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

July 2025

Report on Internal Control
Payment institutions, account information service providers and electronic money institutions

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

Contents

Introduction

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

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

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

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

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

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

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

- annex on the security of non-cash means of payment;
- annex on measures implemented in favour of financially vulnerable customers;
- annex listing transactions entered into with executive directors, members of the supervisory body and, where applicable, with major shareholders;
- annex on Information and Communication Technology (ICT) applicable to institutions subject to European Regulation 2022/2554 on digital operational resilience for the financial sector ("DORA" Regulation), for which the relevant framework template is appended to the letter from the Secretary General to the AFECEI.

The Report on Internal Control shall be sent to the SGACPR at the latest by **30 April** following the end of the financial year.

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

1.1. Description of business conducted

- general description of business conducted, included hybrid activities pursuant to Article L. 522-3 of the French *Code monétaire et financier*;
- 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);
    - for payment activities, specify payment services provided pursuant to Article L. 314-1 of the French *Code monétaire et financier*;
    - an overview of the procedures established for these new activities;
    - a description of the internal control actions applied for the new activities;
- a description of any major changes made in terms of organisation or human resources and of any significant projects launched or conducted during the past year;
- the identity of the professional body affiliated to the *Association Française des Établissements de Crédit et des Entreprises d'Investissement* (French Association of credit insitutions and investment firms) the institution is a member of.

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

- a description, formalised documentation of and updates to the institution's risk mapping, highlights of the main changes made during the past financial year;
- a description of the measures taken to manage the mapped risks;
- a presentation of quantitative and qualitative information on the risks described in the summary reports sent to the members of the management body in its executive function, provided to the supervisory body and specifying the scope of the measures used to assess the level of risk incurred and to set risk limits (cf. Article 230 of the *Arrêté du 3 novembre 2014*, as amended);
- a description of the policies governing the management, quality and aggregation of risk data at different levels within the institution, including for business conducted abroad and outsourced activities: implementation, in a way that is appropriate to the size, nature and complexity of the institution's business, of a uniform or homogeneous data structure that unambiguously identifies risk data, as well as of measures ensuring the accuracy, integrity, exhaustiveness and timely availability of risk data, and definition of a governance process for the risk data aggregation mechanism (see Article 104 of the *Arrêté du 3 novembre 2014*, as amended).

1.3. Major incident

- mechanism implemented to identify major incidents in application of Article 96 of the Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market ("DSP2") and EBA Guidelines No. 2021/03;
- process selected to carry out initial and additional reporting to supervisory authorities.

2. Significant changes made to the internal control system

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

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

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

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

- the identity of the person in charge of the internal audit function and tasked with the third level of control, as defined in Article 12 of the *Arrêté du 3 novembre 2014*, as amended;
- the identity of the member of the management body in its executive function in charge of ensuring the consistency and efficiency of periodic control;
- a description of significant changes to the internal audit function;
- the main initiatives planned in the area of periodic controls (audit plan, etc.; cf. Article 259 f) of the *Arrêté du 3 novembre 2014*, as amended);
- a description of the internal procedure in place governing the appointment and dismissal of the head of the internal audit function (see Article 17 of the Arrêté du 3 novembre 2014, as amended);
- measures taken, where applicable, to ensure that the full investigation cycle of all the activities of the institution or, where applicable, the group, does not exceed five years (see Article 25 of the *Arrêté du 3 novembre 2014*, as amended);
- measures taken, where applicable, to ensure that the audit cycle is determined using an approach that is proportionate to the risks identified within the institution or, where applicable, within the group.

3. Governance

3.1. General principles of governance

- a description of the "*risk culture*" policy applied within the institution: a summary of communication procedures and staff training programmes on risk profile and risk management accountability…;
- a presentation of the ethical and professional standards promoted by the institution (*indicating whether they are in-house standards or the result of the application of standards published by external associations/bodies*), a description of the mechanism implemented to ensure their proper internal

application, the process implemented in the event of a breach and the procedures defined to inform governing bodies…;

- a description of the procedures in place to identify, manage and prevent conflicts of interest, both at the level of the institution, and involving its staff, and a description of the procedures established for the approval and review of these processes (see Article 38 of the *Arrêté du 3 novembre 2014*, as amended).

3.2. Involvement of management bodies in internal control

3.2.1. Procedures used to report to the supervisory body

- the procedures used for the approval of limits by the supervisory body (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedures used to report to the supervisory body on significant incidents as defined in Article 98 (cf. Article 245 of the *Arrêté du 3 novembre 2014*, as amended);
- where necessary, the procedures used by the risk manager to report to the supervisory body, specifying the topics concerned (cf. Article 77 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedure used by the persons responsible for the internal audit function to report to the supervisory body on any failure to carry out corrective measures that have been ordered (cf. Article 26 b) of the *Arrêté du 3 novembre 2014*, as amended);
- the procedure applied by the person in charge of the compliance function to report to the supervisory body on the exercise of his or her missions (see Article 31 of the *Arrêté du 3 novembre 2014*, as amended);
- control findings that have been brought to the attention of the supervisory body, and in particular any shortcomings identified, along with the corrective measures ordered (cf. Article 243 of the *Arrêté du 3 novembre 2014*, as amended).

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

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

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

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

3.2.4. Processing of information by the supervisory body

- as part of the supervisory body's review of major and significant incidents identified through internal control procedures, the main shortcomings identified, related costs, the lessons learned from their analysis, and the measures taken to remediate them (cf. Article 252 of the *Arrêté du 3 novembre 2014*, as amended);
- the dates on which the supervisory body reviewed internal control activities and outcomes during the reporting year under review;

- the dates of approval of aggregate risk limits by the supervisory body (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended).

