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

November 2014

Report on Internal Control

(Report prepared in accordance with Articles 42, 43 and 43-1 of Regulation 97-02 of the Banking and Financial Regulations Committee *(CRBF))*

Contents

Introduction

The Report on Internal Control gives details of the institution's internal control activities during the past financial year and describes its systems 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 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 actually borne by the institution.

Given the late coming into force of the order of 3 November 2014 concerning the internal control of banking sector companies, payment services and investment services subject to ACPR supervision, the supervised institutions can, for the last time (financial year 2014), produce their reports on internal control according to the Regulation 97-02 of 21 February 1997 as amended (repealed by the above-mentioned order). Consequently, the references given below are from the Regulation 97-02 of 21 February 1997 as amended.

This document is based on a 'combined' version of the reports prepared in accordance with Articles 42, 43 and 43-1 of Regulation 97-02. Institutions that wish to do so may continue to submit separate reports, provided that the reports cover all of the points listed below.

The Report on Internal Control should include the most recent internal management reports on risk exposure that have been provided to the institution's supervisory body and, where applicable, to its risk committee.

Moreover, 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 Article 39 of Regulation 97-02, should be sent promptly to the Secretary General of the *Autorité de contrôle prudentiel et de résolution* (SGACPR), without waiting for the corresponding extracts from the minutes of the meetings at which they were reviewed. Those extracts should be sent to the SGACPR as soon as they are available.

N.B.: If the institution is supervised on a consolidated basis, or is subject to supplementary supervision for financial conglomerates, the reports on internal control shall include information on how internal control is applied to the group as a whole or to the conglomerate. If the subsidiary's internal control system is fully integrated into the system of the group, it is not necessary to submit a report on the organisation of internal control in that subsidiary. However, the systems for risk measurement, monitoring and management should be described for each supervised institution.

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

1.1. Description of business conducted

- General description of business conducted;
- For new activities:
  - a detailed description of any new activities conducted by the institution in the past year (by business line, geographical region, and subsidiary);
  - an overview of the procedures established for these new activities;
  - a description of the internal control for the new activities;
- a description of any major changes in organisation or human resources, and of any significant projects launched or conducted during the past year.

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

- description, formalisation and updating of the institution's risk mapping;
- a description of measures taken to manage the risks mapped;
- a presentation of quantitative and qualitative information on the risks described in the summary reports sent to the effective managers, the supervisory body, and (where appropriate) to the risk committee and the ad hoc committee, specifying the scope of the measures used to assess the level of risk incurred and to set risk limits (Article 37 of Regulation 97-02).

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.

N.B.: For the financial year 2014, this part shall include in particular a description of the adaptations taken or to be undertaken by the institution to comply with the new provisions introduced by the order of 3 November 2014 regarding the internal control of banking sector companies, payment services and investment services subject to ACPR supervision (transposing the CRD IV).

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 (Article 42(1)(f) of Regulation 97-02): *specify in particular the identity, the hierarchical and functional position of the person in charge of permanent control and any other functions exercised by this person in the institution or in other entities in the same group;*
- a description of significant changes in the organisation of the compliance control system: *specify in particular the identity, the hierarchical and functional position of the person in charge of compliance and any other functions exercised by this person in the institution or in other entities in the same group;*
- a description of the significant changes in the organisation of the anti-money laundering and combating the financing of terrorism (AML/CFT) system ;
- 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 of foreign business and outsourcing)

- identification and hierarchical and functional position of the person in charge of periodic controls;
- main initiatives planned in the area of periodic controls (audit plan, etc., see Article 42(1)(f) of Regulation 97-02).

3. Governance

N.B.: For the financial year 2014, this part shall include in particular a description of the adaptations taken or to be undertaken by the institution to comply with the new provisions introduced by the order of 3 November 2014 regarding the internal control of banking sector companies, payment services and investment services subject to ACPR supervision (transposing the CRD IV).

3.1. Involvement of management bodies in internal control

3.1.1. Procedures for reporting to the supervisory body

- what procedures exist for reporting to the supervisory body on measures taken to control outsourced activities and associated risks (Article 39(c) of Regulation 97-02)?
- what procedures exist for reporting to the decision-making body on compliance with limits, when the decision-making body was not involved in setting those limits (Article 39, Paragraph 6 of Regulation 97-02)?
- what procedures exist for reporting to the supervisory body, to the central body, and (where appropriate) to the risk committee on significant incidents as defined in Article 17-ter (Article 38-1 of Regulation 97-02)?
- what procedures exist for reporting to the supervisory body, to the central body and (where appropriate) to the risk committee on significant anomalies detected by the system for monitoring and assessing AML/CFT, and on any shortcomings in this system (Article 38-1 of Regulation 97-02)?
- has the supervisory body (or the risk committee) requested the head of the risk management function to report on the exercise of his duties? If so, on what subjects (Article 11-8 of Regulation 97-02)?
- what procedures exist for reporting to the supervisory body and (where appropriate) to the risk, committee, by the persons responsible for periodic controls, of any failures to carry out corrective measures that have been ordered (Article 9-1(b) of Regulation 97-02)?
- what findings from controls have been brought to the attention of the supervisory body, and in particular any shortcomings identified, along with the corrective measures ordered?

3.1.2. Procedures for reporting to the effective managers

- what procedures exist for reporting to the effective managers on significant incidents as defined in Article 17-ter (see Article 38-1 of Regulation 97-02)?
- what procedures exist for reporting to the effective managers on significant anomalies detected by the system for monitoring and assessing AML/CFT, and on any shortcomings in this system (Article 38-1 of Regulation 97-02)?
- what procedures exist allowing the risk management function to report to the effective managers on the exercise of its duties?
- what procedures exist allowing the head of the risk management function to provide a warning of any situation that could have significant repercussions on risk management (Article 11-8 of Regulation 97-02)?

3.1.3. Measures taken by the management bodies

- a description of the measures taken by the effective managers and the supervisory body to verify the effectiveness of internal control systems and procedures.

3.1.4. Processing of information by the supervisory body

- dates on which the supervisory body reviewed the activities and results of the internal control system for the past year;
- as part of the supervisory body's review of significant incidents revealed by internal control procedures, the main shortcomings noted, the conclusions drawn from their analysis, and the measures taken to correct them (Article 39, Paragraph 1 of Regulation 97-02).

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

N.B.: For the financial year 2014, this part shall include in particular a description of the adaptations taken or to be undertaken by the institution to comply with the new provisions introduced by the order of 3 November 2014 regarding the internal control of banking sector companies, payment services and investment services subject to ACPR supervision (transposing the CRDIV).
This part does not apply to payment institutions and electronic money institutions.

This section may be treated in a separate report.

3.2.1. Governance of compensation policies

- a description of general principles of compensation policy established under article L. 511-72 of Monetary and Financial Code (procedures and date of adoption, implementation date, and review procedures) and, where necessary, the identity of external consultants whose services have been used to establish compensation policies (Article 43-1, Paragraph 1 of Regulation 97-02);
- date of creation, composition, mandate, and responsibilities of the Compensation Committee.

