corrective measures taken to remediate the shortcomings observed**,** 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).

### 16.6. Overall conclusion on exposure to liquidity risks

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

## 17. Excessive leverage risk

This section shall 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 bonds) used to identify, manage, and monitor the risk of excessive leverage 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 through expected or realised losses (cf. Article 212 of the *Arrêté du 3 novembre 2014*, as amended), including plans to strengthen own funds in a stressed environment.

## 18. Internal control system covering provisions relating to the protection of the funds of investment firm customers

- the organisational arrangements made for the management of customer cash accounts and links (enabling the various flows to be traced chronologically) with the execution of investment or clearing services;
- a presentation of the method used to protect assets received from customers in accordance with regulations in force (i.e. *Arrêté du 6 septembre 2017* on the ring-fencing of customer funds by investment firms) and a description of the tool used to calculate the amount of funds received from customers that need to be ring-fenced;
- for institutions ensuring the protection of received assets by placing them in one or more account(s), opened specially for this purpose with a credit institution: communication of ring-fencing agreement(s) and of any changes made to the previously sent ring-fencing agreement, description of the procedures to ensure the investment of funds;
- for institutions ensuring the protection of funds received by means of a guarantee: communication of any change made to the guarantee or surety contract and of any information on the adjustment of the amount of coverage provided related to changes in business volumes;
- for institutions ensuring the protection of funds received from a qualifying credit institution, bank or money market fund belonging to the same group as them: communication of the amount deposited with one or more group entities in relation to the total amount of client funds to be ring-fenced, justification for the proportion of ring-fenced funds within the group;

- a presentation of the procedures in place to ensure compliance with the provisions relating to the protection of the assets of investment funds' customers, presentation of the associated checks and of any incidents or insufficiencies identified as a result of such control measures;
- the identification of the single person in charge with the necessary skills and authority that is specifically responsible for matters relating to the institution's compliance with its obligations as regards the safeguarding of customers' financial instruments and funds, in accordance with Article 9 of the *Arrêté du 6 septembre 2017* on the ring-fencing of the funds of investment firm customers;
- communication of the report issued by statutory auditors on compliance with the regulatory provisions in force concerning ring-fencing.

## 19. Provisions for the separation of banking activities

***Nota bene:*** This section concerns the implementation 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*). It is reminded that the mandates of the internal units mentioned in the map shall be sent to the SGACPR along with the report on internal control. This submission, which may be carried out electronically, shall 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 can also submit all mandates, highlighting substantial changes made since the last report sent to the SGACPR.

### 19.1. Mapping of trading activities in financial instruments

- communication of the updated mapping of internal units in charge of transactions in financial instruments as mentioned in Article 1 of *Arrêté du 9 septembre 2014* at the most granular organisational level possible within the institution, identifying any groupings made. The mapping shall at least include the following elements:
    - the literal name of the smallest 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), their average and maximum use over the course of the year,
- a description of any changes made to that mapping,
- a description of the main 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 relating 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 internally by the institution to classify transactions 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[11] | |
| A.1.b. which are significantly invested in or have significant exposure to[12] CIUs or other similar vehicles that make substantial use of leverage | |
| **A.2. that are not directly or indirectly and substantially leveraged 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 on 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 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 sale and repurchase agreements | | | | | |
| A.1.c. Undrawn credit lines | | | | | |
| A.1.d. Guarantee commitments | | | | | |
| **A.2. Market transactions** | | | | | |
| A.2.a. Repurchase agreements and | | | | | |

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

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

| | | | | | |
|---|---|---|---|---|---|
| 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** | | | | | |
| **B. Investments in CIUs or similar vehicles** | | | | | |
| **B.1. Units of CIUs or similar vehicles held** | | | | | |
| **B.2. Other** | | | | | |
| **Total (A+B)** | | | | | |

- for institutions meeting one of the following conditions as at the closing date:
    - the gross carrying amount under IFRS of the "Total (A+B)" item is above EUR 300 million
    - the exposure value before recognition of collateral of the "Total (A+B)" line item is above EUR 300 million
    - the exposure value before recognition of collateral of the "Total (A+B)" item accounts for more than 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. Units of CIUs or similar vehicles held** | |
| **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 attached to these indicators;

- description of the risk management procedures used for the aforementioned risks, and description of the associated controls:
- specify, for each internal business line presented in the general description of activities, which of them are governed by a collateralisation policy;

- for each business line with a collateralisation policy:
    - summarise its principles;
    - set out the criteria used for eligibility, availability and quantity 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 criteria applicable to the quantity and availability of collateral are adapted to the quality of the collateral and the level of risks involved in the transactions secured by this collateral;
    - where the quality and availability criteria are not met, indicate whether a higher quantity requirement is provided for and if so, to what extent;
    - indicate whether the policy provides for any exemptions. If so, describe how they are managed;
    - 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 retained to control the degree of concentration of (i) individual exposures to a CIU or other similar vehicles using substantial leverage, and (ii) collateral obtained from that counterparty.

### 19.4. Control results

- results of the permanent 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 set up to address the identified shortcomings;
- results of the periodic control actions carried out for the purposes of 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

- presentation of the institution's or group's strategy in terms of outsourcing, including in particular a description of existing arrangements made to inform outsourcing decisions (*prior analysis carried out on the criticality of the activity to be outsourced and assessment of associated risks*) before it is effective (especially when it can affect the institution's ICT);
- adjustments made to comply with the requirement to maintain a register including the information referred to in Section 11 of the EBA Guidelines on all outsourcing arrangements (see Article 238 of the *Arrêté du 3 novembre 2014*, as amended);
- description of outsourced activities[13] (under 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 *(as a whole as well as area by area)*;
- communication of the yearly data extraction from the register listing outsourcing arrangements made in relation to core or significant activities (within the meaning of Article 10 of *Arrêté du 3 novembre 2014*, as amended);
- description of the conditions underlying the use of outsourcing: name of the service provider, host country, authorisation and prudential supervision of external providers, procedures implemented to ensure that a written contract 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 Autorité de contrôle prudentiel et de résolution, or the ECB, when appropriate, to conduct on-site inspections at the external provider's premises, etc.;

[13] By precising those which are used resorting to a cloud computing service provider.

- in the specific case of outsourced activities using a cloud computing service provider, description of the conditions underlying the use of outsourcing: cloud computing model (public/private…), dates at which the provision of services begins and ends, name of the potential "n$^{th}$ level" subcontractors and an indication of the substitutability of the service provider concerned (easy/difficult/impossible);
- description of permanent and periodic control procedures 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 linked to outsourced activities;
- description of procedures implemented by the institution to maintain the necessary expertise in order to effectively control outsourced activities and manage risks linked to 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 of the same group;
- description of the business continuity plans and of the exit strategy defined for critical or important outsourced activities: formalised retained scenarii and objectives as well as proposed alternative measures, presentation of the tests carried out (frequency, results…), reporting to senior management (regarding the tests, updates on the defined plans or exit strategy);
- procedures to inform the supervisory body and, when appropriate, the risk committee on measures taken to exercise 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 effective managers 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 used for the permanent and periodic control of outsourced activities (including compliance review procedures);
- results of 2$^{nd}$ 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), follow-up procedures used for the 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), follow-up procedures for the recommendations resulting from periodic control actions.