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

- the mission assignment programme (risks and/or entities that have been audited by the internal audit function during the past year), their respective stage of completion and the resources allocated to them, expressed in man-days;
- the main shortcomings identified;
- the corrective measures taken regarding identified shortcomings**,** the expected date of implementation of these measures, and the state of progress in implementing them as at the date of drafting of this Report;
- the procedures used to follow up on the recommendations issued as a result of periodic controls (*tools*, *persons in charge*) and the outcomes of that follow-up;
- the investigations conducted by the internal audit function of the parent entity and by external bodies (external agencies, etc.), the summary of their main conclusions, and the specifics of the decisions taken to remediate any identified shortcomings.

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

Please attach an annex providing:

- **the characteristics of exposure to main shareholders, members of the management body in its executive function and members of the supervisory body**: identity of the beneficiaries, type of beneficiaries (natural or legal person, shareholder, senior manager or member of the supervisory body), nature of the exposures, gross amount, deductions (if any), weighting applied, date of origination and maturity date.

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

Reminder: *information on the risk of money laundering and terrorist financing (ML-TF) shall be sent in the annual report on the organisation of internal control arrangements for AML-CTF and asset-freezing measures, pursuant to Articles R. 561-38-6 and R. 561-38-7 of the French Code monétaire et financier, according to the terms laid down in the Arrêté du 21 décembre 2018.*

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

6.2. Assessment and control of reputational risk

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

6.4 Procedures used to report non-compliance, breaches and deficiencies

Please specify:

- the procedures set up to enable managers and designated agents to raise concerns, either with the head of compliance of the entity or business line they belong to, or with the person referred to in Article 28 of the *Arrêté du 3 novembre 2014*, as amended, on any potential deficiency of the compliance control framework (cf. Article 37 of the *Arrêté du 3 novembre 2014*, as amended);

- the procedures set up to enable the staff to report to the ACPR any failure to comply with the requirements defined by European regulations and by the French *Code monétaire et financier* (cf. Article L. 634-1 and L. 634-2 of the French *Code monétaire et financier*).

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

- a presentation of the compliance review procedures implemented during the execution of operations relating to new products or services, significant changes to existing products and services or to the systems associated with the products, external or internal growth operations or exceptional transactions: *the opinion of the head of the compliance function shall systematically be required, and provided in writing prior to the execution of these operations* (see Article 35 and Article 221, first paragraph, of the *Arrêté du 3 novembre 2014*, as amended).

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

Please specify:

- the procedures set up to centralise information related to potential deficiencies in the implementation of compliance requirements (cf. Articles 36 and 37 of the *Arrêté du 3 novembre 2014*, as amended);

- the procedures set up to monitor and assess the effective implementation of corrective measures to address deficiencies and meet the compliance requirements (cf. Article 38 of the *Arrêté du 3 novembre 2014*, as amended).

6.7. Description of the main deficiencies identified during the year under review

6.8. Results of 2nd level permanent control actions carried out as regards compliance risk

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

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

***Nota bene**: only payment institutions and electronic money institutions performing credit operations are required to fill in this section in its entirety.*

Other institutions shall only fill in the last sub-section on counterparty risk.

7.1. Credit operation selection procedures

- predefined credit selection criteria;
- factors used in profitability forecasts for credit decisions: *methodology, variables considered (loss ratios, etc.);*
- a description of the credit granting procedures, including when appropriate any delegation, escalation and/or limit mechanism.

7.2. Risk measurement and monitoring framework

- detailed information on the 10 main exposures (after clustering counterparties);
- stress scenarios used to assess risk exposure, underlying assumptions, results and description of their operational integration;
- an overview of credit risk exposure limits – by individual obligor, by connected debtors, by industry sectors, etc. (*specify the level of these limits in relation to own funds and earnings*);
- the procedures used to review credit risk limits and the frequency of such review (*specify the date of the most recent review*);
- any breach of credit risk limits identified during the past year (*specify their causes, the counterparties involved, the total amount of exposure, the number of breaches and their respective amount*);
- the procedures used to authorise credit risk limit breaches;
- the measures taken to rectify credit risk limit breaches;
- the identification, staffing levels, and hierarchical and functional position of the unit in charge of monitoring and managing credit risk;
- a description of the measures in place to monitor early warning risk indicators (*specify the main criteria used to place counterparties under watchlist*);
- the procedures used to assess the quality of credit exposures, and the frequency of such assessments; specify any exposures the internal credit rating of which has changed, along with loans reallocated to doubtul or impaired accounting items; specify any adjustments made to provisioning levels; indicate the date on which this analysis was carried out in the past year;
- the procedures and frequency of revaluation of guarantees and collateral, as well as the main findings of reviews carried out during the year when applicable;
- a presentation of the credit risk measurement and management system in place to detect and manage problem loans, to apply the appropriate value adjustments and to record provisions or adjustments in the appropriate amounts (cf. Article 115 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedures used for provisioning decisions and their frequency, including when appropriate any delegation and/or escalation measures;
- the procedures used for back-testing exercises carried out on collective and statistical provisioning models and their frequency, as well as the main results for the year when applicable;
- the procedure, frequency and results of credit file reviews (at least for counterparties the loans of which are overdue, non-performing or impaired, or which present significant risks or exposure volumes);
- a breakdown of exposures by risk level (cf. Articles 106 and 253 a) of the *Arrêté du 3 novembre 2014*, as amended);
- the procedures used to report to the members of the management body in its executive function (using primary financial statements) and the supervisory body on the level of credit risk (cf. Article 230 of the *Arrêté du 3 novembre 2014*, as amended);
- the roles of the members of the management body in its executive function and the supervisory body in defining, monitoring and reviewing the institution's overall credit risk strategy and in setting up risk limits (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended);
- insights derived from the analysis of changes in margins, in particular for loan production over the past year: *methodology, variables analysed, results;*