3.2.2. Main features of compensation policies

- a description of the institution's compensation policies (Article 43-1, Paragraph 2 of Regulation 97-02), including:
  - criteria used to measure performance and to adjust compensation for risk;
  - criteria for defining the link between compensation and performance;
  - policies concerning deferred compensation;
  - policies concerning guaranteed compensation;
  - criteria for determining the ratio of cash compensation to other forms of compensation.
- a description of compensation policies for personnel responsible for validating and checking transactions (Articles 7 and 31-4 of Regulation 97-02).
- the procedures for taking all risks into account in setting the basis for variable compensation, including the liquidity risk inherent in the activities concerned and the capital needed to cover the risks incurred (Article 31-3 of Regulation 97-02).

3.2.3. Disclosures concerning the compensation of the members of the effective managers and of persons whose professional activities have a significant impact on the institution's risk profile (Article 43-1- 3° of Regulation 97-02)

Please specify:

- the categories of staff concerned;
- the overall amount of compensation for the year, with a breakdown of fixed versus variable components, and the number of beneficiaries. As regards this information, please also provide a breakdown by area of activity;
- the overall amount and type of variable, broken down between cash compensation, compensation in shares or asset-backed securities, and other forms of compensation. Please also specify the

acquisition period or the minimum holding period for securities (Article 31-4-4° of Regulation 97-02);

- the overall amount of deferred compensation with a breakdown between paid and unpaid compensation (Article 31-4, Paragraph 2 of Regulation 97-02);
- the overall amount of deferred compensation awarded during the year, paid or reduced, after adjustment for performance;
- bonuses for new hires and termination indemnities and the number of beneficiaries;
- guaranteed termination indemnities granted during the year, the number of beneficiaries, and the largest amount granted to a single beneficiary.

3.2.4. Transparency and control of compensation policies

- the procedures for verifying that compensation policies are consistent with risk management objectives;
- the procedures for disclosing information on compensation policies and practices.

4. Results of periodic controls conducted during the year (including foreign business and outsourcing)

- risks and/or entities that have been subject to a periodic controls during the year;
- 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 this Report was drafted;
- 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 senior managers and principal shareholders (as defined in article 5 of the order of 23 December 2013 on the prudential regime of financing companies)

For financing companies only, 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 beneficiary (natural or legal person, shareholder or senior manager), type of commitment, gross amount, deductions (if any), risk weight, date of assignment and expiry date;
- **the nature of commitments to principal shareholders and senior managers for which a deduction has not been made from regulatory capital** due either to the date on which the commitment was made or the rating or score assigned to the beneficiary of the commitment. However, it is not necessary to mention commitments whose gross amount does not exceed 3% of the institution's capital.

For the other companies, attach an annex providing the list and the main characteristics of commitments towards most important shareholders and towards senior managers.

6. Process for assessing the adequacy of internal capital

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

- a description of the systems and procedures implemented to ensure that the amount and distribution of internal capital corresponds to the nature and level of the risks to which the institution is exposed (*with particular emphasis on risks that are not taken into account in Pillar 1*); ;
- level of internal capital allocated to risk for the financial year ended and for the year ahead;
- stress tests to assess the adequacy of internal capital: a description of the assumptions and methodologies used, and summary of the results obtained;
- internal control procedures for verifying that these systems and procedures remain in line with the evolution of the institution's risk profile.

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

7.1. Training provided to staff on compliance control procedures, and prompt dissemination to staff of information on changes in the provisions that apply to the transactions they carry out

7.2. Assessment and control of reputational risk

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

7.4. Description of main malfunctions identified during the year

7.5. 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 this Report was drafted;
- 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 (*Articles 5(f) and 9-1(a) of Regulation 97-02*).

8. Money laundering and terrorist financing risk

8.1. Risk classification (AML/CFT)

- a description, formalisation, updates, and presentation of the analyses on which the classification is based.

8.2. Procedures (AML/CFT)

- a description, formalisation and date(s) of updates to the procedures on which the AML/CFT system is based**,** mentioning significant changes during the year in the procedures for:

- identifying new customers and actual beneficiaries;
- identifying occasional customers;
- satisfying 'Know Your Customer' requirements;
- procedures for bringing existing customer files into compliance with continuous due diligence requirements.

- a description of procedures for implementing reduced, complementary and enhanced due diligence requirements;
- a description of procedures for implementing requirements relating to funds transfers (as payment service provider for the payer, intermediary payment service provider, or payment service provider for the beneficiary);
- *where applicable*, the procedures for dissemination within the group of information needed to organise the combat against money laundering and terrorism financing: a description of procedures for the exchange of information on the existence and contents of AML/CFT reporting;
- the procedures for defining criteria and materiality thresholds for AML/CFT anomalies.

8.3. Results of permanent control on money laundering and terrorist financing 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 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 (*Articles 5(f) and 9-1(a) of Regulation 97-02*).

8.4. Main shortcomings observed by national and foreign control authorities, and corrective measures ordered

9. Credit and counterparty risk[1]

NB: For investment services providers (ISP), the special case of ***transactions using the deferred settlement service (service de règlement différé – SRD)*** *is covered in this section, with information on the set of customers for which this type of order is authorised, the limits set, and the management of risk (initial margin, maintenance margin, monitoring of extensions, provisioning of non-performing loans).*

9.1. 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 where appropriate any delegations;
- policy for approving housing loans granted to French customers, in particular criteria regarding repayments as a percentage of borrowers' disposable income, loan-to-value ratios and loan maturities.

9.2. Systems for measuring and monitoring risk

- general description of exposure limits – by beneficiary, by associated debtors, 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);

[1] Payment institutions performing credit operations are also concerned by this point

- 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;
- the procedures for analysing the quality of loans and associated guarantees, 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 for analysing the risk of loss on leased assets (financial leasing) and the frequency of the analysis;
- 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 (*Articles 18 and 39 (a) of Regulation 97-02*);
- the procedures for reporting to the effective managers on the level of credit risk (using summary tables);
- factors considered in analysing changes in margins, in particular for loan production for the past year: *methodology, variables analysed, results;*

• provide details on the calculation of margins: earnings and expenses taken into account; if lending needs to be refinanced, indicate the net borrowing position and the refinancing rate; if there are gains from investing capital allocated to lending, specify the amount and the rate of return;
• identify of the different loan categories (such as retail loans and housing loans) or business lines for which margins are calculated;
• highlight trends in outstanding loans (at year-end and intermediary dates) and, where appropriate, in loan production for the past year.

- the procedures used by the effective managers to analyse the profitability of lending activities, the frequency of the analyses, and their results (*specify the date of the most recent analysis*);
- the procedures used to report to the supervisory body on the institution's credit risk exposure, and the frequency of these reports *(attach the most recent management report produced for the supervisory body).*
- the procedures used to monitor housing loans granted to French customers.