## 21. Specific information requested from financial conglomerates

- balance sheet totals for the group as a whole and for the banking, insurance and non-financial sectors.

### 21.1. Internal control and risk assessment system 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 system;
- a presentation of the procedures used to assess the impact of growth strategies on the risk profile of the conglomerate and to set additional capital requirements;
- a presentation of the procedures used to identify, measure, monitor and carry out controls on intra-conglomerate transactions between different entities of the conglomerate, as well as the concentration of risks;
- the results of 2$^{nd}$ 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;
- a description of the risks specific to the insurance business (*specify which risks are managed centrally, what procedures are used, and which activities remain decentralised*).

### 21.3. Information on intra-group transactions

- information on material intra-group transactions carried out during the year under review between entities of the conglomerate that conduct banking or investment activities on the one hand, and entities that conduct insurance activities on the other hand:
    - a description of these transactions, specifying the degree of interdependence of activities within the conglomerate;
    - for each type of transaction, the type the transaction in the majority of cases (from a banking or investment services entity to an insurance entity, or the opposite), and the purpose of these transactions;
    - the procedures used for the internal pricing of these transactions.
- quantitative information on each intra-group transaction the amount of which exceeds 5% of total capital requirements applicable to the various sectors concerned, calculated on the basis of the previous year's financial statements:
    - if they exceed the threshold: the cumulative nominal amount of such transactions giving rise to financial flows excluding market transactions (loans, collateral; asset sales, etc.), the total amount of commissions paid; and for transactions in financial futures, the total credit risk equivalent (or if that number is not available, the total notional amount);
    - for each individual transaction that exceeds the threshold, the nominal amount of the transaction and the date on which it was carried out. Financial conglomerates should also provide a description of the transaction, indicating the identity of the counterparties, the type of the transaction, and its purpose, using the following format:

| Type of transaction | Transaction conclusion date | Nominal amount for balance sheet items, the notional amount and the equivalent credit risk for financial futures. | Description of the transaction (counterparties, nature, aim, etc.) |
|---|---|---|---|
| | | | |

## 22. Annex on the security of cashless payment instruments 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 devoted to the security of **cashless payment instruments** (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 *Code Monétaire et Financier* and, for annexes drawn up by institutions having their registered headquarters 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[14].

The annex, 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. Furthermore, insofar as the Banque de France's jurisdiction is limited to French territory, this annex is only relevant for means of payment offered in France (or payment accounts opened in France), which excludes the services of institutions provided 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 shall bear 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 means and service of payment, 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 access to accounts (II);
- a section dedicated to collecting the self-assessment of the institution's compliance with the recommendations issued by external bodies as regards the security of non-cash means of payment and the security of account accesses (III);
- a section on the audit report on the implementation of security measures provided for in the RTS (Regulatory Technical Standards)[15] (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).

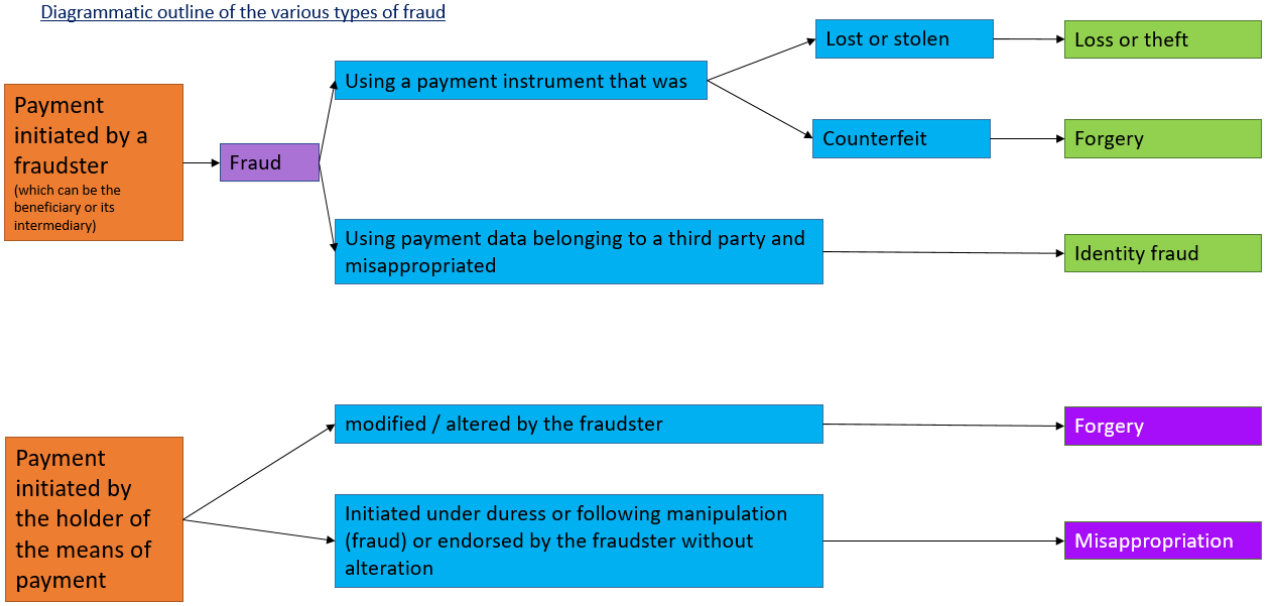
[14] For payment service providers having their head office registered in one of the French territorial communities of the Pacific region (New Caledonia, French Polynesia, Wallis and Futuna Islands), the reference to "Banque de France" should be replaced with one to "IEOM" in this Annex, and references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

[15] 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 scriptural means of payment"[16]. As a consequence, this analysis is carried out:

- on gross fraud and covers both internal and external fraud, and
- based on the definitions and typologies 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 matrices specific to each cashless means of payment, that are presented in the annex, are to be filled in according to the offers specific to each institution. **Starting with the 2023 annual report on the financial year 2022, institutions are also expected 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 concerning the security of means of payment issued by external bodies, presented in section III of this annex, takes into account the entry into force, on 13 January 2018, of the 2nd European Payment Services Directive. Institutions should provide explanatory comments on recommendations for which the full compliance of the institution is not ensured.

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 Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 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

[16] See the fraud reporting form fill-in Guide (in French): https://www.banque-france.fr/stabilite-financiere/securite-des-moyens-de-paiement-scripturaux/collectes-statistiques-reglementaires-espace-declarants

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 case of use of the exemption set out therein, 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 the compliance with the conditions for implementing the exemption based on risk analysis and in particular, on 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 being responsible at central level for internal control and risk management with regard to 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 the activity. However, it is exempted from producing the analysis matrix for risks and main fraud incidents and it must mention that "*it refers to what has been described by the institution in charge of the risk control and risk management mechanism in its own annex*".
- concerning the section dedicated to the presentation of periodic control results (II), if this function is exercised 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 should 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 relieved of this task and must mention that "*it refers to what has been described by the institution in charge of the internal control and risk management mechanism 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 has to mention that "*it refers to what has been described by the institution in charge of the internal control and risk management mechanism in its own annex*".

