

July 2019

# 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 Order of 3 November 2014 on the internal control of banking sector companies, payment services and investment services subjected to the supervision of the *Autorité de contrôle prudentiel et de résolution*)

### Contents

Introduction .....	2
1. Overview of business conducted and risks incurred by the institution.....	3
2. Significant changes made in the internal control system.....	3
3. Governance.....	4
4. Results of periodic controls conducted during the year, including foreign business (cf. Article 17 of the Order of 3 November 2014) .....	5
5. Inventory of transactions with effective managers, members of the supervisory body and principal shareholders (cf. Articles 113 and 259 g) of the order of 3 November 2014).....	5
6. Compliance risk (excluding the risk of money laundering and terrorist financing) .....	5
7. Credit and counterparty risk (cf. Articles 106 to 121 of the Order of 3 November 2014) .....	6
8. Operational risk .....	10
9. Accounting risk .....	12
10. Cash management.....	12
11. Internal control system relating to the protection of funds invested .....	13
12. Outsourcing policy .....	13
13. Information specific to institutions authorised to provide payment initiation services and/or account information services .....	14
14. Annex on the security of cashless payment instruments provided or managed by the institution .....	15
Annex 1 .....	76
Annex 2 .....	78

## Introduction

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

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

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

The Report on Internal Control should include the most recent internal management reports on the analysis and monitoring of risk exposures that have been provided by the effective managers to the institution's supervisory body, in accordance with Article 253 of the Order of 3 November 2014.

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

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

The Report on Internal Control shall be sent to the SGACPR at the latest by **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 Monetary and Financial Code;
- 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 Monetary and Financial Code,
  - an overview of the procedures established for these new activities;
  - a description of the internal control for the new activities;
- a description of any major changes in organisation or human resources and of any significant projects launched or conducted during the past year.

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

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

### 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 (called "DSP2");
- process selected to carry out initial and complementary declarations to supervisory authorities.

## 2. Significant changes made in the internal control system

*If there have been no significant changes in the internal control system, the institution may provide a general description in an annex or provide a copy of the internal control charter in force.*

### 2.1. Changes in permanent control (including the organisation of internal control of foreign business and outsourcing)

- a description of significant changes in the organisation of permanent control, including the main actions planned in relation to internal control (cf. Article 259 f) of the Order of 3 November 2014): *specify in particular the identity, the hierarchical and functional position of the person in charge of permanent control and any other functions exercised by this person in the institution or in other entities in the same group;*
- a description of significant changes in the organisation of the compliance control system: *specify in particular the identity, the hierarchical and functional position of the person in charge of compliance and any other functions exercised by this person in the institution or in other entities in the same group;*
- a description of 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;*

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

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

## 3. Governance

### 3.1. General principles of governance

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

### 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 Order of 3 November 2014);
- procedures for reporting to the supervisory body on significant incidents as defined in Article 98 (cf. Article 245 of the Order of 3 November 2014);
- if necessary, procedures for reporting to the supervisory body by the risk manager, stating the concerned matters (cf. Article 77 of the Order of 3 November 2014);
- procedures for reporting to the supervisory body, by the persons responsible for periodic controls, of any failures to carry out corrective measures that have been ordered (cf. Article 26 b) of the Order of 3 November 2014);
- control findings that have been brought to the attention of the supervisory body, and in particular any shortcomings identified, along with the corrective measures ordered (cf. Article 243 of the Order of 3 November 2014).

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

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

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

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

#### 3.2.4. Processing of information by the supervisory body

- 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 correct them (cf. Article 252 of the Order of 3 November 2014);
- dates on which the supervisory body reviewed the activities and results of the internal control system for the past year;
- dates of approval of the aggregate risk limits by the supervisory body (cf. Article 224 of the Order of 3 November 2014).

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

- schedule of missions (risks and/or entities that have been subjected to periodic controls during the year), stage of completion and resources allocated in man-days;
- 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 periodic controls (*tools, persons in charge*) and the results of that follow-up;
- investigations conducted by the inspection unit of the parent entity and by external institutions (external agencies, etc.), summaries of their main conclusions, and details on the decisions taken to correct any identified shortcomings.

### 5. Inventory of transactions with effective managers, members of the supervisory body and principal shareholders (cf. Articles 113 and 259 g) of the order of 3 November 2014)

Please attach an annex providing:

- **the characteristics of commitments for which a deduction has been made from regulatory capital:** the identity of the beneficiaries, type of beneficiaries (natural or legal person, shareholder, senior manager or member of the supervisory body), type of commitment, gross amount, deductions (if any), risk weight, date of assignment and expiry date;
- **the nature of commitments to principal shareholders, effective managers and members of the supervisory body for which a deduction has not been made from regulatory capital** due either to the date on which the commitment was made or the rating or score assigned to the beneficiary of the commitment. However, it is not necessary to mention commitments below a gross amount of 3% of the institution's capital.

### 6. 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, R. 561-38-7 and R.562-1 of the French Monetary and Financial Code, according to conditions defined in the Order of 21 December 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 Order of 3 November 2014)
- 6.2. Assessment and control of reputational risk
- 6.3. Other compliance risks (including compliance 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 compliance officer of the institution or of their business line, or to the responsible person referred to in Article 28 of the Order of 3 November 2014, of potential malfunctions regarding the compliance monitoring system (cf. Article 37 of the Order of 3 November 2014).
- the procedures set up to enable the staff to report to the ACPR any failure to comply with the obligations defined by European regulations and by the French Monetary and Financial Code (cf. Article L. 634-1 and L. 634-2 of the French Monetary and Financial Code).

#### 6.5. Centralisation and setting up of remedial and monitoring measures

Please specify:

- the procedures set up to centralize information related to potential malfunctions when implementing compliance requirements (cf. Articles 36 and 37 of the Order of 3 November 2014);
- the procedures set up to monitor and assess the effective implementation of corrective actions in order to meet the compliance requirements (cf. Article 38 of the Order of 3 November 2014).

#### 6.6. Description of main malfunctions identified during the year

#### 6.7. Results of permanent control on compliance risk

- main shortcomings observed;
- measures taken to correct the shortcomings observed, the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting 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 period of time (cf. Articles 11 f) and 26 a) of the Order of 3 November 2014).

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

*Nota bene:* This whole part is relevant only for payment institutions and electronic money institutions performing credit transactions.

