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 2020

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

(Report prepared in accordance with Articles 258 to 266 of the Order of 3 November 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 Order of 3 November 2014. 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 Order of 3 November 2014 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 Order of 3 November 2014, 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 computerized format**, according to the technical arrangements defined by the ACPR, **and electronically signed** according to the arrangements defined by Instruction No 2015-I-19 modified 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 direct supervision, excepting 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 direct supervision, the report may be written in English, except for the sections that remain the exclusive responsibility of the ACPR (sections 7, 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

- description, formalisation and updating 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 Order of 3 November 2014).

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 framework and processes used to collect, stock and aggregate data on risks at different levels within the institution, including for foreign business and outsourcing.

2. Significant changes made in the internal control system

If there have been no significant changes in the internal control system, 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 permanent control (including the organisation of internal control of foreign business and outsourcing)

- a description of significant changes in the organisation of permanent control, including the main actions planned in relation to internal control (cf. Article 259 f) of the Order of 3 November 2014): *specify in particular the identity, the hierarchical and functional position of the person in charge of permanent control and any other functions exercised by this person in the institution or in other entities in the same group;*
- a description of significant changes in the organisation of the compliance control system: *specify in particular the identity, the hierarchical and functional position of the person in charge of compliance and any other functions exercised by this person in the institution or in other entities in the same group;*
- 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 mandate, 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;*
- a general description of the modifications to the permanent control system to ensure compliance to the provisions of Title I of the Law n°2013-672 of 26 July 2013 of separation and regulation of banking activities for the supervised entities.

2.2. Changes in periodic control procedures (including the organisation of internal control of foreign business and outsourcing)

- the identification and hierarchical and functional position of the person in charge of periodic controls;
- a description of significant changes in the organisation of the internal audit system;
- the main initiatives planned in the area of periodic controls (audit plan, etc.; cf. Article 259 f) of the Order of 3 November 2014).

3. Governance

3.1. General principles of governance

- description of the policy of "*risk culture*" deployed within the institution: a summary of communication procedures and staff training programmes on risk profile and their responsibility regarding risks management…;
- presentation of ethical and professional standards promoted by the institution (*indicate if they are in-house standards or application of standards published by external associations/bodies*), description of the mechanism implemented to ensure their proper internal application, the process implemented in case of failure and information modalities to governing bodies…;
- description of processes put in place to identify, manage and prevent conflicts of interest within the institution, modalities of approval and review of these latters.

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

- procedures for the approval of the limits by the supervisory body and, when appropriate, by the risk committee (cf. Article 224 of the Order of 3 November 2014);
- procedures 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 Order of 3 November 2014);
- if necessary, procedures for reporting to the supervisory body and, when appropriate, to the risk committee, by the risk manager, stating the concerned matters (cf. Article 77 of the Order of 3 November 2014);
- procedures for reporting to the supervisory body and (when appropriate) to the risk committee, by the persons responsible for periodic controls, of any failures to carry out corrective measures that have been ordered (cf. Article 26 b) of the Order of 3 November 2014);
- control findings 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 (cf. Article 243 of the Order of 3 November 2014);

- procedures for reporting to the supervisory body regarding the periodic review carried out by the Nomination Committee on the knowledge and skills of the supervisory body's members, both individually and collectively (cf. Article L. 511-100 of the MFC). Send the conclusions of this review 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 Order of 3 November 2014 (cf. Article 245 of the Order of 3 November 2014);
- procedures allowing the risk manager to report to the effective managers on the exercise of their duties (cf. Article 77 of the Order of 3 November 2014);
- procedures allowing the risk manager to warn the effective managers of any situation that could have significant repercussions on risk management (cf. Article 77 of the Order of 3 November 2014).

3.2.3. Measures taken by the effective managers and the supervisory body

- a description of the measures taken by the effective managers and the supervisory body to verify the effectiveness of internal control systems and procedures (cf. Articles 241 to 243 of the Order of 3 November 2014).

3.2.4. Processing of information by the supervisory body

- procedures for reviewing the governance system and the periodical evaluation of its efficiency (cf. Article L.511-59 of the French *Code monétaire et financier*);
- procedures for approving and reviewing on a regular basis the risk strategies and policies (cf. Article L. 511-60 of the French *Code monétaire et financier*);
- procedures 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*);
- procedures for adopting and reviewing the general principles of the remuneration policy and its implementation (cf. 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 (cf. Article 252 of the Order of 3 November 2014);
- dates on which the supervisory body reviewed the activities and results of the internal control system for the past year;
- dates of approval of the aggregate risk limits by the supervisory body, after consulting, when applicable, the risk committee (cf. Article 224 of the Order of 3 November 2014).

3.3. Compensation policies and practices (including for foreign subsidiaries and branches)

This section may be treated in a separate report.

3.3.1. Governance of remuneration policies

- date of establishment, composition, term of mandate, functioning modalities and competences 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* (procedures and date of adoption, implementation date, and review procedures) and, when necessary, the identity of external consultants whose services have been used to establish compensation policies (cf. Article 266 of the Order of 3 November 2014);
- a description of the role of risks, compliance and support functions in designing and implementing the remuneration policy (cf. paragraphs 30, 32 to 35, 54 to 56 of the EBA Guidelines);

- date and results of the internal review intended to ensure compliance with remuneration policies and procedures adopted by the supervisory body (cf. Article L. 511-74 of the French *Code monétaire et financier*).

