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 2021

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. 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 the reports cover all the points 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 on a quarterly basis to the Secretary General of the *Autorité de contrôle prudentiel et de résolution* (SGACPR).

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 part relating to 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 part relating to remuneration policy and practices.

The report is 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 3).

N.B.: If the institution is supervised on a consolidated basis, or is subject to supplementary supervision for 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. 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 for the new activities;
- a description of any major changes in organisation or human resources and 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, formalisation and update of 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).

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. Article L.511-55 of the French *Code monétaire et financier*);
- specify the risk appetite framework, the modalities for its setting up and review (cf. Article L.511-93 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).

2. Significant changes made in the internal control system

If there have been no significant changes in 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 in the permanent control system for the "1st and 2nd level of control" (including the organisation of the internal control of foreign business and outsourcing)

- a description of significant changes in 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. Article 259 f) 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 in 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 in 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 in 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 in the organisation of the risk, nomination and remuneration committees (when applicable): *specify in particular for each committee the date of establishment, the composition, the term of office, the functioning modalities and the competences*;
- a description of significant changes 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 outsourcing)

- 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 in the organisation of the internal audit function;
- the main initiatives planned in the area of periodic controls (audit plan, etc.; cf. Article 259 f) 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 ethical and professional standards promoted by the institution (*indicate if 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 for informing senior management…;
- a description of processes put in place to identify, manage and prevent conflicts of interest within the institution itself as well as concerning its staff, and of the conditions for the approval and review of these processes (refer to Article 38 of the *Arrêté du 3 novembre 2014*, as amended).

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 relevant topics (cf. Article 77 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedure for reporting, by the person in charge of the internal audit function, to the supervisory body and (when appropriate) to the risk committee concerning 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.

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 their 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 regular evaluation 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. Article L. 511-60 of the French *Code monétaire et financier*);
- the procedure for determining the orientations and monitoring the implementation of the supervisory systems in order to ensure an effective 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 of the remuneration policy and its implementation (see. Article L. 511-72 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 correct 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 risk 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, functioning modalities and competence of the Remuneration Committee referred to in Article L. 511-102 of the French *Code monétaire et financier* and in part 2.4.2 of the EBA Guidelines;
- a description of the general principles of the remuneration policy established under article L. 511-72 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 30, 32 to 35, 54 to 56 of the EBA Guidelines);
- the date and results of the internal review intended to ensure compliance with remuneration policies and procedures adopted by the supervisory body (see Article L. 511-74 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:
    - criteria (relative as well as absolute, quantitative and qualitative) used to measure performance and to adjust remuneration according to risk (cf. paragraph 194 of the EBA Guidelines);
    - criteria (relative as well as absolute, quantitative and qualitative) used to define the link between remuneration and performance (cf. paragraph 194 of the EBA Guidelines);
    - policies concerning deferred remuneration;
    - policies concerning guaranteed variable remuneration exceptionally paid under the conditions laid down in Article L. 511-74 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 *Code du travail* (cf. paragraphs 144 of the EBA Guidelines);
    - existing policy for preventing circumvention of regulation by the staff through personal hedging strategies (cf. part 10.1 of the Guidelines).
    - pay gaps between women and men.
- when appropriate, a description, as well as the justification and scope of exemptions as provided in Articles 198 and 199 of the *Arrêté du 3 novembre 2014*, as amended, applied by the institution;

- 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 for staff responsible for validating and checking transactions (cf. Article 15 of the *Arrêté du 3 novembre 2014*, as amended and Articles L. 511-71 and L. 511-75 of the French *Code monétaire et financier* and Parts 12 and 14.1.3 of the EBA Guidelines);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 of the French *Code monétaire et financier* and paragraphs 202 and 218 of the EBA Guidelines) as well as the impact of the remuneration policy on capital and liquidity (cf. paragraphs 109 and 111 of the EBA Guidelines);
- the date of communication to the ACPR or, as applicable, to the ECB, of the maximum limit on the variable component of the remuneration proposed to the general meeting concerned (*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 limitation on the variable component of remuneration, as well as the justification of these choices, pursuant to Article L. 511-78 of the French *Code monétaire et financier* and to Part 2.3 of the EBA Guidelines, and mention of any possible reduction of the limit pursuant to paragraph 43 of the 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 of the French Code monétaire et financier)

Please specify:

- the categories of staff concerned;
- the amount of remuneration for the year, with a breakdown of fixed versus 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, broken down 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 specify the acquisition period or the minimum holding period for securities (cf. Articles L. 511-81, R. 511-22 and R. 511-23 of the French *Code monétaire et financier*);
- the overall amount of deferred remuneration with a breakdown between vested and unvested remuneration (cf. Article R. 511-18 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 of the French *Code monétaire et financier*);
- payments made for new hires, termination indemnities and the number of beneficiaries (cf. Article R. 511-18 of the French *Code monétaire et financier*);
- guaranteed termination indemnities granted during the year, the number of beneficiaries, and the largest amount granted to a single beneficiary (cf. Article R. 511-18 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 complete remuneration of each effective manager as well as the one of the head of the risk management function and, when appropriate, 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. Articles 267 and 268 of the *Arrêté du 3 novembre 2014*, as amended, and Part 4 of the EBA Guidelines).

4. Results of periodic controls conducted during the last reporting period, including concerning foreign business (cf. Article 17 of the *Arrêté du 3 novembre 2014*, as amended)

- the missions' programme (risks and/or entities that have been to the subject of checks by the internal audit function during the last reporting period), stage of completion and resources allocated 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 regular checks (*tools, persons in charge*) and the results 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 details on 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) of the *Arrêté du 3 novembre 2014,* as amended)

An annex shall be attached, providing the following:

- **the characteristics of commitments for which a deduction has been made from regulatory capital**: the identity of the beneficiaries, type of beneficiaries (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.

6. Process for assessing the adequacy of internal capital

This section is not mandatory for institutions included in consolidation and exempted from meeting management ratios on a solo or sub-consolidated basis.

- a description of the scope of activities relevant for assessing the capital adequacy and the scope of the approach used to determine the materiality of risks;

- a description of methodologies used to measure, assess and aggregate risks for quantifying internal capital (analysis horizons, economic value approach, description of models and calculation parameters…). This description shall include explanations regarding 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 implemented to ensure that the amount and distribution of internal capital corresponds to the nature and level of the risks to which the institution is exposed, *with particular emphasis on risks that are not taken into account in Pillar 1* (cf. Article 96 of the *Arrêté du 3 novembre 2014*, as amended);
- description of the establishment and update of a capitalisation plan aimed at ensuring a sufficient amount of internal and regulatory capital for 3 years at least, including in adverse conditions (stress tests):
    - level and definition of the internal capital allocated to each type of risks for the last reporting period detailing the main differences between internal capital and regulatory capital, as well as the methods and assumptions used for the allocation of capital within the institution;
    - projections on the internal capital level;
- stress tests to assess the adequacy of internal capital:
    - description of the scope and building process of stress tests: *scope (entities and risks taken into account), frequency of application, 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 for taking into account stress tests in decision-making processes, especially in terms of risk appetite, capital planning and the determination of limits;
- internal control procedures for verifying that these systems and procedures remain in line with the evolution of the institution's risk profile;
- documentation that formalises the preparation and validation process for internal capital adequacy, as well as the assumptions, capitalisation plan, stress tests and methodologies used in the process, including the allocation of responsibility as well as the information to and involvement of management and/or supervisory bodies in the validation step;
- documentation formalising the integration of this process in the global strategy of the institution, including by integrating issues regarding internal capital and risk appetite in the decision-making process through appropriate reporting;
- institutions subject to the CRR that are not under the ECB's direct supervision shall provide a "reader's guide", drawn up as a comprehensive document aimed at facilitating the assessment of the documentation that justifies 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, modified with minor corrections, etc.). The "reader's guide" shall esentially function as an index connecting specific pieces of information required for the report on internal control to the documents sent to the competent authority regarding the capital adequacy assessment. The "reader's guide" shall also include information regarding significant changes made to the information compared with what was submitted previously, elements possibly excluded from information provided and any other information that could be useful to the competent authority for 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.

7. Non-compliance risk (excluding the risk of money laundering and terrorist financing)

Reminder: *information regarding the risk of money laundering and terrorist financing shall be sent in the dedicated annual report on the organisation of internal control arrangements on AML-CFT and asset freeze, according to Articles R. 561-38-6 and R. 561-38-7 of the French Code Monétaire et Financier, according to conditions 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 the reputational risk

7.3. Other non-compliance risks (including regarding 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) of shortcomings or breaches of prudential rules 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, of 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 remedial 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 main deficiencies identified during the reporting period

7.8. Results of 2nd level permanent control on the 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 special 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 limiting mechanism;
- policy for approving housing loans granted to French customers, in particular criteria regarding the repayment burden as a percentage of borrowers' disposable income, loan-to-value ratios and loan maturities.