*Other institutions shall complete 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;
- general description of exposure limits – by beneficiary, by associated debtors, by lines of business etc. (*specify the size of the limits in relation to capital and earnings*);
- the procedures and frequency for reviewing credit risk limits (*specify the date of the most recent review*);
- any breaches of credit risk limits observed during the past year (*specify their causes, the counterparties involved, the size of the overall exposure, the number of breaches, and their amounts*);
- the procedures for authorising credit risk limit breaches;
- measures taken to rectify credit risk limit breaches;
- identification, staffing levels, and hierarchical and functional position of the unit charged with monitoring and managing credit risk;
- description of monitoring measures of risk advanced indicators (*specify the main criteria for placing counterparties under watch-list*);
- the procedures for analysing the quality of loans, and the frequency of the analysis; specify any exposures whose internal credit rating has changed, along with loans classified as non-performing or written down (*specify any adjustments in the level of provisioning; give the date on which this analysis was conducted in the past year*);
- the procedures and frequency of revaluation of guarantees and collaterals, as well as the main results of controls carried out during the year when appropriate;
- a presentation of the credit risk measurement and management system in place for identifying and managing problem credits and for making adequate value adjustments and recording appropriate amounts for provisions or losses (cf. Article 115 of the Order of 3 November 2014); the procedures and frequency of provisioning decisions, including when appropriate any delegation and/or escalation measures;
- the procedures and frequency of back-testing exercises of collective and statistical provisioning models, as well as the main results of the year when appropriate;
- the procedures for updating and reviewing loan files, the frequency of review, and the results of the analysis (at least, for counterparties whose loans are overdue, non-performing or impaired, or who present significant risks or exposure volumes);
- distribution of exposures by risk level (cf. Articles 106 and 253 a) of the Order of 3 November 2014);
- the procedures for reporting to the effective managers and the supervision body on the level of credit risk, using summary tables (cf. Article 230 of the Order of 3 November 2014);
- 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 Order of 3 November 2014);
- factors considered in analysing changes in margins, in particular for the loan production of the past year: *methodology, variables analysed, results*;

- provide details on the calculation of margins: earnings and expenses taken into account; if lending needs to be refinanced, indicate the net borrowing position and the refinancing rate; if there are gains from investing capital allocated to lending, specify the amount and the rate of return;
  - identify 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 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 Order of 3 November 2014);
  - when appropriate, the procedures and frequency for analysing, assessing and monitoring risk linked to intragroup transactions (credit risk and counterparty credit risk).

#### Specific elements on counterparty credit risk:

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

### 7.3. Concentration risk

#### **7.3.1. Concentration risk by counterparty**

- tool for monitoring concentration risk by counterparty: any aggregate measures defined, description of the system for measuring exposures to the same beneficiary (including prudential framework applicable to counterparties considered, financial situation of the counterparty and portfolio, 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;
- system for limiting exposure by counterparty: general description of the system for setting limits on counterparties (*specify their level in relation to capital and earnings*), the procedures for reviewing limits and the frequency of these reviews, any breaches of limits reported, and the procedures for involving the effective managers in setting and monitoring limits;
- amounts of exposures to main counterparties;
- conclusions on the institution's exposure to concentration risk by counterparty.

#### **7.3.2. Sectorial concentration risk**

- tool for monitoring 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 network), and procedures for reporting to the effective managers and the supervisory body;
- system for limiting exposure by business sector: a general description of the system for setting limits on sectorial concentrations (*amount of exposures, specify their level in relation to capital and earnings*), the procedures for reviewing limits and the frequency of these reviews, any breaches of limits reported, and the procedures for involving the effective managers in setting and monitoring limits;
- distribution of exposures by sector;
- conclusions on the institution's exposure to sectorial concentration risk.



### 7.3.3. Geographical concentration risk

- the tool for monitoring geographical concentration risk: any aggregate measures defined, description of the system for measuring exposures in the same geographical region, and procedures for reporting to the effective managers and the supervisory body;
- the system for limiting exposure by geographical region: a general description of the system for setting limits on geographical concentrations (*specify their level in relation to capital and earnings*), the procedures for reviewing limits and the frequency of these reviews, any breaches of limits reported, and the procedures for involving the effective managers in setting and monitoring limits;
- distribution of exposures by geographical region;
- conclusions on the institution's exposure to geographical concentration risk.

### 7.4. Results of permanent control of credit activities

- main shortcomings observed;
- measures taken to correct the shortcomings observed, the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting 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 period of time (cf. Articles 11 f) and 26 a) of the Order of 3 November 2014).

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

Attach an annex providing:

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

### 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 risk for institutions unauthorised to perform credit activity

- 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;
- presentation of main counterparties (banks, 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

- general description of the overall framework for identifying, managing, monitoring and reporting the operational risk, taking into account the complexity of the activities and the risk tolerance of the institution;
- governance: description of the governance system deployed for managing the operational risk and of the governance of the model when appropriate, role and missions of the different committees implemented, structuring decisions taken during the year regarding operational risk;
- organisation: presentation of the different teams in charge of the permanent control of operational risk by lines of business and by geographical areas (numbers of forecasted and effective FTEs, missions, attachment of teams), objectives of the different teams of permanent control, actions carried out during the year and progress of reorganization projects at the end of the year, constraints met and solutions planned/implemented during the implementation of these reorganisation projects, objectives to achieve and period planned for the whole deployment of the target organisation;
- entities' perimeter: integrated entities and methods (in numbers and in proportion of assets), treatment of entities integrated in the perimeter of prudential consolidation during the last two financial years, entities potentially excluded and reasons of exclusion, transactions taken into account;
- definition of a significant incident took on by the supervisory body within the framework of Article 98 of the Order of 3 November 2014 (*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 risk to which the institution is exposed;
- a description of the system used to measure and monitor operational risk (*specify the method used to calculate capital requirements*);
- the monitoring procedures used to ensure that the completeness of incidents to be identified is taken into account in the calculation of own funds requirements, especially regarding legal and compliance risks; identification of risks requiring an improvement of the current monitoring mechanism and remedial actions taken;
- presentation of the risk mapping detailing business/risks not (yet) covered by the mapping organized at the end of the financial year;
- a general description of the reports used to measure and manage operational risk (*specify in particular the frequency of reporting and recipients of the reports, the areas of risk covered, and the use of early warning indicators to signal potential future losses*); documentation and communication of the procedures for monitoring and managing operational risk;
- a 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, low-frequency high-severity events related risks, 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 attendant conclusions drawn.