3.3.2. Main features of remuneration policies

N. B.: the report on information pertaining to remuneration policy and practices will have to make it possible to verify that the remuneration provisions resulting from the transposition of Directive 2019/878 of 20 May 2019 are properly implemented.

- a description of the institution's remuneration policies (cf. Article 266 of the Order of 3 November 2014), including:
    - criteria (relative, absolute, quantitative, qualitative) used to measure performance and to adjust remuneration for risk (cf. paragraph 194 of the EBA Guidelines);
    - criteria (relative, absolute, quantitative, qualitative) for defining 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 Labour Code (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, justification and scope of exemptions provided in Articles 198 and 199 of the Order of 3 November 2014 applied by the institution (account should be taken of the new provisions of Directive 2019/878/EU of 20 May 2019, applicable on 29 December 2020);
- a description of remuneration policies for personnel responsible for validating and checking transactions (cf. Article 15 of the order of 3 November 2014 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 in setting 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 concerned for the subsidiary staff is the one of the subsidiary and not of the parent undertaking*) and the list of the persons concerned by the limitation on the variable component of the remuneration and 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 Order of 3 November 2014, and Article R. 511-18 of the French Code monétaire et financier)

Please specify:

- the categories of staff concerned;

- the overall amount of remuneration for the year, with a breakdown of fixed versus variable components, and the number of beneficiaries. Please also provide a breakdown by area of activity;
- 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 paid and unpaid 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*);
- bonuses for new hires and 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 Order of 3 November 2014);
- 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 head of the compliance function (cf. Article 266 of the Order of 3 November 2014).

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 order of 3 November 2014);
- 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 Order of 3 November 2014 and Part 4 of EBA Guidelines).

4. Results of periodic controls conducted during the year, including foreign business (cf. Article 17 of the Order of 3 November 2014)

- schedule of missions (risks and/or entities that have been subjected to periodic controls during the year), stage of completion and resources allocated in man-days, if use of external provider: frequency of intervention and size of the team;
- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting this Report;
- the procedures for following up on the recommendations generated by periodic controls (*tools, persons in charge*) and the results of that follow-up;
- investigations conducted by the inspection unit of the parent entity and by external institutions (external agencies, etc.), summaries of their main conclusions, and details on the decisions taken to correct 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 order of 3 November 2014)

Please attach an annex providing:

- **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, date of assignment 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 the rating or score assigned to the beneficiary of the commitment. However, it is not necessary to mention commitments whose gross amount 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 a consolidation and exempted from satisfying management ratios on a solo or sub-consolidated basis.

.

- description of the scope of relevant activities for assessing the capital adequacy and the scope of the approach used to determine the materiality of risks;
- description of methodologies used to measure, assess and aggregate risks for quantifying internal capital (analysis horizons, economic value approach, description of models and parameters of calculation…). This description shall include explanations regarding limits or weaknesses of the calculation methodology used, as well as the way these elements are managed, even corrected in the study of 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 Order of 3 November 2014);
- description of the creation and update of a capitalisation plan in order to ensure a sufficient internal and regulatory amount of capital for 3 years at least, including in adverse conditions (stress tests):
    - level and definition of internal capital allocated to each type of risks for the financial year ended detailing the main differences between internal capital and regulatory capital, as well as methods and assumptions used for the allocation of capital within the institution;
    - projection of internal capital level;
- stress tests to assess the adequacy of internal capital:
    - description of the scope and process of creation of stress tests: *perimeter (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 planification and limit setting ;
- internal control procedures for verifying that these systems and procedures remain in line with the evolution of the institution's risk profile;

- documentation formalizing the preparation and validation process of internal capital adequacy, assumptions, capitalisation plan, stress tests and methodologies used in the process and formalizing the integration of this process in the global strategy of the institution, including the allocation of roles as well as the information and involvement of management and/or supervisory bodies in the validation;
- documentation formalising the integration of this process in the global strategy of the institution, including by integrating issues regarding the internal capital and the risk appetite in the decision-making process via appropriate reporting;
- institutions subjected to CRR and that are not under the ECB's direct supervision shall provide a "reader's guide", drawn up as a global document to ease the control 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 the 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.
- institutions subjected to 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.

7. 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, R. 561-38-7 and R.562-1 of the French Code Monétaire et Financier, according to conditions defined in the Order of 21 December 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 Order of 3 November 2014);

7.2. Assessment and control of reputational risk

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

7.4 Procedures for reporting defaults, breaches or failures

Please specify:

- the procedures set up to enable staff to report to the managers and concerned committees of the institution, and to the ACPR (or, when applicable, to the ECB) of defaults 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 Order of 3 November 2014, of potential malfunctions regarding the compliance monitoring system (cf. Article 37 of the Order of 3 November 2014).
- 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 Monetary and Financial Code (cf. Article L. 634-1 and L. 634-2 of the French *Code monétaire et financier*).

7.5. Centralisation and setting up of remedial and monitoring measures

Please specify:

- the procedures set up to centralize information related to potential malfunctions when implementing compliance requirements (cf. Articles 36 and 37 of the Order of 3 November 2014);

- the procedures set up to monitor and assess the effective implementation of corrective actions in order to meet the compliance requirements (cf. Article 38 of the Order of 3 November 2014).

7.6. Description of main malfunctions identified during the year

7.7. Results of permanent control on compliance risk

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting this Report;
- the procedures for following up on the recommendations generated by permanent control (*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 in a reasonable period of time (cf. Articles 11 f) and 26 a) of the Order of 3 November 2014).