8.2. Systems for measuring and monitoring risks

- stress scenarios used to measure incurred risk, selected assumptions, results and description of their operational integration;
- overview of exposure limits – by beneficiary, by associated debtors, by business lines etc. (*specify the size of the 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 size of the overall exposure, the number of breaches, and their amounts*);
- 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 arrangements for monitoring advanced risk indicators (*specify the main criteria for placing counterparties under watch-list*);
- the procedure used for analysing the quality of credit commitments, and the frequency of such analysis; the potential reclassification of commitments within internal risk assessment categories shall also be specified, as well as changes in allocation towards accounting items dedicated to doubtful or impaired loans, any adjustments made to the level of provisioning, and the date on which this analysis was carried out for the last reporting period;
- ajustments made by the institution in order to comply with the EBA Guidelines on the application of the definition of default that came into force on 1 January 2021;
- the procedures and frequency of revaluation of guarantees and collaterals, as well as the main results of controls carried out during the year when appropriate;
- a presentation of the credit risk measurement and management system in place for identifying and managing problem credits and for making adequate value adjustments and recording appropriate amounts for provisions or losses (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 above 5%: presentation of the strategy for the management and reduction of non-performing exposures (*action plan and schedule, assessment of operational environment, quantitative targets, short-term objectives, medium and long-term objectives, objectives by main portfolios, objectives 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 process for restructuring exposures *(criteria taken into account in the restructuring decision, deadlines applied, control procedures in place to ensure the viability of the restructuring measures taken…*) and modalities for monitoring foreborne exposures including key performance indicators (*non-performing exposure parameters, forbearance activities, liquidation activities, agreement to pay, borrower's agreement to pay and liquidity collection…*);
- description of the process used for the accounting assessment of 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 for and frequency of back-testing exercises for collective and statistical provisioning models, as well as the main results of the year when appropriate;
- the procedure used for analysing the risk of loss on leased assets (financial leasing) and the frequency of the analysis;
- the procedure used for analysing risks of impairment losses for financed immovable 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 the analysis (at least, for counterparties the loans of which are overdue, non-performing or impaired, or 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 to the effective managers, the supervisory body and, where applicable, the risk committee, on the level of credit risk, using summary tables (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 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);

- factors considered in analysing changes in margins, in particular for loan production in the past year: *methodology, variables analysed, results;*
    - provision of details on the calculation of margins: earnings and expenses taken into account; if lending needs to be refinanced, indicate the net borrowing position and the retained refinancing rate; if there are gains from investing capital allocated to lending, specify the amount and the rate of return;
    - identification of the different outstanding loan categories (such as retail loans, with housing loans highlighted) or of business lines for which margins are calculated;
    - highlight trends in outstanding loans (at year-end and intermediary dates) and, where appropriate, in loan production for the past year;
- the procedures used by the effective managers to analyse the profitability of lending activities, the frequency of the analyses, and their results (*specify 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 produced for the supervisory body*);
- the procedures used to monitor housing loans granting criteria for French customers;
- a breakdown of housing loans according to the type of guarantee (credit bonding, mortgage, etc.);
- a presentation of the LTV ratio of housing loans according to the type of guarantee (at origination, on average and after revaluation of collaterals);
- the procedures for approval by the supervisory body, assisted, where applicable, by the risk committee, of the limits suggested 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 and frequency for analysing, assessing and monitoring risk linked to intragroup transactions (credit risk and counterparty credit risk)

<u>Specific elements on counterparty credit risk:</u>

- a description of risk metrics used to assess the counterparty credit risk;
- a description of the integration of counterparty credit risk monitoring within the global measures for credit risk monitoring.

8.3. Concentration risk

8.3.1. Concentration risk by counterparty

- tool used for monitoring 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 counterparties' interconnectedness), and procedures for reporting to the effective managers and the supervisory body;
- system used to limit exposure within the same business sector: a general description of the system in place for setting limits on sectorial concentration (*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 monitoring of limits;
- distribution 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 tool used for monitoring geographical concentration risk: any aggregate measures defined, description of the system used to measure exposures in the same geographical region, and procedures for reporting to the effective managers and the supervisory body;
- the system for limiting exposure within the same geographical region: a general description of the system for setting 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;
- distribution of exposures by geographical region;
- 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

- back-testing and comparisons with external data to ensure the accuracy and consistency of internal rating systems, including the methodologies and parameters used;
- the contents and frequency of the permanent control and regular reviews conducted on internal rating systems;
- a description of the operational integration of rating systems ('use test'): the actual use of the parameters generated by the internal rating system in loan approval, loan pricing, loan collection, risk monitoring, provisioning, allocation of internal capital, and corporate governance (including the elaboration of management reports for the effective managers and the supervisory body);
- the procedures for involving the effective managers in the design and update of internal rating systems: including approval of methodologies, ensuring a sound command of the design and operation of the system, and how information relating to the monitoring of these systems' operation are escalated to them;
- a demonstration proving that the internal credit risk assessment methodologies do not rely solely or mechanistically on external credit ratings (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) estimation, loss given default (LGD) estimation, and the treatment of defaulted assets, and, on the other hand, the EBA Guidelines on the estimation of LGD under an economic downturn.

8.5. Risks associated with securitisations

- a presentation of the institution's securitisation and credit risk transfer strategy;
- a presentation of the internal policies and procedures put in place to ensure, before investing, that there is an in-depth knowledge of securitisation exposures and that institutions comply with the requirement to retain 5% of the net economic interest when acting as originator, sponsor or original lender;
- the procedures for assessing, monitoring and controlling the risks associated with securitisations (in particular, an analysis of their economic substance) for institutions that act as originators, sponsors or investors, including via stress tests (assumptions, frequency, consequences);
- for originating banks, description of the internal process used to assess prudentially deconsolidating operations, supported by an audit trail and by the procedures for monitoring risk transfer through a regular review over time.

8.6. Intraday credit risk

Risk incurred in the business of custody by institutions that grant loans to their customers, in cash or securities, during the course of the day to facilitate the execution of securities transactions[1].

- a description of the institution's policies aimed at managing intraday credit risk; a description of limits (procedures for setting and monitoring limits);
- a presentation of the system used to measure exposures and monitor limits on an intraday basis (including the management of any breaches of limits);
- the procedures for granting intraday credit;
- the procedures for assessing the quality of collateral;
- a description of the procedures for reporting to the effective managers and the supervisory body;
- the conclusions regarding risk exposure to intraday credit risk.

8.7. Results of 2nd level permanent control actions for credit activities

- main shortcomings observed;
- measures taken to remediate the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress of that implementation process as at the date of drafting of this Report;
- the procedures for following up on the recommendations issued following permanent control actions (*tools, persons in charge,* etc.);
- the procedures for verifying 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;

1 Intra-day credit risk also covers overnight credit risk for transactions settled during the night.

- a general description of the procedures used to ensure, when credit risk mitigation instruments are put in place, that they are legally valid, that their value is not correlated with that of the mitigated exposure, and that they are properly documented;
- a presentation of the procedures integrating the credit risk associated with the use of credit risk mitigation techniques in the overall credit risk management system;
- a description of stress tests conducted on credit risk mitigation techniques (including the assumptions and methodologies used and the results obtained);
- a summary of incidents that occurred during the year when appropriate (guarantee calls refused, unrealised pledges).

8.9. Stress testing for credit risk

Attach an annex describing the assumptions and methodologies used (including the procedures for considering contagion effects in other markets) and summarising the results obtained.