#### 8.4. Emergency and business continuity plans

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

#### 8.5 Risks linked to information and communication technology (ICT)

##### 8.5.1. Governance

- presentation of the institution's ICT strategy (organisation, coordination with the overall strategy, priority objectives set up, risk appetite framework linked to ICT and resources dedicated to implement it (procedures put in place to ensure its compliance, dedicated budget and steering procedure, number and nature of dedicated staff, measures for risk awareness of staff, planification process and date of last update...);
- presentation of the ICT governance process (roles of effective managers, of the supervisory body in the definition, monitoring and review of the global ICT strategy).

##### 8.5.2 Risk management

- presentation of the organisation of the management of risks caused by ICT (definition of role and responsibilities of players<sup>1</sup>, 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 ICT<sup>2</sup>);
- description of the periodic and permanent control mechanisms of IT systems and synthesis of observations of controls carried out (cf. 8.6);
- summary description of the overall framework for the detection, assessment, management and monitoring of risks linked to ICT;
- presentation of the risk mapping linked to ICT including especially risks for the availability and continuity of ICT, ICT security, data integrity and risk linked to the ICT changes (identifying in particular what systems and services are essential to the proper functioning, availability, continuity and security of the institution's activities)<sup>3</sup>.

##### 8.5.3. Security and resilience

- objectives of the information systems security policy and name of the person responsible for information systems security;

<sup>1</sup> Especially those of the IT function.

<sup>2</sup> Attach the latest dashboard dedicated to inform them

<sup>3</sup> 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 in case of incidents affecting ICT (i.e. one or more adverse or unexpected events likely to seriously compromise the safety of information and to impact the activity of the institution), in particular for major incidents as defined by the EBA Guidelines issued in application of Article 96 of the DSP2 Directive.

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

- main shortcomings observed;
- measures taken to correct the shortcomings observed, the expected date for carrying out these measures, and the state of progress in implementing them as at the date of drafting 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 period of time (cf. Articles 11 f) and 26 a) of the Order of 3 November 2014).

#### 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.*

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

#### 9.2. Results of permanent controls on accounting risk

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

### 10. Cash management

- description of measures put in place for cash monitoring;
- detail the policy for cash management approved by the senior management / the Supervisory Committee;
- detail 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

- complete schemes and description of the overall financial flows according to their type of payment transaction (resp. issuing electronic money transaction) allowing to retrace chronologically (including deadlines), fundraising flows in return for a payment order (resp. the issuance of electronic money) and the feeding of the different accounts, origination of orders at their effective completion date;
- 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 and 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);
- presentation of the procedures implemented to ensure compliance with the provisions related to the protection of the assets of institutions' customers, verifications associated and presentation of possible incidents or insufficiencies highlighted by these verifications.

## 12. Outsourcing policy

- presentation of the institution's or group's strategy in terms of outsourcing;
- description of outsourced activities (under q) and r) of Article 10 of Order of 3 November 2014) and proportion to the institution's overall activity (*as a whole and area by area*);
- description of critical or important activities (within the meaning of Article 10 of Order of 3 November 2014) for which the institution has planned to outsource them by employing a service provider and proportion relative to the overall activity of the institution;
- description of conditions under which the use of outsourcing takes place: host country, authorisation and prudential supervision of external providers, procedures implemented to ensure that a written contract exists and that it complies with the requirements of Article 239 of Order of 3 November 2014, including those allowing the *Autorité de contrôle prudentiel et de résolution* to conduct on-site visits at the external provider, etc.;
- description of procedures of permanent and periodic controls of outsourced activities;
- description of procedures for risk identification, management and monitoring linked to outsourced activities;
- description of procedures implemented by the institution to maintain the necessary expertise in order to control effectively outsourced activities and manage risks linked to outsourcing;
- procedures to inform the supervisory body on measures taken to control outsourced activities and the resulting risks (cf. Article 253 c) of Order of 3 November 2014);
- description of due diligence carried out by the effective managers to verify the efficiency of mechanisms and procedures of internal control for outsourced activities (cf. Article 242 of Order of 3 November 2014);
- description, formalisation and date(s) of update of the procedures used for the permanent and periodic control of outsourced activities (including compliance review procedures);
- results of permanent controls carried out on outsourced activities: main shortcomings detected and corrective measures implemented to address them (provisional date of implementation and progress of their implementation at the time of drafting this report), follow-up procedures for the recommendations resulting from permanent controls (*tools, persons in charge*);

- results of periodic controls carried out on outsourced activities: main shortcomings detected and corrective measures implemented to address them (provisional date of implementation and progress of their implementation at the time of drafting this report), follow-up procedures for the recommendations resulting from periodic controls.

### 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:
- complete 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 unauthorized 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**

### **CONTENTS**

#### **Introduction**

#### **I. Presentation of means of payment and risks of fraud to which the institution is exposed**

1. Card and equivalent
  - 1.1. Presentation of the offer
  - 1.2. Operational organisation for card and equivalent business
  - 1.3. Risk analysis matrix and main fraud incidents
2. Transfer (SEPA and equivalent)
  - 2.1. Presentation of the offer
  - 2.2. Operational organisation for transfer business
  - 2.3. Risk analysis matrix and main fraud incidents
3. Direct debit
  - 3.1. Presentation of the offer
  - 3.2. Operational organisation for direct debit business
  - 3.3. Risk analysis matrix and main fraud incidents
4. Electronic money
  - 4.1. Presentation of the offer
  - 4.2. Operational organisation for electronic money business
  - 4.3. Description of main fraud incidents
5. Services of information on accounts and of payment initiation
  - 5.1. Presentation of the offer
  - 5.2. Operational organisation for the offer
  - 5.3. Presentation of measures for protecting sensitive payment data

#### **II. Presentation of the results of the periodic control in the scope of non-cash means of payment**

#### **III. Assessment of the compliance with recommendations of external entities in terms of security of non-cash means of payment**

#### **IV. Audit report on the implementation of security measures provided in the RTS (Regulatory Technical Standards)**

#### **V. Annexes**

1. Rating fraud risk matrix for the institution
2. Glossary

## INTRODUCTION

### Reminder of legal framework

This annex is devoted to the security of **cashless payment instruments** (as defined in Article L. 311-3 of the French Monetary and Financial Code) issued or managed by the institution. 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 mission as defined in Article L. 141-4 of the aforesaid French Monetary and Financial Code.

The annex, mainly dedicated to the Banque de France, is a document independent from the rest of the reports established pursuant to Articles 258 to 266 of the Order of 3 November 2014.