8. Credit and counterparty risk (cf. Articles 106 to 121 of the Order of 3 November 2014)

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 limits set, and the management of risk (initial margin, maintenance margin, monitoring of extensions, provisioning of non-performing loans).*

8.1. Loan approval procedures

- predefined loan approval criteria;
- factors used in analysing the expected profitability of loans at the time of approval: *methodology, variables considered (loss rates, etc.);*
- a description of the loan approval procedures, including when appropriate any delegations, escalations and/or limits;
- policy for approving housing loans granted to French customers, in particular criteria regarding repayments as a percentage of borrowers' disposable income, loan-to-value ratios and loan maturities.

8.2. Systems for measuring and monitoring risk

- stress scenarios used to measure risk, selected assumptions, results and description of their operational integration;
- general description of exposure limits – by beneficiary, by associated debtors, by lines of business etc. (*specify the size of the limits in relation to capital and earnings*);
- the procedures and frequency for reviewing credit risk limits (*specify the date of the most recent review*);
- any breaches of credit risk limits observed during the past year (*specify their causes, the counterparties involved, the size of the overall exposure, the number of breaches, and their amounts*);

- the procedures for authorising credit risk limit breaches;
- measures taken to rectify credit risk limit breaches;
- identification, staffing levels, and hierarchical and functional position of the unit charged with monitoring and managing credit risk;
- description of monitoring measures of risk advanced indicators (*specify the main criteria for placing counterparties under watch-list*);
- the procedures for analysing the quality of loans, and the frequency of the analysis; specify any exposures whose internal credit rating has changed, along with loans classified as non-performing or written down (*specify any adjustments in the level of provisioning; give the date on which this analysis was conducted in the past year*);
- 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 Order of 3 November 2014);
- 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 scheme (*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 measure taken…*) and modalities for monitoring forebone exposures including key performance indicators (*non-performing exposure parameters, forbearance activities, liquidation activities, promise of payment, borrower's promise of payment and liquidity collection…*);
- description of the process for accounting assessment of expected credit losses (methods used, factors and assumptions taken into account in developed internal models, frequency of review…);
- the procedures and frequency of provisioning decisions, including when appropriate any delegation and/or escalation measures;
- the procedures and frequency of back-testing exercises of collective and statistical provisioning models, as well as the main results of the year when appropriate;
- the procedures for analysing the risk of loss on leased assets (financial leasing) and the frequency of the analysis;
- the procedures and frequency for analysing risks of impairment losses of financed immovable assets (including assets financed on lease);
- the procedures for updating and reviewing loan files, the frequency of review, and the results of the analysis (at least, for counterparties whose loans are overdue, non-performing or impaired, or who present significant risks or exposure volumes);
- distribution of exposures by risk level (cf. Articles 106 and 253 a) of the Order of 3 November 2014);
- the procedures for reporting to the effective managers, the supervision body and, where applicable, the risk committee, on the level of credit risk, using summary tables (cf. Article 230 of the Order of 3 November 2014);
- 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 appetence (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 Order of 3 November 2014);

- factors considered in analysing changes in margins, in particular for the loan production of the past year: *methodology, variables analysed, results;*
    - provide 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 refinancing rate; if there are gains from investing capital allocated to lending, specify the amount and the rate of return;
    - identify of the different loan categories (such as retail loans and housing loans) or 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 granted to French customers;
- distribution of housing loans according to the type of guarantee (bail, mortgage, etc.);
- presentation of the LTV on housing loans according to the type of guarantee (at the origination, on average and after revaluation of collaterals);
- the procedures of 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 Order of 3 November 2014);
- the procedures of approval and review by the supervisory body of the strategies and policies for taking up, 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)

Specific elements on counterparty credit risk:

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

8.3. Concentration risk

8.3.1. Concentration risk by counterparty

- tool 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 considered, 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 mutual funds, 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 for limiting exposure by counterparty: general description of the system for setting limits on counterparties (*specify their level in relation to capital 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 setting and monitoring 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 for monitoring sectorial concentration risk (especially for the shadow banking system): any aggregate measures defined, economic model and risk profile, description of the system for measuring exposures in the same business sector (especially counterparties network), and procedures for reporting to the effective managers and the supervisory body;
- system for limiting exposure by business sector: a general description of the system for setting limits on sectorial concentrations (*amount of exposures, specify their level in relation to capital 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 setting and monitoring 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 for monitoring geographical concentration risk: any aggregate measures defined, description of the system for measuring exposures in the same geographical region, and procedures for reporting to the effective managers and the supervisory body;
- the system for limiting exposure by geographical region: a general description of the system for setting limits on geographical concentrations (*specify their level in relation to capital 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 setting and monitoring 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 periodic controls conducted on internal rating systems;
- a description of the 'use test' to internal rating systems: 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 preparation of management reports for the effective managers and the supervisory body);
- the procedures for involving the effective managers in designing and updating internal rating systems: including approval of methodologies, ensuring a sound command of the design and operation of the system, and monitoring their operation;
- a demonstration that the internal credit risk assessment methodologies do not rely solely or mechanistically on external credit ratings (cf. Article 114 of the Order of 3 November 2014).

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 detailed 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 originators, sponsors or investors including via stress tests (assumptions, frequency, consequences);
- for originating banks, description of the internal process of assessing prudentially deconsolidating operations, supported by an audit trail and by the procedures for monitoring risk transfer by a periodical 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 for managing intraday credit risk; description of limits (procedures for setting and monitoring limits);
- a presentation of the system for measuring exposures and monitoring 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;
- conclusions on risk exposure to intraday credit risk.

