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

July 2023

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

The items listed below are given for illustrative purposes based on their relevance with regard to the institution's activities and organisational structure. The institution should also provide whatever information is needed to enable the reader of the report to understand how the internal control system operates and to assess the risks it actually bears.

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

The Report on Internal Control should include the most recent internal management reports on the analysis and monitoring of risk exposures that have been provided by the effective managers 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, should be sent to the Secretary General of the *Autorité de contrôle prudentiel et de résolution* (SGACPR) on a quarterly basis.

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

The Report on Internal Control shall be sent to the SGACPR at the latest by **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 in 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 credit et des entreprises d'investissement* (French Association for 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, formalisation and updating mechanisms of the institution's risk mapping, highlights of the main evolutions 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 effective managers, 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 foreign business 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 to ensure the accuracy, integrity, completeness and timely availability of risk data, and definition of a governance process for the risk data aggregation process (see Article 104 of the *Arrêté du 3 novembre 2014*, as amended).

1.3. Major incident

- mechanism put in place 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 in the internal control system

If there have been no significant changes in the internal control system, which contains the three lines of defence corresponding to the levels of control described below, the institution may provide a general description in an annex or provide a copy of the internal control charter in force.

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

- a description of significant changes in the organisation of permanent control, which corresponds to the first and second level 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 and functional position of the person(s) in charge of permanent control and any other functions exercised by such person(s) in the institution or in other entities in 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 in the organisation of the compliance audit function: *specify in particular the identity and the hierarchical and functional position of the person in charge of the compliance audit function and any other functions exercised by this person in the institution or in other entities in the same group;*
- a description of the internal procedures put in place to govern the appointment and dismissal of the head of the compliance function (see Article 28 of the *Arrêté du 3 novembre 2014*, as amended);
- a description of significant changes in the organisation of the risk management function: *specify in particular the identity, the hierarchical and functional position of the person in charge of the risk management function and any other functions exercised by this person in the institution or in other entities in the same group;*
- *the identification of the effective manager in charge of the consistency and effectiveness 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 identification 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 mended;
- the identification of the effective manager in charge of the consistency and efficiency of periodic control;
- a description of significant changes in 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 put in place to govern 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 complete cycle of investigations 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, the group.

3. Governance

3.1. General principles of governance

- a description of the policy for "*risk culture*" deployed within the institution: a summary of communication procedures and staff training programmes on risk profile and responsibilities in terms of risks management…;
- a presentation of ethical and professional standards promoted by the institution (*indicate if they are in-house standards or 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 case of failure and information modalities to governing bodies…;

- a description of processes put in place to identify, manage and prevent conflicts of interest, on the one hand, at the level of the institution, and on the other hand, regarding its staff, modalities of approval and review of such 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 for reporting to the supervisory body

- procedures for the approval of the limits by the supervisory body (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended);
- procedures for reporting to the supervisory body on significant incidents as defined in Article 98 (cf. Article 245 of the *Arrêté du 3 novembre 2014*, as amended);
- if necessary, procedures for reporting to the supervisory body by the risk manager, stating the concerned matters (cf. Article 77 of the *Arrêté du 3 novembre 2014*, as amended);
- procedures for reporting to the supervisory body, by the persons responsible for the internal audit function, of any failures to carry out corrective measures that have been ordered (cf. Article 26 b) of the *Arrêté du 3 novembre 2014*, as amended);
- procedure in place for the person in charge of the compliance audit 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 for reporting to the effective managers

- procedures for reporting to the effective managers on significant incidents as defined in Article 98 of the *Arrêté du 3 novembre 2014*, as amended (cf. Article 245 of the *Arrêté du 3 novembre 2014*, as amended);
- procedures allowing the risk manager to report to the effective managers on the exercise of their duties (cf. Article 77 of the *Arrêté du 3 novembre 2014*, as amended);
- procedures allowing the risk manager to warn the effective managers of any situation that could have significant repercussions on risk management (cf. Article 77 of the *Arrêté du 3 novembre 2014*, as amended).

3.2.3. Due diligence practices carried out by the effective managers and the supervisory body

- a description of the due diligence measures carried out by the effective managers and the supervisory body to verify the effectiveness of internal control systems and procedures (cf. Articles 241 to 243 of the *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 revealed by internal control procedures, main shortcomings noted, related costs, conclusions drawn from their analysis, and measures taken to remediate them (cf. Article 252 of the *Arrêté du 3 novembre 2014*, as amended);
- dates on which the supervisory body reviewed the activities and results of the internal control system for the past year;
- dates of approval of the aggregate risk limits by the supervisory body (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended).

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

- programme of missions (risks and/or entities that have been subjected to control missions by the internal audit function during the year), stage of completion and resources allocated in man-days;
- main shortcomings observed;
- measures taken to remediate the shortcomings observed**,** 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 for following up on the recommendations generated by periodic controls (*tools, persons in charge*) and the results of that follow-up;
- investigations conducted by the internal audit function of the parent entity and by external institutions (external agencies, etc.), summaries of their main conclusions, and details on the decisions taken to remediate any identified shortcomings.

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

Please attach an annex providing:

- **the characteristics of commitments to main shareholders, effective managers and members of the supervisory body**: the identity of the beneficiaries, type of beneficiaries (natural or legal person, shareholder, senior manager or member of the supervisory body), type of commitment, gross amount, deductions (if any), risk weight, date of assignment and expiry date.

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

Reminder: *information regarding the risk of money laundering and terrorist financing (ML-FT) shall be sent in the annual report on the organisation of internal control arrangements on AML-CFT and asset freeze, pursuant to Articles R. 561-38-6 and R. 561-38-7 of the French Code monétaire et financier, according to conditions defined in the Arrêté du 21 décembre 2018.*

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 transactions 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 ethics codes)

6.4 Procedures for reporting defaults, breaches or failures

Please specify:

– the procedures set up to enable managers and staff to report to the person responsible for the compliance verification function of the institution or of their business line, or to the responsible person referred to in Article 28 of the *Arrêté du 3 novembre 2014*, as amended, of potential malfunctions regarding the compliance monitoring system (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 operations relating to new products, to external and to internal growth

– a presentation of the compliance review procedures implemented when operations relating to new products or services, significant changes to them or to the systems associated with the products, external or internal growth operations or exceptional transactions are carried out: *opinion required, systematically and in writing, from the head of the compliance verification function 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 setting up of remedial and monitoring measures

Please specify:

– the procedures set up to centralise information related to potential dysfunctions when implementing 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 actions in order to meet the compliance requirements (cf. Article 38 of the *Arrêté du 3 novembre 2014*, as amended).

6.7. Description of the main dysfunctions identified during the year

6.8. Results of 2nd level permanent control actions carried out on the non-compliance risk

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting of this Report;
- the procedures for following up on the recommendations generated by permanent control (*tools, persons in charge, etc.*);
- the procedures for verifying that the corrective measures ordered by the institution have been carried out by the appropriate persons in a reasonable 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**: this whole section is only relevant to payment institutions and electronic money institutions performing credit transactions.*

Other institutions shall fill out the last sub-section relating to counterparty risk.