**When the institution refers the reader to the annex produced by the institution in charge of the internal control and risk management mechanism for the security of means of payment and account access, it shall specify the exact identity and interbank code of the institution in question.**

**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 means:<br>- for cards, 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;<br>- for transfers, the reception channel of the transfer order: desk, online banking, teletransmission solution…;<br>- for direct debit, the reception channel of the direct debit order;<br>- for cheques, the channel of cheque deposit: mail, machine…<br>- for account information and payment initiation services, the means of connection: 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 statistical collection on "Inventory of fraud on non-cash means of payment" by the Banque de France, gross fraud corresponds to the nominal amount of payment transactions authorised which are subject to an *ex post* rejection due to fraud. Therefore, it does not take into account assets which have been recovered after the litigation is processed. |
| Gross risk | Risks likely to affect the proper functioning and security of means of payment, before the institution takes into account procedures and measures to manage them. |
| Residual risk | Risk persisting after taking into account coverage measures. |
| Coverage measures | All actions implemented by the institution in order to better manage its risks, by reducing their impact as well as 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 functions proposed | Target clients | Initiation channel | Comments on the evolution of business volume | Comments on evolutions regarding technology, function and security |
|---|---|---|---|---|---|
| **As an issuing institution** | | | | | |
| *Ex: **payment card**: international card* | *Ex: - Maturity<br>- Date of commercialisation<br>- Equiped with the contactless function by default<br>- Enlistment in an authentication device<br>- Virtual card service* | *Ex: Individuals* | *Ex: at the point-of-sale or at the cash machine, remote payment,…* | *Precise explanatory factors for significant variations of activity (number and amount)* | *Indicate changes that occurred during the reporting period<br>Ex: pilot tests, implementation of SMS alerts for international transactions on high-end cards…* |
| *Ex: **Withdrawal card*** | | | | | |
| *Ex: **Enlistment in wallets*** | | | | | |
| **As an acquiring institution** | | | | | |
| Ex: Offer for the acceptance of proximity card payments | | | | | |
| Ex: Offer for the acceptance of card payments for distance selling | | | | | |
| | | | | | |

#### b. Product and service offering plans

| |
|---|
| *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 the group's entities) 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

| Category of fraud | Description |
|---|---|
| Lost or stolen card | The fraudster uses a payment card obtained as a result of loss or theft, without the legitimate holder's knowledge. |
| Card not received by the legitimate holder | The card has been intercepted during its sending between the issuer and the legitimate holder.<br>This fraud type is similar to loss or theft. However, it is different to the extent that the holder cannot easily notice that a fraudster has a card which was intended for use by the legitimate holder. In this scenario, the frauster exploits vulnerabilities in card sending processes. |
| Counterfeit card | The frauster uses (i) a counterfeit payment card, which involves the creation of a medium that appears to be a genuine payment card and/or a card that is designed to deceive an automated teller machine or the payment terminal of a given merchant, or (ii) a forged payment card, the creation process of which involves altering the magnetic, embossing or programming data of a genuine payment card. In both |

| | |
|---|---|
| | cases, the fraudster makes sure that such a card carries the data necessary to fool the payment acceptance system. |
| Misappropriated card number | The card number of a legitimate holder is collected without his or her knowledge or created by random card number generators and is used in distance selling. |
| Other | Any other type of fraud, such as:<br>- the use of a consistent card number that isn't assigned to a legitimate card holder for distant selling transactions,<br>- alteration by the fraudster of a legitimate payment order (forgery),<br>- manipulation or coercion of the legitimate card holder aiming for that legitime card holder to issue a card payment (misappropriation) etc. |

### b. Overall rating of card and equivalent fraud risk

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

| | |
|---|---|
| Gross risk<br>(*Inherent risk before coverage measures*) | |
| Residual risk<br>*(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 |
|---|---|---|
| Lost or stolen card | *Ex: at the point-of-sale* | |
| Card not received | | |
| Counterfeit card | | |
| Misappropriated card number | | |
| Other | | |

As an acquiring institution:

| Category of fraud | Initiation channel | Coverage measures |
|---|---|---|
| Lost or stolen card | | |
| Card not received | | |
| Counterfeit card | | |

| | | |
|---|---|---|
| Misappropriated card number | | |
| Other | | |

### 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, diversion of SIM card* |
| | | |
| | | |
| | | |
| | | |

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 functions proposed | 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 the evolution of an existing technology, functionality or security offer planned in the short- and medium-term.* |

## 2.2. Operational organisation of the transfer activity

*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

| Category of fraud | Description |
|---|---|
| Fake transfer order | The fraudster counterfeits a transfer order or misappropriates the online banking user ID of the legitimate originator in order to initiate a fraudulent payment order. In this scenario, the online banking user ID may notably have been collected using hacking techniques (phishing, social engineering etc.), or under duress. |
| Counterfeiting of transfer order | The fraudster intercepts and alters a legitimate transfer order, or the remittance file of a legitime transfer order. |

| | |
|---|---|
| Misappropriation | Using deception (notably social engineering, i.e. by impersonating a contact person of the payer -his manager, supplier, bank technician, etc.), the fraudster gets the legitimate account holder to issue a recurring payment transfer to an account number which is not that of the legitimate beneficiary of that payment, or which has no economic substance. Examples of such fraudulent practices include CEO impersonation scams, or change of banking details scams. |

### b. Overall rating of fraud risk for transfers

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

| | |
|---|---|
| Gross risk<br>*(Inherent risk before coverage measures)* | |
| Residual risk<br>*(Risk remaining after coverage measures)* | |

### c. Coverage measures of 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 |
|---|---|---|
| Fake transfer order | | |
| Counterfeiting of transfer order | | |
| 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 proposed | 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 marketing new products/services or upgrading 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 the group's entities) 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

| Category of fraud | Description |
|---|---|
| Fake direct debit | The fraudulent creditor issues direct debits to account numbers obtained illegally and without any authorisation or underlying economic substance ("unauthorised payment transaction" in EBA terminology).<br>Example No 1: the fraudster massively issues direct debits to RIB/IBAN the list of which he obtained illegally and without any authorisation or underlying economic reality. |

| | |
|---|---|
| | Example No 2: the creditor issues unauthorised direct debits after having obtained the details of the debtor's bank information thanks to a loss leader serving as a "hook" (only an authorised direct debit).<br>Example No 3: the creditor knowingly issues direct debits that have already been issued (which have either already been paid or have been rejected due to the debtor having issued a stop payment order). |
| Misappropriation | The fraudulent creditor impersonates a third party and misappropriates their bank details, and obtains the of a direct debit mandate for an account that is not his. |

### b. Overall fraud risk rating for direct debit

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

| | |
|---|---|
| Gross risk<br>*(Inherent risk before coverage measures)* | |
| Residual risk<br>*(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 |
|---|---|---|
| Fake direct debit | | |
| Misappropriation | | |

As the institution of the creditor

| Category of fraud | Initiation channel | Coverage measures |
|---|---|---|
| Fake direct debit | | |
| 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 proposed | 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 marketing new products/services or upgrading existing ones in terms of technology, functionality and security.* |

## 4.2. Operational organisation for 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

| Category of fraud | Description |
|---|---|
| Theft, loss | Fraudulent issue of a commercial paper by a fraudster using a blank form. |
| Counterfeiting | A fake commercial paper entirely fabricated by the fraudster, drawn on an existing bank or on a fake one. |
| Forging | A valid commercial paper that is intercepted by a frauster, who deliberately alters it (either by scratching or erasing it). |
| Misappropriation, double presentment | A commercial paper that has already been cleared in payment systems is stolen or lost, and is presented again for payment. |