8.10. Overall conclusions on credit risk exposure

9. Risks linked to OTC derivative contracts

9.1 Techniques of risk mitigation for OTC derivative contracts not cleared by a central counterparty:

- description of procedures and arrangements used 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 identify disputes between parties early and resolve them, and 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);
- 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);
- 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);
- description of procedures used for the calculation and collection of variation margins;
- description of procedures used for the calculation and collection of initial margins;
- description of models used for the calculation of initial margins;
- description of criteria used for the selection of the collateral exchanged;
- description of methods used for the valuation of collateral;
- description of operational procedures and contractual documentation used for collateral exchange;
- description of the number, volume and evolution of observed collateral disputes with counterparties with which collateral is exchanged, as well as resolution procedures for these disputes;
- 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 Management and monitoring procedures of risks linked to intragroup transactions

- 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;

- description of risk management procedures linked to intragroup transactions 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;
- description of significant changes that could affect the fluidity of own funds transfers or of liabilities repayment 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). Include details on observations or anticipations regarding States for which the situation has significantly changed in this respect;
- information on intragroup transactions carried out during the year and benefiting from the exemptions provided for in paragraphs 6, 8 or 10 of Article 11 of 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. System for measuring market risk

- booking of market transactions; calculation of positions and results (*specify the frequency*);
- comparisons between risk management and accounting results (*specify the frequency*);
- comparisons between prudent valuation, as defined in the Commission Delegated Regulation (EU) 2016/101 of 26 October 2015, and accounting valuation of the portfolio, booked at the fair value of assets;
- assessment of the risks arising from positions in the trading book (*specify the frequency*);
- the procedures for capturing different 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. System for monitoring market risk

- roles of the effective managers, the supervisory body and, when applicable, the risk committee, in identifying the institution's overall strategy regarding market risk and current and future market risk appetite (cf. Articles L. 511-92 and L. 511-93 of the French *Code monétaire et financier*), and the setting up of limits (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended);
- 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 general description of the limits set for market risk (specify the level of limits, by type of risk incurred, in relation to own funds and earnings);
- the frequency with which limits on market risk are reviewed (*indicate the date of the most recent review during the past year*); identity of the body responsible for setting limits;
- the system used for monitoring procedures and limits;

- any breaches of limits noted during the past year (*specify their causes, the number of breaches, and their amounts*);
- the procedures used for authorising such breaches and the measures taken to resolve them;
- the procedures used for reporting 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 activities (*specify the date of the most recent analysis*) and on the level of risk incurred, including the amount of internal capital allocated and the adequate level of internal capital for 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.

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

- main shortcomings observed;
- measures taken to remediate the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress of their implementation as at the date of drafting of this Report;
- the procedures for following up on the recommendations issued following permanent control actions (*tools, persons in charge, etc.*);
- the procedures for verifying 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

For institutions that use their internal models to calculate capital requirements for market risk, attach an annex describing the assumptions and methodologies used and summarising the results obtained; this annex shall provide a comprehensive description of any changes made to the model during the previous year, distinguishing between those identified as material and those identified as non-material, according to the definitions of the Commission Delegated Regulation (EU) 2015/942 of 4 March 2015, and shall explain to what extent the internal control was the motive behind such changes or not.

10.5. Overall conclusions on exposure to market risk

11. Operational risk

11.1 Governance and organisation of operational risk

- general 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 the operational risk and of the governance of the model when appropriate, role and missions of the various committees established, structuring decisions taken during the year regarding operational risk;
- organisation: presentation of the various teams in charge of the permanent control of 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 encountered and solutions planned/implemented during the implementation phase of these reorganisation projects, goals to be achieved and planned schedule for the full deployment within the target organisation;

- entities' scope: integrated entities and methods (in numbers and in proportion of assets), treatment of entities integrated in the scope of prudential consolidation during the last two financial years, entities potentially excluded and reasons for the 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 (*specify the method used to calculate capital requirements*);
- the monitoring mechanisms used to ensure that all incidents to be listed are taken into account in the calculation of own funds requirements, especially regarding legal and non-compliance risks; identification of risks requiring an improvement of the current monitoring mechanism 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 general description of the reports used to measure and manage operational risk (*specify in particular the frequency of reporting and recipients of the reports, the areas of risk covered, and the use of early warning indicators to signal 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, procedures and criteria used for mapping the relevant indicators for business lines, reviewing procedures for new business activities or changes to existing ones;
- for institutions using an advanced measurement approach, a description of the methodology used (*including the factors related to internal control and to the environment in which they operate*) and any changes in methodology made during the course of the year, as well as a description of the procedures used for the quality control of historic data;
- a general description of any insurance techniques used;
- a review of the current discussions on the changes that the institution has to anticipate concerning the calculation methods used for regulatory requirements regarding operational risk.

11.3. Integration of the system for measuring and managing operational risk in the permanent control system

- a description of the procedures for integrating operational risk monitoring into the permanent control system, including, inter alia, risks related to low-frequency high-severity events, internal and external fraud risks set out in Article 324 of Regulation (EU) No 575/2013 and the risks related to the model risk defined in Article 4 of delegated Regulation (EU) No 2018/959;
- a description of the main actual operational risks observed during the course of the year (settlement incidents, errors, fraud, cybersecurity etc.) and the lessons learned from them.

11.4. Emergency and business continuity plans

- objectives defined for the emergency and business continuity plans, definitions and scenarios used, overall architecture (one comprehensive plan versus one plan per business line, overall consistency in the case of multiple plans), responsibilities (*names and positions of the officers responsible for managing and triggering emergency and business continuity plans and for managing incidents*), scope of business covered by the plans, activities with a high level of assigned priority in the event of an incident, residual risks not covered by the plans, timetable for implementing the plans;
- formalisation of procedures, general description of fall-back and backup IT facilities;
- tests of emergency 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 emergency and business continuity plans and results of permanents controls;
- activation of the emergency and business continuity plan(s) and management of incidents occurring during 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

- presentation of the institution's IT strategy (organisation, coordination with the overall strategy, priority objectives and actions plans set up, appetite framework for risks…) and resources dedicated to its implementation (procedures put in place to ensure its compliance, dedicated budget and its 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;
- 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

- presentation of the risk mitigation techniques used for major IT risks, presentation of control measures to monitor the efficiency of these techniques and description of the process followed to inform effective managers and the supervisory body;
- presentation of the organisation of the management of the IT risk (definition of the roles and responsibilities of players[2], assessment framework for the IT risk profile and its results, risk tolerance threshold, audit process, modalities and frequency of reporting to senior management and the supervisory body on the entity's exposure to IT risks[3] …);
- description of the periodic and permanent control mechanisms used for IT systems and summary of the observations derived from controls carried out (cf. 11.6);
- presentation of the IT risk mapping, including especially risk regarding the availability and continuity, security and data integrity as well as the risk linked to the IT system changes (identifying in particular what systems and services are essential to the proper functioning, availability, continuity and security of the institution's activities)[4].

11.5.3. Security of the IT system

- presentation of the objectives of the information systems security policy (protection of the 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 impact the activity of the institution), in particular for major incidents[5] (mechanisms for physical and logical security, for the preservation of data integrity and confidentiality, specific measures put in place for online banking activities, description of penetration testing carried out during the financial year, IT recovery plan…);
- presentation of the process for informing the supervisor in case of major incidents;
- presentation of the IT security awareness programme (for both employees and service providers) and of the regular training sessions.

[2] Especially those of the IT function.

[3] Attach the latest dashboard used that is dedicated to informing them

[4] In particular, specify whether the institution is exposed to specific risks and the specific measures taken to manage them

[5] i.e. those with a financial impact of more than EUR 25 million or 0.5% of the CET 1. For example, a cyber attack.

11.5.4. Management of IT operations

- description of the IT operation management processes : presentation of the processes covering the operation, monitoring and control of IT services and systems;
- description of the process used for the detection and management of operational or security incidents.

11.5.5. Change management and project management

- description of the framework for the conduct of IT projects and software;
- description of the management process dedicated to the acquisition, development and maintenance of IT systems, description of a process dedicated to managing IT software changes (method used to record, test, assess, approve and implement changes made to the IT system).

11.6. Results of 2nd level permanent controls on operational risk including the IT risk

- main shortcomings observed;
- measures taken to remediate the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress of their implementation as at the date of drafting of this Report;
- the procedures for following up on the recommendations issued following permanent controls (*tools, persons in charge, etc.*);
- the procedures for verifying 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

12. Accounting risk

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

If there have been no significant changes in the accounting system, the institution may provide a general description of the accounting system in an annex.

- presentation of modifications that have taken place within the consolidation scope when appropriate (admission and exclusion)

12.2. Results of 2nd level permanents controls on accounting risk

- main shortcomings observed;
- measures taken to remediate the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress of their implementation as at the date of drafting of this Report;
- the procedures for following up on the recommendations issued following permanent controls (*tools, persons in charge, etc.*);
- the procedures for verifying 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);
- presentation of the accouting risk prevention system, including the risk of disruption of information systems (backup site…).

13. Overall interest rate risk

- a general description of the overall framework used for identifying, assessing and managing the overall interest rate risk (*specify the entities and transactions covered, justifying the role of the effective managers and supervisory body as well as the distribution of competences regarding control of the overall interest rate risk*);
- a description of and justification for the possible use of the principle of proportionality in light of the volume, complexity, risk appetite and risk level of their positions sensitive to the 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 capital for the interest rate risk (taking into account both the impact on economic value and on earnings[6]);
    - measurement and monitoring of the interest rate risk (especially using internal and appropriate shock scenarios as referred to in paragraphs 90 to 102 of the EBA Guidelines and using the proportionality measures set out in the "sophistication matrix" 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 the interest rate risk referred to in paragraphs 44 (c) and 44 (d) of the EBA Guidelines);
    - governance arrangements (adaptation of reports to the management body according to the institution's activities, referred to in paragraph 68 of the EBA Guidelines).