7.1. Loan approval procedures

- predefined loan approval criteria;
- factors used in analysing the expected profitability of loans at the time of approval: *methodology, variables considered (loss rates, etc.);*
- a description of the loan approval procedures, including when appropriate any delegations, escalations and/or limits.

7.2. Systems for measuring and monitoring risk

- details on the 10 main exposures (after clustering counterparties);
- stress scenarios used to measure risk, selected assumptions, results and description of their operational integration;
- a general description of exposure limits – by beneficiary, by associated debtors, by lines of business etc. (*specify the size of the limits in relation to capital and earnings*);
- the procedures and frequency for reviewing credit risk limits (*specify the date of the most recent review*);
- any breaches of credit risk limits observed during the past year (*specify their causes, the counterparties involved, the size of the overall exposure, the number of breaches, and their amounts*);
- the procedures for authorising credit risk limit breaches;
- measures taken to rectify credit risk limit breaches;
- the identification, staffing levels, and hierarchical and functional position of the unit charged with monitoring and managing credit risk;
- a description of monitoring measures for advanced risk indicators (*specify the main criteria for placing counterparties under watch-list*);
- the procedures for analysing the quality of loans, and the frequency of the analysis; specify any exposures the internal credit rating of which has changed, along with loans classified as non-performing or written down (*specify any adjustments in the level of provisioning; give the date on which this analysis was conducted in the past year*);
- the procedures and frequency of revaluation of guarantees and collaterals, as well as the main results of controls carried out during the year when appropriate;
- a presentation of the credit risk measurement and management system in place for identifying and managing problem credits and for making adequate value adjustments and recording appropriate amounts for provisions or losses (cf. Article 115 of the *Arrêté du 3 novembre 2014*, as amended);
- the procedures and frequency of provisioning decisions, including when appropriate any delegation and/or escalation measures;
- the procedures and frequency of back-testing exercises carried out on collective and statistical provisioning models, as well as the main results of the year when appropriate;
- the procedures for updating and reviewing loan files, the frequency of review, and the results of the analysis (at least, for counterparties whose loans are overdue, non-performing or impaired, or who present significant risks or exposure volumes);
- the distribution of exposures by risk level (cf. Articles 106 and 253 a) of the *Arrêté du 3 novembre 2014*, as amended);
- the procedures for reporting to the effective managers and the supervision body on the level of credit risk, using summary tables (cf. Article 230 of the *Arrêté du 3 novembre 2014*, as amended);
- the roles of the effective managers and the supervisory body in defining, monitoring and reviewing the institution's overall strategy regarding credit risk and in setting up the limits (cf. Article 224 of the *Arrêté du 3 novembre 2014*, as amended);
- the factors considered in analysing changes in margins, in particular for the loan production of the past year: *methodology, variables analysed, results;*
    - provide details on the calculation of margins: earnings and expenses taken into account; if lending needs to be refinanced, indicate the net borrowing position and the refinancing rate; if there are gains from investing capital allocated to lending, specify the amount and the rate of return;
    - identify the different loan categories (such as retail loans) or business lines for which margins are calculated;

- highlight trends in outstanding loans (at year-end and at intermediary dates) and, where appropriate, in loan production for the past year;

- the procedures used by the effective managers to analyse the profitability of lending activities, the frequency of the analyses, and their results (*specify the date of the most recent analysis*);
- the procedures used to report to the supervisory body on the institution's credit risk exposure, and the frequency of these reports *(attach the most recent management report produced for the supervisory body*);
- the procedures of approval by the supervisory body of the limits suggested by the effective managers (cf. Article 253 of the *Arrêté du 3 novembre 2014, as amended*);
- when appropriate, the procedures and frequency for analysing, assessing and monitoring risks linked to intragroup transactions (credit risk and counterparty credit risk).

Specific elements on counterparty credit risk:

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

7.3. Concentration risk

7.3.1. Concentration risk by counterparty

- the tool used to monitor concentration risk by counterparty: any aggregate measures defined, description of the system used to measure exposures to the same beneficiary (including prudential framework applicable to counterparties considered, financial situation of the counterparty and portfolio, details on procedures used to identify associated beneficiaries, (establishment of a quantitative threshold above which such measures are systematically implemented, etc.), procedures for reporting to the effective managers and the supervisory body;
- the system used to limit exposure by counterparty: general description of the system for setting limits on counterparties (*specify their level in relation to capital and earnings*), the procedures for reviewing limits and the frequency of these reviews, any breaches of limits reported, and the procedures for involving the effective managers in setting and monitoring limits;
- amounts of exposures to main counterparties;
- conclusions on the institution's exposure to concentration risk by counterparty.

7.3.2. Sectorial concentration risk

- the tool used to monitor sectorial concentration risk: any aggregate measures defined, economic model and risk profile, description of the system for measuring exposures in the same business sector (especially counterparties interconnectedness), and procedures for reporting to the effective managers and the supervisory body;
- the system used to limit exposure by business sector: a general description of the system for setting limits on sectorial concentrations (*amount of exposures, specify their level in relation to capital and earnings*), the procedures for reviewing limits and the frequency of these reviews, any breaches of limits reported, and the procedures for involving the effective managers in setting and monitoring limits;
- the distribution of exposures by sector;
- conclusions on the institution's exposure to sectorial concentration risk.

7.3.3. Geographical concentration risk

- the tool used to monitor geographical concentration risk: any aggregate measures defined, description of the system for measuring exposures in the same geographical region, and procedures for reporting to the effective managers and the supervisory body;

- the system for limiting exposure by geographical region: a general description of the system for setting limits on geographical concentrations (*specify their level in relation to capital and earnings*), the procedures for reviewing limits and the frequency of these reviews, any breaches of limits reported, and the procedures for involving the effective managers in setting and monitoring limits;
- the distribution of exposures by geographical region;
- 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 observed;
- measures taken to remediate the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting of this Report;
- the procedures for following up on the recommendations generated by permanent controls (tools, persons in charge, etc.);
- the procedures for verifying that the corrective measures ordered by the institution have been carried out by the appropriate persons in a reasonable 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 put in place, that they are legally valid, that their value is not correlated with that of the mitigated exposure, and that they are properly documented;
- a presentation of the procedures 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 methodologies used and the results obtained);
- a summary of incidents that occurred during the year, when appropriate (denied guarantee calls, unrealised pledges).

7.6. Stress testing of credit risk

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

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 first 20 counterparties contributing to the turnover and the net banking income;
- measures taken to limit the concentration risk;
- controls set up to monitor the concentration risk;
- a presentation of main counterparties (banks, service providers such as agents, etc.) to which the institution's funds are entrusted; procedures for monitoring the ratings of these counterparties;
- controls set up to monitor the counterparty risk.