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

*The rating matrix used by the institution to assess the fraud risk shall be indicated in Part IV of this Annex.*

| | |
|---|---|
| Gross risk<br>*(Risk inherent before coverage measures)* | |
| Residual risk<br>*(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 | | |
| Forging | | |
| 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 functions proposed | 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 marketing new products/services or upgrading existing ones in terms of technology, functionality and safety 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 of the group's entities) and those shared with other institutions. An organisational diagram can be added as necessary.*

| Actors | Roles |
|---|---|
| **Issuer's activity** | |
| | |
| | |
| | |
| **Remitter's 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

| Category of fraud | Description |
|---|---|
| Theft, loss | - The fraudster uses a cheque that was either lost by its legitimate owner or stolen from that person. The cheque bears a forged signature, that is neither the one of the account holder nor the one of its agent.<br>- Fraudulent issue of a cheque by a frauster using a blank form. |
| Counterfeiting | Counterfeit cheque that is entirely fabricated by the fraudster, drawn on an existing bank or a fake one. |
| Forging | A regular cheque is intercepted and deliberately altered by a fraudster using chemical and/or mechanical processes (to scratch or erase) to alter either the amount of that cheque or the name of the entity it is payable to. |
| Misappropriation, double presentment | A legitimately issued, lost or stolen cheque that is intercepted while in transit, before reaching the payee, and cashed in to a different account from that of the legitimate payee. The form is regular, the |

| | |
|---|---|
| | name of the beneficiary is unchanged and the magnetic (MICR) line at the bottom of the cheque rermains valid, as does the customer's signature.<br>- Cheque either lost or stolen after clearing in payment systems and re-presented for collection.<br>- Cheque issued by the legitimate account holder, under duress or through manipulation. |

**b. Overall fraud risk rating for cheques**

*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<br>*(Risk inherent before coverage measures)* | |
| Residual risk<br>*(Risk remaining after coverage measures)* | |

**c. Risk coverage measures in place as regards 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 drawer:

| Category of fraud | Delivery channel used for the forms | Coverage measures |
|---|---|---|
| Theft, loss | | |
| Counterfeiting | | |
| Forging | | |
| Misappropriation, double presentment | | |

As the institution of the remitter (including fight against fraudulent remittances made through the remitting customer):

| Category of fraud | Remittance channel | Coverage measures |
|---|---|---|
| Theft, loss | | |
| Counterfeiting | | |
| Forging | | |
| Misappropriation, double presentment | | |

**d. Evolution of gross fraud during the period under review**

As the institution of the drawer:

| Category of fraud | Delivery channel used for the forms | Description of the main cases of fraud uncountered (in terms of amount and/or frequency) |
|---|---|---|
| Theft, loss | | |
| Counterfeiting | | |
| Forging | | |
| 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 | | |
| Forging | | |
| 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 proposed | 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 marketing new products/services or upgrading existing ones in terms of technology, functionality and security over the short and medium term.* |

## 6.2. Operational organisation for electronic money

*Summarise the processes associated with the payment means/service, specifying in particular outsourced ones (including those outsourced to one of the group's entities) 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. Services of information on accounts and of payment initiation

### 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 offer

| |
|---|
| *Describe the technological, functional and security upgrades 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 of the group's entities) 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 observations and recommendations in terms of security for non-cash means of payment and implementation deadline |
|---|---|---|
| | | |
| | | |
| | | |

## III – ASSESSMENT OF COMPLIANCE WITH THE RECOMMENDATIONS OF EXTERNAL ENTITIES IN TERMS OF THE SECURITY OF NON-CASH MEANS OF PAYMENT AND ACCOUNT ACCESS

| Recommendation statement | Issuing entities | Answer of the institution | |
|---|---|---|---|
| | | **Compliance assessment** (yes / partial / no / N.C.) | **Comments about the assessment (in case of non-compliance or partial compliance)** |
| **Prevention measures of specific risks** | | | |
| Immediate issuing procedures for cards in branches or outlets ("*Instant issuing*") are subject to a risk assessment in order to continuously adjust their level of security. | OSCP[17] | | |
| PCI security measures are adopted and implemented for all processes relating to the acceptance and acquisition of payment cards. | OSCP | | |
| m-POS solutions commercialised by the institution shall comply with the requirements applicable to classic terminals and rely on communication protocols between the different components of the solution which limit to the strict minimum the ability to access transaction data through the terminal. | OSMP[18] | | |
| **Strong authentication and enlisting of the client** | | | |
| For payments via mobile phones, the personal code of payment is different from the PIN code of the SIM card and the confidential code of the user's payment card – when the personal code can be modified by the user, the banking issuer shall recommend that the user uses a different code from other codes in his/her possession. | OSCP | | |

[17] *Observatoire de la sécurité des cartes de paiement*, the French Banking Card Observatory

[18] *Observatoire de la sécurité des moyens de paiement*, the French Banking Means of Payment Observatory

| | | | |
|---|---|---|---|
| For payments via mobile phones and contactless card, specific measures are in place to ensure the holder consents. For example, the provision of simple means to activate and deactivate these new initiation modes or to validate a transaction. | OSCP | | |
| **Management of operational and security risks** | | | |
| The institution set up a framework for managing operational and security risks aiming at mitigating these risks. This framework is documented and reviewed at least annually by a high-level governing body. | EBA | | |
| In case of outsourcing, the institution ensures that the framework of risks management effectively covers outsourced activities. | EBA | | |
| Mechanisms for following transactions are implemented to prevent, detect and block suspicious transactions before they can be authorised. | EBA | | |
| The institution implemented a framework for the continuity of business, aiming at ensuring its ability to provide payment services without interruption and at limiting losses in case of serious disruptions. This framework relies on the definition of crisis scenarios and on the regular testing of contingency plans. | EBA | | |

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

*For the section dedicated to common and secure communication standards, the institution fills out the questionnaire according to the access interface solution implementged for the third party PSP.*

| **Ref. Articles Regulation (EU) 2018/389** | **Questions asked to PSP** | **Assessment of compliance** | |
|---|---|---|---|
| | | **Yes / partially / No / NC** | **For each security measure, specify the conditions for implementation. In case of non-compliance or partial compliance, present the action plan envisaged along with implementation deadlines. If the PSP is not concerned (NC) by the security measure, justify it.** |
| **Security measures for applying the strong customer authentication procedure** | | | |
| **Authentication code** | | | |
| **4** | When the PSP applies the process for strong customer authentication, is this based on two or several items categorised as “knowledge”, “possession” and “inherence”, and does it generate an authentication code? | | |
| | Is the authentication code accepted by the PSP only once when the payer uses this code in the situation detailed below? | | |

| | | | |
|---|---|---|---|
| | - For accessing its online payment account;<br>- For initiating an electronic payment transaction;<br>- For executing an action, using a means of distance communication likely to imply a risk of fraud regarding payment or any other misuse. | | |
| | Does the PSP plan security measures ensuring the compliance with each requirement listed below?<br>- No information on one of the items categorised as “knowledge”, “possession” and “inherence” can be deducted from the disclosure of an authentication code;<br>- It is not possible to generate a new authentication code based on another authentication code generated before;<br>- The authentication code cannot be falsified. | | |