13.1. Systems and methodologies for measuring and monitoring overall interest rate risk

- a description of the tools and methodologies used to manage the overall interest rate risk (*specify the methods used by the institution, such as static or dynamic gap analysis, sensitivity in terms of earnings, 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 99 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 behavioural assumptions used by the institution [*specify their scope of coverage, main assumptions retained, treatment of new production, products not bearing interest (such as own funds), automatic (explicit or implicit) and behavioural options, especially the treatment of non-due deposits (presentation of the methodology used for the segmentation of deposits by categories as well as the identification of stable deposits), early withdrawals and regulated savings products]*;
- a presentation of coverage activities: (*specify 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 own funds' with a uniform shock of +/-200 bps and with the six currency-specific shocks as described in Annex III to the EBA guidelines - *main assumptions*:
    - Shocks applied with integration of a post-shock floor starting with -100 bps (in accordance with paragraph 115 (k) of EBA guidelines)[7],
    - calculation on the economic value of the institution's own funds, taking into account only non-trading activities (except in the case of specific cases of small portfolio activities), including

[6] As specified in paragraph 23 of the EBA Guidelines (EBA/GL/2018/02), 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 (earnings and economic value).

[7] The post-shock floor starting at -100 bps (see paragraph 115) does apply to the two series of Supervisory Outlier tests (+/-200 undifferentiated bps and 6 differentiated shocks per currency).

assets of pension bonds and pension funds (except for the treatment of the overall rate risk within a specific framework);

- excluding own funds of liabilities items (CET 1 instruments and other permanent own funds without a call date) and applying a ceiling on the average revision date of overnight deposits interest rates with a 5 year cap[8];
- Refer to paragraph 115 of the EBA guidelines for the exhaustive list of assumptions for the economic value of own funds for the "Supervisory outlier test";

- a presentation of the results of the "Supervisory outlier test" according to the uniform shock +/-200 bp applied to 20% of the institution's own funds total;
- a presentation of the results of the "Supervisory outlier test" according to 6 differentiated foreign currency shocks detailed in Annex III of the EBA Guidelines and applied to 15% of the institution's TIER 1 capital;
- a description of the results of global interest rate risk measuring indicators used by the institution:
  - *specify the static or dynamic gaps levels, the results of sensitivity calculations in terms of earnings, of net present value and of stress scenarios),*
  - *for the calculation of the economic value, provide a justification for any differences with the standardised assumptions described in the framework of the "Supervisory outlier test",*
  - *for the calculation of earnings measurement, according to the underlying assumptions used by the institution for its internal management of the overall interest rate risk, with a projection basis comprised between one and five years, using at least one basis scenario and one more adverse scenario as stated in paragraph 15 of the EBA Guidelines (also refer to the sophistication matrix in Annex II of the EBA guidelines). Presentation of the assumptions used.*

Annex 1 of this document provides an example, for institutions that do not have their own methodology, of methods that could be used to calculate the consequences of a uniform shock of +/-200 bps. The impact of the shock on the economic value of own funds is related to the institution's regulatory own funds;

- the sensitivity of the shock's results to a change in the underlying assumptions used (*specify the impact of the various (parallel and non-parallel) movements of the rates curve, the impact of the differences between different benchmark rates (basis risk) and that of changes to the retained assumptions and disposal conventions);*
- 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 rate scenarios used by the institution (for example, flattening, steepening, inversion, short rate shocks, etc.) and the results on economic value and income.

13.2. System for monitoring the overall interest rate risk

- for earning measures and economic value measures, a general description of the limits set regarding the overall interest rate risk (*specify the nature and level of the implemented limits, for example in terms of gap, in terms of sensitivity in relation to capital or earnings, the date when the limits were reviewed during the past year, and the procedure for monitoring breaches of limits*);
- a general description of the reports used to manage the overall interest rate risk (*specify in particular the frequency and recipients of the 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 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 the limits (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended).

[8] The 5-year cap applies to the overall level, per currency and volume weighted average (see final report on the 2018 EBA guidelines, Summary of EBA responses to the consultation - Question 9)

13.3. Permanent control system 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;
- measures taken to remediate the shortcomings observed**,** the 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 following 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 of the credit spread risk in the banking book (CSRBB)

- description of the monitoring and assessment of positions affected by the credit spread risk in the banking book: *specify the scope and appropriateness of the institution's risk profile, indicators and methodology applied.*

13.6. Overall conclusions on exposure to overall interest rate risk

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 (security taken, margin calls on 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 intermediation risk exposure limits - by beneficiary, by related debtors, etc. (specify the level of the limits in relation to the volume of transactions of the beneficiaries and in relation to the own funds);
- the procedures and frequency with which the limits on intermediation risk are reviewed (*specify the date of the most recent review*);
- any breaches of credit limits observed during the past year (*specify their causes, the counterparties involved, the size of the overall exposure, the number of breaches, their duration and their amounts*);
- the procedures for authorising such breaches and the measures taken to resolve them;
- the factors analysed to assess the risk associated with the principal when taking an exposure (*methodology, data analysed*);
- a typology of the errors that have occurred in 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 for documenting 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 for measuring settlement/delivery risk (*highlighting the various phases of the settlement process and the treatment of new transactions in addition to pending transactions, etc.*);
- a general description of the settlement/delivery risk limits (*specify the level of the limits, by type of counterparty, in relation to the counterparties' transaction volumes and in relation to capital*);
- the frequency with which settlement/delivery limits are reviewed (*specify the date of the most recent review*);
- any breaches of limits noted during the past year (*specify their causes, the number of breaches, and their number, duration and amounts*);
- the procedures for authorising such breaches and the measures taken to regularise them;
- an analysis of outstanding items (*indicate their anteriority, their causes, and the action plan for clearing them*);
- the results of permanent controls on settlement/delivery risk;
- main conclusions of the risk analysis conducted.

For investment services providers that guarantee performance:

- a description of the different instruments covered and of each settlement system used, identifying the various phases of the settlement process;
- the procedures for monitoring cash and securities flows;
- the procedures for monitoring and treating outstanding items;
- the procedures for measuring funding sources, securities and cash that can easily be transferred to ensure that exposures to counterparties can be covered**.**

16. Liquidity risk

- a general description of the overall framework for identifying, measuring, managing and monitoring liquidity risks: *specify the scope of the framework in terms of entities and transactions, taking into account the off-balance sheet exposures, the role of the effective managers and the supervisory body, and the division of responsibilities pertaining to the management of liquidity risks, the risk profile and the 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 the sources of funding used by the institution (*specify the various funding channels and the intragroup funding links their amounts, maturities, main counterparties and use of liquidity risks 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 in a third country, specify how the internal methodology takes into account the systemic repercussions that could result from the significance of the institution on its market, especially in each Member States of the European Union where it carries out its business (cf. Article 150 of the *Arrêté du 3 novembre 2014*, as amended).

16.1. Tools and methodologies for measuring liquidity risks

- a description of the tools and methodology used to manage liquidity risks: *specify the assumptions and maturities adopted to estimate the indicators used by the institution (cf. Article 156 of the* Arrêté du 3 novembre 2014, as amended*) taking into account the complexity of activities, risk profile and risk tolerance of the institution, describiung information systems, tools and indicators used for each currency in which the institution conducts significant activities and specifying the alternative scenarios as provided for in Article 168 of the* Arrêté du 3 novembre 2014, as amended;