8. Operational risk

8.1 Governance and organisation of operational risk

- a general description of the overall framework for identifying, managing, monitoring and reporting the operational risk, taking into account the complexity of the activities and the risk tolerance of the institution;
- governance: a description of the governance system deployed for managing the operational risk and of the governance of the model when appropriate, role and missions of the various committees implemented, 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 by lines of business and by geographical areas (numbers of forecasted and effective FTEs, missions, organisational attachment of teams), objectives of the various permanent control teams, actions carried out during the year and progress of reorganisation projects at the end of the year, constraints met and solutions planned/implemented during the implementation of these reorganisation projects, objectives to be achieved and expected timeframe for full deployment of the target organisation;
- scope of the entities: integrated entities and methods (in numbers and in proportion of assets), treatment of entities integrated in the scope of prudential consolidation during the last two financial years, entities potentially excluded and reasons for 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 (*attach an annex with the minutes of the meeting during which the threshold has been 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 (*specify the method used to calculate capital requirements*);
- the monitoring procedures used to ensure that the entirety of incidents to be identified is taken into account in the calculation of own funds requirements, especially regarding legal and non-compliance risks; identification of risks requiring an improvement of the current monitoring mechanism and remedial actions taken;
- a presentation of the risk mapping detailing business/risks not (yet) covered by the mapping organised at the end of the financial year;
- a general description of the reports used to measure and manage operational risk (*specify in particular the frequency of reporting and recipients of the reports, the areas of risk covered, and the use of early warning indicators to signal potential future losses*); documentation and communication of the procedures for monitoring and managing operational risk;
- a general description of any insurance techniques used.

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

- a description of the procedures for integrating operational risk monitoring into the permanent control system, including, inter alia, risks related to low-frequency high-severity events, as well as internal and external fraud risks;
- a description of the main operational risks observed during the course of the year and related costs (settlement incidents, errors, fraud, cybersecurity etc.) and the conclusions drawn.

8.4. Emergency and business continuity plans

- the objectives of emergency and business continuity plans, definitions and scenarios used, overall architecture (comprehensive plan versus one plan per business line, overall consistency in the case of multiple plans), responsibilities (*names and positions of the officers responsible for managing and triggering emergency and business continuity plans and for managing incidents*), scope of business covered by the plans, businesses assigned priority in the event of an incident, residual risks not covered by the plans, timetable for implementing the plans;
- formalisation of procedures, general description of IT backup and fall-back sites;
- tests of emergency and business continuity plans (objectives, scope, frequency, results), procedures for updating plans (frequency, criteria), tools for managing continuity plans (software and IT development), reporting to senior management (on tests, and on any changes to systems and procedures);
- audit of emergency and business continuity plans and results of permanents controls;
- activation of the emergency and business continuity plan(s) and management of incidents that occurred during the course of the year (for example, the H1N1 pandemic, Covid).

8.5 IT risk

8.5.1. Governance

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

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

- a presentation of the measures used to mitigate major IT risks and controls carried out to monitor the effectiveness of these measures, and description of the process used to inform effective maangers and the supervisory body;
- a presentation of the organisation of the management of risks caused by IT (definition of role and responsibilities of players[1], assessment framework of the IT risk profile and its results, risk tolerance threshold, audit process, modalities and frequency of reporting to senior management and the supervisory body on the entity's exposure to risks linked to IT[2]);
- a description of the periodic and permanent control mechanisms of IT systems and summary of observations related to control actions carried out (cf. 8.6);
- a presentation of the IT risk mapping including especially risks for the availability and continuity, security, data integrity and risk linked to IT system changes (identifying in particular what systems and services are essential to the proper functioning, availability, continuity and security of the institution's activities)[3].

8.5.3. Security of the information system

- a presentation of the objectives of the information systems' security policy (protection of the confidentiality, integrity and availability of IT information, assets and services, as well as of customer data) and name of the person responsible for information system security;

[1] Especially those of the IT function

[2] Attach the latest dashboard dedicated to informing them

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

- a description of the procedures set up to prevent and address incidents (i.e. one or more adverse or unexpected events likely to seriously compromise the safety of information and to impact the activity of the institution), in particular for major incidents as defined by the EBA Guidelines issued in application of Article 96 of the DSP2 Directive;
- a presentation of the information system security awareness programme (awareness of employees and service providers) and regular training (cf. last subparagraph of Article 270-3 of the *Arrêté du 3 novembre 2014*, as amended).

8.5.4. Management of IT operations

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

8.5.5. Management of changes and projects

- a description of the IT project and software management framework;
- a description of the process used to manage the acquisition, development and maintenance of IT systems, description of a process used to manage software changes: procedure for the recording, testing, assessment, approval and implementation of changes made to the IT system (cf. Article 270-5 of the *Arrêté du 3 novembre 2014*, as amended).

8.6. Results of 2nd level permanent control actions for operational risk including IT risk

- main shortcomings observed;
- measures taken to remediate the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting of this Report;
- the procedures for following up on the recommendations generated by permanent controls (*tools, persons in charge, etc.*);
- the procedures for verifying that the corrective measures ordered by the institution have been carried out by the appropriate persons in a reasonable timeframe (cf. Articles 11 f) and 26 a) of the *Arrêté du 3 novembre 2014*, as amended).

8.7. Overall conclusions on exposure to operational risk

9. Accounting risk

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

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

- a presentation of changes that have taken place within the consolidation scope, when appropriate (admission and exclusion).

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

- main shortcomings observed;
- measures taken to remediate the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date this Report was drafted;

- the procedures for following up on the recommendations generated by permanent controls (*tools, persons in charge, etc.*);
- the procedures for verifying that the corrective measures ordered by the institution have been carried out by the appropriate persons in a reasonable timeframe (cf. Articles 11 f) and 26 a) of the *Arrêté du 3 novembre 2014*, as amended);
- a presentation of the prevention system for the accounting risk, including the risk of disruption of information systems (backup site…).

10. Cash management

- a description of measures put in place for cash monitoring;
- a detailed description of the policy for cash management approved by the senior management / the supervisory committee;
- a detailed description of the nature of cash investments by 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/electronic money issuing transaction enabling the collection of funds in return for a payment/electronic money issuing order to be traced chronologically (including deadlines), as well as the funding of the various accounts concerned, from the origination of the orders to their actual execution;
- a presentation of the method used to protect assets received from customers and a description of the tool used for the calculation of the amount of assets received from customers to be ring-fenced;
- for institutions ensuring the protection of received assets by placing them in one account, or more, opened specially for this purpose at a credit institution: communication of any modification to the account agreement for ring-fencing (attach an annex with the new agreement where appropriate), description of procedures to ensure the investment of assets;
- for institutions ensuring the protection of received assets through a guarantee: communication of any modification to the collateral arrangement or guarantee contract and any element linked to the adjustment of the amount of the coverage created in respect of the development of business volume (attach an annex with the new collateral agreement or guarantee contract where appropriate);
- a presentation of the procedures implemented to ensure compliance with the provisions related to the protection of the assets of institutions' customers, associated verifications and presentation of the potential incidents or insufficiencies highlighted by these checks.