  - provide detailed information on the margin calculation method used: earnings and expenses included, whether refinancing needs are taken into account, indicate the net borrowing position and the retained refinancing rate; where gains from the investment of allocated own funds are taken into account, specify the amount and the remuneration rate;
  - identify the various categories of exposure (such as loans to retail clients) or business lines for which margins are calculated;
  - highlight trends identified in outstanding loans through calculations based on outstanding amounts (at year-end and at intermediary dates) and, where appropriate, calculations based on loan production over the past year;
- the procedures used by the members of the management body in its executive function to analyse the profitability of credit operations, the frequency and results of such analysis (*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 generated to inform the supervisory body*);
- the procedures used for the approval by the supervisory body of the limits suggested by the members of the management body in its executive function (cf. Article 253 of the *Arrêté du 3 novembre 2014, as amended*);
- when applicable, the procedures used for the analysis, assessment and monitoring of risks associated with intragroup transactions (credit risk and counterparty credit risk), as well as their frequency.

Elements specific to counterparty credit risk:

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

7.3. Concentration risk

7.3.1. Counterparty concentration risk

- the tool used to monitor counterparty concentration risk: definition of any relevant aggregates, description of the system used to measure exposures to a single beneficiary (including the prudential framework applicable to the counterparties concerned, the financial situation of the counterparty and the portfolio), detailed information on procedures used to identify connected beneficiaries, (establishment of a quantitative threshold beyond which the identification procedure is systematically implemented, etc.), procedures used to report to the members of the management body in its executive function and the supervisory body;
- the system used to set counterparty exposure limits: summary description of the system used to set counterparty limits (*specify limit levels in relation to own funds and earnings*), the procedures used to review limits and the frequency of these reviews, any breach of limits identified, and the procedures used to involve the members of the management body in its executive function in the setting of limits and arrangements in place to communicate monitoring reports;
- amounts of exposure to main counterparties;
- conclusions on the institution's exposure to counterparty concentration risk.

7.3.2. Sectoral concentration risk

- the tool used to monitor sectoral concentration risk: any aggregate measures defined, economic model and risk profile, description of the system used to measure exposures to a single business sector (including counterparty interconnectedness), and procedures used to report to the members of the management body in its executive function and the supervisory body;
- the mechanism used to limit sectoral exposure: a concise description of the system used to limit sectoral concentration (*exposure amounts, specifying their amount in relation to own funds and earnings*), the procedures used to review limits and the frequency of such reviews, any breach of limits identified, and the procedures used to involve the members of the management body in its executive function in the determination and monitoring of limits;
- the breakdown of exposures by sector;
- conclusions on the institution's exposure to sectoral concentration risk.

7.3.3. Geographical concentration risk

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

7.4. Results of 2nd level permanent controls carried out for credit activities

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

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

Attach an annex providing:

- a description of the system used to identify, measure and monitor the residual risk to which the institution is exposed when it uses credit risk mitigation techniques;
- a general description of the procedures used to ensure, when credit risk mitigation instruments are implemented, that they are legally valid, that their value is not correlated with that of the mitigated exposure, and that they are duly documented;
- a presentation of the procedures used to integrate the credit risk associated with the use of credit risk mitigation techniques in the overall credit risk management system;
- a description of stress tests conducted on credit risk mitigation techniques (including the assumptions and methodological principles used and the results obtained);

- a summary of any incident that occurred during the year, where applicable (rejected collateral calls, non-enforcement of pledged collateral).

7.6. Stress testing for credit risk

Attach an annex describing the assumptions and methodological principles used (including the procedures used to take into account contagion effects on other markets) and summarising the results obtained.

7.7. Overall conclusions on credit risk exposure

7.8. Management of counterparty and concentration risks for institutions that are not authorised to perform credit activities

- a presentation of the share of the top 20 counterparties in terms of revenue and net banking income;
- measures taken to limit concentration risk;
- controls set up to monitor concentration risk;
- a presentation of main counterparties (banks, service providers such as agents, etc.) to which the institution's funds are entrusted; procedures used to monitor the credit ratings of these counterparties;
- controls set up to monitor counterparty risk.

8. Operational risk

8.1 Governance and organisation of operational risk

- a general description of the overall framework used to identify, manage and monitor operational risk, and to report on operational risk, taking into account the complexity of activities carried out by the institution as well as its risk appetite;
- governance: a description of the governance framework implemented for the management of operational risk as well as for model governance where applicable, the role and responsibilities of the various committees established, any structuring decisions taken during the year regarding operational risk;
- organisation: a presentation of the various teams in charge of the permanent control actions carried out in respect of operational risk, broken down by business line and geographical area (numbers of forecasted and actual FTEs, responsibilities, organisational line of reporting of teams), objectives of the various permanent control teams, actions carried out during the year and state of progress of reorganisation projects at year-end, constraints faced and solutions considered/implemented in the course of implementing these reorganisation projects, objectives and expected timeline for full deployment of the target organisation;
- scope of entities: integrated entities and consolidation methods (expressed as numbers and as a proportion of total assets), treatment of entities integrated in the scope of prudential consolidation in the last two financial years, entities potentially excluded and the reasons for such exclusion, transactions taken into account;
- the definition of a significant incident retained by the supervisory body within the framework of Article 98 of the *Arrêté du 3 novembre 2014*, as amended (*append the minutes of the meeting during which the threshold was approved*).

8.2. Identification and assessment of operational risk

- a description of the types of operational risks to which the institution is exposed;
- a description of the system used to measure and monitor operational risk;

- the monitoring procedures used to ensure that all incidents to be identified are taken into account, especially concerning legal and compliance risks; identification of risks requiring an improvement to the current monitoring mechanism and remedial actions taken;
- a presentation of the risk mapping detailing business lines/risks not (yet) covered by the mapping established at the end of the financial year;
- a general description of the reports used to measure and manage operational risk (*specify in particular the frequency of reporting and recipients of reports, the areas of risk covered, and the use or lack of early warning indicators to signal potential future losses*); documentation and communication of the procedures used to monitor and manage operational risk;
- a general description of any insurance techniques used.