Institutions managing payment instruments, without issuing them, shall fill in this annex. Institutions that neither issue nor manage cashless payment instruments should be labelled “Institution that neither issues nor manages cashless payment instruments as part of its business”.

### Features and contents of this annex

This annex aims at assessing the level of security reached by all the non-cash means of payment issued or managed by the institution.

This annex is divided into five parts:

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

Regarding Part I, the analysis of the fraud risks of each means of payment is carried out from fraud data as declared by the institution to the Banque de France within the framework of the collection of statistics “Inventory of fraud on scriptural means of payment”<sup>4</sup>. As a consequence, this analysis is carried out:

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

To this end, analysis matrices of fraud risks specific to each non-cash means of payment presented in the annex shall be completed depending on offers specific to each institution. However, concerning electronic money and service of information on accounts and without a specific collect of fraud, institutions are exempted from

<sup>4</sup> 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>



carrying out this analysis. Nevertheless, they have to report the main fraud incidents encountered over the financial year under review.

The list of recommendations, linked to the security of means of payment issued by external bodies presented in the part III of the annex, takes account of the application, on 13 January 2018, of the 2<sup>nd</sup> 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 collect 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*). The purpose of this report is to assess the institution's compliance with security requirements provided for in the RTS. It takes the form of a questionnaire covering the security measures provided for in the RTS and for which the institution must provide reasoned answers on their implementation or, when applicable, on the action plan envisaged to comply with them. Pursuant to Article 3 of the RTS, it is recalled that this audit report has to be established annually by periodic control teams of the institution. However, regarding the assessment of the institution's compliance with Article 18 of the RTS in case of 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); it shall be annexed to the audit report (part IV).

### **Remark concerning providers of information on accounts services**

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

### **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: <ul style="list-style-type: none"> <li>- For card, to the channel of use of the card: payment at point-of-sale, withdrawal, remote payment, contactless payment, enlistment in e-wallets or mobile payment solutions;</li> <li>- For transfer, to the reception channel of the transfer order: desk, online banking, teletransmission solution...;</li> <li>- For direct debit, to the reception channel of the direct debit order;</li> <li>- For services of information on accounts and of payment initiation, to the connection mean: website, mobile application, dedicated protocol...</li> </ul>
External fraud	In the field of means of payment, misappropriation of them, by acts of third parties, for the benefit of an illegitimate beneficiary.
Internal fraud	In the field of means of payment, misappropriation of them, by acts of third parties involving at least a member of the company, for the benefit of an illegitimate beneficiary.

Gross fraud	Within the meaning of the statistical collection “Inventory of fraud on non-cash means of payment” of the Banque de France, gross fraud corresponds to the nominal amount of payment transactions authorised which are subject to an <i>ex post</i> rejection for fraud reason. Therefore, it does not take into account assets which could have been collected after the processing of litigation.
Gross risk	Risks likely to affect the proper functioning and security of means of payment, before the institution takes into account procedures and measures to manage them.
Residual risk	Risk persisting before taking into account coverage measures.
Coverage measures	All actions implemented by the institution in order to better manage its risks, by reducing their impact as well as their frequency of occurrence.

## I – PRESENTATION OF MEANS 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
<b>As an issuing institution</b>					
Ex: <b>payment card:</b> international card	Ex: - Maturity - Date of commercialisation - Equiped with the contactless function by default - Enlistment in an authentication device - Virtual card service	Ex: Individuals	Ex: at the point-of-sale or at the cash machine, remote payment,...	Precise explanatory factors of significant variations of activity (number and amount)	Indicate evolutions occurred during the reporting period Ex: pilot realisation , implementation of SMS alerts for transactions of high-end international cards...
Ex: <b>Withdrawal card</b>					
Ex: <b>Enlistment in wallets</b>					
<b>As an acquiring institution</b>					
Ex: Acceptation offer of proximity card payments					
Ex: Acceptation offer of card payments for distance selling					

**b. Planned projects for products and services**

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

**1.2. Operational organisation of the activities**

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

Actors	Roles
<b>Issuing and management activity</b>	
Directorates, departments, service providers,...	
<b>Acquisition activity</b>	

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

**1.3. Risk analysis matrix and main fraud incidents****a. Reminder of applicable fraud typology**

Category of fraud	Description
Theft/loss of card	The fraudster uses a payment card obtained as a result of a loss or a thief.
Card not received	The card has been intercepted during its sending between the issuer and the legitimate holder. This origin type is close to loss or thief. However, it is different to the extent that the holder can less easily notice that a fraudster has a card which belongs to him/her and that he exploits vulnerabilities specific to card sending processes.

Falsified or counterfeit card	An authentic payment card is falsified by modification of magnetic data, embossing or programming data; a counterfeited card is made from data collected by the fraudster.
Stolen card number or non-assigned card number	<ul style="list-style-type: none"> <li>- 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.</li> <li>- Use of a consistent PAN (Personal Account Number) but non assigned to a holder and generally used in distance selling.</li> </ul>

### b. Global fraud risk rating on card and equivalent

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

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

### c. Coverage measures of fraud risk

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

As an issuing institution:

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

As an acquiring institution:

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

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

As an issuing institution:

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

As an acquiring institution:

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

**e. Presentation of emerging risks of fraud**

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

<b>2. Transfer</b>	
--------------------	--

## 2.1. Presentation of the offer

### a. Description of products and services

[illegible]

**b. Planned projects for products and services**

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

**2.2. Operational organisation for transfer business**

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

Actors	Roles
<b>Issuing and management activity</b>	

*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	<ul style="list-style-type: none"> <li>- The fraudster issues a fake transfer order (including when it has been made on coercion by the legitimate holder).</li> <li>- Usurpation of online bank user ID of the legitimate originator (including when the online bank user ID has been collected on coercion or through processes as phishing or social engineering).</li> </ul>
Counterfeiting of transfer order	The transfer order is intercepted and modified by the fraudster.
Misappropriation	The payer issues a transfer to a RIB/IBAN which is not the one of the legitimate beneficiary. Typically done after the beneficiary misused identity (social engineering for example).