- financing companies shall provide an annex to their Internal Control Report which includes:
  - a description of the characteristics and assumptions used to construct a projected cash-flow statement, and any changes in these characteristics and assumptions made during the year;
  - an analysis of changes during the year in the liquidity gaps computed on the basis of cash flow statements.
- when applicable, a description and justification of the scenarios that are specific to certain foreign institutions, legal entities or business lines (cf. Article 171 of the *Arrêté du 3 novembre 2014*, as amended);
- information on deposits and their diversification (*in terms of the number of depositors*);
- description of the assumptions used to constitute the stock of liquid assets in connection with the system of limits concerning the liquidity risk;
- description of the means implemented to ensure that the institution is always aware of the stock of liquid assets needed, and the assumptions used to adjust this stock level to the different time horizons under consideration;
- description of the methodology used regarding regular assessment, in accordance with Article 23 of Delegated Regulation (EU) 2015/61, as amended, on liquidity coverage requirements (LCR) for credit institutions, 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 which would not be considered in Decision 2016-C-26 of the ACPR;
- the procedures for taking into account the internal cost of liquidity and analysis of the evolution of liquidity cost indicators during the past financial year;
- procedures for taking into account, assessing, monitoring and supervising intra-day liquidity risk;
- description of financing plans (methods for assessing the institution's ability to raise funds from its funding sources under normal conditions and in periods of stress for all maturities and all currencies (*underlying assumptions, test results,* etc.), procedures for taking into account reputation risk;
- description of the stress scenarios used to measure the risk incurred in the event of significant variations in market parameters (indicate the assumptions used, the frequency with which they are reviewed, and the process for validating them; summarise the results of the stress tests and the procedures for reporting them to the supervisory body), as well as main conclusions of the analysis of the risk incurred in the event of significant variations in market parameters;
- description of contingency plans implemented in order to face a liquidity crisis (this plan has to take into account both the own funding risk, the risk of markets drying up and the interactions between these two risks, integrating also the dimension of intra-day liquidity risk when appropriate): *specify procedures implemented (identity and hierarchic level of persons concerned, solutions to access the liquidity considered, communication to the public, regular tests of contingency plans…)*;
- description of the liquidity restoration plans setting up the strategies and measures implemented in order to address a potential liquidity shortage, which should be regularly tested: *specify the operational measures used to ensure an immediate implementation of these recovery plans (holding immediately available collateral…)*.

16.2. System for monitoring liquidity risk

- a general description of the limits on liquidity risks and the liquidity risk tolerance level (*specify and justify the levels by type of business, by currency and by type of counterparty, in relation to the counterparties' transaction volume and in relation to capital*);
- the procedure and frequency with which limits on liquidity risk are reviewed (*specify the date of the most recent review, contributors, method applied*);
- the frequency of review of the criteria 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 financing situation, the liquidity positions and the risk mitigation factors *(specify the date of the most recent review)*;
- any breaches of limits noted during the past year (*specify their causes, the number of breaches, and their amounts*);
- the procedures for authorising such breaches and the measures taken to remediate them;
- a general description of the reports used to manage liquidity risk (*including their frequency and recipients*);
- a description of incidents that occurred during the last financial year;
- a description of the quality and composition of liquidity buffer measurement and management systems and a description of the measurement and monitoring systems for encumbered and unencumbered assets;
- control processes carried out by the risk management function on liquid assets;
- the procedures for the approval and review by the supervisory body of the strategies and policies for taking up, managing, monitoring and mitigating 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 global document to facilitate the inspection of the documentation that justifies 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, modified with minor corrections, etc.). The "reader's guide" shall mainly have the same function as an index connecting specific pieces of information required for the report on internal control to the documents sent to the competent authority regarding capital adequacy assessment. The "reader's guide" shall also include information regarding significant changes made to the information compared with those sent previously, elements possibly excluded from information provided and any other information that could be useful to the competent authority for the assessment. Furthermore, the "reader's guide" shall provide references for any information made public by the institution on its capital adequacy.

16.3. Liquidity risk and pro-cyclicality arising from margin calls due to central clearing by clearing members or due to exposures that are not centrally cleared

- presentation of the procedures aimed at avoiding for the provision of central clearing services to customers to trigger sudden and significant changes in terms of margin calls, margin collection and credit rating downgrades;
- presentation of the procedures aimed at avoiding for the risk management procedures of OTC derivatives and securities financing transactions not cleared by a central counterparty to trigger sudden and significant changes with respect to margin calls, margin collection and credit ratings downgrades;
- presentation of the procedures aimed at limiting liquidity constraints linked with margin collection (for example, using the excess initial margin collateral rather than collecting additional collateral, taking into account customers' operational constraints).

16.4. Permanent control system for the management of liquidity risks

- presentation of the control environment 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 observed;
- 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 for following up on the recommendations issued following permanent control actions (*tools, persons in charge, etc.*);
- the procedures for verifying 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 conclusions on exposure to liquidity risks

- institutions subject to the CRR and 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.

17. Risk of excessive leverage

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

- a description of policies, processes and indicators (including leverage ratio and mismatches between assets and obligations) used for identifying, managing, and monitoring the risk of excessive leverage in a prudent manner (cf. Article 211 of the *Arrêté du 3 novembre 2014*, as amended);
- the leverage ratio target determined by the institution;
- the stress scenarios used to assess the institution's resilience in case of a reduction of its own funds through expected or realised losses (cf. Article 212 of the *Arrêté du 3 novembre 2014*, as amended), including plans to strengthen own funds under stressed circumstances.

18. Internal control system relating to the protection of customers' funds invested by investment firms

- mode of organisation for the management of customer cash accounts and articulation (allowing to trace the different flows chronologically) with the execution of investment or clearing services;
- presentation of the method used to protect assets received from customers in accordance with current regulations (i.e. *Arrêté du 6 septembre 2017* on client funds the ring-fencing of customer funds by investment firms) and a description of the tool used for the calculation of the amount of assets received from customers that need to be ring-fenced;
- for institutions ensuring the protection of received assets by placing them in one account, or more, opened specially for this purpose at a credit institution: communication of account agreement(s) for ring-fencing and of any changes made to the account agreement for ring-fencing previously transmitted, description of procedures to ensure the investment of funds;
- for institutions ensuring the protection of funds received under a guarantee: communication of any modification to the collateral arrangement or guarantee contract and any element linked to the adjustment of the amount of the coverage created in respect of the evolution of the business volume;
- 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;

- presentation of the procedures implemented to ensure compliance with the provisions relating to the protection of the assets of investment funds' customers, verifications associated with and presentation of possible incidents or insufficiencies highlighted by these verifications;
- communication of the single manager with the necessary skills and authority, specifically responsible for issues relating to the institution's compliance with its obligations relating to the safeguarding of client financial instruments and funds, in accordance with Article 9 of the *Arrêté du 6 septembre 2017* on the ring-fencing of investment firm clients' funds;
- communication of the report issued by the statutory auditors on compliance with the regulatory provisions on ring-fencing.

19. Provisions for banking separation

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 recalled that the mandates of the internal units mentioned in the mapping 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 to the SGACPR (ii) at a minimum, the updated mandates of those internal units. It is also possible to submit all mandates, highlighting substantial changes since the last submission to the SGACPR.

19.1. Mapping of trading activities in financial instruments

- communication of the updated mapping of internal units in charge of operations in financial instruments as mentioned in Article 1 of *Arrêté du 9 septembre 2014* within the smallest scale of business organisation, identifying any groupings that were made. The mapping shall at least mention the following elements:
    - literal name of the smallest organisational level,
    - summary description of activities carried out,
    - category(ies) of separation exemptions as provided for in Article L.511-47 of the French *Code monétaire et financier*,
    - number of traders,
    - GNP generated over the year,
    - main risk limits (VaR, other internal measures), average and maximum use of these limits over the course of the year,
- description of the mapping evolutions,
- description of the main new activities and ceased activities.

19.2. Monitoring indicators

- a description of the indicators in place to monitor the 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 of the indicators put in place and the analysis carried out over the course of the past year (identifying atypical desks).

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

- description of activities, specifying especially the business lines chosen internally by the institution to classify transactions with Collective Investment Undertakings (CIU) and other similar vehicles using leverage on a substantial basis;
- inventory of leverage funds:

	Number of funds
A. CIUs or similar foreign vehicles through which the institution is exposed to credit or counterparty risk	
A.1. that directly or indirectly employ leverage on a substantial basis and not explicitly excluded	
A.1.a. that employ leverage on a substantial basis[9]	
A.1.b. significantly invested in or exposed to[10] CIUs or other similar vehicles that employ leverage on a substantial basis	
A.2. that do not directly or indirectly employ leverage on a substantial basis or explicitly excluded	
including: explicitely excluded under Article 7, paragraph I, sections 1 to 4 of the Arrêté du 9 septembre 2014	

- specify at which frequency CIUs and similar vehicles are inventoried and categorised within the abovementionned classes;

- assessment of results and risks generated (credit and counterparty risks):

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

- summary of transactions broken down by transaction type:

Expressed in thousands of EUR	Gross carrying amount under IFRS	Nominal amount under IFRS	Notional amount under IFRS	Exposure value before taking collateral into account	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					

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

[10] 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 that meet one of the following conditions as at the closing date:
    - the gross carrying amount under IFRS for the "Total (A+B)" item is above EUR 300 million
    - the exposure value before taking into account collateral from the "Total (A+B)" item is above EUR 300 million
    - the exposure value before taking into account collateral from 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 that have CIUs or similar vehicles as a counterparty	
A.1. Financing activities excluding 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 risks and return for the various activities;
        - indicate the level of granularity in the calculation and monitoring of those indicators and the frequency at which they are calculated and reviewed;
        - specify the potential quantitative targets or limits associated with the indicators;

- description of the risk management procedures pertaining to the aforementioned risks, and description of the related controls:
- specify, for each internal business line presented in the overall description of activities, which of those activities are framed within a collateralisation policy;

- for each business line framed within a collateralisation policy :
    - summarise its principles;
    - set out the eligibility, availability and quantity criteria applicable to collateral to ensure that such collateral covers the exposures generated by such transactions, in accordance with the provisions of Article 7 of the SRAB Law;
    - specify how the criteria applicable to the quantity and availability of collateral are adjusted to the quality of the collateral and the level of risks implied by the transactions secured by it;
    - when 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 application exemptions. Where applicable, describe how they are framed;
    - identify 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 frame the degree of concentration of (i) individual exposures to a CIU or another similar vehicle employing leverage on a substantial basis, and (ii) collateral obtained from such counterparty.