8.3. Integration of the system used to measure and manage operational risk in the permanent control system

- a description of the procedures used to integrate operational risk monitoring into the permanent control system, including, inter alia, risks related to low-frequency high-severity events, as well as internal and external fraud risks;
- a description of the main operational risks identified in the course of the year, the associated costs (settlement incidents, errors, fraud, etc.) and the lessons learned from them.

8.4. Results of 2nd level permanent control actions for operational risk

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

8.5. Overall conclusions on exposure to operational risk

9. Accounting risk

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

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

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

9.2. Results of 2nd level permanent control actions for accounting risk

- main shortcomings identified;
- measures taken to remediate identified shortcomings**,** the expected date of completion of these measures, and the state of progress of their implementation as at the date of drafting of this Report;
- the procedures used to follow up on recommendations issued as a result of permanent controls (*tools, persons in charge, etc.*);

- the procedures used to verify that the corrective measures ordered by the institution have been carried out by the appropriate persons within a reasonable timeframe (cf. Articles 11 f) and 26 a) of the *Arrêté du 3 novembre 2014*, as amended);
- a presentation of the accounting risk prevention framework, covering the risk of IT system failure (fallback sites…).

10. Cash management

- a description of the cash monitoring measures in place;
- a detailed description of the cash management policy approved by senior management / the supervisory committee;
- a detailed description of the nature of cash investments specifying their level of availability and their evolution during the financial year.

11. Internal control system relating to the protection of customers' funds

- exhaustive diagrams and description of all financial flows according to type of payment transaction/electronic money issuance operation, making it possible to trace, in chronological order (including timeframes), the flows of funds collected in return for a payment order/issuance of electronic money, as well as the funding of the various accounts concerned, from the origination of orders to their actual execution;
- a presentation of the method used to safeguard funds received from customers and a description of the tool used to calculate the amount of funds received from customers to be ring-fenced;
- for institutions ensuring the protection of funds received by placing them in one or more account(s), opened specifically for this purpose with a credit institution: notification of any changes made to the account segregation agreement (attach an annex with the updated agreement where applicable), description of the procedures in place to ensure the investment of funds;
- for institutions ensuring the protection of assets received through a guarantee mechanism: notification of any changes made to the collateral arrangement or guarantee contract, and of any element related to the adjustment of the amount of coverage in line with changes in business volume (attach an annex with the new collateral agreement or guarantee contract where applicable);
- a presentation of the procedures implemented to ensure compliance with the provisions relating to the safeguarding of customers' assets by the institution, of the associated controls, and presentation of the any incidents or deficiencies identified following these checks.

12. Outsourcing policy

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

- a presentation of the institution's or group's strategy in terms of outsourcing;
- a description of outsourced activities (within the meaning of q) and r) of Article 10 of the *Arrêté du 3 novembre 2014*, as amended), and expressed as a proportion of the institution's total activity *(as a whole and area by area)*;
- a description of the conditions underlying the use of outsourcing: host country, authorisation and prudential supervision of external service providers, procedures implemented to ensure that a written contract exists and that it complies with the requirements of Article 239 of the *Arrêté du 3 novembre 2014*, as amended, including those allowing the *Autorité de contrôle prudentiel et de résolution* to conduct on-site inspections at the external service provider's premises, etc.;

- a description of the permanent and periodic control system in place for outsourced activities;
- a description of procedures used for the identification, management and monitoring of the risks associated with outsourced activities;
- a description of the methodology used for the assessement of service quality and the frequency of review;
- a description of procedures implemented by the institution to maintain the necessary expertise to effectively control outsourced activities and manage the risks associated with outsourcing;
- a description of the procedures used for the identification, assessment and management of conflicts of interest associated with the outsourcing mechanism of the institution, including between entities of the same group;
- a description of the business continuity plans and of the exit strategy defined for critical or important outsourced activities: formalisation of retained scenarii and objectives as well as proposed alternative measures, presentation of the carried out tests (frequency, results…), reporting to senior management (regarding the tests, updates on the defined plans or exit strategy);
- procedures used to inform the supervisory body on measures taken to ensure control over outsourced activities and the resulting risks (cf. Article 253 c) of the *Arrêté du 3 novembre 2014*, as amended);
- a description of due diligence carried out by the members of the management body in its executive function to verify the efficiency of internal control mechanisms and procedures for outsourced activities (cf. Article 242 of the *Arrêté du 3 novembre 2014*, as amended);
- description, formalisation and date(s) of update of the procedures used for the permanent and periodic control of outsourced activities (including compliance review procedures);
- results of 2nd level permanent control actions carried out on outsourced activities: main shortcomings detected and corrective measures implemented to address them (provisional date of implementation and progress of their implementation as at the date of drafting of this report), follow-up procedures for the recommendations resulting from permanent control actions (*tools*, *persons in charge*);
- results of periodic control actions carried out on outsourced activities: main shortcomings detected and corrective measures implemented to address them (provisional date of implementation and progress of their implementation as at the time of drafting of this report), follow-up procedures on recommendations resulting from periodic control actions.