12. Outsourcing policy

- a presentation of the institution's or group's strategy in terms of outsourcing;
- adjustments made to comply with the requirements to keep a register, including information referred to in section 11 of the EBA guidelines on outsourcing arrangements (see Article 238 of the *Arrêté du 3 novembre 2014*, as amended);
- 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 as a proportion of the institution's overall activity *(as a whole and area by area)*;

- communication of the annual extraction from the register mentioning the outsourcing arrangements concerning critical or important activities (within the meaning of Article 10 of the *Arrêté du 3 novembre 2014*, as amended);
- a description of critical or important activities (within the meaning of Article 10 of *Arrêté du 3 novembre 2014*, as amended) the institution has planned to outsource by employing a service provider and proportion relative to the overall activity of the institution;
- a description of the conditions under which the recourse to outsourcing takes place: 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 visits at the external service provider's premises, etc.;
- a description of procedures for the permanent and periodic control actions to be performed on outsourced activities;
- a description of procedures for risk identification, management and monitoring linked to outsourced activities;
- a description of procedures implemented by the institution to maintain the necessary expertise in order to effectively control outsourced activities and manage risks linked to outsourcing;
- a description of the procedures used for the identification, assessment and management of conflicts of interest related to the outsourcing mechanism of the institution, including between entities of the same group;
- a description of the business continuity plans and of the exit strategy defined for the critical or important outsourced activities: formalisation of retained scenarii and objectives as well as proposed alternative measures, presentation of the carried out tests (frequency, results…), reporting to senior management (regarding the tests, updates on the defined plans or exit strategy);
- procedures to inform the supervisory body on measures taken to control 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 effective managers to verify the efficiency of mechanisms and procedures of internal control 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 at the time 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 at the time of drafting of this report), follow-up procedures for the 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 equivalent guarantee valid for the financial year. The provided proof must specify that the insurance contract of professional liability or ongoing equivalent guarantee is not completed by any separate act establishing an excess of any kind whatsoever;
- should the initially subscribed contract have been modified, provide its amended version;
- for payment institutions authorised to provide the service of payment initiation:
  - complete the following table:

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

- provide the details, where appropriate, of unregulated activities carried out within the institution, and the proof of professional liability insurance or equivalent guarantee covering these activities if such a 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 their responsibility to the payment service provider acting as account manager or the user of payment services following an unauthorised or fraudulent access to payment accounts data or an unauthorised or fraudulent use of this data	
Number of payment accounts the institution acceded to	
Number of clients	

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

14. Annex on the security of cashless payment instruments 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 devoted to the security of **cashless payment instruments** (as defined in Article L. 311-3 of the French *Code Monétaire et Financier*) issued or managed by the institution, and to **the security of accesses to payment accounts and payment account information** within the framework of the provision of payment initiation and payment account information services. Any instrument enabling a person to transfer funds, whatever the medium or technical process used, is considered as a payment instrument.

The annex is sent by the General Secretariat of the *Autorité de contrôle prudentiel et de résolution* to the Banque de France in accordance with its missions as defined in Article L. 141-4 and Article L. 521-8 of the aformeentioned 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 tasks as defined in Article L. 721-20 of the same Code[4].

The annex, mainly dedicated to the Banque de France, is a document independent from the rest of the reports established pursuant to Articles 258 to 266 of the *Arrêté du 3 novembre 2014*, as amended. Additionally, insofar as the Banque de France's jurisdiction covers French territory, this Annex only applies for means of payment offered in France (or payment accounts opened in France), thus 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 should be labelled "Institution that neither issues nor manages cashless payment instruments as part of its business".

Features and contents of this annex

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

This annex is divided into five sections:

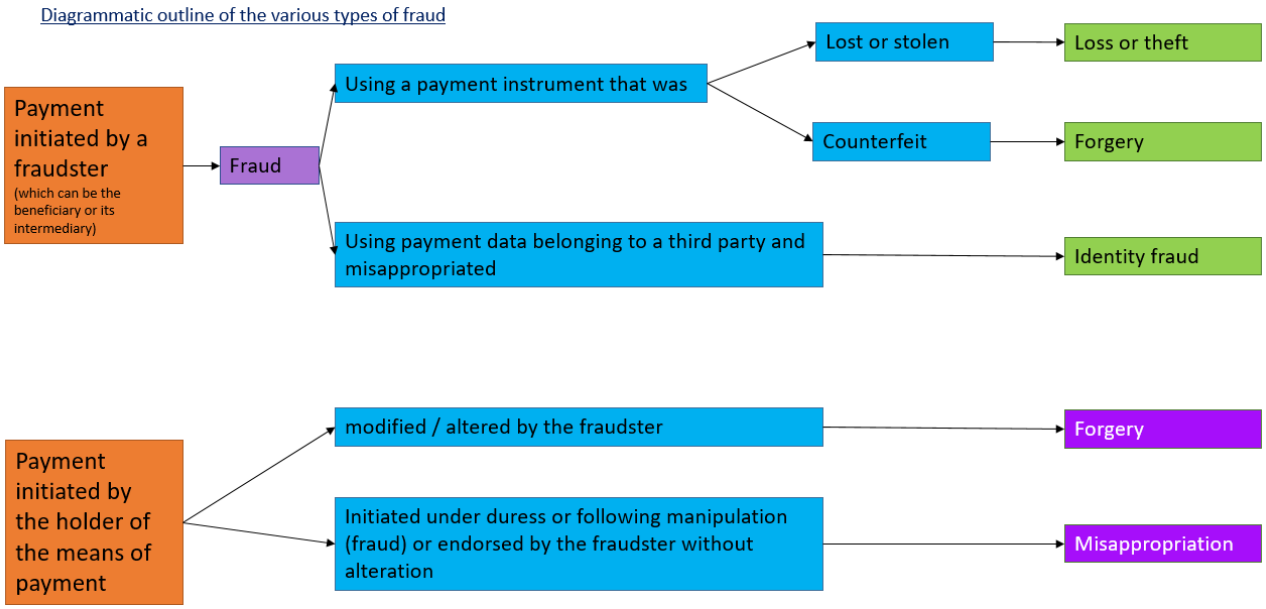
- a section on the presentation of each means and service of payment, risks of fraud associated and risk management mechanisms put in place (I);
- a section dedicated to the results of the periodic review on the scope of non-cash means of payment and access to accounts (II);
- a section dedicated to collect the institution's self-assessment of compliance with the recommendations regarding external bodies as regards the security of non-cash means of payment and the security of account accesses (III);
- a section on the audit report on the implementation of security measures provided in the RTS (*Regulatory Technical Standards*) (IV)[5];
- an annex including the fraud risk rating matrix and a glossary of definitions of technical terms/acronyms used by the institution in the annex (V).

