February 2012

Appraisal of on-site supervisory missions concerning compliance with the AML/CFT obligations in the field of wealth management in the banking and insurance sectors

The General Secretariat of the Autorité de contrôle prudentiel *(SGACP) analysed seventeen on-site supervisory reports conducted during the course of 2010 and 2011 concerning twenty-one credit institutions, investment firms and insurance companies belonging to French and foreign financial groups engaged in wealth management activities. The analysis focused on the anti-money laundering and combating the financing of terrorism (AML/CFT) systems implemented by these financial institutions.*

Generally the financial institutions controlled had made significant efforts to ensure that their AML/CFT systems complied with the legislative and regulatory obligations resulting from Order no. 2009-104 of 30 January 2009. In certain cases, however, analysis of the implementation of these obligations highlighted failings that prevented the systems in place from achieving the desired levels of efficiency, a situation which led or could lead to disciplinary or administrative procedures being implemented against the financial institutions concerned.

In particular, the parent companies' governance of the internal control and AML/CFT systems implemented by the entities belonging to these groups demonstrated major failings in several cases. Similarly, the permanent and periodic control systems of several financial institutions demonstrated deficiencies. The AML/CFT systems could be improved in several areas (in particular the business relations profile, updated knowledge of customers, constant due diligence, tighter scrutiny of transactions, suspicious activity reporting, and the freezing of assets).

Due to the risks presented by wealth management activities in terms of money laundering and terrorism financing, the Autorité de contrôle prudentiel *(ACP) expects the financial institutions under its supervision to demonstrate particular and appropriate due diligence. ACP's expectations in the field of wealth management concern the following main points:*

- *stronger governance, and more particularly increased coherence of internal control and AML/CFT systems within the group;*
- *the identification of high-risk customers and the implementation of appropriate due diligence measures;*
- *improved knowledge of the business relationship and the customer, both when entering into the relationship and for the entire duration thereof;*
- *improved automated monitoring systems of business relationships;*
- *greater diligence in complying with the notifications to the Tracfin financial intelligence unit, particularly shorter reporting times;*
- *improved detection devices concerning the assets-freeze lists;*
- *increased human and technical resources allocated to the units responsible for the compliance control system.*

Table of contents

Introduction

Wealth management: one of the ACP supervision priorities in 2010 and 2011

1. **The mission of the *Autorité de contrôle prudentiel* (ACP) is to ensure the continued stability of the financial system.** To this end, it ensures that the financial institutions under its supervision comply with the provisions of the Monetary and Financial Code (MFC) as well as the regulatory provisions for its application, the Insurance Code, book IX of the Social Security Code and the Mutuality Code[1]. **In particular, the ACP oversees banking and insurance-sector organisation compliance with the obligations on anti-money laundering and combating the financing of terrorism (AML/CFT) stipulated in section VI of book V of the MFC**[2].

2. **The supervision priorities in the field of AML/CFT are defined every year by the plenary session of the ACP's College**. In particular, these priorities take account of the information communicated by the relevant national and international authorities concerning the activities and geographic areas identified as risk-bearing and the alerts provided by the public authorities with respect to certain financial institutions in accordance with the risk-based approach on supervision[3]. They incorporate the regulatory developments implemented during the course of the previous months. **In 2011, they concerned in particular the activity of wealth management**, pursuing the supervisory programme previously adopted by the Banking Commission in 2010. As part of these priorities, the General Secretary of the ACP draws up the list of financial institutions shortlisted for an on-site supervisory mission[4].

3. **In the January 2010 guidelines of the Banking Commission, wealth management is defined as the "management of assets totalling more than a certain amount determined by each institution"**[5]. Wealth management covers the provision of:

   – banking services (account management, Lombard facility, etc.);
   – investment services (including investment consulting, asset consulting, etc.);
   – insurance products (life insurance contracts, bond investments).

4. **Wealth management activities were identified as a supervision priority by the ACP in light of the**:

   – customer characteristics: non-resident customers residing in countries where the legislation concerning AML/CFT is too lax, or customers residing abroad for tax purposes, politically exposed persons, resident customers directly managing substantial assets or who conduct large-scale international transactions, etc.;

   – products or services provided: possibility of large cash deposits and withdrawals, etc.;

   – terms or conditions specific to the transactions performed: customers exclusively represented by a third party, etc.;

   – distribution channels used: introduction of the customer by a third party, etc.

[1] Cf. Article L. 612-1 of the MFC.

[2] Cf. Article L. 561-36 of the MFC.

[3] Cf. the Interpretative Note on the risk-based approach of the Financial Action Task Force (FATF) and the FATF reports concerning the risk-based approach in the banking and insurance sectors on the FATF website.

[4] Cf. Article L. 612-23 of the MFC.

[5] These guidelines are published on the AML/CFT page of the ACP website.

Appraisal of the observations resulting from the on-site supervisory missions on AML/CFT systems: all-round compliance with the obligations, although several points require improvement

5. The General Secretariat of the *Autorité de contrôle prudentiel* (SGACP) analysed seventeen on-site supervisory reports concerning twenty one credit institutions, investment firms and insurance companies belonging to French and foreign financial groups and engaged in wealth management activities. The analysis focussed on the anti-money laundering combating the financing of terrorism (AML/CFT) systems implemented by these financial institutions.