13. Information specific to institutions authorised to provide payment initiation services and/or account information services

- provide a proof of professional liability insurance or an equivalent guarantee valid for the current financial year. The provided proof must eplicitly state that the professional liability insurance policy or equivalent guarantee currently in force is not supplemented by any separate document establishing an excess of any kind;
- should the initially underwritten contract have been amended, provide its amended version;
- for payment institutions authorised to provide payment initiation services:
  - fill in the following table:

	Data in EUR for the last calendar year
Amount of reimbursement and compensation claims submitted by users and by account servicing payment service providers	
Number of payment operations initiated	
Total amount of payment operations initiated	

  - provide, where applicable, detailed information on unregulated activities carried out within the institution, and the proof of professional liability insurance or equivalent guarantee covering these activities if such coverage has been underwritten;

- for institutions authorised to provide account information services:
  - fill in the following table:

	Data in EUR for the last calendar year
Amount of reimbursement and compensation claims resulting from liability incurred towards the account servicing payment service provider or the payment service user following unauthorised or fraudulent access to payment account data or unauthorised or fraudulent use of such data	
Number of payment accounts accessed by the institution	
Number of clients	

  - provide, where applicable, detailed information on unregulated activities carried out within the institution, and the proof of professional liability insurance or equivalent guarantee covering these activities if such coverage has been underwritten.

14. Annex on the security of non-cash means of payment provided or managed by the institution and the access to payment accounts and information thereof

CONTENTS

INTRODUCTION

Reminder of the legal framework

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

The annex is sent by the General Secretariat of the *Autorité de contrôle prudentiel et de résolution* to the Banque de France for the performance of its tasks as defined in Article L. 141-4 and Article L. 521-8 of the aforementioned French *Code Monétaire et Financier* and, for the annexes drawn up by institutions having their registered office in the French territorial communities of the Pacific region, to the *Institut d'Émission d'Outre-Mer* (IEOM) for the performance of its duties as defined in Article L. 721-20 of the same Code[1].

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

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

Features and contents of this annex

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

This annex is divided into five sections:

- a section dedicated to the presentation of each payment method and service, the associated fraud risks and risk management mechanisms in place (I);
- a section dedicated to the results of periodic control procedures applied to the scope of non-cash means of payment and account access (II);
- a section dedicated to collecting the institution's self-assessment of compliance with the recommendations issued by external bodies as regards the security of non-cash means of payment and account access (III);
- a section on the audit report on the implementation of security measures provided for in the RTS (*Regulatory Technical Standards*) (IV)[2];
- an annex including the fraud risk rating matrix and a glossary for the definitions of technical terms/acronyms used by the institution in the annex (V).

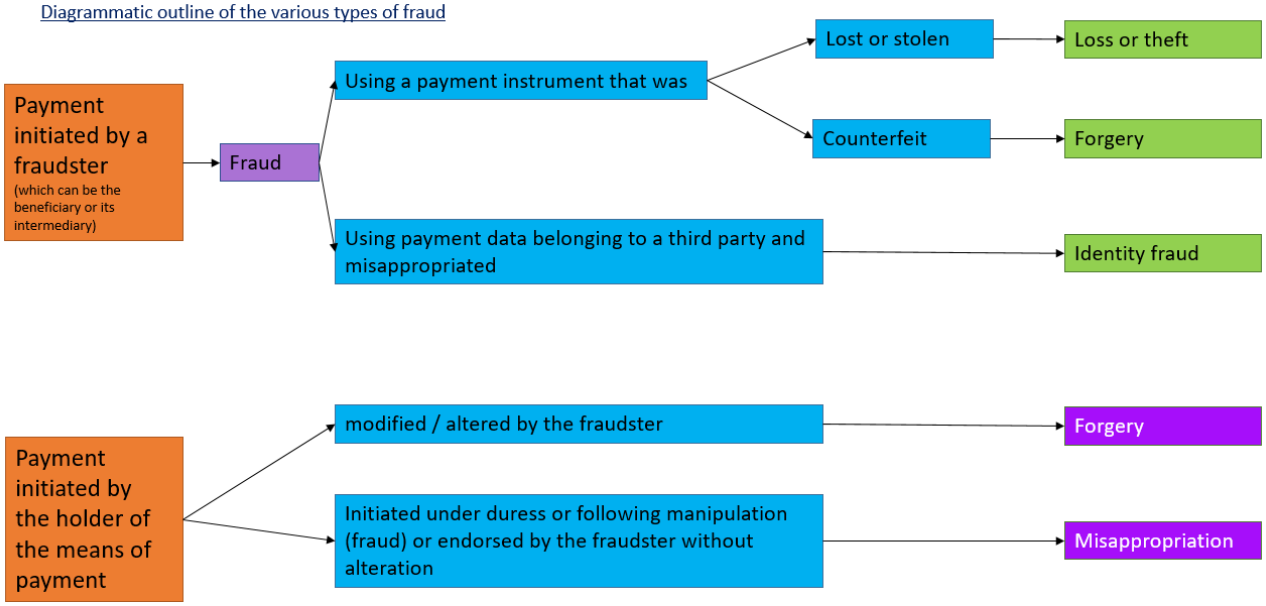
[1] For payment service providers having their head office in a French territorial community of the Pacific region (New Caledonia, French Polynesia, Wallis and Futuna Islands), reference to the "Banque de France" should be replaced with one to "IEOM" in this Annex, and references to the "French territory"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

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

Regarding Section I, the analysis of fraud risks for each means of payment is carried out using fraud data as submitted by the institution to the Banque de France within the framework of the collection of statistics on the "Inventory of fraud on non-cash means of payment"[3]. As a consequence, this analysis is carried out:

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

Diagrammatic outline of the various types of fraud



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

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

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

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

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

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

Remark concerning account information service providers

Concerning section I, account information service providers shall only fill in the section dedicated to account information services (I.5). In addition, they shall fill in the sections dedicated to periodic control results (II), to the self-assessment of compliance with recommendations from external bodies regarding the security of means of payment (III) and the sections dedicated to the audit report on the implementation of security measures provided for in the RTS (IV).