| | | | |
|---|---|---|---|
| | Does the PSP ensure that the authentication through the generation of an authentication code integrates each of the measures listed below?<br>- When the authentication for remote access, remote electronic payments and every other actions by remote means of communication likely to involve a fraud risk regarding payment or any other misuse did not generate an authentication code, it is not possible to determine which items (knowledge, possession and inherence) were incorrect;<br>- The number of consecutive unsuccessful authentication attempts at which the actions provided for in Article 97(1) of Directive (EU) No 2015/2366 are blocked on a temporary or permanent basis | | |

| | | | |
|---|---|---|---|
| | shall not exceed five within a given period of time;<br>- Communication sessions are protected against interception of authentication data communicated during the authentication and manipulation by unauthorised third parties;<br>- The payer's maximum period of inactivity, once authenticated to access his/her online payment account, does not exceed five minutes. | | |
| | In the event of temporary blocking following unsuccessful authentication attempts, is the duration of the freeze and the number of retries determined on the basis of the features of the service provided to the payer and on the basis of all associated risks, taking into account, at a minimum, the factors set out in Article 2 (2) of the RTS? | | |

| | | | |
|---|---|---|---|
| | Is the payer well informed before the freeze becomes permanent? | | |
| | In the event of a permanent freeze, is a secure procedure in place to enable the payer to reuse the blocked electronic payment instruments? | | |
| **Dynamic linking** | | | |
| **5** | When the PSP applies the customer's strong authentication procedure (in accordance with Article 97 (2) of Directive (EU) 2015/2366), does it comply with the requirements listed below?<br>- The payer shall be informed of the amount of the payment transaction and the identity of the payee.<br>- The generated authentication code is specific to the payment transaction amount and to the payee approved by the payer when initiating the transaction.<br>- The authentication code accepted by the | | |

| | | | |
|---|---|---|---|
| | payment service provider corresponds to the specific original amount of the payment transaction and the identity of the payee approved by the payer.<br>- Any changes to the amount or beneficiary result in the invalidation of the generated authentication code. | | |
| | Does the PSP apply security measures that ensure the confidentiality, authenticity and integrity of each of the elements listed below?<br>- The amount of the transaction and the identity of the payee during all phases of authentication;<br>- the information that is displayed for the payer during all authentication phases, including the generation, transmission and use of the authentication code. | | |
| | When the PSP applies strong customer authentication (in | | |

| | | | |
|---|---|---|---|
| | accordance with Article 97(2) of Directive (EU) 2015/2366) does the PSP meet the requirements listed below?<br><br>- regarding card-related 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 his consent and to the payer approved when initiating the transaction;<br><br>- regarding payment transactions for which the payer has approved the execution of a series of remote electronic payment transactions in favour 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 revealed or disclosed to third parties? | | |
| | Is the use by the payer of strong authentication items categorised as "knowledge" subject to risk mitigation measures to avoid their disclosure to unauthorised third parties? | | |
| **Requirements for items categorised as "possession"** | | | |
| **7** | Has the PSP implemented measures to mitigate the risk that the customer strong 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 avoid their copying? | | |
| **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 "inherent" that are read by access devices and software provided to the payer be exposed to unauthorised third parties?<br>At least, does the PSP ensure that it is very unlikely, with these access devices and software, that an unauthorised third party is authenticated as the payer? | | |
| | Is the payer's use of authentication items categorised as "inherent" subject to measures ensuring that such devices and software avoid any unauthorised use of those items that would result in access to said devices and software? | | |
| **Independence of items** | | | |
| **9** | Does the PSP ensure that the use of the customer strong authentication items categorised as "possession", "knowledge" and "inherent" is subject to measures ensuring that, in terms of | | |

| | | | |
|---|---|---|---|
| | technology, algorithms and parameters, the breach of one of the items does not question the reliability of others? | | |
| | When one of the strong customer authentication items or the authentication code is used through a multi-functional device, has the PSP implemented security measures to reduce the risk that would result from the alteration of this multi-functional device, and do these mitigation measures provide for any of the elements listed below?<br>- the use of separate secure execution environments through the software installed on the multi-functional device;<br>- mechanisms to ensure that the software or device has not been altered by the payer or a third party;<br>- in the event of alterations, mechanisms to reduce | | |

| | | | |
|---|---|---|---|
| | the consequences thereof. | | |
| **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 de Moyens de Paiement*, OSMP) on exemptions based on transaction risk analysis, which will be available shortly on its website.<br><br>In the event of a risk analysis exemption, does the PSP meet the requirements listed below?<br>- the fraud rate for this type of transaction is equivalent to or below the reference fraud rates mentioned 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 mentioned in the Annex to Delegated Regulation 2018/389;<br>- the PSP did not identify any of the following elements after a real-time risk analysis:<br>(i) abnormal expenses or abnormal behavioural pattern of the payer;<br>(ii) unusual information on the use of the payer's device or software access;<br>(iii) signs of malware infection during a session of the authentication procedure<br>(iv) a known scenario of fraud in the provision of payment services;<br>(v) an abnormal location of the payer;<br>(vi) high-risk location of the beneficiary.<br>- The factors related to risks listed below are at | | |

| | | | |
|---|---|---|---|
| | least taken into account:<br>(i) the previous expense habits of the individual payment service user;<br>(ii) the payment transaction history of each payment service user of the payment service provider;<br>(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;<br>(iv) the identification of abnormal payment behaviours 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 as defined in the Annex to the RTS? | | |

| | | | |
|---|---|---|---|
| | For each type of transaction ("remote electronic card-based payments" and "remote electronic credit transfers"), are the fraud rates duly calculated by the PSP:<br>- using the initial amount of fraudulent payment transactions ("gross fraud approach") divided by the total value of all payment transactions with or without strong authentication;<br>- and on a rolling quarterly basis (90 days). | | |
| **Cessation of exemptions based on the analysis of transaction risks** | | | |
| **20** | If the PSP makes use of the risk analysis exemption (Article 18), does the PSP have a procedure in place for notifying the Banque de France immediately as regards any overrun of the maximum permissible fraud rate (as set out in the Annex to the RTS), and for providing a description of the measures envisaged to | | |

| | | | |
|---|---|---|---|
| | restore compliance of the fraud rate? | | |
| | Does the PSP effectively intend to immediately suspend the implementation of the risk analysis exemption (Article 18) if the maximum permissible rate is exceeded for two consecutive quarters? | | |
| | After the suspension, does the PSP intend to make use of the risk analysis exemption again (Article 18) only when the calculated fraud rate is equal to or below the maximum permitted rate for a quarter and does it have a procedure for informing the Banque de France by communicating the elements proving that the fraud rate became compliant again with the maximum rate allowed? | | |
| **Monitoring** | | | |
| **21** | Should exemptions to high authentication be used (Articles 10 to 18), has the PSP set up a device for recording and controlling, for each type of payment transaction and on a | | |

| | | | |
|---|---|---|---|
| | quarterly basis, the data listed below?<br>- the total value of unauthorised or fraudulent payment transactions, the total value of all payment transactions and the resulting fraud rate, including a breakdown by payment transactions initiated by the strong customer authentication and under each of the exemptions;<br>- the average value of operations, including a breakdown by payment transactions initiated through strong customer authentication and under each of the exemptions;<br>- the number of payment transactions for which each of the waivers has been applied and the percentage that they represent in relation to the total number of payment transactions. | | |