[4] 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), the reference to the "Banque de France" should be changed to one to "IEOM" in this Annex, and references to "French territory" should be changed to "French territorial communities of the Pacific region".

[5] 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 Part I, the analysis of the fraud risks of each means of payment is carried out from fraud data as declared by the institution to the Banque de France within the framework of the collection of statistics "Inventory of fraud on scriptural means of payment"[6]. 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 statistical declaration to the Banque de France.



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, fraud risk analysis matrices specific to each non-cash means of payment presented in the annex shall be completed depending on offers specific to each institution. **Starting with the 2023 annual report on the financial year 2022, institutions are also expected to fill in the cheque section 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* (also referred to as RSC and meaning the French cheque security reference framework) of the Banque de France (RSC) does not allow.

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

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

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

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

Remark concerning providers of information on accounts services

Concerning part I, providers of information on accounts services shall only fill out the section dedicated to account information services (I.5). In addition, they shall complete the parts dedicated to periodic control results (II), to the self-assessment of the compliance with recommendations for 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 system 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	According to the different services and means of payment, the notion of initiation channel corresponds: - for cards, to the channel of use of the card: payment at point-of-sale, withdrawal, remote payment, contactless payment, enlistment in e-wallets or mobile payment solutions; - for 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 statistical collection "Inventory of fraud on non-cash means of payment" of the Banque de France, gross fraud corresponds to the nominal amount of payment transactions authorised which are subject to an *ex post* rejection due to fraud. Therefore, it does not take into account assets which can be 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 procedures and measures to manage them.
Residual risk	Risk persisting after taking into account coverage measures.
Coverage measures	All actions implemented by the institution in order to better manage its risks, by reducing their impact as well as their frequency of occurrence.

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

1. Card and equivalent

1.1. Presentation of the offer

a. Description of products and services

Product and/or service	Characteristics, age and functions proposed	Target clients	Initiation channel	Comments on the evolution of business volume	Comments on evolutions regarding technology, function and security
As an issuing institution					
*Ex: **payment card**: international card*	*Ex: - Maturity - Date of commercialisation - Equiped with the contactless function by default - Enlistment in an authentication device - Virtual card service*	*Ex: Individuals*	*Ex: at the point-of-sale or at the cash machine, remote payment,…*	*Precise explanatory factors of significant variations of activity (number and amount)*	*Indicate evolutions that occurred during the reporting period Ex: pilot realisation , implementation of SMS alerts for the international transactions of high-end cards…*
*Ex: **Withdrawal card***					
*Ex: **Enlistment in wallets***					
As an acquiring institution					
Ex: Acceptation offer of proximity card payments					
Ex: Acceptation offer of card payments for distance selling					

b. Planned projects for products and services

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

1.2. Operational organisation of the activities

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

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

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

1.3. Risk analysis matrix and main fraud incidents

a. Reminder of applicable fraud typology

Category of fraud	Description
Stolen or lost card	The fraudster uses a payment card as a result of a loss or a theft, without the legitimate holder's knowledge.
Card not received	The card has been intercepted during its sending between the issuer and the legitimate holder. This fraud type is similar to loss or theft. However, it is different to the extent that the holder cannot easily notice that a fraudster has a card which was intended for use by the legitimate holder. In this scenario, the fraudster exploits vulnerabilities in card sending processes.

Counterfeit card	The frauster uses (i) a counterfeit payment card, which involves the creation of a medium that appears to be a genuine payment card and/or a card that is designed to deceive an automated teller machine or the payment terminal of a given merchant, or (ii) a forged payment card, the creation process of which involves altering the magnetic, embossing or programming data of a genuine payment card. In both cases, the fraudster makes sure that such a card carries the data necessary to fool the payment acceptance system.
Misappropriated card number	The card number of a holder is collected without him knowing it or created by random card number generators and is used in distance selling.
Other	Any other type of fraud, such as: - the use of a consistent card number that isn't assigned to a legitimate card holder for distant selling transactions, - alteration by the fraudster of a legitimate payment order (forgery), - manipulation or coercion of the legitimate card holder aiming for that legitime card holder to issue a card payment (misappropriation) etc.

b. Global fraud risk rating on card and equivalent

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

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

c. Fraud risk coverage measures

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

As an issuing institution:

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

As an acquiring institution:

Category of fraud	Initiation channel	Coverage measures
Stolen or lost card		
Card not received		
Counterfeit card		
Misappropriated card number		
Other		

d. Evolution of gross fraud over the period under review

As an issuing institution:

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

As an acquiring institution:

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

e. Presentation of emerging fraud risks

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

2. Transfer

2.1. Presentation of the offer

a. Description of products and services

Product and/or service	Characteristics, age and functions proposed	Clients targeted	Initiation channel	Comments on the evolution of business volume	Comments on evolutions regarding technology, functions and security
As an institution of the originator					

b. Planned projects for products and services

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

2.2. Operational organisation for transfer business

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

Actors	Roles
Issuing and management activity	

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

2.3. Risks analysis matrix and main fraud incidents

a. Reminder of applicable fraud typology

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

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

b. Global fraud risk rating on transfer

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

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

c. Fraud risk coverage measures

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

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

d. Evolution of gross fraud over the period under review

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

e. Presentation of emerging fraud risks

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

3. Direct debit

3.1. Presentation of the offer

a. Description of products and services

Product and/or service	Characteristics, age and functions proposed	Clients targeted	Initiation channel	Comments on the evolution of business volume	Comments on evolutions regarding technology, functions and security
As the institution of the debtor					
As the institution of the creditor					

b. Planned projects for products and services

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

3.2. Operational organisation for direct debit

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

Actors	Roles
Issuing and management activity	

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

3.3. Risks analysis matrix and main fraud incidents

a. Reminder of applicable fraud typology

Category of fraud	Description
Fake direct debit	The fraudulent creditor issues direct debits to account numbers obtained illegally and without any authorisation or underlying economic substance ("unauthorised payment transaction" in EBA terminology).