8.7. Results of permanent control of credit activities

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting this Report;
- the procedures for following up on the recommendations generated by 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 in a reasonable period of time (cf. Articles 11 f) and 26 a) of the Order of 3 November 2014).

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

Attach an annex providing:

- a description of the system for identifying, measuring and monitoring the residual risk to which the institution is exposed when it uses credit risk mitigation technics;
- a general description of the procedures for ensuring, 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 for 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 synthesis of incidents occurred during the year when appropriate (guarantee calls refused, unrealised pledges).

8.9. Stress testing of credit risk

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

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 for ensuring the timely confirmation of the terms of OTC derivative contracts not cleared by a central counterparty, reconciling portfolios, managing the associated risk and identifying disputes between parties early and resolving them, and monitoring 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 for valuating OTC derivative contract not cleared by a CCP (cf. paragraph 2 of Article 11 of the Regulation (EU) No 648/2012);
- description of procedures for counterparty risk management and for 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 for calculating and collecting variation margins;
- description of procedures for calculating and collecting initial margins;
- description of models used for calculating initial margins;
- description of criteria used for selecting the collateral exchanged;
- description of methods used for valuating collateral;
- description of operational procedures and contractual documentation used for collateral exchange;
- description of number, volume and evolution of observed collateral disputes with counterparties which collaterals are exchanged with, as well as resolution procedures of these disputes;
- description of the methods and frequencies of the calculation of the amount of capital allocated to manage the risk not covered by 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 centralized procedures for valuating, assessing and monitoring 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 derogations provided 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 derogations provided 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 derogations provided 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 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 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 use an aggregate risk measure);
- the scope of risks covered (business lines and portfolios; within establishments 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 appetence (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 Order of 3 November 2014);
- 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 control of the validity of the tools for measuring 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 capital 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 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 for authorising such breaches and the measures taken to regularise them;
- the procedures 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 Order of 3 November 2014):
    - attach a copy of the documents provided to the effective managers that enable it to assess the risk incurred by the institution, in particular in relation to its capital and earnings.

10.3. Results of permanent control of market risk

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting this Report;
- the procedures for following up on the recommendations generated by 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 in a reasonable period of time (cf. Articles 11 f) and 26 a) of the Order of 3 November 2014).

10.4. Stress testing of 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 than 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 or not the motive of such changes.

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 for identifying, managing, monitoring and reporting the operational risk, taking into account the complexity of the activities and the risk tolerance of the institution ;
- governance: description of the governance system deployed for managing the operational risk and of the governance of the model when appropriate, role and missions of the different committees implemented, structuring decisions taken during the year regarding operational risk;
- organisation: presentation of the different teams in charge of the permanent control of operational risk by lines of business and by geographical areas (numbers of FTEs forecasted and effective, missions, attachment of teams), objectives of the different teams of permanent control, actions carried out during the year and progress of reorganization projects at the end of the year, constraints met and solutions planned/implemented during the implementation of these reorganisation projects, objectives to achieve and period planned for the whole deployment of the target organisation;
- entities' perimeter: integrated entities and methods (in numbers and in proportion of assets), treatment of entities integrated in the perimeter of prudential consolidation during the last two financial years, entities potentially excluded and reasons of 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 procedures used to ensure that the completeness of incidents to be identified is taken into account in the calculation of own funds requirements, especially regarding legal and 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 -not (yet) covered by the mapping organized 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 for monitoring and managing operational risk;
- a description of the specific procedures for managing 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 indicator for business lines, reviewing procedures for new or changing business activities;
- 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, description of the procedures for quality control of historic data;
- a general description of any insurance techniques used.
- a review of the current discussions on the evolutions that the institution has to anticipate concerning the conditions of calculation of 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, low-frequency high-severity events related risks, 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 operational risks observed during the course of the year (settlement incidents, errors, fraud, cybersecurity etc.) and the attendant conclusions drawn.

11.4. Emergency and business continuity plans

- objectives of emergency and business continuity plans, definitions and scenarios used, overall architecture (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, businesses 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 IT backup sites;
- tests of emergency and business continuity plans (objectives, scope, frequency, results), procedures for updating plans (frequency, criteria), tools for managing continuity plans (software and IT development), reporting to senior management (on tests, and on any changes 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 flu pandemic, the Covid pandemic).

11.5 Risks linked to information and communication technology (ICT)

N.B.: For the 2020 financial year, this section shall include a description of the adjustements made by the institution to comply with the new provisions introduced by the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04).

11.5.1. Governance

- presentation of the institution's ICT strategy (organisation, coordination with the overall strategy, priority objectives set up, appetite framework for risks linked to ICT…) and resources dedicated to implement it (procedures put in place to ensure its compliance, dedicated budget and its steering procedure, number

and nature of dedicated staff, measures for risk awareness of staff, planification process and date of last update…);

- presentation of the ICT governance process (roles of effective managers, supervisory body and where appropriate, risks committee in the definition, monitoring and review of the global ICT strategy).

11.5.2. Risk management

- presentation of the organisation of the management of risks caused by ICT (*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 risks linked to ICT*[3] *…*);
- description of the periodic and permanent control mechanisms of IT systems and synthesis of the observations derived from controls carried out (cf. 11.6);
- presentation of the risk mapping linked to ICT including especially risks for the availability and continuity of ICT, ICT security, data integrity and risk linked to the ICT change (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 and resilience

- objectives of the information systems security policy and name of the person responsible for information systems security;
- a description of the procedures set up to prevent and address incidents affecting ICT (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] (schemes for physical and logical security, for preservation of data integrity and confidentiality, specific measures put in place for online banking activity, description of intrusion tests carried out during the financial year, IT recovery plan…);
- presentation of the process for informing the supervisor in case of major incidents affecting ICT.