19.4. Control results

- results of the permanent control actions concerning 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 observed shortcomings;
- results of the periodic control 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 offset shortcomings detected.

20. Outsourcing policy

- presentation of the institution's or group's strategy in terms of outsourcing, including in particular the description of existing provisions to inform outsourcing decision-making (*prior analysis carried out on the criticality of the activity to be outsourced and the 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[11] (under q) and r) of Article 10 of the *Arrêté du 3 novembre 2014*, as amended) and proportion when compared to the overall activity of the institution *(as a whole as well as area by area)*;
- transmission of the yearly data retrieval from the register mentioning the outsourcing arrangements relating 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 of 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 visits at the external provider's premises, etc.;
- for the specific case of outsourced activities through the use of a cloud computing service provider, description of the conditions underlying the use of outsourcing: cloud computing model

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

(public/private…), dates at which the provision of services begins and ends, name of the potential "n^{th} level" subcontractors and an indication on the substitutability of the service provider (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 its 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: formalisation of retained scenarii and objectives as well as proposed alternative measures, presentation of the carried out tests (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 control 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 internal control mechanisms and procedures 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 detected and corrective measures implemented to address them (provisional date of implementation and progress of their implementation at the time of drafting of this report), follow-up procedures for the recommendations resulting from permanent controls (*tools, persons in charge*);
- results of periodic controls carried out on outsourced activities: main shortcomings detected and corrective measures implemented to address them (provisional date of implementation and progress of their implementation at the time of drafting of this report), follow-up procedures for the recommendations resulting from periodic controls.

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 in which the activities of insurance entities are covered by the conglomerate's internal control system;
- a presentation of the procedures for assessing the impact of growth strategies on the risk profile of the conglomerate and for setting additional capital requirements;
- a presentation of the procedures for identifying, measuring, monitoring and controlling intra-conglomerate transactions between different entities within the conglomerate, as well as risk concentrations;
- 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 and what procedures are used, and which activities remain decentralised*).

21.3. Information on intra-group transactions

- information on material intra-group transactions during the year between entities within the conglomerate that conduct banking or investment services activities on the one hand, and entities that conduct insurance activities on the other hand:
    - a description of these transactions, noting the degree of interdependence of the activities within the conglomerate;
    - for each type of transaction, the direction of the transaction in the majority of cases (from a banking or investment services entity to an insurance entity, or the opposite), and the objective of the transactions;
    - the procedures for the internal pricing of these transactions.
- quantitative information on each intra-group transaction the amount of which exceeds 5% of the sum of the capital requirements for the different sectors, 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 is not available, the total notional amount);
    - for each individual transaction that exceeds the threshold, the nominal amount of the transaction and the date it was completed. Financial conglomerates should also provide a description of the transaction, indicating the identity of the counterparties, the direction of the transaction, and the objectives sought, 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, direction, 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. Rating matrix for fraud risks
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, whatever the medium or technical process used, is considered as 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 in accordance with its missions as defined in Article L. 141-4 and Article L-521-8 of the aforementioned *Code Monétaire et Financier*.

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.

Institutions managing payment instruments, without issuing them, shall fill in this annex. Institutions that neither issue nor manage cashless payment instruments should be labelled "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 the access to payment accounts held by the institution.

This annex is divided into five parts:

- A part on the presentation of each means and service of payment, risks of fraud associated and risk management mechanisms put in place (I);
- A part dedicated to the results of the periodic review on the perimeter of non-cash means of payment and access to accounts (II);
- A part dedicated to collect the self-assessment of the institution's compliance with the recommendations from external bodies as regards the security of non-cash means of payment and the security of account accesses (III);
- A part on the audit report on the implementation of security measures provided in the RTS (Regulatory Technical Standards) (IV)
- An annex including the fraud risk rating matrix and a glossary of definitions of technical terms/acronyms used by the institution in the annex (V).

Regarding Part I, the analysis of the fraud risks of each means of payment is carried out from fraud data as declared by the institution to the Banque de France within the framework of the collection of statistics on "Inventory of fraud on scriptural means of payment"[12]. As a consequence, this analysis is carried out:

- On gross fraud and covers both internal and external fraud, and
- Based on the definitions and typology of fraud retained for the statistical reporting to the Banque de France (cf. supra).

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

To this end, analysis matrices of fraud risks specific to each non-cash means of payment presented in the annex shall be completed depending on offers specific to each institution. However, concerning cheques, institutions that have answered the evaluation questionnaire on "cheque security frameworks" (*Référentiel de la sécurité du chèque* - RSC) of the Banque de France, are exempted from carrying out this analysis. Nevertheless, they have to report the main fraud incidents encountered over the financial year under review. The same applies for electronic money in so far as the fraud of this means of payment is not the subject of a specific collection.

The list of recommendations, linked to the security of means of payment issued by external bodies presented in part III of the annex, takes account of the application, on 13 January 2018, of the 2nd European Directive on payment services. Institutions should provide explanatory comments on recommendations for which the full compliance of the institution is not ensured.

Regarding part IV, it 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 or, when applicable, on the action plan envisaged to comply with them. Pursuant to Article 3 of the RTS, it is recalled that this audit report has to be established 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 derogation set out therein, it has to be performed by an external independent and qualified auditor for the first year of its implementation, and then every three years. The purpose of this assessment is to check the compliance of the implementation conditions of the derogation with the risk analysis and in particular, the fraud rate measured by the institution for the type of payment operation 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 part IV concerning the conclusions of the audit report

Important remark concerning banking institutions affiliated to a group, network or central body

In the case of banking institutions affiliated to a group, network or central body where the latter is responsible for the internal control mechanism on a central level, as well as for the risk management concerning the security of means of payment and account access:

- Concerning the part on the presentation of each means of payment (I), the affiliated institution shall present its offer of products and services as well as the operational organisation of the activity. Nevertheless, it is exempted from producing the analysis matrix of 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 part dedicated to the presentation of results of the periodic control (II), if this function is exercised under the responsibility of the group, nework or central bodyand described by the latter in its own annex, only the controls specific to the affiliated institution should be provided by the latter.
- Concerning the part dedicated to the self-assessment of the compliance with recommendations from external bodies regarding 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 specifies the exact identity and interbank code of the institution in question.

Definition of the main concepts used in the annex

Terms	Definitions
Initiation channel	According to the different services and means of payment, the notion of initiation channel corresponds: - For card, to the channel of use of the card: payment at point-of-sale, withdrawal, remote payment, contactless payment, enlistment in e-wallets or mobile payment solutions; - For transfer, to the reception channel of the transfer order: desk, online banking, teletransmission solution…; - For direct debit, to the reception channel of the direct debit order; - For cheque, to the channel of cheque deposit: mail, machine… - For services of information on accounts and of payment initiation, to the means of connection: website, mobile application, dedicated protocol…
External fraud	In the field of means of payment, misappropriation of them, by acts of third parties, for the benefit of an illegitimate beneficiary.
Internal fraud	In the field of means of payment, misappropriation of them, by acts of third parties involving at least one member of the company, for the benefit of an 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 - Date of commercialisation - Equiped with the contactless function by default - Enlistment in an authentication device - 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 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. Planned projects for products and services

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

1.2. Operational organisation of the activities

Sum up processes concerning means/services of payment from issuing/reception to remittance to systems dedicated to the exchange/charge to account, precising in particular outsourced ones (including outsourced to the group's entities) and those shared with other institutions. An organisational diagram can be added if necessary.