   During the course of 2010 and 2011, these financial institutions were subjected to on-site supervisory missions by the Banque de France Inspectors (Delegation charged with the on-site inspection of credit institutions and investment firms) for the banking sector and by staff from the Anti-money laundering Mission (Cross-functional and Specialised Supervision Division) for the insurance sector. Despite different supervision scopes (general missions with an AML/CFT dimension or missions focusing on the AML/CFT system), **all the missions examined the AML/CFT systems of financial institutions belonging to a financial group, whether they were the parent company in France or one of its subsidiaries set up in France or abroad.** They were conducted in accordance with a strict supervision control methodology[6]. The on-site supervisory missions conducted in financial institutions belonging to the same group helped to visualise the coherence of the measures applied by the parent company within these entities and thus to assess the quality of the controls on a consolidated basis.

6. **The financial institutions analysed within these supervisory missions present a range of different profiles with regard to their presence** (financial institutions in France and abroad); **the organisation of the wealth management business activity** (activities localised in dedicated bodies or incorporated into other business lines, for example retail banking); **their staffing numbers** (ranging from a few dozen persons to several hundred or more at group level); **their financial capacity** (in particular a net banking income ranging from a few million euros to several hundred million euros or more at group level); **their clientele** (private customers, legal persons or special-purpose funds, French or foreign customers, resident or non-resident customers, politically exposed persons, etc.); **the assets managed** (in terms of value – from several hundred million euros to several hundred billion euros for the largest groups – or concentration – from a wide range of assets to a strong concentration); **and the products and services provided** (under mandate or direct management; banking, investment or insurance products; low-risk or complex products; related services).

7. **The seventeen on-site supervisory reports drawn up following these missions[7] were analysed by the ACP's divisions[8]. This study presents the main conclusions of the on-site supervisory reports and takes into account the follow-up to these reports implemented by the ACP (cf. § 11). It provides a comparative analysis of the AML/CFT systems implemented** by these financial institutions with regard to the obligations introduced by Order no. 2009-104 of 30 January 2009, transposing into French law Directive no. 2005/60/EC of the European Parliament and the Council of the European Union[9], and identifies the areas for improvement highlighted by this analysis and which the ACP judges that all the financial institutions under its supervision should be made aware of.

---

6 Cf. annex 1 concerning the on-site supervisory control methodology in the banking sector. The on-site supervisory control methodology of the insurance sector is similar.

7 These on-site supervisory reports concerned one or more establishments in the same group (for example the parent company of the group and one or more of its subsidiaries).

8 These on-site supervisory reports are analysed by the Off-site Control Divisions for the banking sector and by the Cross-functional and Specialised Supervision Division for the insurance sector calling on the expertise of the on-site supervisory units and, where necessary, the Legal Affairs Division.

9 Directive no. 2005/60/EC of the European Parliament and the Council dated 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorism financing.

8. **Due to the exposure of the wealth management activities to the risk of money laundering and terrorism financing, the ACP expects these financial institutions to demonstrate particular and appropriate due diligence within the framework of the obligations of due diligence and reporting stipulated in section VI of book V of the MFC**. These obligations are specified in Article 11-7 of Regulation no. 97-02 of the Banking and Financial Regulation Committee (CRBF) [10] for the banking sector and in Articles A. 310-8 and A. 310-9 of the Insurance Code for the insurance sector. Several specific aspects of these obligations are clarified in the ACP guidelines[11].

9. **Generally, the financial institutions controlled had made significant efforts to ensure that their AML/CFT systems complied with the legislative and regulatory obligations resulting from Order No. 2009-104 of 30 January 2009. The analysis of the implementation of these obligations nevertheless highlighted failings which prevented the existing systems from achieving the desired levels of efficiency**. In particular, the parent companies' governance of the internal control and AML/CFT systems implemented by the establishments belonging to these groups demonstrated, in several cases, major failings in relation to the objective of fully effective consolidated management of these risks. Similarly, the permanent and periodic control systems often demonstrated numerous deficiencies. The AML/CFT systems could be improved in several areas (in particular the business relations profile, updated knowledge of the customers, constant due diligence, tighter scrutiny of transactions, suspicious transactions reporting, and the freezing of assets).

10. **Several AML/CFT obligations are particularly important due to the impact of a failing at their level on compliance with the other obligations**: in particular, the quality of parent-company governance over the AML/CFT systems within the group, the effectiveness and speed of information exchange within the group, the accuracy of the business relationship profiles, the permanent quality of the elements relating to customer identity and to the knowledge of the business relationship, and finally the suitability of the automated monitoring of activities. **These points are reiterated in the main body of the appraisal and in the conclusion**.

11. **Up to now, more than two-thirds of the supervision reports have been processed. In most cases, they have given rise to requests for corrective measures formulated in follow-up letters which are closely monitored by the ACP (cf. annex 2). The application of the requests for corrective measures formulated in these follow-up letters is closely monitored by the ACP.** By means of written exchanges, interviews and/or on-site visits, the General Secretariat ensures from the financial institutions concerned that the requests for corrective measures have been implemented within the timeframes indicated. One case led to a disciplinary procedure being opened. Whether or not the processing of the cases in progress will lead to other administrative or disciplinary procedures remains to be established. New on-site supervisory missions could be initiated within a short timeframe, in particular if the implementation of corrective measures appears to be slow or unsatisfactory. Some corrective measures must also be backed up by appropriate analysis in the annual internal control reports drawn up by the financial institutions[12].