11.6. Results of permanent controls on operational risk including risks linked to ICT

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting this Report;
- the procedures for following up on the recommendations generated by 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 in a reasonable period of time (cf. Articles 11 f) and 26 a) of the Order of 3 November 2014).

11.7. Overall conclusions on exposure to operational risk

12. Accounting risk

12.1. Significant changes made in 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.

[2] Especially those of the IT function.

[3] Attach the latest dashboard dedicated to inform 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.

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

12.2. Results of permanents controls on accounting risk

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date this Report was drafted;
- the procedures for following up on the recommendations generated by 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 in a reasonable period of time (cf. Articles 11 f) and 26 a) of the Order of 3 November 2014);
- presentation of the prevention system of the accounting risk, including the risk of disruption of information systems (backup site…).

13. Global Interest rate risk

- a general description of the overall framework for identifying, assessing and managing global interest rate risk (*specify the entities and transactions covered, justifying the role of the effective managers and supervisory body as well as the division of responsibilities for controlling global 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 interest rate risk as well as the size, strategy and business model of the institution, applicable to the following guidelines' requirements:
    - calculation and allocation of capital for interest rate risk (taking into account both the impact on economic value and on earnings[6]);
    - measurement and monitoring of interest rate risk (especially with internal scenarios of appropriate shocks as referred to in paragraphs 90 to 102 of the EBA Guidelines and the use of 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 only for 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 global interest rate risk

- a description of the tools and methodologies used to manage global 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 present 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), impact of changes in global interest rate risk on the institution's business during the past year, methodology used for the aggregation of exposures, impacts 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 interests (such as own funds),*

[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).

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 own funds' economic value of a uniform shock of +/-200 bps and of 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 assets of pension bonds and pension funds (except for the treatment of 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 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 "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 calculations of sensitivity in terms of earnings, of net present value and of stress scenarios),*
    - for the calculation of the economic value, 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 global interest rate risk, basis of projections 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 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 results of the shock to a change in the underlying assumptions used (*specify the impact of different changes (parallel and non-parallel) in the yield curve, differences between different market rates (basis risk) and changes to assumptions about customer behaviour; the economic capital allocated in respect of the institution's exposure to global interest rate risk);*
- presentation of internal capital allocated in relation to the global interest rate risk incurred by the institution and the methodology chosen for allocation;
- presentation of scenarios of alternative rates used by the institution (for example, flattening, steepening, inversion shock on short rates, etc.) and results on the economic value and revenues.

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

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

13.2. System for monitoring global interest rate risk

- for earning measures and economic value measures, a general description of the limits set on global interest rate risk (*specify the nature and level of limits, for example in terms of gaps, sensitivity in terms of capital or earnings, the date during the past year when the limits were reviewed, and the procedure for monitoring breaches of limits*);
- a general description of the reports used to manage global 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 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 Order of 3 November 2014).

13.3. Permanent control system for global interest rate risk management

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

13.4. Results of permanent controls on global interest rate risk

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting this Report;
- the procedures for following up on the recommendations generated by 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 in a reasonable period of time (cf. Articles 11 f) and 26 a) of the Order of 3 November 2014).

13.5. Monitoring framework of 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 global interest rate risk

14. Intermediation risk for investment services providers

- statements of the overall distribution of exposures by group of counterparties and by principal (by internal rating, financial instrument, market, or 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 the failure of a principal (insufficient margin, refusal of the transaction);
- a general description of the system of exposure limits for intermediation risk – by beneficiary, by associated debtors, etc. (*specify the level of limits in relation to the transaction volume of the beneficiaries and in relation to capital*);
- 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 regularise 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 pending 'fails' (*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 completion:

- 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 "fails";
- the procedures for measuring funding sources, securities and cash that can easily be transferred to ensure that exposures to counterparty 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 for managing liquidity risks, the risk profile and the risk tolerance* (cf. Articles 181 and 183 of the Order of 3 November 2014).
- 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 Order of 3 November 2014).

- for credit institutions and branches of credit institutions with head office in a third country, specify how the internal methodology takes into account 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 Order of 3 November 2014).

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 Order of 3 November 2014) taking into account the complexity of activities, risk profile and risk tolerance of the institution, describe information systems, tools and indicators used for each currency in which the institution conducts significant activities and specify the alternative scenarios as provided for in Article 168 of the Order of 3 November 2014*;
- 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 table, 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 tables.
- when applicable, a description and justification of the scenarios that are specific to certain foreign implantations, legal entities or business lines (cf. Article 171 of the Order of 3 November 2014);
- 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[9] on liquidity coverage requirement (LCR) for credit institutions, of the likelihood and potential volume of liquidity outflows during 30 calendar days for products or services which are not referred to in Articles 27 to 31. Where appropriate, information on the existence of actual 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 liquidity cost indicators evolution 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 large 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 large 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 crowding out in markets and 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…)*;

[9] This regulation was amended by delegated regulation (EU) 2018/1620 that entered into force on 30 April 2020.