| | | | |
|---|---|---|---|
| **CONFIDENTIALITY AND INTEGRITY OF THE PAYMENT SERVICE USERS' CUSTOMISED SECURITY DATA** | | | |
| **General requirements** | | | |
| **22** | Does the PSP ensure the confidentiality and integrity of the user's customised security data, including authentication codes, during all authentication phases by meeting the following requirements?<br>- Customised security data is masked when it is displayed and is not readable in its entirety when it is entered by the payment service user during authentication;<br>- customised security data in data format, as well as cryptographic equipment related to the encryption of customised security data, are not stored in plain text;<br>- secret cryptographic equipment is protected from unauthorised disclosure. | | |
| | Does the PSP fully document the cryptographic | | |

| | | | |
|---|---|---|---|
| | equipment management process used to encrypt or otherwise render the customised security data unreadable? | | |
| | Does the PSP ensure that the processing and routing of customised security data and authentication codes takes place in secure environments according to rigorous and widely recognised sectorial standards? | | |
| **Data creation and transmission** | | | |
| **23** | Does the PSP ensure that the creation of customised security data takes place in a secure environment? | | |
| | Are the risks of unauthorised use of customised security data, as well as of authentication devices and software following their loss, theft or copy before delivery to the payer well managed? | | |
| **Association with the payment service user** | | | |
| **24** | Does the PSP ensure that the payment service user is the only one associated, in a secure way, with the customised security data, authentication devices and | | |

| | | | |
|---|---|---|---|
| | software according to the requirements listed below?<br>- the association of the payment service user's identity with the customised security data and the authentication devices and software takes place in secure environments that fall within the responsibility of the payment service provider, including at least 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 taking into account the risks associated with the underlying devices and components used in the association process that are not under the | | |

| | | | |
|---|---|---|---|
| | responsibility of the PSP;<br>- the association, by means of distance communication, of the identity of the payment service user with the personalised security data and the authentication devices or software, is performed using customer authentication. | | |
| **Delivery of data, authentication devices and software** | | | |
| **25** | Does the PSP ensure that the delivery of the customised security data, as well as the payment service user devices and software, is made in a secure manner that prevents the risks associated with their unauthorised use following their loss, theft or copying, by applying at least each of the measures listed below?<br>- efficient and secure delivery mechanisms ensure that customised security data and authentication devices and software are | | |

| | | | |
|---|---|---|---|
| | delivered to the legitimate payment service user;<br>- mechanisms enable the payment service provider to verify the authenticity of the authentication software delivered to the payment service user via the Internet;<br>- provisions ensure that, when the delivery of the customised security data takes place outside the premises of the payment service provider or by means of remote communication:<br>(i) no unauthorised third parties may obtain more than one element of the customised security data or devices or authentication software when delivery is made through the same means of communication; | | |

| | | | |
|---|---|---|---|
| | (ii) the customised security data or authentication devices or software must be activated before they can be used;<br>- provisions ensure that if the customised security data or authentication devices or software must be activated before their first use, this activation is carried out in a secure environment in accordance with the association procedures referred to in Article 24. | | |
| **Renewal of customised security data** | | | |
| **26** | Does the PSP ensure that the renewal or reactivation of customised security data complies with the procedures for the creation, association and delivery of this data 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?<br>- the secure destruction, deactivation or revocation of customised security data and authentication devices and software;<br>- when the payment service provider distributes reusable authentication devices and software, the secure reuse of a device or software shall be established, described in writing and implemented before it is made available to another payment service user;<br>- the deactivation or revocation of information related to customised security data maintained in the payment service provider's systems and databases and, where applicable, in public registers. | | |

| **Common open and secure communication standards** | | | |
|---|---|---|---|
| **Applicable by the account manager PSP in case of non-implementation of a dedicated access interface: access via the Internet online banking website with third party authentication** | | | |
| **29** | Does the PSP ensure that all transactions (authentication, consultation and payment initiation) with the payment service user, including merchants, other PSPs and other entities, are correctly traced with unique, unpredictable identifiers stamped with the date and time? | | |
| **30-1** | Has the PSP made available to third party PSPs an access interface that meets the requirements listed below?<br>- third party PSPs are able to identify themselves towards the account servicing PSP;<br>- third party PSPs are able to communicate securely with the PSP to execute their payment services. | | |
| **30-2** | Does the PSP make all authentication procedures offered to payment service users available to third party PSPs for the purposes of authentication of payment service users? | | |
| **30-2-a-b** | Does the PSP access interface meet the requirements listed below?<br>- the PSP is in a position to start strong authentication at the | | |

| | | | |
|---|---|---|---|
| | request of a third party PSP that has previously obtained the consent of the user;<br>- the communication sessions between the PSP and third party PSPs are established and maintained throughout the authentication. | | |
| **34-1** | Is the access by third party PSPs to the PSP's online banking website based on certificates marked with electronic stamps or certified authentication certificates? | | |
| **35-1** | Are the integrity and confidentiality of customised security data and authentication codes transiting through communication flows or stored in the PSP's information systems insured? | | |
| **35-5** | Does the PSP ensure that the customised security data and authentication codes they communicate are not directly or indirectly readable by a staff member? | | |
| **36-1** | Does the PSP meet the requirements listed below?<br>- it provides third party PSPs with the same information from the designated payment accounts and associated payment transactions that are made available to the payment | | |

| | | | |
|---|---|---|---|
| | service user in case of direct request for access to the account information, provided that such information does not contain sensitive payment data;<br>- immediately after receiving the payment order, they provide third party PSPs with the same information on the initiation and execution of the payment transaction as those provided or made available to the payment service user when the payment service user initiates the transaction directly;<br>- upon request, it shall immediately communicate to third party PSPs, in the form of a simple "yes" or "no" answer, whether the amount necessary for the execution of a payment transaction is available or not on the payer's payment account. | | |
| **36-2** | If an error or unforeseen event occurs 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 unforeseen event? | | |

| **Applicable by the account manager PSP in case of implementation of a dedicated access interface with a back-up mechanism (online banking access with third party authentication)** | | | |
|---|---|---|---|
| **29** | Does the PSP ensure that all transactions (authentication, consultation and payment initiation) with the payment service user, including merchants, other PSPs and other entities, are correctly traced with unique, unpredictable identifiers stamped with the date and time? | | |
| **30-1** | Has the PSP made available to third party PSPs an access interface that meets the requirements listed below?<br>- third party PSPs are able to identify themselves to the account servicing PSP;<br>- third party PSPs are able to communicate securely with the PSP to execute their payment services. | | |
| **30-2** | Does the PSP make all authentication procedures offered to payment service users available for use by third party PSP for the purposes of payment service user authentication? | | |
| **30-2-a-b** | Does the PSP access interface meet the requirements listed below?<br>- the PSP is in a position to start strong authentication at the request of a third party PSP | | |