[10] Regulation No. 97-02 of the Banking and Financial Regulation Committee (CRBF) relating to the internal supervision of credit institutions, investment firms and payment institutions.

[11] Cf. the AML/CFT page of the ACP website. Wherever necessary, the document refers to the guidelines and sectorial principles of application concerning specific themes. The ACP sectorial principles of application relating to AML/CFT for the insurance sector covering several themes examined in the document are only cursorily mentioned in this footnote.

[12] Cf. annex 2 concerning the appraisal of the follow-up to the on-site supervisory missions.

1 Governance of the AML/CFT system: the group-wide approach

1.1 Governance framework

The ACP expects:

- *that the executive and deliberative bodies of the financial institutions periodically assess and control the effectiveness of internal control and AML/CFT policies, systems and procedures implemented to comply with their obligations and take the appropriate measures to remedy any failings observed;*
- *that, to this end and within the required timeframe, the financial institutions provide the executive and deliberative bodies with the information necessary to complete their mission both in terms of quantity and quality.*

12. **For the most part, the executive and deliberative bodies appeared to be engaged in implementing and monitoring the internal control and AML/CFT systems within the financial institutions. In performing their tasks, the majority of the executive bodies relied on internal committees in which they were represented** (e.g. the internal control committee, compliance committee, *politically exposed persons* committee, *high-risk customers* committee, etc.). **The executive and deliberative bodies also had access to information on the functioning of the internal control and AML/CFT systems by examining the periodic reports provided for under the regulations** (report on internal control[13], report on the measurement and monitoring of risks[14]) **as well as other documents** (indicators, spot analyses, periodic – e.g. monthly or quarterly – reports, etc.).

13. **Nevertheless, the executive and/or deliberative bodies of six financial institutions either did not have access to information relating to the internal control and AML/CFT systems necessary to completing their mission** (these points missing from meeting agendas) **or only had access to summary written information or oral information on these themes, or only scarcely had access to any information** (once every semester or even just once a year, e.g. during the presentation of the internal control annual report). The ACP required from three of the financial institutions concerned to improve the quantity and quality of the information provided to the executive and/or deliberative bodies with regard to internal control and AML/CFT, including the data provided in the internal control reports and any monitoring elements on the implementation of the recommendations resulting from the internal control. The ACP also asked them to formalise, in written reports, the themes raised during the meetings of the executive and deliberative bodies as well as the resulting discussions and decisions taken, in order to ensure that the executive and deliberative bodies have sufficient information to take their decisions.

14. With two exceptions, all the financial institutions had designated a member of the management board as manager of the AML/CFT system.

[13] Cf. Article 42 of CRBF Regulation no. 97-02 for the banking sector and Article R. 336-1 of the Insurance Code for the insurance sector.

[14] Cf. Article 43 of CRBF Regulation no. 97-02 for the banking sector.

1.2 Group-wide approach

The ACP expects the parent companies of the groups supervised on a consolidated basis to:

- *apply equivalent AML/CFT measures in their foreign branches to those provided for in the MFC in terms of customer due diligence and the keeping of information, and to ensure that these equivalent measures are applied in their subsidiaries headquartered abroad;*
- *thus ensure oversight of the compliance[15] monitoring and AML/CFT systems both centrally and locally, in particular by developing procedures defining the minimum AML/CFT measures equivalent to those provided for by the MFC in terms of customer due diligence and the keeping of information that the various group entities are to apply; ensuring that the procedures adopted locally as an extension of these group procedures are harmonised; making sure that all of these procedures are effectively applied; organising information exchanges within the group; and centralising the transaction monitoring and analysis system as well as the Tracfin reporting process for financial institutions located in France;*
- *check the suitability of the compliance and AML/CFT control systems to the local context, within the framework defined by the group.*

1.2.1 Organisation and steering of the activities

15. **The internal control and AML/CFT systems implemented by the financial institutions had, in general, been frameworked at group level. The group's parent company was responsible for ensuring convergence between local systems and for these systems not to be inconsistent with the framework established by the group, both in terms of organisation of the internal control system** (hierarchical or functional integration of permanent control and compliance, information exchanges on control activities through periodic committees or reports, on-site visits by the units in charge of the compliance control system, group audit missions in the local entities) **and through the steering of the AML/CFT system by the group's parent company** (dissemination of a basic procedural framework, regulatory intelligence, integration of information systems, information exchanges on customer files and notably high-risk customers, transactions requiring tighter scrutiny and suspicious transactions reporting, tools parametering). **One financial institution had not implemented such a structured oversight framework. The oversight framework of another financial institution did not encompass the wealth management activities of several of the group's entities, either due to the specific configuration of the group's institution** (incorporation in a different business line) **or as a result of insufficient oversight of certain entities** (lack of group-level leadership). The ACP expects the group concerned to revise the oversight framework for these activities by adapting them to the risks encountered.