- 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 risks 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*);
- 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 reviewing the criteria for the identification, valuation, liquidity, assets availability and consideration of liquidity risks mitigation instruments (*specify the date of the most recent review*);
- the frequency of reviewing 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 regularise them;
- a general description of the reports used to manage liquidity risk (*including their frequency and recipients*);
- a description of incidents occurring in the past year;
- a description of the quality and composition of liquidity buffer measurement and management systems and a description of measurement and monitoring systems of encumbered and unencumbered assets;
- control processes executed by the risk management function of 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 CRR and that are not under the ECB's direct supervision shall provide a "reader's guide", drawn up as a global document to ease the control 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. 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*).

16.4. Results of permanent controls on liquidity risks

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting this Report;
- the procedures for following up on the recommendations generated by permanent controls (*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 in a reasonable period of time (cf. Articles 11 f) and 26 a) of the Order of 3 November 2014).

16.5. Overall conclusions on exposure to liquidity risks

- institutions subject to 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 Order of 3 November 2014).

- 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 precautionary manner (cf. Article 211 of the Order of 3 November 2014);

- target of leverage ratio determined by the institution;

- stress scenarios used to assess the institution resistance in case of reductions of its own funds through expected or realised losses (cf. Article 212 of the Order of 3 November 2014), including plans to strengthen own funds under stress circumstances.

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

- mode of organisation for the management of customers' cash accounts and articulation (allowing to retrace chronologically the different flows) with investment or compensation services' execution;
- presentation of the method used to protect assets received from customers in accordance with current regulations (i.e. Order of 6 September 2017 on client funds ring-fencing of investment firms) and a description of the tool used for the calculation of the amount of assets received from customers 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 or any modification to the account agreement for ring-fencing previously transmitted, description of procedures to ensure the investment of assets;
- for institutions ensuring the protection of received assets through 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 development of 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 segregated, justification for the proportion of segregated funds within the group;
- presentation of the procedures implemented to ensure compliance with the provisions related to the protection of the assets of institutions' customers, verifications associated 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 Order of 6 September 2017 on the client funds ring-fencing of investment firms;
- communication of the report of the statutory auditors on the compliance with regulatory provisions on segregation.

19. Provisions for banking separation

***Nota bene**:* This part deals with the implementation of Title I of the Law of Separation and Regulation of Banking Activities (*loi de séparation et de régulation bancaire n° 2013-672 du 26 juillet 2013*, known as Loi SRAB). The mandates of internal units mentioned in the mapping shall be sent to the SGACPR along with the report on internal control.

19.1. Mapping of trading activities on financial instruments

- communication of the updated mapping of internal units in charge of operations on financial instruments as mentioned in Article 1 of Order of 9 September 2014 within the smallest scale of the business organisation, with identification of combinations achieved. The mapping shall at least mention the following elements:
    - literal name of the smallest scale of the business organisation,
    - global description of activities,
    - category(ies) of exemptions of separation 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 consumption over 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 of Separation and Regulation of Banking Activities, in particular those relating to market making activities (cf. Article 6 of the Order of 9 September 2014 implementing Title I of the law of Separation and Regulation of Banking Activities);
- a general description of the results of indicators put in place and analysis carried out over the past year (with identification of atypical desks).

19.3. Assessment of activities with leverage assets under loi SRAB

- description of activities;
- assessment of results and risks generated (market, credit and counterparty risks);
- description of procedures for aforesaid risks' management and related controls.

19.4. Results of control

- results of the permanent control concerning the requirements set out in Article 2 of the Order of 9 September 2014 implementing Title I of the Law n°2013-672 of 26 July 2013 of 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 of 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 the decision-making of outsourcing (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);
- description of outsourced activities[10] (under q) and r) of Article 10 of Order of 3 November 2014) and proportion to the institution's overall activity *(as a whole and area by area)*;
- description of core or significant activities (under Article 10 of Order of 3 November 2014) for which the institution has planned to outsource them by using a service provider and proportion of the institution's global activity;
- description of conditions under which the use of outsourcing takes place: 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 Order of 3 November 2014, 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, etc.;
- for the specific case of outsourced activities by using a cloud computing service provider, description of the conditions in which the use of outsourcing takes place: cloud computing model (public/private…), dates of beginning and end of provided services, name of potential subcontractors of "n^{th} level" and an indication on the sustituability of the service provider (easy/difficult/impossible);
- description of procedures of permanent and periodic controls of outsourced activities;
- description of methodology for assessment of service quality and its frequency of review;
- description of procedures for risk identification, management and monitoring linked to outsourced activities
- description of procedures implemented by the institution to maintain the necessary expertise in order to control effectively 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 the 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 Order of 3 November 2014);
- description of due diligence carried out by the effective managers to verify the efficiency of mechanisms and procedures of internal control for outsourced activities (cf. Article 242 of Order of 3 November 2014);
- 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 permanent 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 this report), follow-up procedures for the recommendations resulting from permanent controls (*tools, persons in charge*);

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

- 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 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 permanent controls 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 internal pricing for these transactions.
- quantitative information on each intra-group transaction whose amount 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, aims, 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 of 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 dedicated to the Banque de France, is a document independent from the rest of the reports established pursuant to Articles 258 to 266 of the Order of 3 November 2014.

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.

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 "Inventory of fraud on scriptural means of payment"[11]. As a consequence, this analysis is carried out:

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

[11] 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 to the evaluation questionnaire on the "cheque security frameworks" (*Référentiel de la sécurité du chèque* - RSC) of the Banque de France, are exempted to carry 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 the 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 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 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 operation); it shall be annexed to the audit report (part IV).