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

Describe changes and/or organisational projects launched or conducted over 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
Theft/loss of card	The fraudster uses a payment card obtained as a result of loss or theft.
Card not received	The card has been intercepted during its sending between the issuer and the legitimate holder. This origin type is close to loss or theft. However, it is different to the extent that the holder can less easily notice that a fraudster has a card which belongs to him/her and that he exploits vulnerabilities specific to card sending processes.
Falsified or counterfeit card	An authentic payment card is falsified by modification of magnetic data, embossing or programming data; a counterfeited card is made from data collected by the fraudster.
Stolen card number or non-assigned card number	- The card number of a holder is collected without him knowing it or created by random card number generators and is used in distance selling.

	- Use of a PAN (Personal Account Number) that is coherent but non assigned to a holder and is generally used in distance selling.

b. Global fraud risk rating on card and equivalent

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

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

c. Coverage measures of fraud risk

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

As an issuing institution:

Category of fraud	Initiation channel	Coverage measures
Theft/loss of card	*Ex: at the point-of-sale*	
Card not received		
Falsified or counterfeit card		
Stolen card number or non-assigned card number		

As an acquiring institution:

Category of fraud	Initiation channel	Coverage measures
Theft/loss of card		
Card not received		
Falsified or counterfeit card		
Stolen card number or non-assigned card number		

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 evolutions regarding technology, functions and security
As an institution of the originator					

b. Planned projects for products and services

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

2.2. Operational organisation for transfer business

Sum up processes for means/services of payment from issuing/reception to remittance to systems of exchange/charge to account, precising in particular outsourced ones (including those outsourced to the group's entities) and those shared with other institutions. An organisational diagram can be added if necessary.

Actors	Roles
Issuing and management activity	

Describe organisational changes and/or projects launched or conducted over 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 issues a fake transfer order (including when it has been made by the legitimate holder under coercion). - Usurpation of the online bank user ID of the legitimate originator (including when the online bank user ID has been collected under coercion or through processes such as phishing or social engineering).
Counterfeiting of transfer order	The transfer order is intercepted and modified by the fraudster.

Misappropriation	The payer issues a transfer to a RIB/IBAN which is not the one of the legitimate beneficiary. Typically done after the beneficiary's identity is stolen (through social engineering for example).

b. Global fraud risk rating for transfers

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

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

c. Coverage measures of fraud risk

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

Category of fraud	Initiation channel	Coverage measures
Fake transfer order		
Counterfeiting of transfer order		
Misappropriation		
Others		

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 functions proposed	Clients targeted	Initiation channel	Comments on the evolution of business volume	Comments on evolutions regarding technology, functions and security
As the institution of the debtor					
As the institution of the creditor					

b. Planned projects for products and services

Describe the commercialisation projects for new products/services or the projects pertaining to changes to the existing offer regarding technology, functions and security planned in the short- and medium-term.

3.2. Operational organisation for direct debit

Sum up processes for means/services of payment from issuing/reception to remittance to systems of exchange/charge to account, precising in particular outsourced ones (including those outsourced to the group's entities) and those shared with other institutions. An organisational diagram can be added if necessary.

Actors	Roles
Issuing and management activity	

Describe organisational changes and/or projects launched or conducted over 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	Direct debit issued by a creditor without a licit direct debit authorisation from the debtor. 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).
Misappropriation	-Modification by the fraudster of the account number to be credited associated to direct debit files. -The creditor deliberately issues a direct debit order the amount of which is largely higher than the amount due (for example: the creditor obtains the signature of the direct debit mandate for a given service serving as a "hook" and uses this mandate to obviously extort funds from the debtor). - Issuer usurping a creditor ID (NNE/ICS) which is not his.
Replay	The creditor deliberately issues direct debits orders that have already been issued (that have already been paid or that have been subjected to rejections due to debtor opposition for example).

b. Global fraud risk rating for direct debit

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

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

c. Fraud risk coverage measures

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

As the institution of the debtor

Category of fraud	Initiation channel	Coverage measures
Fake direct debit		
Misappropriation		
Replay		
Others		

As the institution of the creditor

Category of fraud	Initiation channel	Coverage measures
Fake direct debit		
Misappropriation		
Rejeu		
Others		

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 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 the commercialisation projects of new products/services or the projected changes to the existing offer regarding technology, functions and security planned in the short and medium term.

4.2. Operational organisation for bill of exchange and promissory note activity

Sum up processes for means/services of payment from issuing/reception to remittance to systems of exchange/charge to account, precising in particular outsourced ones (including those outsourced to the group's entities) and those shared with other institutions. An organisational diagram can be added if necessary.

Actors	Roles
Drawee'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.

4.3. Risk analysis matrix and main fraud incidents

a. Reminder of applicable fraud typology

Category of fraud	Description
Theft, loss (fake, apocryphal)	Lost or stolen bill, bearing a forged signature
Counterfeit	Bill entirely created by the fraudster
Falsification	Alteration of a validly issued bill
Misappropriation, replay	Presentation of a bill that has already been paid

b. Overall rating of the 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 *(Risk inherent before coverage measures)*	
Residual risk *(Risk remaining after coverage measures)*	

c. Fraud risk coverage measures

Describe the coverage measures precising in bold, on the one hand, those implemented during the financial year and, on the other, those planned by indicating in this case their deadline for implementation.

Category of fraud	Initiation channel	Risk mitigation measures
Theft, loss (fake, apocryphal)		
Counterfeit		
Falsification		
Misappropriation, replay		

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 of 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	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 the commercialisation projects of new products/services or the projected changes to the existing offer regarding technology, functions and security planned in the short and medium term.

5.2. Operational organisation for cheque

Sum up processes for means/services of payment from issuing/reception to remittance to systems of exchange/charge to account, precising in particular outsourced ones (including those outsourced to the group's entities) and those shared with other institutions. An organisational diagram can be added if 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. Evolution of fraud during the period under review

a. Reminder of applicable fraud typology

Category of fraud	Description
Theft, loss (fake, apocryphal)	Cheque lost or stolen, bearing a fake signature
Counterfeit	Cheque entirely created by the fraudster
Falsification	Alteration of a validly issued cheque
Misappropriation, replay	Presentation of a cheque that has already been paid

b. Main fraud incidents

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

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 the commercialisation projects for new products/services or the projected changes to the existing offer regarding technology, functions and security planned in the short and medium term.

6.2. Operational organisation for electronic money

Sum up processes for means/service of payment precising in particular outsourced ones (including those outsourced to the group's entities) and those shared with other institutions. An organisational diagram can be added if 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 evolution projects planned in the short and medium term pertaining to the existing offer regarding technology, functions and security.

7.2 Operational organisation of the offer

Sum up implementation processes for account information services and payment initiation services precising in particular the arrangements for access to information on accounts along with the associated security measures as well as outsourced processes (including those outsourced to the group's entities) and those shared with other institutions. An organisational diagram can be added if 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 IN THE SCOPE OF NON-CASH MEANS OF PAYMENT AND ACCESS TO ACCOUNTS

Describe the results of periodic control missions carried out over the year under review in the scope of non-cash means of payment (including inter general inspections 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 THE 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[13]		
For payments via mobile phones and contactless payment cards, a risk assessment is conducted before any large-scale deployment, in order to ensure the same global security level as for proximity transactions and payments on machines.	OSCP		
In the case where biometrics are used as an identification factor, the payment service provider conducted a risk analysis so that the protection level of implemented solutions is at least equivalent to the one provided by techniques already in place (confidential number and smart card for proximity payments, and a one-time use number for remote payments).	OSCP		
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[14]		

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

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

Strong authentication and enlisting of the client			
The initiation of payments (individually or en masse) on the Internet, the access to sensitive payment data or the modification of lists of registered beneficiaries are protected through strong authentication.	OSMP		
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		
Rules define the validity period of authentication devices (including One-Time Passwords), the maximum number of identification/authentication errors or connection attempts and the expiration of the sessions for payment services on the Internet.	SecuRe Pay EBA		
The registration of the client and supply of tools, software and authentication data to the client, required for using payment services (including on the Internet) is securely carried out.	SecuRe Pay EBA		
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		
The institution ensures the protection of sensitive payment data during storage, treatment and transmission.	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 response plans.	EBA		