1.2.2 Adaptation to the local context within the group-defined framework

16. **The parent companies of several groups had entrusted the steering of part of the AML/CFT systems to the units responsible for the compliance control system in the different financial institutions of the group in order to ensure localized processing or comply with local regulations** (e.g. the oversight of new business relations, transaction monitoring, suspicious transactions reporting, etc.). **Errors in adapting the group-defined AML/CFT systems to the local context were observed** (e.g. no adaptation of the classification defined by the group within the local entity leading to incoherent criteria being adopted – inappropriate asset thresholds with regard to the average outstanding amounts – etc.), **with the risk of adopting an AML/CFT system poorly adapted to the risk of money laundering or terrorism financing actually encountered within the entity.** The ACP asked two financial institutions to revise and adapt their criteria.

[15] All establishments controlled, including in the insurance sector, had adopted a compliance function. Consequently, this will be referred to throughout the entire document for all establishments without distinction.

1.2.3 Coherence of the procedures

17. **In several cases, the local measures demonstrated insufficient integration in the framework defined by the group. Overall coherence between the group procedures and local procedures was not systematically guaranteed**. This sometimes led to divergences between the measures applied by the different entities of the group. These divergences had a particular impact on the **implementation of due diligence measures concerning high-risk business relations** (e.g. no conditions defined at group level concerning new business relations and transaction monitoring, inconsistent risk criteria – lists of high-risk and non-cooperative jurisdictions defined by the FATF[16] – leading to the creation of diverging business relation profiles, extension of deadlines to meet a customer introduced by a third party or a business facilitator after the beginning of the business relationship, different spelling parameters from one entity to another in relation to the asset-freezing mechanism, etc.). **Not all the financial institutions had conducted a formal analysis of the scope of these divergences** (e.g. no inventory of the points of divergence, analysis of points of divergence based solely on a questionnaire submitted to the financial institutions without examining the local procedures or on-site controls). The ACP required from two financial institutions to strengthen and harmonise their risk monitoring systems across the group, to define coordinated procedures ensuring a level of due diligence within the group's entities at least equivalent to that imposed in France, and to check that these procedures are correctly applied by means of in-depth periodic audit missions.

1.2.4 Information exchanges[17]

18. **In several financial institutions, the information exchanges implemented within the group demonstrated certain failings. These failings primarily resulted from a lack of satisfactory procedures** (e.g. lack of or imprecise procedures relating to information exchanges, in particular in cases where customers belonged to different business lines – wealth management and retail banking – or to different activities – banking and insurance activities – etc.). **They also resulted from the insufficient integration of information management tools within the group** (for example fragmentation and heterogeneity of customer databases, no interfacing between customer databases and monitoring tools, insufficient knowledge of the local tools and parameters by the parent company, etc.).

19. **Consequently, information exchanges relating to the organisation of due diligence and the existence and content of suspicious transactions reports were, in several cases, limited, thereby impacting the functioning of the centralised mechanism for detecting and monitoring anomalies**, for example:

- no information feedback to the group's parent company, in particular with regard to files on high-risk customers (either when entering into a business relationship or for the duration thereof), transactions subject to enhanced scrutiny and suspicious transaction reporting;
- no dissemination of information in the possession of the group's parent company to the local entities, in particular with regard to necessary elements relating to the identity and knowledge of the customer when entering into a business relationship;
- heterogeneity of customer transaction monitoring systems from one entity to another;
- lack of parent company-level consolidation of information concerning a single customer provided by different entities, etc.

With particular regard to the monitoring of high-risk business relations, the ACP asked the financial institutions concerned to define the means of circulating, within the group, information relating to the

[16] Cf. FATF website.

[17] Cf. the guidelines concerning information exchanges within and outside the group published on the AML/CFT page of the ACP website.

organisation of due diligence and to the existence and content of suspicious transaction reporting, and in particular to facilitate access of the group's parent company to customer information in the possession of the local entities in order to obtain a consolidated vision. The group's tools must be deployed and coordinated across and within all the entities.

Information exchange with financial institutions located in countries where legislation on professional confidentiality is restrictive or is presented as such was particularly weak. These limitations prevented several financial institutions from complying with the AML/CFT obligations, despite the fact that in some countries they were not founded on any legal impossibility (e.g. limited transmission of nominative information concerning customers, including high-risk customers, and transactions, including transactions subject to enhanced scrutiny, outsourcing of all IT centres in subsidiaries located in countries with increased professional confidentiality, etc.). The ACP asked the financial institutions concerned to take every measure to organise information exchange. Furthermore, the group's parent company must have easy access to the information systems and data belonging to the group's foreign subsidiaries and branches with a view to facilitating consolidated AML/CFT oversight. The ACP also asked these financial institutions to make sure money laundering questionnaires[18] systematically mention the subsidiaries and branches located in countries where the legal insufficiencies or practices present an obstacle to AML/CFT and to inform it of any new refusal on the part of group entities to communicate or access the information required for consolidated AML/CFT oversight.