	Example No 1: the fraudster massively issues direct debits to RIB/IBAN the list of which he obtained illegally and without any authorisation or underlying economic reality. Example No 2: the creditor issues unauthorised direct debits after having obtained the debtors's bank details through a loss leader serving as a "hook" (authorised direct debit only). Example No 3: the creditor knowingly issues direct debits that have already been issued (which have either already been paid or have been rejected due to the debtor having issued a stop payment order).
Misappropriation	The fraudulent creditor impersonates a third party and misappropriates their bank details, obtaining the signature of a direct debit mandate for an account that is not his

b. Global fraud risk rating on direct debit

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

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

c. Coverage measures of fraud risk

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

As the institution of the debtor

Category of fraud	Initiation channel	Coverage measures
Fake direct debit		
Misappropriation		

As the institution of the creditor

Category of fraud	Initiation channel	Coverage measures
Fake direct debit		
Misappropriation		

d. Evolution of gross fraud over the period under review

As the institution of the debtor:

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

As the institution of the creditor:

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

e. Presentation of emerging fraud risks

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

4. 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 evolutions regarding technology, functions and security

b. Planned projects concerning the offer of products and services

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

4.2. Operational organisation for cheque remittance

Sum up cheque handling processes, from receipt to remittance to the exchange/charge to account systems, specifying in particular outsourced ones (including those outsourced to the group's entities) and those shared with other institutions. An organisational diagram can be added if 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 grid and main fraud incidents

a. Reminder of applicable fraud typology

Category of fraud	Description
Theft, loss	- The fraudster uses a cheque that was either lost by its legitimate owner or stolen from that person. The cheque bears a forged signature, that is neither the one of the account holder nor the one of its agent. - Fraudulent issue of a cheque by a frauster using a blank form.
Counterfeiting	Counterfeit cheque that is entirely fabricated by the fraudster, drawn on an existing bank or a fake one.
Forging	A regular cheque is intercepted and deliberately altered by a fraudster using chemical and/or mechanical processes (to scratch or

	erase) to alter either the amount of that cheque or the name of the entity it is payable to.
Misappropriation, double presentment	A legitimately issued, lost or stolen cheque that is intercepted while in transit, before reaching the payee, and cashed in to a different account from that of the legitimate payee. The form is regular, the name of the beneficiary is unchanged and the magnetic (MICR) line at the bottom of the cheque rermains valid, as does the customer's signature. - Cheque either lost or stolen after clearing in payment systems and re-presented for collection. - Cheque issued by the legitimate account holder, under duress or through manipulation.

b. Overall fraud risk rating for cheques

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

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

c. Risk coverage measures in place as regards fraud risk

Description of the 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		
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 the 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 proposed	Customers targeted	Initiation channel	Comments on the evolution of business volume	Comments on evolutions regarding technology, functions and security

b. Planned projects for products and services

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

5.2. Operational organisation for electronic money

Sum up processes of means/service of payment precising in particular outsourced ones (including those outsourced to the group's entities) and those shared with other institutions. An organisational diagram can be added if necessary.

Actors	Roles

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

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. Services of information on accounts and of payment initiation

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 evolutions regarding technology, functions and security

b. Planned projects for the service offer

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

6.2. Operational organisation for the offer

Sum up implementation processes for information on accounts services precising in particular arrangements for access to information on accounts with associated security measures as well as outsourced processes (including those outsourced to the group's entities) and those shared with other institutions. An organisational diagram can be added if necessary.

Participants	Roles

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

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 THE PERIODIC CONTROL IN THE SCOPE OF NON-CASH MEANS OF PAYMENT AND ACCESS TO ACCOUNTS

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

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

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

Recommendation statement	Issuing entities	Answer of the institution	
		Compliance assessment (yes / partial / no / N.C.)	**Comments about the assessment**
Prevention measures of specific risks			
Immediate issuing procedures for cards in branches or outlets ("*Instant issuing*") are subject to a risk assessment in order to permanently adjust their level of security.	OSCP[7]		
PCI security measures are adopted and implemented for all processes relating to the acceptance and acquisition of payment cards.	OSCP		
m-POS solutions commercialised by the institution shall respect requirements applicable to classic terminals and rely on communication protocols between the different components of the solution which limit to the bare minimum the ability to access of the transaction data through the terminal.	OSMP[8]		
Strong authentication and enlisting of the client			
For payments via mobile phones, the personal code of payment is different from the PIN code of the SIM card and the confidential code of the user's payment card – when the personal code can be modified by the user, the banking issuer shall recommend that he uses a code different from other codes in his/her possession.	OSCP		

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

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

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

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

For the part relating to common and secure communication standards, the institution only answers the questionnaire if it is a payment account manager and depending on the access interface solution put in place for third party PSPs.

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

	- For initiating an electronic payment operation; - For executing an action, thanks to a means of distance communication likely to imply a risk of fraud regarding payment or any other abusive use.		
	Does the PSP plan security measures ensuring the compliance with each requirement listed below? - No information on one of the items categorised as “knowledge”, “possession” and “inherence” can be deduced from the disclosure of an authentication code; - It is not possible to generate a new authentication code based on another authentication code generated before; - The authentication code cannot be falsified.		
	Does the PSP ensure that the authentication through the		

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

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

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

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

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

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

	subject to measures to avoid their copying?		
Requirements for devices and software associated to items categorised as "inherence"			
8	Has the PSP implemented measures to mitigate the risk that authentication items categorised as "inherent" that are read by access devices and software provided to the payer be exposed to unauthorised third parties? At least, does the PSP ensure that it be very unlikely, with these access devices and software, that an unauthorised third party is authenticated as the payer?		
	Is the payer's use of authentication items categorised as "inherent" subject to measures ensuring that such devices and software avoid any unauthorised use of those items that would result in access to said devices and software?		
Independence of items			
9	Does the PSP ensure that the use of the customer strong authentication items		

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

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

	and “remote electronic credit transfers” respectively; - the amount of the transaction does not exceed the corresponding exemption threshold value mentioned in the Annex to Delegated Regulation 2018/389; - the PSP did not identify any of the following elements after a real-time risk analysis: (i) abnormal expenses or abnormal behavioural pattern of the payer; (ii) unusual information on the use of the payer's device or software access; (iii) signs of malware infection during a session of the authentication procedure (iv) a known scenario of fraud in the provision of payment services; (v) an abnormal location of the payer; (vi) high-risk location of the beneficiary.		

	- The factors related to risks listed below are at least taken into account: (i) the previous expense habits of the individual payment service user; (ii) the payment transaction history of each payment service user of the payment service provider; (iii) the location of the payer and the beneficiary at the time of the payment transaction when the access device or software is provided by the payment service provider; (iv) the identification of abnormal payment behaviours of the payment service user compared to the aforementioned user's payment transaction history.		
Calculation of fraud rate			
19	For each type of transaction ("remote electronic card-based payments" and		

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

	regards any overrun of the maximum permissible fraud rate (as set out in the Annex to the RTS) and for providing a description of the measures envisaged to restore compliance regarding the fraud rate?		
	Does the PSP effectively intend to immediately suspend the implementation of the risk analysis exemption (Article 18) if the maximum permissible rate is exceeded for two consecutive quarters?		
	After the suspension, does the PSP intend to make use of the risk analysis exemption again (Article 18) only when the calculated fraud rate is equal to or below the maximum permitted rate for a quarter and does it have a procedure for informing the Banque de France by communicating the elements proving that the fraud rate became compliant again with the allowed maximum rate?		
Monitoring			