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

Definition of the main concepts used in the annex

Terms	Definitions
Initiation channel	Depending on which of the various services and means of payment is meant, the concept of initiation channel refers: - for cards, to the channel of use of the card: payment at point-of-sale, withdrawal, remote payment, contactless payment, enrolment in e-wallets or mobile payment solutions; - for transfers, to the reception channel of the transfer order: desk, online banking, teletransmission solution…; - for direct debit, to the reception channel of the direct debit order; - for information on accounts and payment initiation services, to the connection means used: website, mobile application, dedicated protocol…
External fraud	In the field of means of payment, misappropriation of the latter, through the acts of third parties, for the benefit of an illegitimate beneficiary.
Internal fraud	In the field of means of payment, misappropriation of the latter, through the acts of third parties involving at least a member of the company, for the benefit of an illegitimate beneficiary.
Gross fraud	Within the meaning of the Banque de France's statistical collection "Inventory of fraud on non-cash means of payment", gross fraud corresponds to the nominal amount of payment transactions authorised which are subject to an *ex post* rejection due to fraud. Therefore, it does not take into account assets which have been recovered after the relevant litigation process is through.
Gross risk	Risks likely to affect the proper functioning and security of means of payment, before the institution takes into account the procedures and measures used to mitigate them.
Residual risk	Remaining risk after taking into account risk coverage measures.
Coverage measures	All actions undertaken by the institution in order to improve risk control, by reducing both the impact of risks and their frequency of occurrence.

I – PRESENTATION OF PAYMENT MEANS AND SERVICES AND OF FRAUD RISKS INCURRED BY THE INSTITUTION

1. Card and equivalent

1.1. Presentation of the offer

a. Description of products and services

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

b. Planned projects for products and services

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

1.2. Operational organisation of activities

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

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

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

1.3. Risk analysis matrix and main fraud incidents

a. Applicable fraud typology

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

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

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

Gross risk (*Inherent risk before coverage measures*)	

Residual risk *(Risk remaining after coverage measures)*	

c. Coverage measures for fraud risk

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

As an issuing institution:

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

As an acquiring institution:

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

d. Evolution of gross fraud over the period under review

As an issuing institution:

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

As an acquiring institution:

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

e. Presentation of emerging fraud risks

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

2. Transfer

2.1. Presentation of the offer

a. Description of products and services

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

b. Planned projects for products and services

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

2.2. Operational organisation of transfer activities

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

Actors	Roles
Issuing and management activity	

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

2.3. Risk analysis matrix and main fraud incidents

a. Reminder of applicable fraud typology

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

b. Overall risk rating for transfer fraud

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

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

c. Fraud risk coverage measures

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

Category of fraud	Initiation channel	Coverage measures
Forgery		
Counterfeiting		
Misappropriation		

d. Evolution of gross fraud over the period under review

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

e. Presentation of emerging fraud risks

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

3. Direct debit

3.1. Presentation of the offer

a. Description of products and services

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

b. Planned projects for products and services

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

3.2. Operational organisation of direct debit activities

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

Actors	Roles
Issuing and management activity	

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

3.3. Risk analysis matrix and main fraud incidents

a. Reminder of applicable fraud typology

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

b. Overall risk rating for direct debit fraud

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

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

c. Fraud risk coverage measures

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

As the institution of the debtor

Category of fraud	Initiation channel	Coverage measures
Forgery		
Misappropriation		

As the institution of the creditor

Category of fraud	Initiation channel	Coverage measures
Forgery		
Misappropriation		

d. Evolution of gross fraud over the period under review

As the institution of the debtor:

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

As the institution of the creditor:

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

e. Presentation of emerging fraud risks

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

4. Cheque cashing

4.1. Presentation of the offer

a. Description of the cheque-cashing offer

Customers targeted	Cashing channel	Comments on the evolution of business volume	Comments on developments regarding technology, functions and security

b. Planned projects concerning the offer of products and services

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

4.2. Operational organisation of cheque remittance

Summarise cheque handling processes, from receipt to remittance to the exchange/charge to account systems, specifying in particular outsourced ones (including those outsourced to other entities of the group) and those shared with other institutions. An organisational diagram can be added as necessary.

Actors	Roles
Activity of the remitter	

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

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

b. Overall risk rating for cheque fraud

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

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

c. Risk coverage measures in place for fraud risk

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

Category of fraud	Remittance channel	Description of the main fraud cases encountered (in terms of amount and/or frequency)
Theft, loss (forgery, doubtful authenticity)		
Conterfeiting		
Forgery		
Misappropriation, double presentment		

d. Evolution of gross fraud during the period under review

Category of fraud	Remittance channel	Description of the main cases of fraud uncountered (in terms of amount and/or frequency)

e. Presentation of emerging risks

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

5. Electronic money

5.1. Presentation of the offer

a. Description of products and services

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

b. Planned projects for products and services

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

5.2. Operational organisation of electronic money activities

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

Actors	Roles

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

5.3. 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)

6. Account information and payment initiation services

6.1. 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 developments regarding technology, functions and security

b. Planned projects for the service offer

Describe the technological, functional and security upgrades planned in the short- and medium-term.

6.2. Operational organisation of the offer

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

Participants	Roles

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

6.3. Description of protection measures for sensitive payment data

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

II - PRESENTATION OF THE RESULTS OF PERIODIC CONTROL ACTIONS IN THE SCOPE OF NON-CASH MEANS OF PAYMENT ACCOUNT ACCESS

Describe the results of periodic control missions carried out over the year under review in the scope of non-cash means of payment.

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

III – ASSESSMENT OF COMPLIANCE WITH THE RECOMMENDATIONS ISSUED BY EXTERNAL BODIES ON THE SECURITY OF MEANS OF PAYMENT AND ACCOUNT ACCESS

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

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

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

Concerning the section dedicated to common and secure communication standards, institutions should fill in the questionnaire only if they act as an account servicing payment service provider, and depending on the type of access interface solution implemented for third-party PSPs.