9.3. Concentration risk

9.3.1. Concentration risk by counterparty

- tool for monitoring concentration risk by counterparty, including central counterparties : any aggregate measures defined, description of the system for measuring exposures to the same beneficiary (including details on procedures used to identify associated beneficiaries, (establishment of a quantitative threshold above which such measures are systematically implemented, etc.); use of the transparency approach notably for exposures to mutual funds, securitisations or refinancing of trade receivables (factoring, etc.) and the inclusion of credit risk mitigation techniques), procedures for reporting to the effective managers;
- system for limiting exposure by counterparty: general description of the system for setting limits on counterparties (specify their level in relation to capital and earnings), the procedures for reviewing limits and the frequency of these reviews, any breaches of limits reported, and the procedures for involving the effective managers in setting and monitoring limits;
- amounts of exposures to main counterparties;

- conclusions on the institution's exposure to concentration risk by counterparty, including central counterparties

9.3.2. Sectoral concentration risk

- tool for monitoring sectoral concentration risk: any aggregate measures defined, description of the system for measuring exposures in the same business sector, and procedures for reporting to the effective managers;
- system for limiting exposure by business sector: a general description of the system for setting limits on sectoral 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 sector;
- conclusions on the institution's exposure to sectoral concentration risk.

9.3.3. 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;
- 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.

9.4. Requirements relating to the use of internal rating systems to calculate capital requirements for credit risk

- back-testing and comparisons with external data to ensure the accuracy and consistency of internal rating systems, including the methodologies and parameters used;
- the contents and frequency of the permanent control and periodic controls conducted on internal rating systems;
- a description of the 'use test' to internal rating systems: the actual use of the parameters generated by the internal rating system in loan approval, loan pricing, loan collection, risk monitoring, provisioning, allocation of internal capital, and corporate governance (including the preparation of management reports for the effective managers and the supervisory body);
- the procedures for involving the effective managers in designing and updating internal rating systems: including approval of methodologies, ensuring a sound command of the design and operation of the system, and monitoring their operation.

9.5. Risks associated with securitisations

- a presentation of the institution's securitisation and credit risk transfer strategy;
- a presentation of the internal policies and procedures put in place to ensure, before investing, that there is detailed knowledge of securitisation exposures and that institutions comply with the requirement to retain 5% of the net economic interest when acting as originator, sponsor or original lender;
- the procedures for assessing, monitoring and controlling the risks associated with securitisations (in particular, an analysis of their economic substance), for originators, sponsors or investors including via stress tests (assumptions, frequency, consequences).

- for originating banks, description of the internal process of assessing prudentially deconsolidating operations, supported by an audit trail and by the procedures for monitoring risk transfer by a periodical review over time.

9.6. Intraday credit risk

Risk incurred in the business of custody by institutions that grant loans to their customers, in cash or securities, during the course of the day to facilitate the execution of securities transactions[2].

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

9.7. Results of permanent control of credit activities

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date 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 (*Articles 5(f) and 9-1(a) of Regulation 97-02*).

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

Attach an annex providing:

- a description of the system for identifying, measuring and monitoring the residual risk to which the institution is exposed when it uses credit risk mitigation 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*).

9.9. 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.

9.10. Overall conclusions on credit risk exposure

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

10. Market risk

A description of the institution's policies on proprietary trading:

10.1. System for measuring market risk

- booking market transactions; calculation of positions and results (*specify the frequency*);
- comparisons between risk-management and accounting results (*specify the frequency*);
- assessment of the risks arising from positions in the trading book (*specify the frequency*);
- the procedures for capturing different components of risk (particularly for institutions with high trading volumes that use an aggregate risk measure);
- the scope of risks covered (business lines and portfolios; within establishments in different geographical areas).

10.2. System for monitoring market risk

- identification, staffing levels, and hierarchical and functional position of the unit charged with monitoring and managing market risk;
- controls conducted by that unit**,** and in particular regular control of the validity of the tools for measuring aggregate risk (back-testing);
- a general description of limits set for market risk (specify the level of limits, by type of risk incurred, in relation to capital and earnings);
- the frequency with which limits on market risk are reviewed (indicate the date of the most recent review during the past year); identity of the body responsible for setting limits**;**
- the system for monitoring procedures and limits;
- any breaches of limits noted during the past year (*specify their causes, the number of breaches, and their amounts*);
- the procedures for authorising such breaches and the measures taken to regularise them;
- the procedures for reporting on compliance with limits (*frequency, recipients*);
- the procedures, frequency and conclusions of the analysis provided to the effective managers on the results of market activities (*specify* the date of the most recent analysis) and on the level of risk incurred, including the amount of internal capital allocated:

• attach a copy of the documents provided to the effective managers that enable it to assess the risk incurred by the institution, in particular in relation to its capital and earnings;

- the procedures, frequency and conclusions of the analysis provided to the supervisory body on the results of market activities (*specify the date of the most recent analysis*) and on the level of risk *incurred, including the amount of internal capital allocated*.

10.3. Results of permanent control of market risk

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date 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 (*Articles 5(f) and 9-1(a) of Regulation 97-02*).

10.4. Stress testing of market risk

For institutions that use their internal models to calculate capital requirements for market risk, attach an annex describing the assumptions and methodologies used and summarising the results obtained.

10.5. Overall conclusions on exposure to market risk

11. Operational risk

A general description of the overall framework for managing operational risk (specify the scope in terms of entities and transactions covered, the roles of the effective managers and the supervisory body, and the division of responsibilities for managing operational risk).

11.1. 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 for measuring and monitoring operational risk (specify the method used to calculate capital requirements);
- a general description of the reports used to measure and manage operational risk (specify in particular the frequency of reporting and recipients of the reports, the areas of risk covered, and the use of early warning indicators to signal potential future losses;
- documentation and communication of the procedures for monitoring and managing operational risk;
- a description of the specific procedures for managing the risk of internal and external fraud, as defined in article 324 of EU regulation n°575/2013 (Article 4(j));
- for institutions using an advanced measurement approach, a description of the methodology used (*including the factors related to internal control and to the environment in which they operate*) and any changes in methodology made during the course of the year;
- a general description of any insurance techniques used.

11.2. 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;
- a description of the main operational risks observed during the course of the year (settlement incidents, errors, fraud, etc.) and the attendant conclusions drawn.

11.3. 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 plans;
- formalisation of procedures, general description of IT backup sites;
- tests of emergency and business continuity plans (objectives, scope, frequency, results), procedures for updating plans (frequency, criteria), tools for managing continuity plans (software and IT development), reporting to senior management (on tests, and on any changes to systems and procedures);
- audit of emergency and business continuity plans and results of permanents controls;
- activation of the emergency and business continuity plan(s) and management of incidents occurring during the course of the year (for example, the H1N1 flu pandemic).