2 Risk classification and profiles

2.1 Classification of the risks of money laundering and terrorism financing

The ACP expects the financial institutions to:

- *adopt a classification of the risks of money laundering and terrorism financing;*
- *ensure that this classification is adapted to their activities, customers, sites, and risks in the wealth management activity, and in particular that it is based on relevant risk criteria relating to the characteristics of the customers, the nature of the products and services provided, the distribution channels used, and the conditions in which the transactions are performed;*
- *revise their classification on a regular basis.*

2.1.1 Defining a risk classification

20. **With the exception of three entities, all the financial institutions had adopted a risk classification. These classifications had either been defined in 2010 to take account of the new legal obligations or had been updated during that year on the basis of existing classifications**, sometimes rather late (autumn 2010). The ACP asked the financial institutions concerned which had not formalised a risk classification to do so in a limited time frame.

21. **Generally speaking, the classifications covered the wealth management activities, both for activities in the dedicated entities and those integrated in other business lines** (e.g. retail banking). **One single financial institution had not developed its risk classification according to specific wealth management factors.** The ACP asked this financial institution to complete its risk classification by integrating distinctly the wealth management activities, to adapt the content of the due diligence measures to the wealth management activities (e.g. information and documents relating to knowledge of

[18] "BLANCHIMT" statuses to be communicated to the ACP by the institutions concerned.

the customer, due diligence criteria, etc.) and to perform separate statistical monitoring of the customers (e.g. with regard to the anomalies detected by the monitoring and analysis systems, suspicious transactions reporting, etc.).

2.1.2 Definition of risk criteria

22. **The risk criteria on which the classifications were based included aspects as diverse as**:

- **the customer's characteristics** (e.g. natural or legal person, sector of activity, amount of the assets, etc.);
- **the nature of the services and/or products offered** (e.g. management method, amount of the transactions, types of transaction – i.e. cash transactions or early repayments of credit – etc.);
- **the distribution channels** (e.g. internal or external channel, etc.);
- **the customer's country of residence or the country in which the transactions were carried out** (e.g. high-risk and non-cooperative jurisdictions identified by the FATF, countries which have not signed an administrative assistance agreement with France concerning tax matters[19], etc.);
- **the history of the business relationship** (e.g. the volume of incoming and outgoing transactions, previous suspicious transactions reports, previous legal record, the customer's stated requirement not to receive mail at home, etc.).

23. **However, in more than a quarter of the financial institutions audited, failings impacted the relevance of the classifications developed**:

- **certain important risk criteria were not taken into account** (e.g. the nature of the products and services, distribution channels, existence of suspicious transactions reports, etc.);
- **the references of these criteria were incomplete** (e.g. the absence of certain high-risk and non-cooperative jurisdictions identified by the FATF, due notably to the lack of a regular updating of the lists of countries or of the downloading of lists from websites such as Wikipedia, absence of certain regulatory categories of politically exposed persons, absence of certain sectors of activity – real estate professionals – etc.);
- **the risk criteria did not appear to be adapted to the customers' characteristics** (e.g. asset threshold too high with regard to the average outstandings, etc.).

The ACP asked the financial institutions concerned to include all the criteria mentioned in Article R. 561-38 I 2° of the MFC[20] in the classification.

2.2 Profile of business relations and corresponding due diligence measures

The ACP expects the financial institutions to:

- *Establish, for each business relationship, a risk profile adapted to the risk of money laundering and terrorism financing;*
- *ensure that these risk profiles take account in particular of the customer's characteristics, the nature of the products and services, the conditions of the transactions and the distribution channels;*
- *justify the allocation of a risk profile built on a formal analysis;*
- *implement due diligence measures adapted to the risk of money laundering and terrorism financing and which are consistent with the business relationship profile.*

[19] Cf. Article D. 561-32-1 of the MFC.

[20] Cf. the guidelines of the Banking Commission relating to politically exposed persons and to the notions of equivalent third-party countries and wealth management in the field of anti-money laundering and combating the financing of terrorism published on the AML/CFT page of the ACP website.

2.2.1 Categories of business relationship profiles

24. **With the exception of three financial institutions which had not formalised a risk classification (cf. §20), all the entities had defined business relationship profiles based on their classification. The number and nature of these profiles varied according to the sensitivity of the business relations to the risk of money laundering or terrorism financing** (binary categorisation – customers demonstrating a high risk or not – or more granular – four or five risk categories defined) **and to the means of determining which customers present a high risk** (categorisation on the basis of a single criterion – politically exposed persons, opaque legal structures, asset thresholds, etc. – or by combining several of these criteria).

25. **The profiles thus established nevertheless sometimes lacked relevance, either due to the fact that one or more important risk criteria were not taken into account in the classification or in the construction of the profiles** (e.g. non-incorporation of the different parties to the business relationship, the history of the business relationship, the nature of the transactions handled, the volume of assets managed, etc.), **or as a result of the incomplete nature of the information collected when identifying and developing knowledge of the customer, or the lack of relevance of the criteria governing the creation of the profiles** (cf. § 22 to 23 and 34 to 37). **These weaknesses led to failings being observed in several financial institutions in the process of detecting high-risk customers**. The ACP asked the financial institutions concerned to formalise the process for defining high-risk customers on the basis of relevant criteria. In some cases, the detection of high-risk customers also suffered from absent or insufficient detection mechanisms implemented by the financial institutions.