**b. Global fraud risk rating on transfer**

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

<u>Gross risk</u> (Inherent risk before coverage measures)	
<u>Residual risk</u> (Risk remaining after coverage measures)	

**c. Coverage measures of fraud risk**

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

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

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

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

**e. Presentation of emerging fraud risks**

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

--

**3. Direct debit****3.1. Presentation of the offer****a. Description of products and services**

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

**b. Planned projects for products and services**

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

**3.2. Operational organisation for direct debit**

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

Actors	Roles
<b>Issuing and management activity</b>	

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

**3.3. Risks analysis matrix and main fraud incidents****a. Reminder of applicable fraud typology**

Category of fraud	Description
Fake direct debit	Direct debit issued by a creditor without a licit direct debit authorisation from the debtor. Example n°1: the fraudster issues massively direct debits to RIB/IBAN which list he obtained illegally and without any authorisation or underlying economic reality.

	Example n°2: the creditor issues unauthorised direct debits after having obtained the details of the debtor's bank thanks to a loss leader serving as a "hook" (only an authorised direct debit).
Misappropriation	-Modification by the fraudster of the account number to be credited associated to direct debit files. -The creditor issues deliberately a direct debit whose amount is largely higher than the amount owed (for example: the creditor obtains the signature of the direct debit mandate for a given service serving as a "hook" and uses this mandate to obviously extort funds to the debtor). - Issuer usurping a creditor ID (NNE/ICS) which is not his.
Replay	The creditor issues deliberately direct debits already issued (that have already been paid or that have been subjected to rejections for debtor opposition for example).

### b. Global fraud risk rating on direct debit

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

<u>Gross risk</u> (Inherent risk before coverage measures)	
<u>Residual risk</u> (Risk remaining after coverage measures)	

### c. Coverage measures of fraud risk

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

As the institution of the debtor

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

As the institution of the creditor

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

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

As the institution of the debtor:

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

As the institution of the creditor:

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

**e. Presentation of emerging fraud risks**

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

--

## 4. Electronic money

### 4.1. Presentation of the offer

#### a. Description of products and services

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

**b. Planned projects for products and services**

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

**4.2. Operational organisation for electronic money**

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

Actors	Roles

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

**4.3. 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)

## 5. Services of information on accounts and of payment initiation

### 5.1 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.*

**5.2 Operational organisation for the offer**

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

Participants	Roles

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

**5.3. 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

*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

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 agency or outlets (" <i>Instant issuing</i> ") are subject to a risk assessment in order to permanently adjust their level of security.	OSCP <sup>5</sup>		
For payments via mobile phones and contactless payment cards, a risk assessment is conducted before any large-scale deployment, in order to ensure the same global security level as for proximity transactions and payments on machines.	OSCP		
In the case where biometrics is used as an identification factor, the payment service provider conducted a risk analysis so that the protection level of implemented solutions is at least equivalent to the one provided by techniques already in place (confidential number and smart card for proximity payments, and a one-time use number for remote payments).	OSCP		
PCI security measures are adopted and implemented for all processes of 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 necessary the ability of access of the mobile machine to transaction data.	OSMP <sup>6</sup>		

#### Strong authentication and enlisting of the client

<sup>5</sup> *Observatoire de la sécurité des cartes de paiement*, the French Banking Card Observatory

<sup>6</sup> *Observatoire de la sécurité des moyens de paiement*, the French Banking Means of Payment Observatory

The initiation of payments (individually or en masse) on the Internet, the access to sensitive payment data or the modification of lists of registered beneficiaries are protected by a strong authentication.	OSMP		
For payments via mobile phones, the personal code of payment is different from the PIN code of the SIM card and the confidential code of the user's payment card – when the personal code can be modified by the user, the banking issuer shall recommend that he uses a code different from other codes in his/her possession.	OSCP		
Rules define the validity period of authentication devices (including One-Time Passwords), the maximum number of identification/authentication errors or connection attempts and the expiration of the sessions for payment services on the Internet.	SecuRe Pay EBA		
The registration of the client and supply of tools, software and authentication data to the client, required for using payment services (including on the Internet) is securely carried out.	SecuRe Pay EBA		
For payments via mobile phones and contactless card, specific measures are in place to ensure the holder consents. For example, the provision of simple means to activate and deactivate these new initiation modes or to validate a transaction.	OSCP		
<b>Management of operational and security risks</b>			
The institution set up a framework for managing operational and security risks aiming at mitigating these risks. This framework is documented and reviewed at least annually by a high-level governing body.	EBA		
In case of outsourcing, the institution ensures that the framework of risks management effectively covers outsourced activities.	EBA		
The institution ensures the protection of sensitive payment data during its storage, treatment and transmission.	EBA		
Mechanisms for following transactions are implemented to prevent, detect and block suspicious transactions before their authorisations.	EBA		

The institution implemented a framework for the continuity of activity, aiming at ensuring its ability to provide payment services without interruption and at limiting losses in case of serious disruptions. This framework relies on the definition of crisis scenarios and regular test of response plans.	EBA		
--	-----	--	--



**IV – AUDIT REPORT ON THE IMPLEMENTATION OF SECURITY MEASURES PROVIDED FOR IN THE RTS (REGULATORY TECHNICAL STANDARDS)** *For the part relating to common and secure communication standards, the institution answers the questionnaire only if it is a payment account manager and in function of the access interface solution put in place for third party PSP.*

Ref. Articles Regulation (EU) 2018/389	Questions asked to PSP	Assessment of compliance	
		Yes / partially / No / NC	For each security 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;		

	<ul style="list-style-type: none"> <li>- For initiating an electronic payment operation;</li> <li>- 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.</li> </ul>		
	<p>Does the PSP plan security measures ensuring the respect of each requirement listed below?</p> <ul style="list-style-type: none"> <li>- No information on one of the items categorised as “knowledge”, “possession” and “inherence” can be deducted from the disclosure of an authentication code;</li> <li>- It is not possible to generate a new authentication code based on another authentication code generated before;</li> <li>- The authentication code cannot be falsified.</li> </ul>		
	Does the PSP ensure that the authentication through the		



	<p>generation of an authentication code integrates each of the measures listed below?</p> <ul style="list-style-type: none"> <li>- 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 determinate which items (knowledge, possession and inherence) were incorrect;</li> <li>- The number of consecutive unsuccessful authentication attempts at which the actions provided for in Article 97(1) of Directive (EU) No 2015/2366 are blocked on a temporary or permanent basis</li> </ul>		
--	---	--	--