Important remark concerning credit unions

In the case of a company affiliated to a central body that issues and/or manages a cashless payment instrument (responsible for overall risk analysis):

- 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 analysis matrix of risks and main fraud incidents and it must mention that "it refers to the central body's decisions 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 central body's responsibility and described by this body, 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 the central body's decisions 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 to provide it and has to mention that "it refers to what has been described by the central body in its own annex".

In the case where the central body neither issues nor manages payment instruments, but remains responsible for the control function (in particular controls focusing on payment instruments):

- The affiliated institution shall complete the annex in its entirety and concerning the part dedicated to the presentation of the results of the periodic control (II), it shall describe, clearly and accurately, all controls focusing on payment instruments implemented by the central body and should at no time refer to the central body's internal control report (which does not include an annex on the security of payment instruments).

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 connection mean: 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 a member of the company, for the benefit of an illegitimate beneficiary.
Gross fraud	Within the meaning of the statistical collection "Inventory of fraud on non-cash means of payment" of the Banque de France, gross fraud corresponds to the nominal amount of payment transactions authorised which are subject to an *ex post* rejection for fraud reason. Therefore, it does not take into account assets which could have been collected after the processing of litigation.
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 before 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 of significant variations of activity (number and amount)*	*Indicate evolutions occurred during the reporting period Ex: pilot realisation, implementation of SMS alerts for transactions of high-end international cards…*
*Ex: **Withdrawal card***					
*Ex: **Enlistment in wallets***					
As an acquiring institution					
Ex: Acceptation offer of proximity card payments					
Ex: Acceptation offer of card payments for distance selling					

b. Planned projects for products and services

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

1.2. Operational organisation of the activities

Sum up processes of means/service of payment from its issuing/reception to its remittance to systems of exchange/charge to account precising in particular outsourced ones (including 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 a loss or a thief.
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 thief. 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 consistent PAN (Personal Account Number) but non assigned to a holder and 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 the 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 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 risks of fraud

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

2.2. Operational organisation for transfer business

Sum up processes of means/service of payment from its issuing/reception to its remittance to systems of exchange/charge to account precising in particular outsourced ones (including 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 on coercion by the legitimate holder). - Usurpation of online bank user ID of the legitimate originator (including when the online bank user ID has been collected on coercion or through processes 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 misused identity (social engineering for example).

b. Global fraud risk rating on transfer

The rating matrix used by the institution to assess the fraud risk has to be provided in the 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 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 of new products/services or evolution projects of 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 of means/service of payment from its issuing/reception to its remittance to systems of exchange/charge to account precising in particular outsourced ones (including 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 n°1: the fraudster issues massively direct debits to RIB/IBAN which list he obtained illegally and without any authorisation or underlying economic reality.

	Example n°2: the creditor issues unauthorised direct debits after having obtained the details of the debtor's bank 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 issues deliberately a direct debit whose amount is largely higher than the amount owed (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 to the debtor). - Issuer usurping a creditor ID (NNE/ICS) which is not his.
Replay	The creditor issues deliberately direct debits already issued (that have already been paid or that have been subjected to rejections for debtor opposition for example).

b. Global fraud risk rating on direct debit

The rating matrix used by the institution to assess the fraud risk has to be provided in the 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 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 evolution projects of 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 of means/service of payment from its issuing/reception to its remittance to systems of exchange/charge to account precising in particular outsourced ones (including to the group's entities) and those shared with other institutions. An organisational diagram can be added if necessary.

Actors	Roles
Drawer'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 forgery signature
Counterfeit	Bill totally created by the fraudster
Falsification	Alteration of the bill validly issued
Misappropriation, replay	Presentation of a bill already paid

b. Overall rating of the fraud risk on bill of exchange and promissory note

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. Coverage measures of the fraud risk

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 drawer:

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 evolution projects of the existing offer regarding technology, functions and security planned in the short and medium term.

5.2. Operational organisation for cheque

Sum up processes of means/service of payment from its issuing/reception to its remittance to systems of exchange/charge to account precising in particular outsourced ones (including 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 totally created by the fraudster
Falsification	Alteration of the cheque validly issued
Misappropriation, replay	Presentation of a cheque already 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 of new products/services or evolution projects of 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 of means/service of payment precising in particular outsourced ones (including 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 of the existing offer regarding technology, functions and security planned in the short and medium term.

7.2 Operational organisation for the offer

Sum up implementation processes of the information on accounts services and of payment initiation precising in particular arrangements for access to information on accounts with associated security measures as well as outsourced processes (including 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 of sensitive payment data

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

II - PRESENTATION OF THE RESULTS OF THE 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 providers of outsourced core services).

Mission statement	Scope and goals of the mission	Main observations and recommendations in terms of security of non-cash means of payment and date of completion

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

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 agency or outlets ("*Instant issuing*") are subject to a risk assessment in order to permanently adjust their level of security.	OSCP[12]		
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 is 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 of acceptation and acquisition of payment cards.	OSCP		
m-POS solutions commercialised by the institution shall respect requirements applicable to classic terminals and rely on communication protocols between the different components of the solution which limit to the bare necessary the ability of access of the mobile machine to transaction data.	OSMP[13]		

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

[13] *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 by a 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 he uses a code different 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 its storage, treatment and transmission.	EBA		
Mechanisms for following transactions are implemented to prevent, detect and block suspicious transactions before their authorisations.	EBA		

The institution implemented a framework for the continuity of activity, 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 regular test of response plans.	EBA		

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

For the part relating to common and secure communication standards, the institution answers the questionnaire only if it is a payment account manager and in function of 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 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 only once by the PSP when the payer uses this code in the situation detailed below?		