26. **In particular, the mechanism for detecting politically exposed persons was found to be unsatisfactory in five financial institutions** (e.g. simple registration of the customer at the start of the business relationship without any additional background checks being conducted by the financial institution, customer databases not screened during the business relationship, use of restrictive spelling parameters ("exact match" function), direct members of the family (spouse) not recognised as being politically exposed persons, etc.). **The financial institutions were therefore not always capable of implementing the enhanced or additional due diligence measures required by law**. With this in mind, the ACP asked the financial institutions concerned to strengthen their mechanism for detecting politically exposed persons, for example, for one financial institution, to ensure that the information systems automatically applied the status of politically exposed persons to direct members of the family and representatives of politically exposed persons. The ACP also asked these financial institutions to formally report back to the executive body on any new politically exposed person, as provided for in the financial institutions' procedures, and to inform the executive body on a regular basis of the developments of the existing files of politically exposed persons[21].

2.2.2 Adaptation of due diligence measures to the business relationship profiles

27. **Generally speaking, business relations with high-risk customers who had been identified as such were subject to appropriate oversight as regard the risk of money laundering or terrorism financing. With the exception of two financial institutions, entering into business relations with high-risk customers was subject to prior authorisation from the unit responsible for the compliance control system and/or the executive body. Some financial institutions had introduced a launch committee**. In particular, politically exposed persons and, where applicable, people exercising similar functions at national level were subject to systematic authorisation by the executive body itself.

[21] Cf. the Banking Commission guidelines relating to politically exposed persons and to the notions of equivalent third-party countries and wealth management in the field of anti-money laundering and combating the financing of terrorism published on the AML/CFT page of the ACP website.

28. **Enhanced or additional due diligence measures were implemented when entering into a business relationship, once the profile of the relationship was determined with regard to the risk of money laundering or terrorism financing** (e.g. the collection of additional information and documents concerning knowledge of the customer and the business relationship, etc.) **and throughout the duration of the business relationship** (e.g. increased frequency of customer file revision by the case officers and the units responsible for the compliance control system, lower detection thresholds within the framework of transaction monitoring, etc.).

29. **One financial institution did not apply additional due diligence measures with regard to politically exposed persons**. **Several other financial institutions also operated insufficiently strict monitoring of business relations with politically exposed persons** (e.g. no updates concerning the function held, etc.). The ACP asked the financial institutions concerned to strengthen their due diligence mechanism with regard to politically exposed persons[22].

30. **In one third of the financial institutions, the failings observed in relation to data collection on the customer's identity and the knowledge of the business relationship facilitating the creation of business relationship profiles (cf. § 34 to 37) reduced the efficiency of the due diligence mechanisms implemented with regard to these high-risk customers** (e.g. revision of customer files not adapted to the risk of money laundering and terrorism financing, etc.).

3 Obligations of due diligence

3.1 AML/CFT procedures

The ACP expects the financial institutions to:

- *adopt written internal procedures defining the rules relating to the implementation of due diligence, suspicious activity reporting, record keeping, asset freezing and internal control measures;*
- *define operational procedures geared to their activities, customers, sites and risks;*
- *regularly update their procedures, in particular taking account of legislative and regulatory developments as well as any change affecting their activity (customers, products and services, geographic coverage, etc.);*
- *provide their personnel with permanent access to the procedures in printed or electronic format.*

3.1.1 Updating the procedures

31. **Generally speaking, when the on-site supervisory missions were carried out, the financial institutions had adapted their AML/CFT procedures to the new legislative and regulatory obligations resulting from the transposition in France, in 2009, of Directive no. 2005/60/EC. This compliance process was occasionally delayed**, taking place during the course of summer and autumn 2010. **Three financial institutions had not undertaken this revision**: at the time of the on-site supervisory missions, their procedures did not integrate the new legislative and regulatory obligations concerning in particular the enhanced scrutiny of transactions, politically exposed persons, etc. **In the absence of appropriate procedures, these financial institutions' AML/CFT systems demonstrated major failings**. The ACP requested the financial institutions concerned to update their procedures as soon as possible.

[22] Cf. the guidelines of the Banking Commission relating to politically exposed persons and to the notions of equivalent third-party countries and wealth management in the field of anti-money laundering and combating the financing of terrorism published on the AML/CFT page of the ACP website.

3.1.2 Content of the procedures

32. **In general, the content of the updated procedures adopted by the financial institutions was satisfactory. The main obligations relating to AML/CFT were identified** (identification and verification of the identity of the customer and effective beneficiary, knowledge of the business relationship, constant due diligence, modulation of due diligence obligations with regard to the risk, keeping of documents, suspicious transaction reporting and asset freezing). **The framework procedures within which these major principles were defined were generally subject to operational adaptations** (e.g. drafting sheets indicating the information and accompanying proof to be collected from the customer when entering into a business relationship and throughout the duration thereof). **Two financial institutions had not provided a precise definition of the content of the due diligence mechanisms relating to customers considered to be high-risk** (no mention of the additional information and documents to be collected from the customer), in one case in the complete absence of a risk classification. The ACP asked them to ensure compliance of the AML/CFT systems with the regulations and to define the appropriate due diligence measures.