	<p>shall not exceed five within a given period of time;</p> <ul style="list-style-type: none"> <li>- Communication sessions are protected against interception of authentication data communicated during the authentication and manipulation by unauthorised third parties</li> <li>- The payer's maximum period of inactivity, once authenticated to access his/her online payment account, does not exceed five minutes</li> </ul>		
	<p>In the event of temporary blocking following unsuccessful authentication attempts, shall the duration of the test and the number of retries be determined on the basis of the features of the service provided to the payer and all associated risks, taking into account, at a minimum, the factors set out in Article 2 (2) of RTS?</p>		

	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?		
<b>Dynamic linkage</b>			
<b>5</b>	<p>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?</p> <ul style="list-style-type: none"> <li>- The payer shall be informed of the amount of the payment transaction and the payee.</li> <li>- The generated authentication code is specific to the payment transaction amount and to the payee approved by the payer when initiating the transaction.</li> <li>- The authentication code accepted by the</li> </ul>		

	<p>payment service provider shall correspond to the specific original amount of the payment transaction and the identity of the payee approved by the payer.</p> <ul style="list-style-type: none"> <li>- Any changes to the amount or beneficiary result in the invalidation of the generated authentication code.</li> </ul>		
	<p>Does the PSP apply security measures that ensure the confidentiality, authenticity and integrity of each of the elements listed below?</p> <ul style="list-style-type: none"> <li>- The amount of the operation and the payee during all phases of authentication;</li> <li>- the information that is displayed for the payer during all authentication phases, including the generation, transmission and use of the authentication code.</li> </ul>		
	When the PSP applies strong customer authentication (in		

	<p>accordance with Article 97(2) of Directive (EU) 2015/2366) does the PSP meet the requirements listed below?</p> <ul style="list-style-type: none"> <li>- Regarding card-related payment transactions for which the payer has approved the exact amount of funds to be blocked under Article 75 (1) of that Directive, the authentication code is specific to the amount for which the payer gave its consent and the payer approved at the initiation of the transaction;</li> <li>- 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</li> </ul>		
--	---	--	--

	payment transactions and to the designated beneficiaries.		
<b>Requirements for items categorised as “knowledge”</b>			
<b>6</b>	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?		
<b>Requirements for items categorised as “possession”</b>			
<b>7</b>	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?		
<b>Requirements for devices and software associated to items categorised as “inherence”</b>			

8	<p>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?</p> <p>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?</p>		
	<p>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?</p>		
<b>Independence of items</b>			
9	<p>Does the PSP ensure that the use of the customer strong authentication items categorised as “possession”, “knowledge” and “inherent” is subject to measures</p>		

	ensuring that, in terms of technology, algorithms and parameters, the breach of one of the items does not question the reliability of others?		
	<p>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?</p> <ul style="list-style-type: none"> <li>- the use of separate secure execution environments through the software installed on the multi-functional device;</li> <li>- mechanisms to ensure that the software or device has not been altered by the payer or a third party;</li> <li>- in the event of alterations, mechanisms to reduce</li> </ul>		



	the consequences thereof.		
<b>EXCEPTIONS TO THE STRONG CUSTOMER AUTHENTICATION OBLIGATION</b>			
<b>Analysis of transaction risks</b>			
<b>18</b>	<p>In the event of a risk analysis exemption, does the PSP meet the requirements listed below?</p> <ul style="list-style-type: none"> <li>- 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;</li> <li>- the amount of the transaction does not exceed the corresponding exemption threshold value mentioned in the Annex to Delegated Regulation 2018/389;</li> <li>- the PSP did not identify any of the following elements after a real-time risk analysis:</li> </ul>		

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

	<p>at the time of the payment transaction when the access device or software is provided by the payment service provider;</p> <p>(iv) the identification of abnormal payment behaviours of the payment service user compared to the aforementioned user's payment transaction history.</p>		
<b>Calculation of fraud</b>			
<b>19</b>	<p>For each type of transaction ("remote electronic card-based payments" and "remote electronic credit transfers"), does the PSP ensure that the overall fraud rates measured for each of the reasons for the exemption from strong authentication (referred to in Articles 13 to 18) are equivalent to or below the maximum allowed rate per amount tranche as defined in the Annex to the RTS?</p>		
	<p>For each type of transactions ("remote electronic card-based payments" and</p>		

	<p>“remote electronic credit transfers”), are the fraud rates for each of the reasons for strong authentication exemptions (referred to in Articles 13 to 18) well calculated by the PSP:</p> <ul style="list-style-type: none"> <li>- by the initial amount of fraudulent payment transactions (“gross fraud approach”) divided by the total value of all payment transactions with or without strong authentication;</li> <li>- and on a rolling quarterly basis (90 days).</li> </ul>		
<b>Suspension of derogations based on the analysis of transaction risks</b>			
<b>20</b>	<p>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</p>		

	restore the compliance of the fraud rate?		
	Does the PSP effectively intend to immediately suspend the implementation of the risk analysis exemption (Article 18) if the maximum permissible rate is exceeded for two consecutive quarters?		
	After the suspension, does the PSP intend to make use again of the risk analysis exemption (Article 18) only when the calculated fraud rate is equal to or below the maximum permitted rate for a quarter and does it have a procedure for informing the Banque de France by communicating the elements proving that the fraud rate became compliant again with the allowed maximum rate?		
<b>Monitoring</b>			
<b>21</b>	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		

	<p>quarterly basis the data listed below?</p> <ul style="list-style-type: none"> <li>- 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;</li> <li>- the average value of operations, including a breakdown by payment transactions initiated through strong customer authentication and under each of the waivers;</li> <li>- 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.</li> </ul>		
--	---	--	--

<b>CONFIDENTIALITY AND INTEGRITY OF THE CUSTOMISED SECURITY DATA OF PAYMENT SERVICE USERS</b>			
<b>General requirements</b>			
<b>22</b>	<p>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?</p> <ul style="list-style-type: none"> <li>- 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;</li> <li>- custom security data in data format as well as cryptographic hardware related to the encryption of customised security data are not stored in plain text;</li> <li>- secret cryptographic equipment is protected from unauthorized disclosure.</li> </ul>		
	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?		
<b>Data creation and transmission</b>			
<b>23</b>	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?		
<b>Association with the payment service user</b>			
<b>24</b>	Does the PSP ensure that only the payment service user is associated, in a secure way, with the customised security data, authentication devices and		



	<p>software according to the requirements listed below?</p> <ul style="list-style-type: none"><li>- 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</li></ul>		
--	--	--	--