11.4. Security of IT systems

- name of the person responsible for IT system security;
- identification and reassessment of IT risk mapping;
- objectives of IT security policy (in particular, the procedures for ensuring data integrity and confidentiality, and the specific measures taken for online banking);
- a description of permanent controls of the security level for IT systems, and the results of these controls.

11.5. Results of permanent controls on operational 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 (*Articles 5(f) and 9-1(a) of Regulation 97-02*).

11.6. Overall conclusions on exposure to operational risk

12. Accounting risk

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

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

12.2. Results of permanents controls on accounting risk

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date this Report was drafted;
- the procedures for following up on the recommendations generated by permanent controls (*tools, persons in charge, etc.*);
- the procedures for verifying that the corrective measures ordered by the institution have been carried out by the appropriate persons in a reasonable period of time (*Articles 5(f) and 9-1(a) of Regulation 97-02*).

13. Global Interest rate risk

- a general description of the overall framework for managing global interest rate risk (specify the entities and transactions covered, justifying the use of the proportionality principle in the case of consolidated management, and specify the roles of the effective managers and supervisory body as well as the division of responsibilities for controlling global interest rate risk).

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

- a description of the tools and methodologies used to manage global interest rate risk (specify the methods used by the institution, such as static or dynamic gap analysis, sensitivity in terms of

earnings, calculation of net present value, the assumptions and results of stress tests, and the impact of changes in global interest rate risk on the institution's business during the past year);

- a description of the behavioural assumptions used by the institution (specify their scope of coverage, main assumptions, and the treatment of explicit or implicit behavioural options and new loan issuance);
- the impact of a uniform upwards or downwards shock of at least 200-basis points over one year (applying a 0% floor), on the institution's current net banking income and economic value, , taking into consideration only activities other than trading. A presentation of the assumptions used. Annex 1 of this document provides an example, for institutions that do not have their own methodology, of methods that could be used to calculate the consequences of a uniform shock of 200 basis points. The change in economic value is expressed as a percentage of the institution's regulatory own funds;values of the indicators used by the institution to measure global interest rate risk (specify the values of static or dynamic gaps, the results of sensitivity analysis of earnings, calculations of net present value, and stress tests);
- the sensitivity of the shock results to a change in the underlying assumptions used (specify the impact of a non-parallel change in the yield curve, differences between different market rates (basis risk) and changes to assumptions about customer behaviour; the economic capital allocated in respect of the institution's exposure to global interest rate risk

13.2. System for monitoring global interest rate risk

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

13.3. Permanent control system for global interest rate risk management

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

13.4. Results of permanent controls on global interest rate risk

- main shortcomings observed;
- measures taken to correct the shortcomings observed**,** the expected date for carrying out these measures, and the state of progress in implementing them as at the date 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 (*Articles 5(f) and 9-1(a) of Regulation 97-02*).

13.5. Overall conclusions on exposure to global interest rate risk

14. Intermediation risk for investment services providers

- statements of the overall distribution of exposures by group of counterparties and by principal (by internal rating, financial instrument, market, or any other criteria that is significant in the context of the business conducted by the institution);
- information on risk management (security taken, margin calls on positions, collateral, etc.) and on the procedures followed in the event of the failure of a principal (insufficient margin, refusal of the transaction);

- a general description of the system of exposure limits for intermediation risk – by beneficiary, by associated debtors, etc. (*specify the level of limits in relation to the transaction volume of the beneficiaries and in relation to capital*);
- the procedures and frequency with which the limits on intermediation risk are reviewed (specify the date of the most recent review);
- any breaches of credit limits observed during the past year (specify their causes, the counterparties involved, the size of the overall exposure, the number of breaches, their duration and their amounts);
- the procedures for authorising such breaches and the measures taken to regularise them;
- the factors analysed to assess the risk associated with the principal when taking an exposure (*methodology, data analysed*);
- a typology of the errors that have occurred in the past year in the acceptance and execution of orders (methods and frequency of analysis conducted by the head of internal control, threshold set by the effective managers for documenting such errors);
- results of permanent controls on intermediation risk;
- main conclusions of the risk analysis conducted.

15. Settlement/delivery risk

- a description of the system for measuring settlement/delivery risk (highlighting the various phases of the settlement process and the treatment of new transactions in addition to pending transactions, etc.);
- a general description of the settlement/delivery risk limits (specify the level of the limits, by type of counterparty, in relation to the counterparties' transaction volumes and in relation to capital);
- the frequency with which settlement/delivery limits are reviewed (*specify the date of the most recent review*);
- any breaches of limits noted during the past year (*specify their causes, the number of breaches, and their number, duration and amounts*);
- the procedures for authorising such breaches and the measures taken to regularise them;
- an analysis of pending 'fails' (indicate their anteriority, their causes, and the action plan for clearing them);
- the results of permanent controls on settlement/delivery risk;
- main conclusions of the risk analysis conducted.

For investment services providers that guarantee completion :

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

16. Liquidity risk[3]

N.B.: For the financial year 2014, this part shall include in particular a description of the adaptations taken or to be undertaken by the institution to comply with the new provisions introduced by the order of 3 November 2014 regarding the internal control of banking sector companies, payment services and investment services subject to ACPR supervision (transposing the CRD IV).

- a general description of the overall framework for managing liquidity risk (specify the scope of the framework in terms of entities and transactions, the role of the effective and supervisory body, and the division of responsibilities for managing liquidity risk);
- information on the sources of funding and their diversification: description of the sources of funding used by the institution (specify the various funding channels, their amounts, maturities, and main counterparties), description of the indicators used to measure the diversification of funding sources.

16.1. Tools and methodologies for measuring and monitoring liquidity risk

- a description of the tools and methodology used to manage liquidity risk (*specify the assumptions and maturities adopted to estimate the indicators used by the institution and describe the tools and indicators used for each currency in which the institution conducts significant activities*;
- information on deposits and their diversification (*in terms of the number of depositors*);
- information on financing plans (methods for assessing the institution's ability to raise funds from its funding sources under normal conditions and in periods of stress for all maturities and all currencies (*underlying assumptions, test results*, etc.);
- the stress scenarios used to measure the risk incurred in the event of large variations in market parameters (indicate the assumptions used, the frequency with which they are reviewed, and the process for validating them; summarise the results of the stress tests and the procedures for reporting them to the supervisory body);
- main conclusions of the analysis of the risk incurred in the event of large variations in market parameters;
- a description of contingency plans to deal with a liquidity crisis (the plan should cover the institution's funding risk, the risk that market liquidity will dry up, and the interactions between the two risks).). Specify the procedures in place (identity and position of the persons involved, planned solutions for accessing liquidity, communication with the public, regular testing of contingency plans, etc.).

16.2. System for monitoring liquidity risk

- a general description of the limits on liquidity risk (specify the level of the limits by type of business, by currency and by type of counterparty, in relation to the counterparties' transaction volume and in relation to capital);
- the frequency with which limits on liquidity risk are reviewed (*specify the date of the most recent review*);
- any breaches of limits noted during the past year (*specify their causes, the number of breaches, and their amounts*);
- the procedures for authorising such breaches and the measures taken to regularise them;
- a general description of the reports used to manage liquidity risk (*including their frequency and recipients*);
- a description of incidents occurring in the past year.