3.1.3 Accessibility of procedures for staff

33. **The staff involved could access AML/CFT procedures in printed or electronic format. Three financial institutions nevertheless presented a very fragmented procedural corpus, making it difficult for the staff to ensure the effective application of these procedures** (directory of procedures comprising different or even obsolete versions, hazy architecture of the company's intranet). The ACP asked them to take the necessary steps to harmonise this procedural corpus.

3.2 Identification and knowledge of the customer[23]

The ACP expects the financial institutions to:

- *identify and check via the appropriate documents, the identity of the customer and, where necessary, the person acting on the customer's behalf as well as the beneficial owners before entering into any business relationship;*
- *apply strict oversight of the conditions for delaying verification of the customer's identity and, where necessary, that of the effective beneficiary while establishing the business relationship under conditions laid down in Article R. 561-6 of the MFC;*
- *collect and keep all relevant information and documents relating to the object and nature of the business relationship and to the customer in order to obtain satisfactory knowledge when entering into a business relationship;*
- *define the conditions for recourse to third parties (business facilitators, third-party introducers, etc.) and integrate them into their internal control system;*
- *update their customer files according to a periodicity adapted to the risk of money laundering and terrorism financing or in response to any significant event (e.g. a large transaction);*
- *collect and keep, when updating the customer files, any relevant information and documents relating to the object and nature of the business relationship and the client in order to obtain an up-to-date vision;*
- *reconsider where necessary, while updating customer files, the profile of the business relationship with regard to the risk of money laundering and terrorism financing based on a formal analysis, in particular taking account of any new information and documents collected.*

[23] Cf. joint ACP and Tracfin guidelines concerning suspicious activity reporting published on the AML/CFT page of the ACP website.

3.2.1 Identification and verification of the customer's identity

34. **The procedures for identifying the customers, individuals acting on their behalf and beneficial owners generally complied with the provisions of the MFC, and the information and documents collected in applying these procedures generally satisfied the requirements stipulated in the regulations**. One financial institution had extended the mechanism for identifying and checking the identity of the beneficial owners beyond the provisions of Article R. 561-1 of the MFC to include any natural person holding 20% or more of the actions or voting rights of a company (10% in the event of increased risk).

35. **Four other financial institutions had nevertheless implemented exemption procedures intended to delay the collection of supporting documents relating to the customer's identity, in one case by up to 6 months, after entering into a business relationship**. These exemption procedures were applied by some financial institutions on a very regular basis (up to 14% of accounts opened during one semester). While the implementation of these procedures was subject to the authorisation of the members of the management team or the compliance officer for each new business relationship, **these procedures did not comply with the conditions presented in Article R. 561-6 of the MFC insofar as transactions were carried out before the customer's identity was checked. Furthermore, the regularisation measures stipulated in the procedures concerning the customer files were not systematically respected**. The ACP required the financial institutions concerned to take the necessary steps to ensure that their exemption procedures complied with the regulatory requirements and to complete the customer files which had been subject to such derogations as quickly as possible. It also required them to increase the monitoring of any derogation to be granted in the future within the framework of the procedures revised in accordance with the regulations.

3.2.2 Knowledge of the customer and the business relationship

36. **The procedures defined by the financial institutions included the obligation of collecting information and documents relating to knowledge of the customer and the business relationship. The on-site supervisory missions nevertheless highlighted failings in applying these obligations, including for high-risk customers. The information concerning the customers often proved to be either incomplete** (e.g. no mention of the start date of the business relationship, failure to take into account different parties to the business relationship – in particular individuals acting on behalf of the customers and the beneficial owners – no information concerning the expected functioning of the account, the activities, the source of the funds provided, the incomes, assets and financial situation for legal persons, etc.), **or too general** (e.g. vague activity categories – "senior executive" with no mention of the sector of activity – income and asset brackets that are too large – "income of more than 500,000 euros" whereas the average outstanding of assets managed by the establishment is 250,000 euros – etc.). **The supporting documents stipulated in the financial institutions' procedures were often lacking** (e.g. no proof of residence, residence for tax purposes and source of funds, etc.). The ACP required the financial institutions concerned to update the customer files as quickly as possible by including the missing information and supporting documents, with high-risk customer files given top priority.

3.2.3 Updating customer files

37. **The financial institutions had implemented processes to update the information and documents relating to the customer's identity and knowledge of the business relationship. Where applicable, the files were revised within the framework of a review committee, in particular for high-risk customers. The revision was applied according to a schedule which varied considerably from one financial institution to another** (ranging from three months to three years for high-risk customers and between two and four years for non-high-risk customers and according to specific events occurring at any time in the business relationship, e.g. when carrying out large transactions). **The revision process**

had been implemented very late in six financial institutions: a high proportion of their customer files had still not been updated in autumn 2010 (e.g. at one establishment, only 5% of high-risk customer files had been revised in September 2010). **The scope of the updates seemed limited: new data entered in the customer files was often very general in nature, the documents supporting this data were rarely collected, the conclusions of the revisions were rarely formalised and, in two financial institutions, no analysis had been conducted on the basis of this new data with a view to reviewing the profile of the business relationship**. The ACP required the financial institutions concerned to implement a periodic customer file revision process, the results of which should be formalised, controlled and added to the business relationship profile.