	<p>responsibility of the PSP;</p> <ul style="list-style-type: none"> <li>- 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.</li> </ul>		
<b>Delivery of data as well as authentication devices and software</b>			
<b>25</b>	<p>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?</p> <ul style="list-style-type: none"> <li>- efficient and secure delivery mechanisms ensure that customised security data and authentication devices and software are</li> </ul>		

	<p>delivered to the legitimate payment service user;</p> <ul style="list-style-type: none"> <li>- mechanisms enable the payment service provider to verify the authenticity of the authentication software delivered to the payment service user via the Internet;</li> <li>- 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: <ul style="list-style-type: none"> <li>(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;</li> </ul> </li> </ul>		
--	---	--	--

	<p>(ii) the customised security data or authentication devices or software must be activated before they can be used;</p> <ul style="list-style-type: none"> <li>- 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.</li> </ul>		
<b>Renewal of customised security data</b>			
<b>26</b>	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?		
<b>Destruction, deactivation and revocation</b>			
<b>27</b>	Does the PSP have effective procedures in place to apply		

	<p>each of the security measures listed below?</p> <ul style="list-style-type: none"> <li>- the secure destruction, deactivation or revocation of customised security data and authentication devices and software;</li> <li>- 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;</li> <li>- 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.</li> </ul>		
--	--	--	--

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 site with third party authentication			
29	Does the PSP ensure that all transactions (authentication, consultation and payment initiation) with the payment service user, including merchants, other PSP and other entities are correctly traced with unique, unpredictable identifiers stamped with the date and time?		
30-1	Has the PSP made available to third party PSP an access interface that meets the requirements listed below? <ul style="list-style-type: none"> <li>- third party PSP are able to identify themselves towards the account servicing PSP;</li> <li>- third party PSP are able to communicate securely with the PSP to execute their payment services.</li> </ul>		
30-2	Does the PSP make all authentication procedures offered to payment service users to be usable by third party PSP for the purposes of authentication of payment service users?		
30-2-a-b	Does the PSP Access Interface meet the requirements listed below? <ul style="list-style-type: none"> <li>- the PSP is in a position to start strong identification at the</li> </ul>		

	<p>request of a third party PSP that has previously obtained the consent of the user;</p> <ul style="list-style-type: none"> <li>- the communication sessions between the PSP and third party PSP are established and maintained throughout the identification.</li> </ul>		
<b>34-1</b>	Is the access of third party PSP to the PSP online banking site based on certificates marked as electronic stamp or certified authentication certificates?		
<b>35-1</b>	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?		
<b>35-5</b>	Does the PSP ensure that the customised security data and authentication codes they communicate are not readable directly or indirectly by a staff member?		
<b>36-1</b>	<p>Does the PSP meet the requirements listed below?</p> <ul style="list-style-type: none"> <li>- it provides third party PSP with the same information from the designated payment accounts and associated payment transactions that are made available to the payment</li> </ul>		

	<p>service user in case of direct request for access to the account information, provided that such information does not contain sensitive payment data;</p> <ul style="list-style-type: none"> <li>- immediately after receiving the payment order, they shall provide third party PSP with the same information on the initiation and execution of the payment transaction as those provided or made available to the payment service user when the payment service user directly initiates the transaction;</li> <li>- upon request, it shall immediately provide to third party PSP, in the form of a simple “yes” or “no”, whether the amount necessary for the execution of a payment transaction is available or not on the payer's payment account.</li> </ul>		
<b>36-2</b>	<p>If there is an error or unforeseen event during the identification or authentication process or when exchanging information, do the PSP procedures provide for the sending of a notification message to third parties, indicating the reasons for the error or unforeseen event?</p>		



Applicable by the account manager PSP in case of implementation of a dedicated access interface with a back-up mechanism (banking access online with third party authentication)			
<b>29</b>	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?		
<b>30-1</b>	Has the PSP made available to third parties an access interface that meets the requirements listed below? <ul style="list-style-type: none"> <li>- third party PSP are able to identify themselves towards the account servicing PSP;</li> <li>- third party PSP are able to communicate securely with the PSP to execute their payment services.</li> </ul>		
<b>30-2</b>	Does the PSP make all authentication procedures offered to payment service users to be usable by third party PSP for the purposes of authentication of payment service users?		
<b>30-2-a-b</b>	Does the PSP access interface meet the requirements listed below? <ul style="list-style-type: none"> <li>- the PSP is in a position to start strong identification at the request of a third party PSP</li> </ul>		

	<p>that has previously obtained the consent of the user;</p> <ul style="list-style-type: none"> <li>- the communication sessions between the PSP and third party PSP are established and maintained throughout the identification.</li> </ul>		
<b>30-3</b>	<p>Does the PSP ensure that its access interface follows communication standards published by European or international standardisation organisations?</p> <p>Do the technical specifications of the access interface documentation mention a series of routines, protocols and tools that third party PSP need to enable interoperability of their software and applications with the PSP's systems?</p>		
<b>30-4</b>	<p>If the technical specifications for the access interface are changed, except in emergencies, did the PSP plan to make them available to third parties at least three months prior to their implementation?</p> <p>Do the PSP procedures provide in writing for the emergency situations in which the changes have been implemented and for making this documentation available to the ACPR and the BDF?</p>		
<b>32-1</b>	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?		
<b>32-2</b>	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?		
<b>32-4</b>	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?		
<b>33-1</b>	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?		
<b>33-2</b>	Does the PSP have communication plans to inform third-party PSP that use the dedicated interface of measures to restore the system and a description of the other readily available options that they can use in the meantime?		

<b>33-3</b>	Do the PSP procedures provide for the timely notification of the dedicated interface problems to the ACPR?		
<b>33-5</b>	For access to the back-up interface, does the PSP ensure that third parties are identified and authenticated according to the authentication procedures planned for its own customers?		
<b>34-1</b>	Is the access of third party PSP to the PSP online banking site based on certificates marked as electronic stamp or certified authentication certificates?		
<b>35-1</b>	Are the integrity and confidentiality of customised security data and authentication codes transiting through communication flows or stored in the PSP information systems insured?		
<b>35-5</b>	Does the PSP ensure that the customised security data and authentication codes they communicate are not readable directly or indirectly by a staff member?		
<b>36-1</b>	Does the PSP meet the requirements listed below? - it provides third party PSP with the same information from the designated payment accounts and associated payment transactions		