3. In accordance with Article 45 of Regulation 97-02, branches of institutions whose registered offices are in another EU Member State, or in a country that is a member of the European Economic Area, should provide a report on the measurement and supervision of liquidity risk.

16.3. Permanent control system for the management of liquidity risk

- presentation of the control environment for the management of liquidity risk (*specify the role of permanent control*).

16.4. For credit institutions (and branches of credit institutions whose registered office is in a foreign country)

- the method used to take into account the internal cost of liquidity and an analysis of the change in liquidity cost of indicators over the year;
- institutions using the Standard Approach for liquidity risk should provide an annex to their Internal Control Report which includes:
  - a description of the characteristic and assumptions used to construct a projected cash-flow table, and any changes in these characteristics and assumptions made during the year;
  - an analysis of liquidity gaps in the cash flow tables during the year.
- institutions using the Advanced Approach for liquidity risk should specify how their internal methodology takes into account the systemic repercussions that could be caused by the institution's size relative to its market, in each of the EU Member States in which it conducts business *(cf. article 25 e) of the Order of 5 May 2009 on the identification, measurement, management and control of liquidity risk)*;
- a description of the assumptions used to constitute the stock of liquid assets;
- a description of the means implemented to ensure the institution is always aware of the stock of liquid assets it needs, and the assumptions used to adjust this stock level to the different time horizons under consideration.

16.5. Results of permanent controls on liquidity and funding 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 (*Articles 5 f) and 9-1(a) of Regulation 97-02*).

16.6. Overall conclusions on exposure to liquidity risk

17. Internal control system relating to the segregation of funds invested by investment firms, payments institutions and electronic money institutions

- a description of the tool for calculating the amount of customers' assets, the procedures for investing them, and related verifications (in particular article 40 (g) of Regulation 97-02);
- communication of the report of the statutory auditors on the adequacy of the arrangements for complying with regulatory provisions on segregation.

18. Specific information requested of financial conglomerates

- balance sheet totals for the group as a whole and for the banking, insurance and non-financial sectors.

18.1. Internal control and risk assessment system applied to all of the entities belonging to the financial conglomerate

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

18.2. Information on risks associated with entities in the insurance sector

- a description of the risks borne by insurance entities that are of the same nature as the risks associated with banking and finance;
- a description of the risks specific to the insurance business (specify which risks are managed centrally and what procedures are used, and which activities remain decentralised).

18.3. Information on intra-group transactions

- information on material intra-group transactions during the year between entities within the conglomerate that conduct banking or investment services business on the one hand, and entities that conduct insurance business on the other hand:

- a description of these transactions, differentiating between the categories defined in Article 4 of *Commission Bancaire* Instruction 2005-04, and noting the degree of interdependence of the activities within the conglomerate;
- for each type of transaction, the direction of the transaction in the majority of cases (from a banking or investment services entity to an insurance entity, or the opposite), and the objective of the transactions);
- the procedures for internal pricing for these transactions.

- quantitative information on each intra-group transaction whose amount exceeds 5% of the sum of the capital requirements for the different sectors, calculated on the basis of the previous year's financial statements:

- if they exceed the threshold: the cumulative nominal amount of such transactions giving rise to financial flows excluding market transactions (loans, collateral; asset sales, etc.), the total amount of commissions paid; and for transactions in financial futures, the total credit risk equivalent (or if that is not available, the total notional amount);
- for each individual transaction that exceeds the threshold, the nominal amount of the transaction and the date it was completed. Financial conglomerates should also provide a description of the transaction, indicating the identity of the counterparties, the direction of the transaction, and the objectives sought, using the following format:

Type of transaction	Transaction conclusion date	Nominal amount for balance sheet items, the notional amount and the equivalent credit risk for financial futures.	Description of the transaction (counterparties, direction, aims, etc.)

19. Annex on the security of cashless payment instruments provided or managed by the institution

Document to be sent in duplicate.

Background

This annex is devoted to the security of **cashless payment instruments** (as defined in Article L. 311-3 of the 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 Monetary and Financial Code aforesaid.

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

Since this Annex is mainly intended for the Banque de France, it shall be treated separately from the rest of the reports prepared in accordance with Articles 42 and 43 of amended CRBF Regulation 97-02.

Using this Annex, the "institutions concerned" present how they **assess, measure and monitor the security of the cashless payment instruments** that they issue or manage with regard to any internal procedures and the recommendations of external institutions such as those listed in the Annex.

The Banque de France expects institutions to provide information on the following four points:

- identification of the payments instruments issued or managed by the institution;
- procedures and measures implemented to manage risks stemming from the operational processes associated with the payment instruments issued or managed;
- types of controls focusing on the security of payment instruments put in place by the institution;
- expected changes in the landscape of the payment instruments issued or managed by the institution;

This annex is comprised of:

- a **descriptive section** summing up the four points mentioned above and that is set out in the completion methodology of the Annex;
- an **assessment section**, which enables the institution to gauge the quality of its answers in relation to the defined security objectives (Annex A).

The following is excluded from the scope of this Annex: all data on fraud relating to payment instruments as a whole, which are now reported in the questionnaire entitled "Inventory of fraud in cashless payment systems" (*Recensement de la fraude sur les moyens de paiement scripturaux* on ONEGATE/OSCAMPS).

The content shall be:

- comprehensive (any information necessary for a proper assessment of payment instruments is relevant).
- delimited (only the information regarding payment instruments is relevant).

The institutions concerned may also consult a list of most frequently asked questions, which is regularly updated on the ACPR's website.

Completion methodology of the annex

This completion guide explains each of the points mentioned above and defines the terms used. Unless there are internal constraints, the format of the table provided in this document must be rigorously respected when providing the relevant information.

Institutions that have responded to the Banque de France's Cheque Security Framework questionnaire (*Référentiel de Sécurité Cheque - RSC*) for the year under review, are exempted from following the plan proposed for cheques; they are exempted as well from submitting the RSC statement in the cashless payment instruments annex of the annual report.
It may be useful for institutions members of the French Bankcard Consortium GIE Cartes Bancaires to draw on the response format proposed by this consortium, but they must supplement this with their specific features.

This does not exempt institutions from having to complete the table provided in the Annex for the other four-party cards (VISA-only, MasterCard-only, etc.) and three-party cards that they issue or manage.

I. Identification of the payments instruments issued or managed by the institution

Provide, for each payment instrument issued or managed, a brief description (e.g. SDD, SCT etc.), the type of customer (individuals, professionals, etc.) and its characteristics (phase in the life cycle[4], how they work for new payment instruments[5], etc.).

The institution shall provide at least once the detailed features of all payment instruments issued or managed. For financial years to come, only new innovative payment instruments or those with new functions require a detailed description.