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

Regarding the section dedicated to common and secure communication standards, the institution answers the questionnaire depending on the access interface solution put in place for 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 the application of the process for strong customer authentication			
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; - For initiating an electronic payment transaction; - 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? - No information on one of the items categorised as “knowledge”, “possession” and “inherence” can be deducted from the disclosure of an authentication code; - It is not possible to generate a new authentication code based on another authentication code generated before; - 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? - 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; - 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; - Communication sessions are protected against interception of authentication data communicated during the authentication and manipulation by unauthorised third parties - 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 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 linkage			
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? - The payer shall be informed of the amount of the payment transaction and the identity of the payee. - The generated authentication code is specific to the payment transaction amount and to the payee approved by the payer when initiating the transaction. - The authentication code accepted by the		

	payment service provider corresponds to the specific original amount of the payment transaction and the identity of the payee approved by the payer. - Any changes to the amount or beneficiary 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? - The amount of the transaction and the identity of the payee during all phases of authentication; - 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? - 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; - 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? 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? - the use of separate secure execution environments through the software installed on the multi-functional device; - mechanisms to ensure that the software or device has not been altered by the payer or a third party; - in the event of alterations, mechanisms to reduce		

	the consequences thereof.		
EXCEPTIONS TO THE STRONG CUSTOMER AUTHENTICATION OBLIGATION			
Analysis of transaction risks			
18	In the event of a risk analysis exemption, does the PSP meet the requirements listed below? - 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; - the PSP did not identify any of the following elements after a real-time risk analysis:		

	(i) abnormal expenses or abnormal behavioural pattern of the payer; (ii) unusual information on the use of the payer's device or software access; (iii) signs of malware infection during a session of the authentication procedure (iv) a known scenario of fraud in the provision of payment services; (v) an abnormal location of the payer; (vi) high-risk location of the beneficiary. - The factors related to risks listed below are at least taken into account: (i) the previous expense habits of the individual payment service user; (ii) the payment transaction history of each payment service user of the payment service provider; (iii) the location of the payer and the beneficiary at the time of the payment transaction when the access		

	device or software is provided by the payment service provider; (iv) the identification of 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 measured for each of the reasons for the exemption from strong authentication (referred to in Articles 13 to 18) are equivalent to or below the maximum allowed rate per amount tranche 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 for each of the reasons for strong authentication exemptions (referred to in		

	Articles 13 to 18) duly calculated by the PSP: - 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; - and on a rolling quarterly basis (90 days).		
Suspension of derogations 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 allowed maximum rate?		
Monitoring			
21	Should derogations 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? - 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 waivers; - the average value of operations, including a breakdown by payment transactions initiated through strong customer authentication and under each of the waivers; - 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 CUSTOMISED SECURITY DATA OF PAYMENT SERVICE USERS			
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? - 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; - 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; - 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? - 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; - 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 as well as 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? - efficient and secure delivery mechanisms ensure that customised security data and authentication devices and software are delivered to the legitimate payment service user; - mechanisms enable the payment service provider to verify the		

	authenticity of the authentication software delivered to the payment service user via the Internet; - 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: (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;		

	- 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? - the secure destruction, deactivation or revocation of customised security		

	data and authentication devices and software; - 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; - 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? - third party PSPs are able to identify themselves towards the account servicing PSP; - 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? - 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; - 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? - 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; - 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; - 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 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?		

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? - third party PSPs are able to identify themselves to the account servicing PSP; - third party PSPs are able to communicate securely with the PSP to 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? - 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; - 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? 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? 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? - 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; - 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; - 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? - third party PSPs are able to identify themselves to the account servicing PSP; - third party PSPs are able to communicate securely with the PSP to 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? - 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; - 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? 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? 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? - 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; - 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; - 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. Rating matrix for fraud risks

Present the methodology 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 global rating matrix highlighting the levels of criticality.

2. Glossary

Define technical terms and acronyms used in the Annex.

Annex 1

Method for calculating the effect of a uniform shock on activities other than trading

Institutions subject to supervision should calculate the effect on current net banking income of a uniform shock over one year – and, when appropriate, the effect on capital of a uniform upwards or downwards shock– and include the results of those calculations in their Internal Control Reports. These results should be based on a calculation methodology adapted to each institution. This annex describes the principal steps that an institution may need to include in its methodology.

Calculating the effect on own funds of a uniform upwards or downwards shock

In the following example, the shock is set to 200 basis points.

1st step: assign all balance sheet and off-balance sheet lines to maturity bands and calculate a net position, in euro for each maturity band. Use residual maturities.

Institutions may treat certain assets and liabilities in accordance with the following:

- Inclusion of fixed assets and own funds;
- Balance sheet and off-balance sheet items may be recognised at book value. The treatment of off-balance sheet items may be limited to financing commitments recognised at their nominal value;
- Balance sheet and off-balance sheet items may be treated without taking into account new production data. Early repayments may be taken into consideration, based on the institution's own historical data;
- Fixed-rate instruments may be treated according to their residual maturity, and variable-rate instruments on the basis of the residual maturity to the next fixing date;
- Operations consisting of a large number of small-size transactions may be estimated statistically;
- Derivative maturities may be calculated on the basis of the maturity of the underlying instruments, and options should be treated as their delta equivalents;
- Futures and forwards, including forward rate agreements, should be treated as a combination of a short position and a long position. The maturity of a future or a forward rate agreement should be defined as the period until the exercise of the contract, plus the maturity of the underlying instrument, if applicable;
- Swaps should be treated as two notional positions with distinct maturities. For example, a swap in which the bank receives variable and pays fixed may be treated as a long position with a maturity equal to the time until the next pricing, and a short position with a maturity equal to the duration of the swap;
- Institutions should assume linear runoff over 10 years for checking accounts, ordinary savings accounts, young person's passbooks savings accounts, people's passbook savings accounts, housing savings accounts, industrial development savings accounts, and other savings accounts; and linear runoff over 8 years for *PEL* home savings accounts (alternatively, the runoff of *PEL* can be assumed to be non-linear, according to the generation of contracts).

2nd step: assign to each net position a weight reflecting its sensitivity to a given change in interest rate. The following table provides an illustrative example. The weights are based on the assumption of an upward or downward movement of 200 basis points, and the modified duration is approximated from the midpoint of each maturity band using a discount rate of 5%. There are eight maturity bands.

Weighting factors by maturity band of an upward and downward interest rate shock

Maturity band	Midpoint of the maturity band	Proxy of the modified duration	Rate change	Weighting factor
Less than 3 months	1.5 months	0.12	+ or - 2%	+ or - 0.24%
3 to 6 months	4.5 months	0.36	+ or - 2%	+ or - 0.72%
6 months to one year	9 months	0.71	+ or - 2%	+ or - 1.43%
1 to 3 years	2 years	1.83	+ or - 2%	+ or - 3.66%
3 to 5 years	4 years	3.55	+ or - 2%	+ or - 7.09%
5 to 10 years	7.5 years	6.09	+ or - 2%	+ or - 12.17%
10 to 15 years	12.5 years	8.92	+ or - 2%	+ or - 17.84%
Over 15 years	17.5 years	11.21	+ or - 2%	+ or - 22.43%

3rd step: the weighted positions are summed to produce a net short or long position for the banking book (defined as including all activities other than trading) in a given currency. Each currency representing more than 5% of the banking book can be reported separately.

4th step: calculate the weighted position for the entire banking book by summing the net position in the different currencies.

5th step: compare the weighted position for the entire banking book with the amount of own funds (Tier 1 and Tier 2).

Calculating the effect on current net banking income of a uniform 200 basis point shock over one year

1st step: assign all balance sheet and off-balance sheet lines that are exposed to interest rate risk to maturity bands (less than 3 months, 3 to 6 months, 6 months to 1 year) in euro up to 1 year.

2nd step: calculate the gap between assets and liabilities for each maturity band.

3rd step: sum the resulting gaps and multiply by 2%.

4th step: compare the value obtained with net banking income for the year

Annex 2

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

1. Overview of internal control systems[15]

1.1. General internal control system:

- attach an organisation chart showing the units devoted to permanent control(s) (including compliance control) and periodic control, and showing the hierarchical position of their heads;
- expected coordination between the various persons involved in internal control;
- steps taken in the case of an 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 adequate data protection;
- the procedures for monitoring and controlling 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 participate 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, formalisation and date(s) of updates to permanent control procedures, including those that apply to foreign business (including inspections of compliance);
- the procedures for reporting 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 for monitoring 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);

[15] 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 concerning 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, formalisation 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 for defining the frequency and priority of audit cycles, particularly in relation to the risks identified within the institution.

2. Overview of accounting arrangements

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

Annex 3

Measures implemented for customers in fragile financial situations (*Arrêté du 16 septembre 2020* on the certification of the banking inclusion charter and on the prevention of over indebtedness)

I. Training :

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

1.2 Systematic training reminder 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 for customers in fragile situations: %

1.4 Systematic refresher training for the persons referred to in 1.3 above that are already trained: 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 for customers in fragile situations: %

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

II. Internal control[16]

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 over indebtedness/detecting it? Yes/ No

2.1.3. - preventing over indebtedness/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 during permanent control actions and, where applicable, periodic control actions in the past year? Yes / No.

If the answer is « No », do not answer questions 2.4 and 2.5

2.4. If the 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 over-indebtedness prevention (optional)

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