	- For accessing its online payment account; - For initiating an electronic payment operation; - For executing an action, thanks to a means of distance communication likely to imply a risk of fraud regarding payment or any other abusive use.		
	Does the PSP plan security measures ensuring the respect of 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, shall the duration of the attempts and the number of retries be determined on the basis of the features of the service provided to the payer and 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 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 shall correspond 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 operation and 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 its consent and the payer approved at the initiation of 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 be 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			
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) well calculated by the PSP: - by 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 the 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 again of the risk analysis exemption (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; - custom security data in data format, as well as cryptographic hardware related to the encryption of customised security data, are not stored in plain text; - secret cryptographic equipment is protected from unauthorized 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 take 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 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 only the payment service user is 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 websitesused 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 personalised security data or authentication devices or software must be activated before their first use, this activation shall be 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 banking site 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 PSP 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 PSP an access interface that meets the requirements listed below? - third party PSP are able to identify themselves towards the account servicing PSP; - third party PSP 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 to be usable by third party PSP 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 identification 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 PSP are established and maintained throughout the identification.		
34-1	Is the access of third party PSP to the PSP online banking site based on certificates marked as electronic stamp 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 readable directly or indirectly by a staff member?		
36-1	Does the PSP meet the requirements listed below? - it provides third party PSP 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 shall provide third party PSP 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 directly initiates the transaction; - upon request, it shall immediately provide to third party PSP, in the form of a simple “yes” or “no”, 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 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 with a back-up mechanism (banking access online 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 PSP 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 parties an access interface that meets the requirements listed below? - third party PSP are able to identify themselves towards the account servicing PSP; - third party PSP 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 to be usable by third party PSP 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 identification 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 PSP are established and maintained throughout the identification.		
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 PSP need to enable interoperability of their software and applications with 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 procedures provide in writing for 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 to inform third-party PSP that use the dedicated interface of measures to restore the system and a description of the other readily available options that they can use in the meantime?		

33-3	Do the PSP procedures provide for the timely notification of the dedicated interface problems to the ACPR?		
33-5	For access to the back-up interface, does the PSP ensure that third parties are identified and authenticated according to the authentication procedures planned for its own customers?		
34-1	Is the access of third party PSP to the PSP online banking site based on certificates marked as electronic stamp 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 information systems insured?		
35-5	Does the PSP ensure that the customised security data and authentication codes they communicate are not readable directly or indirectly by a staff member?		
36-1	Does the PSP meet the requirements listed below? - it provides third party PSP 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 shall provide third party PSP 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 directly initiates the transaction; - upon request, it shall immediately provide to third party PSP, in the form of a simple "yes" or "no", 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 procedures provide for sending 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 PSP 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 parties an access interface that meets the requirements listed below? - third party PSP are able to identify themselves towards the account servicing PSP; - third party PSP 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 to be usable by third party PSP 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 identification 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 PSP are established and maintained throughout the identification.		
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 PSP need to enable interoperability of their software and applications with the PSP 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 procedures provide in writing for 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 made an application for exemption from an emergency mechanism to the ACPR?		
34-1	Is the access of third party PSP to the PSP online banking site based on certificates marked as electronic stamp 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 information systems insured?		
35-5	Does the PSP ensure that the customised security data and		

	authentication codes they communicate are not readable directly or indirectly by a staff member?		
36-1	Does the PSP meet the requirements listed below? - it provides third party PSP 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 shall provide third party PSP 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 directly initiates the transaction; - upon request, it shall immediately provide to third party PSP, in the form of a simple “yes” or “no”, 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 procedures provide for sending a notification message to third parties, 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 for 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 subjected 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 uniform 200 basis point shock upwards or downwards – 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 capital of a uniform shock upwards or downwards

In the following example, the shock is at 200 basis point.

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.

These calculations may use the following techniques:

- 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;
- Derivatives 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[14]

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;
- coordination between the various persons involved in internal control;
- steps taken in the case of an establishment in a country where local regulations prevent the application of the rules stipulated in the Order of 3 November 2014;
- 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 authority of permanent control and compliance control, including foreign activity (*activities, processes and entities*);
- human resources assigned to permanent control and compliance control (Article 13, first indent of the Order of 3 November 2014) (full-time equivalent staff relative to 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 of permanent control and 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, from significant changes in existing products, from internal and external growth, and from unusual transactions (cf. Article 221 of the Order of 3 November 2014);
- summary of the analysis conducted on these new products and transactions.

[14] Institutions may tailor this section according to their size and organisation, the nature and volume of their activities and establishments, 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).

1.4. Periodic control system:

- a description of the organisation of the different levels that participate in periodic control, including foreign business (*activities, processes and entities*);
- human resources assigned to periodic control (cf. Article 25 of the Order of 3 November 2014) (full-time equivalent staff relative to 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 periodic control procedures, including those that apply to foreign business (including inspections of compliance), highlighting significant changes during the year.

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 to 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 (cf. Article 92 of the Order of 3 November 2014);
- 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 (Order of 5 November 2015 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 recall 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[15]

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/detection? Yes/ No

2.1.3. - preventing over indebtedness/assistance? Yes / No

2.1.4. - staff training, in particular as referred to 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 controls and, where applicable periodic controls in the past year? Yes / No.

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

2.4. If yes, please specify the principal deficiencies (maximum 3)

2.5. Have corrective actions been set up? Yes/ No

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

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