II. Procedures and measures implemented to manage risks stemming from the operational processes associated with the payment instruments issued or managed

For each payment instrument:

- summarise the main risks to which the operational processes associated with the payment instrument in question are exposed **(gross risks)**. Assess the probability that an event or a situation might occur and its impact before taking into account preventive or corrective measures;
- specify the procedures and measures adopted by the institution to manage these risks **(risk mitigation measures implemented)**, including the first-level controls carried out by operational staff and that do not come within the remit of compliance personnel (they are described in Section III "types of controls focusing on the security of payment instruments").
- provide information on the implementation of recommendations issued by external institutions regarding the security of payment instruments (see annex B).

As regards the solutions implemented in the area of risk management, briefly describe the risks that persist after applying the above-mentioned risk mitigation measures (**residual risks).**

Banque de France expects consistency between the fraud actually noted by the institution and the provided residual risks estimate.

[4] Phases in the life cycle include: study, launch, development, maturity, decline, withdrawal, etc.

[5] List here the different versions of the payment instrument (e.g. debit card, credit card, contactless cards, mobile payment, etc.) and briefly explain how this payment instrument works.

Care must be taken to keep this section separate from the description of operational processes implemented by the institution. In this section, only the analysis, processing and monitoring of the risks to which these processes are exposed should be addressed.

III. Different types of controls focusing on the security of payment instruments

The institutions concerned should give a brief description **of the controls implemented in the area of the security of payment instruments** (specify, for each control, whether it is conducted for a specific payment instrument or for all payment instruments across the board), with a view to ensuring their compliance with internal standards and external recommendations. In this description, the institution should specify:

– *the entity conducting the control;*

- the person who has carried out the control(s) (specify the person in charge of the control);
- the hierarchical and, where appropriate, functional position of this entity. For example: the control has been carried out by the head of the Compliance, Internal Control and Risk Department, reporting to the General Directorate, etc.

– *the controlled entity;*

- which elements have been controlled?
- at which level of the process has/have the control(s) been conducted? It is not necessary to describe all the processes but identify, using a common language, which task is being referred to.

– *frequency of controls:*

- whether the control(s) are periodic or permanent?
- what is the frequency of these control(s)?

– *observations made during the control(s):*

- which problems were brought to light by the control(s)?

– *corrective actions (taken or planned):*

- in the light of the above observations, which solutions have been implemented or planned to resolve these problems? The institution shall complete its answer with the implementation timeline of these solutions.

IV. Expected outlook and developments

This section concerns the developments expected by the institution, such as the issuance of a new payment instrument or any change affecting payment instruments currently issued or managed.

A clear distinction must be made between the **expected outlook and developments** and the corrective actions taken or planned in the framework of the above-mentioned controls.

Examples for outlook and developments: Migration to SEPA for credit transfers and direct debits, the launch of a virtual or prepaid card, withdrawal of a payment instrument, etc.

Important remark concerning mutual banking groups

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

- the central body alone should produce risk analysis in this Annex. The affiliated company is therefore relieved of this task. It must nevertheless mention "that it refers to the central body's decisions in the area of risk analysis and risk mitigation measures". The risks specific to the company itself, which have not been described in the analysis provided by the central body, must nevertheless be specified by the affiliated company.

- this also applies to the periodic control function. If this function is exercised under the central body's responsibility and described by this body in the "periodic control" section, only the controls specific to the affiliated company should be provided by the latter.

- lastly, this applies to the description of expected developments. The affiliated company should only describe the developments specific to it and not addressed by the central body.

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

- the affiliated company should describe, clearly and accurately, all controls focusing on payment instruments implemented by the central body and should at no time refer to the central body's internal control report (which does not include an annex on the security of payment instruments).

Reporting table:

Presentation: in order to help the reporting institution to prepare their responses and to harmonise the data from different institutions, all information may be reported using the reporting table presented hereafter. The use of this reporting model is encouraged, however the institution may use its own reporting format if it contains at least the data mentioned below.

Payment instrument:		
A) Identification and Management of Risks (by payment instrument)		
Gross risks[6]	**Risk mitigation measures implemented** & Recommendations of external institutions	**Residual** risks
B) Expected outlook and developments (by payment instrument)		

C) The control function (focusing on payment instrument)				
Entity conducting the control	The controlled entity	Frequency of the control	Observations	Corrective actions (implemented or planned)

[6] If the institution is unable to rate its gross risks, it shall put "unrated gross risks" in the corresponding column.

Terminology

Cashless payment instrument: payment instruments other than banknotes and coins that allow for the transfer of funds, irrespective of the product or technical process used:

Operational processes: all related and interacting activities necessary for operating payment instruments.

Operational risk: risk of a loss resulting from a deficiency or failure attributable to processes, persons, systems or external events**.**

Gross risks: risks that could affect the smooth functioning and security of payment instruments, before the institution has implemented procedures and measures to manage them.

Risk mitigation measures: all actions taken by the institution to better contain its risks by reducing their impact and their frequency of occurrence.

Residual risk: the risk persisting after taking account of risk mitigation measures.

Compliance: compliance with rules, regulations, codes and professional guidelines.

Internal control: system to provide a reasonable assurance that compliance obligations are met.

Periodic control (or audit): compliance control carried out in the form of investigations (audit missions).

Permanent control: all procedures, systems and controls implemented to check, on an ongoing basis, compliance with the rules, recommendations and codes of conduct concerning the security of payment instruments.

Developments: all the major technological or organisational changes that could have an impact on the security of payment instruments, excluding corrective actions taken in the framework of permanent or periodical controls.

Annex A

Analytical matrix

Introduction

This analytical matrix allows supervised institutions to perform self-assessments. It is complementary to the risk reporting and internal control table focused on cashless payments, but it is not a substitute for these processes.

Since 2011, these two documents have been used to provide annual reporting on the degree of control over the payment instruments issued or managed by an institution, and the level of security achieved.

The ultimate aim of this analytical matrix is to assess the security of the systems in place. It allows for four levels of security, with each level corresponding to criteria based on specific objectives.

The matrix must be completed on the basis of information provided in the reporting table transmitted by the institution in the framework of the annex. In effect, the institution must assess whether the elements provided in its reporting table meet the security objectives listed in the questionnaire.

The institution must tick the corresponding box and justify this choice in the commentaries field associated with each answer.

Criteria for the analysis of the contents of annexes (Fundamental criteria)

Six criteria have been selected for a formalised analysis of the contents of annexes. These criteria aim to determine the level of control of the security of payment instruments by the institution and to give a view of its control activities in this domain.

1) **Assessment of the risk identification system:** implementation of a system aimed at identifying and analysing main internal and external factors likely to undermine the security of payment instruments.

No answer	
Incorrect	
Incomplete	
Correct	

Commentary on the assessment:

Assessment criteria:

a) Does the institution have a risk classification framework (standard typology, criteria for identification, analysis and monitoring, etc.) based on a recognised methodology and has it set up an integrated system for the analysis and identification of risks?
b) Do the institution's risk analysis systems take into account internal and external changes?
c) Are all risks identified classified in order of priority (from the largest to the smallest in terms of their potential impact and their likelihood)?