| | | | |
|---|---|---|---|
| | that has previously obtained the consent of the user;<br>- the communication sessions between the PSP and third party PSPs are established and maintained throughout the authentication. | | |
| **30-3** | Does the PSP ensure that its access interface follows the communication standards published by European or international standardisation organisations?<br>Do the technical specifications of the access interface documentation mention a series of routines, protocols and tools that third party PSPs need to allow for interoperability between their software and applications and the PSP's systems? | | |
| **30-4** | If the technical specifications for the access interface are changed, except in emergencies, did the PSP plan to make them available to third parties at least three months prior to their implementation?<br>Do the PSP's procedures provide, in writing, for a description of the emergency situations in which the changes have been implemented and for making this documentation available to the ACPR and the BDF? | | |

| | | | |
|---|---|---|---|
| **32-1** | Does the PSP ensure that its dedicated access interface offers the same level of availability and performance, including support, than the interface(s) made available to the payment service user to directly access its online payment account? | | |
| **32-2** | Has the PSP defined key performance indicators and service level target values for its access interface that are transparent and at least as demanding as those set for the interface used by their payment service users, both in terms of availability and data supplied? | | |
| **32-4** | Are the availability and performance of the access interface controlled by the PSP and are the related statistics published on its website on a quarterly basis? | | |
| **33-1** | Has the PSP anticipated the implementation of the back-up mechanism after five consecutive requests for access to the third-party PSP's dedicated interface are unanswered 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 to restore the system, and does the PSP provide a description of the other readily | | |

| | | | |
|---|---|---|---|
| | available options that they can use in the meantime? | | |
| **33-3** | Do the PSP's procedures provide for the timely notification of issues encountered with the dedicated interface to the ACPR? | | |
| **33-5** | For access to the back-up interface, does the PSP ensure that third party PSPs are identified and authenticated according to the authentication procedures planned for its own customers? | | |
| **34-1** | Is the access of third party PSPs to the PSP's online banking website based on certificates marked as electronic stamps or certified authentication certificates? | | |
| **35-1** | Are the integrity and confidentiality of customised security data and authentication codes transiting through communication flows or stored in the PSP's information systems insured? | | |
| **35-5** | Does the PSP ensure that the customised security data and authentication codes they communicate are not directly or indirectly readable by a staff member? | | |
| **36-1** | Does the PSP meet the requirements listed below?<br>- 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 in case of direct request for access to the account information, provided that such information does not contain sensitive payment data;<br>- immediately after receiving the payment order, they shall provide 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 directly initiates the transaction;<br>- upon request, it shall immediately provide information to third party PSPs, in the form of a simple “yes” or “no” answer, whether the amount necessary for the execution of a payment transaction is available or not on the payer's payment account. | | |
| **36-2** | If there is an error or unforeseen 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 parties, indicating the reasons for the error or unforeseen event? | | |
| **Applicable by the account manager PSP in case of implementation of a dedicated access interface without an emergency mechanism** | | | |
| **29** | Does the PSP ensure that all transactions (authentication, consultation and payment initiation) with the payment service user, including merchants, other PSPs and other entities, are correctly traced with unique, unpredictable identifiers stamped with the date and time? | | |
| **30-1** | Has the PSP made available to third party PSPs an access interface that meets the requirements listed below?<br>- third party PSPs are able to identify themselves to the account servicing PSP;<br>- third party PSPs are able to communicate securely with the PSP to execute 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 purposes of payment service user authentication? | | |
| **30-2-a-b** | Does the PSP's access interface meet the requirements listed below?<br>- the PSP is in a position to start strong authenticiation at the | | |

| | | | |
|---|---|---|---|
| | request of a third party PSP that has previously obtained the consent of the user;<br>- the communication sessions between the PSP and third party PSPs are established and maintained throughout the authentication. | | |
| **30-3** | Does the PSP ensure that its access interface follows communication standards published by European or international standardisation organisations?<br>Do the technical specifications of the access interface documentation mention a series of routines, protocols and tools that third party PSPs need in order to allow for interoperability between their software and applications and the PSP's systems? | | |
| **30-4** | If the technical specifications for the access interface are changed, except in emergencies, did the PSP plan to make them available to third party PSPs at least three months prior to their implementation?<br>Do the PSP's procedures provide in writing for a description of the emergency situations in which the changes have been implemented and for making this documentation available to the ACPR and the BDF? | | |

| | | | |
|---|---|---|---|
| **32-1** | Does the PSP ensure that its dedicated access interface offers the same level of availability and performance, including support, than the interface(s) made available to the payment service user to directly access its online payment account? | | |
| **32-2** | Has the PSP defined key performance indicators and service level target values for its access interface that are transparent and at least as demanding as those set for the interface used by their payment service users, both in terms of availability and data supplied? | | |
| **32-4** | Are the availability and performance of the access interface controlled by the PSP and are the related statistics published on its website on a quarterly basis? | | |
| **33-6** | Has the PSP submitted an application for exemption from an emergency mechanism to the ACPR? | | |
| **34-1** | Is the access of third party PSPs to the PSP's online banking website based on certificates marked as electronic stamps or certified authentication certificates? | | |
| **35-1** | Are the integrity and confidentiality of customised security data and authentication codes transiting | | |

| | | | |
|---|---|---|---|
| | through communication flows or stored in the PSP's information systems insured? | | |
| **35-5** | Does the PSP ensure that the customised security data and authentication codes they communicate are not directly or indirectly readable by a staff member? | | |
| **36-1** | Does the PSP meet the requirements listed below?<br>- 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 in case of direct request for access to the account information, provided that such information does not contain sensitive payment data;<br>- immediately after receiving the payment order, they shall provide 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 directly initiates the transaction;<br>- upon request, it shall immediately provide information to | | |

| | | | |
|---|---|---|---|
| | third party PSPs, in the form of a simple “yes” or “no” answer, regarding whether the amount necessary for the execution of a payment transaction is available or not on the payer's payment account. | | |
| **36-2** | If there is an error or unforeseen 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 unforeseen event? | | |

# V- ANNEXES

## 1. Fraud risk rating matrix

*Present the methodology used for the rating of fraud risks by indicating in particular the rating matrix dedicated to the probability/frequency of occurrence and impact (financial, non-financial - in particular linked to the media) and the overall rating matrix highlighting the levels of criticality.*

## 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 system and accounting arrangements

## 1. Overview of internal control systems[19]

### 1.1. General internal control system:

- attach an organisational chart presenting the units dedicated to permanent control(s) (including compliance checks) and periodic control, and including the hierarchical position of their managers;
- expected coordination between the various persons involved in internal control actions;
- steps taken in the event of presence of the institution in a country where local regulations prevent the application of the rules stipulated in the *Arrêté du 3 novembre 2014*, as amended;
- steps taken in the case of a transfer of data to entities (such as to service providers) operating in a country that does not provide appropriate data protection;
- the procedures used to monitor and carry out control actions on transactions conducted under the freedom to provide services.

### 1.2. Permanent control system (including compliance control):

- a description of the organisation of the different levels that are involved in permanent control and compliance control;
- scope of intervention of permanent control and compliance control, including foreign business (*activities, processes and entities*);
- human resources assigned to permanent control and compliance control (Article 13, first indent of the *Arrêté du 3 novembre 2014*, as amended) (full-time equivalent staff as a proportion of the total staffing of the institution);
- description, formalised documentation and date(s) of updates to permanent control procedures, including those that apply to foreign business (including compliance checks);
- the procedures used to report to the head(s) of permanent control and to the effective managers on the activities and results of compliance control.