	<p>that are made available to the payment service user in case of direct request for access to the account information, provided that such information does not contain sensitive payment data;</p> <ul style="list-style-type: none"> <li>- immediately after receiving the payment order, they shall provide third party PSP with the same information on the initiation and execution of the payment transaction as those provided or made available to the payment service user when the payment service user directly initiates the transaction;</li> <li>- upon request, it shall immediately provide to third party PSP, in the form of a simple “yes” or “no”, whether the amount necessary for the execution of a payment transaction is available or not on the payer's payment account.</li> </ul>		
<b>36-2</b>	<p>If there is an error or unforeseen event during the identification or authentication process or when exchanging information, do the PSP procedures provide for sending a notification message to third parties, indicating the reasons for the error or unforeseen event?</p>		
<b>Applicable by the account manager PSP in case of implementation of a dedicated access interface without an emergency mechanism</b>			

<b>29</b>	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?		
<b>30-1</b>	Has the PSP made available to third parties an access interface that meets the requirements listed below? - third party PSP are able to identify themselves towards the account servicing PSP; - third party PSP are able to communicate securely with the PSP to execute their payment services.		
<b>30-2</b>	Does the PSP make all authentication procedures offered to payment service users to be usable by third party PSP for the purposes of authentication of payment service users?		
<b>30-2-a-b</b>	Does the PSP access interface meet the requirements listed below? - the PSP is in a position to start strong identification at the request of a third party PSP that has previously obtained the consent of the user;		

	- the communication sessions between the PSP and third party PSP are established and maintained throughout the identification.		
<b>30-3</b>	Does the PSP ensure that its access interface follows communication standards published by European or international standardisation organisations? Do the technical specifications of the access interface documentation mention a series of routines, protocols and tools that third party PSP need to enable interoperability of their software and applications with the PSP systems?		
<b>30-4</b>	If the technical specifications for the access interface are changed, except in emergencies, did the PSP plan to make them available to third parties at least three months prior to their implementation? Do the PSP procedures provide in writing for the emergency situations in which the changes have been implemented and for making this documentation available to the ACPR and the BDF?		
<b>32-1</b>	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?		
<b>32-2</b>	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?		
<b>32-4</b>	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?		
<b>33-6</b>	Has the PSP made an application for exemption from an emergency mechanism to the ACPR?		
<b>34-1</b>	Is the access of third party PSP to the PSP online banking site based on certificates marked as electronic stamp or certified authentication certificates?		
<b>35-1</b>	Are the integrity and confidentiality of customised security data and authentication codes transiting through communication flows or stored in the PSP information systems insured?		
<b>35-5</b>	Does the PSP ensure that the customised security data and		



	authentication codes they communicate are not readable directly or indirectly by a staff member?		
<b>36-1</b>	<p>Does the PSP meet the requirements listed below?</p> <ul style="list-style-type: none"> <li>- it provides third party PSP with the same information from the designated payment accounts and associated payment transactions that are made available to the payment service user in case of direct request for access to the account information, provided that such information does not contain sensitive payment data;</li> <li>- immediately after receiving the payment order, they shall provide third party PSP with the same information on the initiation and execution of the payment transaction as those provided or made available to the payment service user when the payment service user directly initiates the transaction;</li> <li>- upon request, it shall immediately provide to third party PSP, in the form of a simple “yes” or “no”, whether the amount necessary for the execution of a payment transaction is available or not on the payer's payment account.</li> </ul>		

36-2	If there is an error or unforeseen event during the identification or authentication process or when exchanging information, do the PSP procedures provide for sending a notification message to third parties, indicating the reasons for the error or unforeseen event?		
------	---	--	--

## V- ANNEXES

### 1. Rating matrix for fraud risks

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

### 2. Glossary

*Define technical terms and acronyms used in the Annex.*

## Annex 1

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

### 1. Overview of internal control systems<sup>7</sup>

#### 1.1. General internal control system:

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

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

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

#### 1.3. Risk management function:

- a description of the organisation of the risk management function (*scope of authority, staffing levels in the units responsible for risk measurement, monitoring and control, and the technical resources at their disposal*);
- for groups, organisation of the risk management function;
- a description of the procedures and systems for monitoring risks arising from new products, from significant changes in existing products, from internal and external growth, and from unusual transactions (cf. Article 221 of the Order of 3 November 2014);
- summary of the analysis conducted on these new products and transactions.

#### 1.4. Periodic control system:

<sup>7</sup> Institutions may tailor this section according to their size and organisation, the nature and volume of their activities and establishments, and the types of risk to which they are exposed (in particular, when the functions of permanent and periodic control are conferred on the same person, or on the effective managers).

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

## **2. Overview of accounting arrangements**

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

## Measures implemented for customers in fragile financial situations (Order of 5 November 2015 on the certification of the banking inclusion charter and on the prevention of over-indebtedness)

### I. Training :

- 1.1 Percentage of customer advisors that have, in the past year, undergone appropriate training on the specific offer, the targeted customers and the follow-up of customers who receive basic banking service: %
- 1.2 Systematic training recall for trained customer advisors: Yes/No
- 1.3 Percentage of employees who are in contact with customers that have, in the past year, undergone training on the specific arrangements in place in the institution aimed for customers in fragile situations: %
- 1.4 Systematic refresher training for the persons referred to in 1.3 above that are already trained: Yes/No
- 1.5 Percentage of persons acting on behalf of the institution (excluding employees) that have, in the past year, undergone appropriate training on the specific mechanisms in place aimed for customers in fragile situations: %
- 1.6 Systematic refresher training for the persons referred to in 1.5 above that are already trained: Yes/No

### II. Internal control<sup>8</sup>

- 2.1. Does the permanent control system (1<sup>st</sup> and 2<sup>nd</sup> level) cover all measures relating to:
    - 2.1.1. - improving access to banking and payment services and facilitating their use? Yes/No
    - 2.1.2. - preventing over-indebtedness/detection? Yes/ No
    - 2.1.3. - preventing over-indebtedness/assistance? Yes / No
    - 2.1.4. - staff training, in particular as referred to points 1.1 to 1.6 above? Yes / No
  - 2.2. Are points 2.1.1 to 2.1.4 all covered by the periodic control cycle? Yes / No
  - 2.3. Have significant deficiencies been identified during permanent controls and, where applicable periodic controls in the past year? Yes / No.
- If the answer is « No », do not answer questions 2.4 and 2.5*
- 2.4. If yes, please specify the principal deficiencies (maximum 3)
  - 2.5. Have corrective actions been set up? Yes/ No

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

<sup>8</sup> Explanatory comments to be provided part III if answer is « No » to either of the questions below.