	Correspondence table
No answer	No communication from the institution concerning the identification of risks.
Incorrect	None of the assessment criteria are satisfied.
Incomplete	Satisfaction of at least one of the three criteria.
Correct	Satisfaction of all the criteria.

2) <u>Risk mitigation:</u> Implementation of an effective assessment of the risks identified and of appropriate solutions.

No answer	
Incorrect	
Incomplete	
Correct	

<u>Commentary on the assessment</u>:

<u>Assessment criteria</u>:

a) For the principal risks identified, does the institution analyse the potential impacts (quantified or not, financial or non-financial) and its estimated degree of control of these risks?
b) Based on the conclusions of these analyses, does the institution determine specific actions for which responsibility is clearly defined?
c) Are operational staff involved in selecting risk mitigation measures?
d) Are preventive measures put in place in order to guard against risks that are not accepted by the institution and that are likely to undermine the security of payment instruments?

	Correspondence table
No answer	No communication from the institution concerning risk mitigation measures.
Incorrect	None of the assessment criteria are satisfied.
Incomplete	Satisfaction of at least one of the four criteria.
Correct	Satisfaction of all the assessment criteria.

3) <u>Application of the principles and recommendations of external bodies:</u> Implementation of recommendations issued by external bodies regarding payment instruments security (see the indicative list of these recommendations in the annex).

No answer	
Incorrect	
Incomplete	
Correct	

<u>Commentary on the assessment</u>:

<u>Assessment criteria</u>:

a) Are the above-mentioned recommendations concerning payment instruments security clearly indentified and integrated into the institution's procedures?
b) Is the implementation of the different recommendations monitored by the institution's compliance officer or by an employee with specifically defined compliance duties?

	Correspondence table
No answer	No communication from the institution concerning risk mitigation measures.
Incorrect	None of the assessment criteria are satisfied.
Incomplete	Satisfaction of at least one of the two criteria.
Correct	Satisfaction of all the assessment criteria.

4) <u>The impact of risk mitigation and risk monitoring measures:</u> The mitigation strategies adopted should aim to strengthen the security of payments means and limit the identified risks.

No answer	
Incorrect	
Incomplete	
Correct	

<u>Commentary on the assessment</u>:

Assessment criteria:

a) Do the measures implemented contribute to enhancing the security of payment instruments by diminishing the impact of the risk and/or the likelihood of its occurrence?
b) Does the institution ensure that the measures adopted do not create other risks?
c) Has a system for monitoring the identified risks and the evolution of these risks been set up?

	Correspondence table
No answer	No communication from the institution concerning the organisation of controls.
Incorrect	None of the assessment criteria are satisfied.
Incomplete	Satisfaction of at least one of the three criteria.
Correct	Satisfaction of all the assessment criteria.

5) <u>The risk control framework</u> The controls implemented should be appropriate and correspond to the nature and the complexity of the identified risks.

No answer	
Incorrect	
Incomplete	
Correct	

<u>Commentary on the assessment:</u>

Assessment criteria:

a) Are the control activities commensurate with the scale of each risk and conceived to diminish each risk?
b) Does the institution ensure that its control activities fully satisfy compliance requirements and all applicable regulations?
c) Is the implementation of remedial measures subject to regular monitoring by the audit and control services?

	Correspondence table
No answer	No communication from the institution concerning the organisation of controls.
Incorrect	None of the assessment criteria are satisfied.
Incomplete	Satisfaction of at least one of the three criteria.
Correct	Satisfaction of all the assessment criteria.

6) <u>Frequency of controls:</u> The internal control system for cashless payment instruments should be subject to permanent control.

No answer	
Incorrect	
Incomplete	
Correct	

<u>Commentary on the assessment:</u>

Assessment criteria:

a) Are there regular controls aimed at strengthening the existing process and enhancing the security of all the activities relating to payment instruments?
b) Does the institution conduct unannounced inspections to ensure that the principles and procedures of control of the activity are respected?
c) Has the institution implemented precise guidelines regarding the frequency of controls?
d) Does the periodic control system have the capacity to cover the entire auditable scope within a reasonable timeframe?

	Correspondence table
No answer	No communication from the institution concerning the organisation of controls.
Incorrect	None of the assessment criteria are satisfied.
Incomplete	Satisfaction of at least one of the three criteria.
Correct	Satisfaction of all the assessment criteria.

Respect of response format (Presentation criteria)

Respect the response format below is required so that the Banque de France can obtain harmonised response data that is easy to exploit. This aspect of the response is subject to a specific score.

Response format: The institution has fully respected the format recommendations and has completed the reporting table.

No answer	
Incorrect	
Incomplete	
Correct	

Commentary on the assessment:

Assessment criteria:

a) Has the reporting table has been completed by the institution?
b) Has the reporting table not been used by the institution for expressly communicated internal reasons?

	Correspondence table
No answer	No information concerning this institution.
Incorrect	None of the assessment criteria are satisfied.
Incomplete	Partial satisfaction of one of the two criteria (e.g. table only partially completed or not completed for all payment instruments)
Correct	Satisfaction of criteria A or B without restriction.

Annex B

Examples of recommendations

In the framework of the annex to the Banking and Financial Regulation Committee's (*Comité de la réglementation bancaire et financière – CRBF*) amended regulation 97-02 concerning payment instruments, the institution should indicate if it has complied with the recommendations relating to payment means security issued by external bodies. A non-exhaustive list of these recommendations is summarised below:

A- Recommendations issued by the European Forum on the Security of Retail Payments (SecuRe Pay):

SecuRe Pay published its first report on the security of internet payments on 31 January 2013. It contains a number of recommendations and good practices which should be implemented by 1 February 2015 at the latest.

The full recommendations can be viewed at:
http://www.ecb.int/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

– Recommendations on governance and risk assessment

- Drafting of a comprehensive security policy that is properly documented and regularly reviewed;
- Detailed risk assessments for internet payments, drafting of a procedure for change management and for the management of incidents;
- A procedure for reporting security incidents to senior management and to the competent authorities, assessment of how e-merchants handle sensitive payment data;
- Implementation of security measures to mitigate identified risks. These measures should comply with security principles such as the "least privilege" principle, and use state-of-the-art technology, and should incorporate multiple layers of security defence (defence in depth);
- Procedure for business continuity and for the traceability of transactions.

– Recommendations on customer identification

- Implementation of Know Your Customer procedures (KYC), provision of information to the customer on how to perform secure internet payment transactions and on the procedures to follow in the event of a security incident;

– Strong customer authentication

- Strong customer authentication for the issue of electronic direct debit mandates (except where the beneficiary has previously been authenticated using the same procedure, or in the case of low-value payments or transfers between two accounts of the same customer. Transfers within the same payment service provider (PSP) must be justified by a transaction risk analysis);
- Strong customer authentication for any changes to sensitive payment data (including data used for the actual authentication);

- Strong customer authentication for higher-risk card payments, including those made via wallet services;
- Secure procedures for customer enrolment.