### 1.3. Risk management function:

- a description of the organisation of the risk management function (*scope of authority, staffing levels in the units responsible for risk measurement, monitoring and control, and the technical resources at their disposal*);
- for groups, organisation of the risk management function;
- a description of the procedures and systems used to monitor risks arising from new products and services, from significant changes in existing products, services or processes, from internal and external growth, and from unusual transactions (see Article 221 of the *Arrêté du 3 novembre 2014*, as amended);

[19] Institutions may tailor this section according to their size and organisation, the nature and volume of their activities and locations, and the types of risk to which they are exposed (in particular, when the functions of permanent and periodic control are conferred on the same person, or on the effective managers).

- summary of the risk assessment carried out by the risk management function according to appropriate scenarios with regard to the significance of risks induced by these new products and transactions.

1.4. Periodic control system:

- a description of the organisation of the internal audit function and a description of its scope of action, including for foreign business (*activities, processes and entities*);
- human resources assigned to the internal audit function (cf. Article 25 of the *Arrêté du 3 novembre 2014*, as amended) (full-time equivalent staff as a proportion of total staffing of the institution);
- if use of an external provider : frequency of intervention and size of the team;
- description, formalised documentation and date(s) of updates to procedures the audit function relies on, including those that apply to foreign business (including inspections of compliance), highlighting significant changes made during the year under review;
- methods used to set the frequency and priority of audit cycles, particularly in relation to risks identified within the institution.

## 2. Overview of accounting arrangements

- description, formalised documentation and date(s) of updates to control procedures relating to audit trails for information contained in accounting documents, information included in statements prepared for the Autorité de contrôle prudentiel et de résolution (ACPR), or when applicable for the ECB, and information needed to calculate accouting standards;
- organisation adopted to ensure the quality and reliability of the audit trail;
- the procedures used to ring-fence and monitor assets held for third parties (see Article 92 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedures used to monitor and address discrepancies between the accounting information system and the management information system.

**Annex 2**

# Measures implemented in favour of financially vulnerable customers (*Arrêté du 16 septembre 2020* approving the certification of the banking inclusion charter and overindebtedness prevention charter)

## I. Training:

1.1 Percentage of customer advisors that have, in the past year, undergone appropriate training on the specific offer, its target customers and follow-up procedures for customers who receive basic banking service: %

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

1.3 Percentage of employees who are in contact with customers that have, in the past year, undergone training on the specific arrangements in place in the institution aimed at financially vulnerable customers: %

1.4 Systematic refresher training in place for the persons referred to in 1.3 above that already received training: Yes/No

1.5 Percentage of persons acting on behalf of the institution (excluding employees) that have, in the past year, undergone appropriate training on the specific mechanisms in place aimed at financially vulnerable customers: %

1.6 Systematic refresher training in place for the persons referred to in 1.5 above that already received training: Yes/No

## II. Internal control[20]

2.1. Does the permanent control system (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 overindebtedness/detecting it? 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 points 2.1.1 to 2.1.4 all covered by the periodic control cycle? Yes / No

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

*If your answer is « No », do not answer 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)

[20] Explanatory comments to be provided in section III if the answer is « No » to either of the questions below.

**Annex 3**

# K-factors summary table

| Risk to | K-factor | Definition | IFR definition (Art. 4) | Regulatory reference |
|---|---|---|---|---|
| **Customer** | **AUM** | Assets under management | Value of assets that an investment firm manages for its clients **under** both **discretionary portfolio management** and nondiscretionary arrangements constituting **investment advice of an ongoing nature** | IFR, Art. 4, paragraph 1, indent (27) (definition); IFR, Art. 17 (calculation method) |
| **Customer** | **CMH** | Client money held | Amount of **client money** that an investment firm holds, taking into account the legal arrangements in relation to asset segregation and irrespective of the national accounting regime applicable to client money held by the investment firm | IFR, Art. 4, paragraph 1, indents (28) and (49) (definition); IFR, Art. 18 (calculation method); Art. 1 of the IFR RTS for the definition of segregated accounts |
| **Customer** | **ASA** | Assets safeguarded and administered | Value of assets that an investment firm safeguards and administers for clients, irrespective of whether assets appear on the investment firm's own balance sheet or are in third-party accounts | IFR, Art. 4, paragraph 1, indent (29) (definition); IFR, Art. 19 (calculation method) |
| **Customer** | **COH** | Client orders handled | Value of orders that an investment firm handles for clients, **through the reception and transmission of client orders** and through the | IFR, Art. 4, paragraph 1, indent (30) (definition) IFR, Art. 20 (calculation method) MiFID II, Art. 4, paragraph 1, indent |

| | | | | |
|---|---|---|---|---|
| | | | execution of orders on behalf of clients | (5) (definition of order issuance services) |
| **Firm** | **TCD** | Trading counterparty default | Exposures in the **trading book** of an investment firm in **instruments and transactions** referred to in **Article 25 of IFR**, giving rise to the risk of trading counterparty default | IFR, Art. 4, paragraph 1, indent (35) (definition)<br>IFR, Art. 25 (contracts and transactions concerned)<br>IFR, Art. 26 to 32 (calculation method and applicable models) |
| **Firm** | **DTF** | Operational risk[21] | Daily value of transactions that an investment firm enters **through dealing on own account** or **the execution of orders on behalf of clients in its own name**, excluding the value of orders that an investment firm handles for clients through the reception and transmission of client orders and through the execution of orders on behalf of clients which are already taken into account in the scope of client orders handled | IFR, Art. 4, paragraph 1, indent (33) (definition)<br>IFR, Art. 33 (calculation method) |
| **Firm** | **CON** | Concentration risk (risk of exceeding large exposure limits) | Exposures **in the trading book** of an investment firm to a client or a group of connected clients the value of which exceeds the limits in Article 37(1) | IFR, Art. 4, paragraph 1, indent (31) (definition)<br>IFR, Art. 37 (limits)<br>IFR, Art. 36 and 37 (calculation method)<br>IFR, Art. 38 (obligation to notify where limits are exceeded)<br>IFR, Art. 39 (new OF requirements in |

[21] On daily trading flow (transactions involving cash and derivative instruments)

| | | | | |
|---|---|---|---|---|
| | | | | the event limits are exceeded)<br>**Instruments listed in Art. 25** (transactions and contracts concerned, cf. K-TCD) and **all instruments in the trading book**;<br>IFR, Art. 22 (calculation of the net position for each instrument) |
| **Market** | **NPR** | Net position risk (net position margin) | Value of transactions recorded in the **trading book** of an investment firm | IFR, Art. 4, paragraph 1, indent (34) (definition)<br>IFR, Art. 22, indent (a) (calculation method)<br>CRR, Title IV, Part III, chapters 2, 3, 4 (3 standardised approaches TSA)<br>CRR, Title IV, Part III, chapter 1a (alternative standard ASA)<br>CRR, Title IV, Part III, chapter 1c (alternative methods based on AMA internal models) |
| **Market** | **CMG** | Clearing margin given | Amount of **total margin** required by a clearing member or qualifying central counterparty, where the execution and settlement of transactions of an investment firm **dealing on own account** take place under the responsibility of a **clearing member** or **qualifying central counterparty** | IFR, Art. 4, paragraph 1, indent (32) (definition)<br>IFR, Art. 23 (calculation method) |