21	Should derogations to high authentication be used (Articles 10 to 18), has the PSP set up a device for recording and controlling for each type of payment transaction and on a quarterly basis the data listed below? - the total value of unauthorised or fraudulent payment transactions, the total value of all payment transactions and the resulting fraud rate, including a breakdown by payment transactions initiated by the strong customer authentication and under each of the waivers; - the average value of operations, including a breakdown by payment transactions initiated through strong customer authentication and under each of the waivers;		

	- the number of payment transactions for which each of the waivers has been applied and the percentage that they represent in relation to the total number of payment transactions.		
CONFIDENTIALITY AND INTEGRITY OF THE CUSTOMISED SECURITY DATA OF PAYMENT SERVICE USERS			
General requirements			
22	Does the PSP ensure the confidentiality and integrity of the user's customised security data, including authentication codes, during all authentication phases by meeting the following requirements? - Customised security data is masked when it is displayed and is not readable in its entirety when it is entered by the payment service user during authentication; - custom security data in data format as well as cryptographic equipment related to the encryption of customised security		

	data are not stored in plain text; - secret cryptographic equipment is protected from unauthorised disclosure.		
	Does the PSP fully document the cryptographic equipment management process used to encrypt or otherwise render the customised security data unreadable?		
	Does the PSP ensure that the processing and routing of customised security data and authentication codes take place in secure environments according to rigorous and widely recognised sectorial standards?		
Data creation and transmission			
23	Does the PSP ensure that the creation of customised security data takes place in a secure environment?		
	Are the risks of unauthorised use of customised security data as well as authentication devices and software following their loss,		

	theft or copy before delivery to the payer well managed?		
Association with the payment service user			
24	Does the PSP ensure that the payment service user is the only one associated, in a secure way, with the customised security data, authentication devices and software according to the requirements listed below? - the association of the payment service user's identity with the customised security data and the authentication devices and software takes place in secure environments that fall within the responsibility of the payment service provider, including at least the premises of the payment service provider and the Internet environment provided by the payment service provider, or other similar secure websites used by the PSP and by its withdrawal services		

	at automated teller machines, and taking into account the risks associated with the underlying devices and components used in the association process that are not under the responsibility of the PSP; - the association, by means of distance communication, of the identity of the payment service user with the personalised security data and the authentication devices or software is performed using customer authentication.		
Delivery of data as well as authentication devices and software			
25	Does the PSP ensure that the delivery of the customised security data as well as the payment service user devices and software is made in a secure manner that prevents the risks associated with their unauthorised use following their loss, theft or copying by		

	applying at least each of the measures listed below? - efficient and secure delivery mechanisms ensure that customised security data and authentication devices and software are delivered to the legitimate payment service user; - mechanisms enable the payment service provider to verify the authenticity of the authentication software delivered to the payment service user via the Internet; - provisions ensure that, when the delivery of the customised security data takes place outside the premises of the payment service provider or by means of remote communication: (i) no unauthorised third parties may obtain more than one element of the customised security data or		

	devices or authentication software when delivery is made through the same means of communication; (ii) the customised security data or authentication devices or software must be activated before they can be used; - provisions ensure that if the personalised security data or authentication devices or software must be activated before their first use, this activation shall be carried out in a secure environment in accordance with the association procedures referred to in Article 24.		
Renewal of customised security data			
26	Does the PSP ensure that the renewal or reactivation of customised security data complies with the procedures for the creation, association and delivery of		

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

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

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

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

	and associated payment transactions that is made available to the payment service user in case of direct request for access to the account information, provided that such information does not contain sensitive payment data; - immediately after receiving the payment order, they shall provide third party PSPs with the same information on the initiation and execution of the payment transaction as that provided or made available to the payment service user when the payment service user directly initiates the transaction; - upon request, it shall immediately provide third party PSPs with a response, in the form of a simple “yes” or “no” answer, regarding whether the amount necessary for the execution of a payment transaction is available or not on the payer's payment account.		
36-2	If there is an error or unforeseen event during the identification or authentication process or when exchanging information, do the		

	PSP's procedures provide for the sending of a notification message to third party PSPs, indicating the reasons for the error or unforeseen event?		
Applicable by the account manager PSP in case of implementation of a dedicated access interface with a back-up mechanism (online banking access with third party authentication)			
29	Does the PSP ensure that all transactions (authentication, consultation and payment initiation) with the payment service user, including merchants, other PSPs and other entities are correctly traced with unique, unpredictable identifiers stamped with the date and time?		
30-1	Has the PSP made available to third party PSPs an access interface that meets the requirements listed below? - third party PSPs are able to identify themselves to the account servicing PSP; - third party PSPs are able to communicate securely with the PSP to execute their payment services.		
30-2	Does the PSP make all authentication procedures offered to payment service users available for use by third party PSPs for the purposes of authentication of payment service users?		

30-2-a-b	Does the PSP's access interface meet the requirements listed below? - the PSP is in a position to start the strong authentication process at the request of a third party PSP that has previously obtained the consent of the user; - the communication sessions between the PSP and third party PSPs are established and maintained throughout the authentication.		
30-3	Does the PSP ensure that its access interface follows communication standards published by European or international standardisation organisations? Do the technical specifications of the access interface documentation mention a series of routines, protocols and tools that third party PSPs need in order to allow for interoperability between their software and applications and the PSP's systems?		
30-4	If the technical specifications for the access interface are changed, except in emergencies, did the PSP plan to make them available to third party PSPs at least three months prior to their implementation?		

	Do the PSP's procedures provide in writing for the emergency situations in which the changes have been implemented, and for making this documentation available to the ACPR and the BDF?		
32-1	Does the PSP ensure that its dedicated access interface offers the same level of availability and performance, including support, than the interface(s) made available to the payment service user to directly access its online payment account?		
32-2	Has the PSP defined key performance indicators and service level target values for its access interface that are transparent and at least as demanding as those set for the interface used by their payment service users, both in terms of availability and data supplied?		
32-4	Are the availability and performance of the access interface controlled by the PSP and are the related statistics published on its website on a quarterly basis?		
33-1	Has the PSP anticipated the implementation of the back-up mechanism after that five consecutive requests for access to the third-party PSP's dedicated		

	interface are unanswered within 30 seconds?		
33-2	Does the PSP have communication plans to inform third-party PSPs that use the dedicated interface of measures to restore the system and a description of the other readily available options that they can use in the meantime?		
33-3	Do the PSP's procedures provide for the timely notification of the dedicated interface problems to the ACPR?		
33-5	For access to the back-up interface, does the PSP ensure that third party PSPs are identified and authenticated according to the authentication procedures planned for its own customers?		
34-1	Is the access of third party PSPs to the PSP's online banking website based on certificates marked as electronic stamps or certified authentication certificates?		
35-1	Are the integrity and confidentiality of customised security data and authentication codes transiting through communication flows or stored in the PSP's information systems insured?		
35-5	Does the PSP ensure that the customised security data and authentication codes they		

	communicate are not directly or indirectly readable by a staff member?		
36-1	Does the PSP meet the requirements listed below? - it provides third party PSPs with the same information from the designated payment accounts and associated payment transactions that is made available to the payment service user in case of direct request for access to the account information, provided that such information does not contain sensitive payment data; - immediately after receiving the payment order, they shall provide third party PSPs with the same information on the initiation and execution of the payment transaction as that provided or made available to the payment service user when the payment service user directly initiates the transaction; - upon request, it shall immediately provide third party PSPs with a response, in the form of a simple “yes” or “no” answer, regarding whether the amount necessary for the execution of a payment transaction is available or not on the payer's payment account.		