– Management of log-in sessions

- Definition of log-in and time-out rules for internet payment service sessions;
- Monitoring of payment transactions, implementation of fraud detection systems;
- Protection of sensitive data.

– Communication with customers

- Implementation of secured channels for communicating with customers where necessary;
- Procedures for customer assistance;
- Setting of limits for internet payment transactions, provision of a facility for customers to disable internet payments;
- Provision of a facility for customers to check the status of the execution of their payment transactions, provision of detailed electronic statements, accessible in a safe and trusted environment.

B- Eurosystem supervisory framworks for payment instruments

These frameworks cover transfer, taking and payment card. They are available online, respectively, under the following links:
http://www.ecb.europa.eu/pub/pdf/other/oversightframeworkcredittransferschemes2010en.pdf

http://www.ecb.europa.eu/pub/pdf/other/oversightframeworkdirectdebitschemes2010en.pdf

http://www.ecb.europa.eu/pub/pdf/other/oversightfwcardpaymentsss200801en.pdf

C) Recommendations of the Banking Card Observatory

The Banking Card Observatory is a body whose purpose is to encourage the exchange of information and consultation between all parties concerned by the smooth operation of the security of payment card systems. Every year it issue recommendations to this effect.

– Payments by mobile telephone and contactless smart cards:

- Implementation of measures allowing, whenever necessary, to verify the holder’s consent. For example, by setting up simple tools for activating or deactivating the new initiation methods or for confirming transactions;
- Conduct of risk analyses and security studies before any large-scale deployment;
- For the mobile telephone payments, provision of a personal payment code that is different from the SIM card activation PIN, and from the user's payment card PIN; if the user can modify the personal

code, the issuing bank should recommend choosing a code that is different from the user's other codes;

- Entities involved in transactions relating to contactless payments by mobile phone, should implement cryptographic protection measures to ensure the integrity and confidentiality of data exchanged between systems.

– Security measures applied to in-branch and in-store instant card issuance systems:

- Conduct of an analysis of the risks and permanent adjustment of the security levels of these measures.

– Security of remote payments:

- Strengthening of security methods in order to make remote transactions as secure as face-to-face and UPT transactions.
  For example: Giving preference to remote payment methods that allows strong holder authentication, i.e. a system that allows vendors to verify not only card and holder authenticity but also the holder's consent to the transaction.

- Facilitate the use of already available technical solutions (one-time codes, stand-alone EMV card readers, etc.) whilst controlling the cost of their development and ensuring that their deployment is accompanied by measures to inform and educate cardholders.

– Impact of co-branding on payment card security:

- whenever an institution introduces a new co-branded card, it should ensure full implementation of the existing security measures in the payment card environment regarding the collection, storage and management of sensitive data;

- If several applications are carried on the same card, issuers should select cards that can deliver a proven and recognised level of protection for the payment application.

– Payment Card Industry (PCI) security measures:

- Adoption and implementation of PCI security measures across the entire acceptance and acquisition process.

– Security tips for cardholders:

- The security tips published by the Observatory must be communicated to cardholders informing them of good practices to adopt and the risks they may face.

– Prepaid cards:

- the distribution of prepaid cards should be accompanied by measures aimed at protecting consumers, notably by informing users of how to use these instruments and by the provision of transparent tariff information;

- these cards have a similar risk profile to conventional payment cards and should therefore be subject to the same security measures both with respect to both for face-to-face transactions and for remote transactions;

- Prepaid cards are also subject to risks that are specific to the reload process and to the way they are distributed. Institutions should implement appropriate security systems to mitigate these specific risks.

D) Recommendations issued by the Banque de France

La Banque de France has, for its part, issued recommendations concerning online banking security and online card payments:

– Online banking security:

- Implementation of one-time authentication solutions for all clients using online banking services.

– The security of online card payments:

- Implementation of one-time authentication of the card holder for all online purchases.

Annex 1

Method for calculating the effect of a uniform 200 basis point shock on activities other than trading

Institutions subject to supervision should calculate the effect on current net banking income of a uniform 200 basis point shock over one year – and, where appropriate, the effect on capital of uniform 200 basis point shock upwards or downwards – and include the results of those calculations in their Internal Control Reports. These results should be based on a calculation methodology adapted to each institution. This annex describes the principal steps that an institution may need to include in its methodology.

Calculating the effect on capital of a uniform 200 basis point shock upwards or downwards

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

These calculations may use the following techniques:

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

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

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

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

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

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

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

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

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

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

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

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

Annex 2

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

1. Overview of internal control systems[7]

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;
- a description of the control of outsourced activities (*as defined in Article 4(q) and (r) of Regulation 97-02*) and the circumstances in which the institution uses outsourcing: country, authorisation and prudential supervision of external service providers, drawing up of a contract (*including a description of the principal provisions*), etc.;
- steps taken in the case of an establishment in a country where local regulations prevent the application of the rules stipulated in Regulation 97-02;
- 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*);
- number of staff assigned to permanent control and compliance control (Article 6(a), first indent of Regulation 97-02) (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 and outsourcing (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. The system for combating money laundering and terrorist financing (AML/CFT):

- a description of the AML/CFT system: staffing levels, training conducted, and procedures for keeping concerned personnel informed;
- a description of monitoring and analysis systems for detecting anomalous transactions;
- a description of monitoring and analysis systems for identifying persons and entities whose assets have been frozen;
- the procedures for control of due diligence at foreign subsidiaries and branches;

[7] 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).

- conditions for using third parties to identify customers – Articles L. 561-7 and R. 561-13-I of the Monetary and Financial Code: a description of the circumstances in which third parties are used, a description of the procedures adhered to when using third parties and the procedures for control of due diligence conducted by third parties, specifying the country where the third party is located and describing the main provisions of the contract, if applicable;
- conditions for using service providers to identify customers – Article R. 561-13-II of the Monetary and Financial Code: a description of the circumstances in which service providers are used, a description of the procedures and the control system for due diligence conducted by the service providers, specifying the country where the service provider is located and describing the main provisions of the contract, if applicable;
- conditions for using the services of agents – Article L. 523-1 of the Monetary and Financial Code: a description of the procedures and the control system for due diligence conducted by agents and a description of the main provisions of the mandate pertaining to the AML/CFT system.

1.4. 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 (Article 32-1 of Regulation 97-02);
- summary of the analysis conducted on these new products and transactions.

1.5. Periodic control system:

- a description of the organisation of the different levels that participate in periodic control, including foreign business and outsourcing (*activities, processes and entities*);
- number of staff assigned to periodic control (Article 6(b) of Regulation 97-02) (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 and outsourcing (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 segregating and monitoring assets held for third parties (Article 16 of Regulation 97-02);
- the procedures for monitoring and addressing discrepancies between the accounting information system and the management information system.