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

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

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

	within a specified period; - Communication sessions are secured against interception of authentication data transmitted during the authentication process and against manipulation by unauthorised third parties; - The payer's maximum period of inactivity before session timeout, following successful authentication to that payer’s online payment account, does not exceed five minutes.		
	In the event of a temporary lockout following unsuccessful authentication attempts, are the account lockout duration and the number of additional retries determined based on the features of the service provided to the payer and the associated risks, taking into account, at a minimum, the factors set out in Article 2 (2) of the RTS?		

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

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

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

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

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

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

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

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

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

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

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

21	Should exemptions from strong authentication be used (Articles 10 to 18), has the PSP implemented a mechanism to record and monitor the data listed below, for each type of payment transaction and at least on a quarterly basis? - the total value of unauthorised or fraudulent payment transactions, the total value of all payment transactions and the resulting fraud rate, including a breakdown of payment transactions initiated using strong customer authentication and initiated under each exemption type; - the average transaction value, including a breakdown by payment transactions initiated using strong customer authentication and by exemption type; - the number and percentage of payment transactions processed		

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

	Has the PSP formally documented the entire process governing the management of the cryptographic material used to encrypt or otherwise obfuscate the personalised security credentials?		
	Does the PSP ensure that the processing and routing of personalised security credentials and authentication codes take place in secure environments that comply with strict and widely recognised industry standards?		
Data creation and transmission			
23	Does the PSP ensure that the creation of personalised security credentials take place in a secure environment?		
	Are the risks of unauthorised use of personalised security credentials, authentication devices and software, following their loss, theft or duplication prior to delivery to the payer adequately mitigated?		
Association with the payment service user			

24	Does the PSP ensure that the payment service user is the only person securely associated with the personalised security credentials, authentication devices and software, in compliance with the requirements listed below? - the association of the payment service user's identity with the personalised security credentials and the authentication devices and software is carried out in secure environments under the responsibility of the payment service provider, such as the premises of the payment service provider and the Internet environment provided by the payment service provider, or other similar secure websites used by the PSP and by its withdrawal services at automated teller machines, and takes		

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

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

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

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

	information related to personalised security credentials recorded in the payment service provider's systems and databases and, where applicable, in public registers.		

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

30-2	Does the PSP ensure that all authentication procedures offered to payment service users are also made available for use by third-party PSPs for the purpose of authenticating such payment service users?		
30-2-a-b	Does the access interface provided by the PSP comply with the requirements listed below? - the PSP is able to initiate the strong authentication process at the request of a third-party PSP that has previously obtained the user's consent; - communication sessions between the PSP and third-party PSPs are established and maintained throughout the authentication process.		
34-1	Is access to the PSP's online banking interface by third-party PSPs secured using qualified certificates for electronic seals or qualified website authentication certificates?		
35-1	Does the PSP ensure the integrity and confidentiality of personalied security credentials and authentication codes both during transit through communication channels and when stored within its information systems?		

35-5	Does the PSP ensure that personalised security credentials and authentication codes communicated to users can never directly or indirectly be read by any staff member?		
36-1	Does the PSP comply with the requirements listed below? - it provides third-party PSPs with the same information from the designated payment accounts and associated payment transactions that is made available to the payment service user when accessing account information directly, provided that such information does not include sensitive payment data; - immediately upon receipt of the payment order, the PSP provides third-party PSPs with the same information on the initiation and execution of the payment transaction as is provided or made available to the payment service user when the transaction is initiated directly by the payment service user; - upon request, the PSP immediately provides third-party PSPs with a simple “yes”		

	or “no” answer as to whether or not the amount necessary for the execution of a payment transaction is available on the payer's payment account.		
36-2	In the event of an error or unexpected event during the identification or authentication process, or when exchanging information items, do the PSP’s procedures provide for the sending of a notification message to third-party PSPs, indicating the reason for the error or unexpected event?		
To be applied by the account servicing PSP in the event of implementation of a dedicated access interface with a fallback mechanism (online banking access with third-party authentication)			
29	Does the PSP ensure that all operations involving the payment service user (authentication, account information access and payment initiation), including with merchants, other PSPs and other entities are duly logged using unique, non-predictable identifiers and are time-stamped?		
30-1	Has the PSP made an access interface available to third-party PSPs that complies with the requirements listed below? - third-party PSPs are able to identify themselves to the account servicing PSP;		

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

	their software and applications with the PSP's systems?		
30-4	In the event of changes to the technical specifications of the access interface, does the PSP ensure, excluding in case of emergency, that such changes are made available to third-party PSPs at least three months prior to their implementation? Do the PSP's procedures provide for emergency situations during which changes have been made to be documented in writing, including the reasons for the changes, and for this documentation to be made available to the ACPR and the Banque de France?		
32-1	Does the PSP ensure that its dedicated access interface offers, at all times, the same level of availability and performance, including support, as the interface(s) made available to the payment service user for direct access to their online payment account?		
32-2	Has the PSP defined transparent key performance indicators and service level targets for its dedicated access interface that are at least as stringent as those set for the interface used by its payment		

	service users, both in terms of availability and data provided?		
32-4	Does the PSP monitor the availability and performance of its access interface and publish the corresponding statistics on its website on a quarterly basis?		
33-1	Has the PSP implemented a fallback mechanism that is triggered after five consecutive access requests to the dedicated interface by a third-party PSP, where no response is received within 30 seconds?		
33-2	Does the PSP have communication plans in place to inform third-party PSPs that use the dedicated interface of the measures taken to restore the system and do the plans include a description of the other immediately available options that they may use in the meantime?		
33-3	Do the PSP's procedures provide for the immediate notification of any issues related to the dedicated interface to the ACPR?		
33-5	Regarding access to the fallback interface, does the PSP ensure that third-party PSPs are identified and authenticated using the same authentication procedures as those applied to its own customers?		
34-1	Is access by third-party PSPs to the PSP's dedicated access interface		