36-2	If there is an error or unforeseen event during the identification or authentication process or when exchanging information, do the PSP's procedures provide for the sending of a notification message to third party PSPs, indicating the reasons for the error or unforeseen event?		
Applicable by the account manager PSP in case of implementation of a dedicated access interface without an emergency mechanism			
29	Does the PSP ensure that all transactions (authentication, consultation and payment initiation) with the payment service user, including merchants, other PSP and other entities are correctly traced with unique, unpredictable identifiers stamped with the date and time?		
30-1	Has the PSP made available to third party PSPs an access interface that meets the requirements listed below? - third party PSPs are able to identify themselves to the account servicing PSP; - third party PSPs are able to communicate securely with the PSP to execute their payment services.		
30-2	Does the PSP make all authentication procedures offered to payment service users available for use by third party PSPs for the		

	purposes of authentication of payment service users?		
30-2-a-b	Does the PSP's access interface meet the requirements listed below? - the PSP is in a position to start the strong authentication process at the request of a third party PSP that has previously obtained the consent of the user; - the communication sessions between the PSP and third party PSPs are established and maintained throughout the authentication.		
30-3	Does the PSP ensure that its access interface follows communication standards published by European or international standardisation organisations? Do the technical specifications of the access interface documentation mention a series of routines, protocols and tools that third party PSPs need to enable interoperability between their software and applications and the PSP's systems?		
30-4	If the technical specifications for the access interface are changed, except in emergencies, did the PSP plan to make them available to third party PSPs at least three months prior to their implementation?		

	Do the PSP's procedures provide in writing for the emergency situations in which the changes have been implemented and for making this documentation available to the ACPR and the BDF?		
32-1	Does the PSP ensure that its dedicated access interface offers the same level of availability and performance, including support, than the interface(s) made available to the payment service user to directly access its online payment account?		
32-2	Has the PSP defined key performance indicators and service level target values for its access interface that are transparent and at least as demanding as those set for the interface used by their payment service users, both in terms of availability and data supplied?		
32-4	Are the availability and performance of the access interface controlled by the PSP and are the related statistics published on its website on a quarterly basis?		
33-6	Has the PSP submitted an application for exemption from an emergency mechanism to the ACPR?		
34-1	Is the access of third party PSPs to the PSP's online banking website		

	based on certificates marked as electronic stamps or certified authentication certificates?		
35-1	Are the integrity and confidentiality of customised security data and authentication codes transiting through communication flows or stored in the PSP's information systems insured?		
35-5	Does the PSP ensure that the customised security data and authentication codes they communicate are not directly or indirectly readable by a staff member?		
36-1	Does the PSP meet the requirements listed below? - it provides third party PSPs with the same information from the designated payment accounts and associated payment transactions that is made available to the payment service user in case of direct request for access to the account information, provided that such information does not contain sensitive payment data; - immediately after receiving the payment order, they shall provide third party PSPs with the same information on the initiation and execution of the payment transaction as that provided or		

	made available to the payment service user when the payment service user directly initiates the transaction; - upon request, it shall immediately provide to third party PSPs with a response, in the form of a simple “yes” or “no” answer, regarding whether the amount necessary for the execution of a payment transaction is available or not on the payer's payment account.		
36-2	If there is an error or unforeseen event during the identification or authentication process or when exchanging information, do the PSP’s procedures provide for the sending of a notification message to third party PSPs, indicating the reasons for the error or unforeseen event?		

V- ANNEXES

1. Rating matrix for fraud risks

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

2. Glossary

Define technical terms and acronyms used in the annex.

Annex 1

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

1. Overview of internal control systems[9]

1.1. General internal control system:

- attach an organisation chart showing the units devoted to permanent control(s) (including compliance control) and periodic control, and showing the hierarchical position of their heads;
- coordination between the various persons involved in internal control;
- steps taken in the case of establishment in a country where local regulations prevent the application of the rules stipulated in the *Arrêté du 3 novembre 2014*, as amended;
- steps taken in the case of a transfer of data to entities (such as to service providers) operating in a country that does not provide adequate data protection;
- the procedures for monitoring and controlling transactions conducted under the freedom to provide services.

1.2. Permanent control system (including compliance control):

- a description of the organisation of the different levels that participate in permanent control and compliance control;
- scope of authority of permanent control and compliance control, including foreign business (*activities, processes and entities*);
- human resources assigned to permanent control and compliance control (Article 13, first indent of the the *Arrêté du 3 novembre 2014*, as amended) (full-time equivalent staff as a propotion of the total staffing of the institution);
- description, formalisation and date(s) of updates to permanent control procedures, including those that apply to foreign business (including inspections of compliance);
- the procedures for reporting to the head(s) of permanent control and the effective managers on the activities and results of compliance control.

1.3. Risk management function:

- a description of the organisation of the risk management function (*scope of authority, staffing levels in the units responsible for risk measurement, monitoring and control, and the technical resources at their disposal*);
- for groups, organisation of the risk management function;
- a description of the procedures and systems for monitoring risks arising from new products and services, from significant changes in existing services, processes or products, from internal and external growth, and from unusual transactions (cf. Article 221 of the *Arrêté du 3 novembre 2014*, as amended);
- summary of the risk assessment carried out by the risk management function according to scenarios that are appropriate in view of the significance of the risks induced by these new products and transactions.

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

1.4. Periodic control system:

- a description of the organisation of the audit function, a description of its scope of intervention, including foreign business (*activities, processes and entities*);
- human resources assigned to the internal audit function (cf. Article 25 of the *Arrêté du 3 novembre 2014*, as amended) (full-time equivalent staff as a proportion of total staffing of the institution);
- description, formalisation and date(s) of updates to the procedures the internal control function relies on, including those that apply to foreign business (including inspections of compliance), highlighting significant changes during the year;
- procedure used for defining the frequency and priorities of audit cycles, particularly in relation to the risks identified within the institution .

2. Overview of accounting arrangements

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

Annex 2

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

I. Training

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

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

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

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

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

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

II. Internal control[10]

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

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

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

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

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

2.2. Are points 2.1.1 to 2.1.4 all covered by the periodic control cycle? Yes / No

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

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

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

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

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

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