	secured using qualified certificates for electronic seals or qualified website authentication certificates?		
35-1	Does the PSP ensure the integrity and confidentiality of personalised security credentials and authentication codes, both during transit through communication channels and when stored in the PSP's information systems?		
35-5	Does the PSP ensure that the personalised security credentials and authentication codes communicated to users are never directly or indirectly readable by any staff member?		
36-1	Does the PSP comply with the requirements listed below? - it provides third-party PSPs with the same information from designated payment accounts and associated payment transactions as is made available to the payment service user when directly accessing account information, provided that such information does not include sensitive payment data; - immediately upon receipt of the payment order, the PSP provides third-party PSPs with the same information on the initiation and execution of the payment transaction as that provided or		

	made available to the payment service user when the transaction is initiated directly by the payment service user; - upon request, the PSP immediately provides third-party PSPs with a simple “yes” or “no” answer as to whether or not the amount necessary for the execution of a payment transaction is available on the payer's payment account.		
36-2	In the event of an error or unexpected event during the identification or authentication process or during the exchange of information, do the PSP’s procedures provide for the sending of a notification message to third-party PSPs, indicating the reasons for the error or unexpected event?		
To be applied by the account servicing PSP in the event of implementation of a dedicated access interface without a fallback mechanism			
29	Does the PSP ensure that all operations (authentication, access to account information and payment initiation) involving the payment service user, including with merchants, other PSPs and other entities, are duly logged using unique, non-predictable identifiers and time-stamped?		
30-1	Has the PSP made an access interface available to third-party		

	PSPs that complies with the requirements listed below? -third-party PSPs are able to identify themselves to the account servicing PSP; -third-party PSPs are able to communicate securely with the PSP in order to perform their payment services.		
30-2	Does the PSP make all authentication procedures offered to payment service users available for use by third-party PSPs for the purpose of authenticating payment service users?		
30-2-a-b	Does the PSP's access interface comply with the requirements listed below? -the PSP is able to initiate the strong authentication process at the request of a third-party PSP that has previously obtained the user's consent; - communication sessions between the PSP and third-party PSPs are established and maintained throughout the authentication process.		
30-3	Does the PSP ensure that its access interface complies with the communication standards issued by European or international standardisation bodies?		

	Are the technical specifications of the access interface documented, including a set of routines, protocols and tools that third-party PSPs need to ensure interoperability of their their software and applications with the PSP's systems?		
30-4	In the event of changes to the technical specifications of the access interface, has the PSP ensured that, excluding in an emergency, they are made available to third-party PSPs at least three months prior to their implementation? Do the PSP's procedures provide for the emergency situations in which such changes have been made to be documented in writing, and made available to the ACPR and the Banque de France?		
32-1	Does the PSP ensure that its dedicated access interface offers, at all times, the same level of availability and performance, including support services, as the interface(s) made available to the payment service user for direct access to their online payment account?		
32-2	Has the PSP defined key performance indicators and service level targets for its access interface that are transparent and at least as		

	stringent as those set for the interface used by their payment service users, both in terms of availability and data provided?		
32-4	Are the availability and performance of the access interface monitored by the PSP and are the associated statistics published on its website on a quarterly basis?		
33-6	Has the PSP submitted an application for exemption from the implementation of a contingency mechanism to the ACPR?		
34-1	Is the access of third-party PSPs to the PSP's dedicated access interface secured using qualified certificates for electronic seals or qualified website authentication certificates?		
35-1	Are the integrity and confidentiality of personalised security credentials and authentication codes ensured, whether when transiting through communication channels or when stored in the PSP's information systems?		
35-5	Does the PSP ensure that the personalised security credentials and authentication codes communicated to users are never directly or indirectly accessible in readable form by any staff member?		
36-1	Does the PSP comply with the requirements listed below?		

	- it provides third-party PSPs with the same information from designated payment accounts and associated payment transactions as is made available to the payment service user in case of direct access to the account information, provided that such information does not include sensitive payment data; -immediately upon receipt of the payment order, the PSP provides third-party PSPs with the same information on the initiation and execution of the payment transaction as is provided or made available to the payment service user when the transaction is directly initiated by the payment service user; -upon request, the PSP immediately provides third-party PSPs with a simple “yes” or “no” answer as to whether or not the amount necessary for the execution of a payment transaction is available on the payer's payment account.		
36-2	In the event of an error or unexpected event during the identification or authentication process or during the exchange of information, do the PSP’s procedures provide for the sending of a notification to third-party PSPs,		

	indicating the reasons for the error or unexpected event?		

V- ANNEXES

1. Rating matrix for fraud risks

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

2. Glossary

Define technical terms and acronyms used in the annex.

Annex 1

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

1. Overview of the internal control framework[4]

1.1. Overall internal control framework:

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

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

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

1.3. Risk management function:

- description of the organisation of the risk management function (*scope of intervention, staffing levels of the units responsible for risk measurement, monitoring and control, and the technical resources at their disposal*);
- for groups, organisation of the risk management function;
- description of the procedures and systems implemented to monitor risks associated with operations involving new products and services, significant changes to existing services, processes or products, internal and external growth operations, and exceptional transactions (cf. Article 221 of the *Arrêté du 3 novembre 2014*, as amended);

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

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

1.4. Periodic control framework:

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

2. Overview of accounting arrangements

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

Annex 2

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

Nota bene: Only payment institutions and electronic money institutions offering payment account management services associated with payment instruments (transfer, direct debit, payment card, etc.) are required to submit this annex.

I. Training

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

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

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

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

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

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

II. Internal control[5]

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

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

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

2.1.3. - preventing over-indebtedness/providing support? Yes / No

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

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

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

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

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

2.5. Have the necessary corrective actions been implemented? Yes/ No

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

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