3.3 Constant due diligence [24]

The ACP expects the financial institutions to:

- *adopt monitoring and analysis systems concerning their business relationships based on knowledge of the customers and appropriate criteria with a view to detecting transactions representing an anomaly in light of the business relationship profile and which could be subject to enhanced scrutiny or suspicious transaction reporting;*
- *implement automated monitoring systems concerning the business relationships covering all the customer databases and transactions when relevant to the activities of the financial institution;*
- *ensure that first-level permanent controls are implemented and that the alerts produced by the monitoring systems are satisfactorily processed and monitored in a reasonable timeframe.*

3.3.1 Monitoring systems

38. **All the financial institutions had adopted systems for monitoring and analysing the business relations. The automated monitoring systems implemented by the financial institutions were based on the definition of transaction thresholds and, with the exception of three financial institutions, behavioural criteria** (e.g. a high credit volume compared to the debit volume, cash deposits and foreign transfers, dormant accounts, etc.) with a particular view to detecting the transactions which should be subject to enhanced scrutiny or a suspicious activity reporting. **Several of these mechanisms demonstrated failings with regard to**:

    - **IT databases screened by monitoring tools** (e.g. no networking of customer databases thereby preventing the consolidation of information for a single business relationship, failure to take into account the different parties to the business relationship - in particular individuals acting on behalf of the customer and the beneficial owners - etc.);
    - **information documented in these databases** (e.g. an absence of or too generalised data and documents relating to the identity and knowledge of the customer entered in the databases on the basis of physical files, absence of data concerning the profile of the business relationships, etc.);
    - **the scope of the transactions under monitoring** (e.g. the exclusion of certain transactions from the control scope – transactions dating back more than 1 month, transactions other than cash transactions – no control of cheques with regard to the risks of money laundering and terrorism financing);
    - **the periodicity and coverage of the controls carried out** (e.g. half-yearly or annual *a posteriori* controls only, controls on a limited sample of transactions: e.g. 10 cheques per year for a total volume of 1,120 cheques drawn or cashed abroad, 20 contracts a month for a total volume of 26,000 life insurance contracts, etc.);

[24] Cf. joint ACP and Tracfin guidelines on suspicious transaction reporting, published on the AML/CFT page of the ACP website.

– **the parameters of these systems** (e.g. no modulation of alerts with regard to the risk of money laundering and terrorism financing, transaction thresholds and analysis scenarios not adapted to the profile of the business relationship – frequent recourse to the former threshold of 150,000 euros[25]– no detection device for split transactions or repetitive or abnormal transaction patterns, no periodic revision of the transaction thresholds and analysis scenarios, etc.). Some financial institutions were unable to justify the parameters adopted.

The ACP asked the financial institutions concerned to formalise and implement a monitoring system for all the transactions integrating the elements of identification and knowledge of the customers and based on detection criteria permanently adapted to the activity of wealth management, the activities of the financial institution and the profile of the business relations. This monitoring system must be subject to periodic revision.

3.3.2 Constant due diligence concerning business relationships

39. The implementation of business relations monitoring and analysis was based on both the business teams and certain agents exercising operational functions within the units responsible for the compliance control system (e.g. processing alerts generated by the automated monitoring systems). **While highlighting an in-depth knowledge of the business relationship, the chargés d'affaires in several financial institutions relied to a considerable extent on staff from the units responsible for the compliance management system to perform the monitoring tasks** (e.g. no information or support documents collected concerning the economic rationale of transactions or the source or destination of funds, customer sheets incorrectly documented or even missing when alerts are triggered, etc.). **One financial institution had even entrusted the implementation of its constant due diligence obligations to introducers, which is prohibited by the regulations (Article L. 561-7 of the MFC)**. The ACP asked the financial institutions concerned to ensure that their commercial teams implement the obligatory AML/CFT controls correctly and formalise them (for example drafting of an alert sheet)[26].

40. **Anomalies were generally detected by the automated monitoring systems** (e.g. transactions higher than a given amount), **and more rarely by chargés d'affaires** (e.g. complex transactions or transactions where the economic or licit objectives are not clear). **On several occasions, the operatives handling these alerts within the units responsible for the compliance management system were observed not to disseminate relevant information in a systematic manner which would have enabled the chargés d'affaires to exercise appropriate due diligence concerning the business relations** (e.g. the alerts triggered with regard to a customer's transactions or the existence of a suspicious transaction report, etc.).

3.3.3 Handling alerts

41. **The on-site supervisory reports also identified numerous failings with regard to the handling of alerts generated by the detection devices, in particular in relation to the information and documents used to analyse the alerts** (e.g. simple linear reading on the transactions screen, supported documents not requested from chargés d'affaires, simple verbal exchanges with charges d'affaires, no formal analysis explaining post-alert's follow-up actions, payment service providers not re-contacted in the event of missing information on the instructing party in the event of a fund transfer, etc.) **and monitor the alerts handled** (e.g. no tracking file recording the alerts handled, imprecise knowledge of the exact number of files examined or alerts handled, etc.). The ACP asked the financial institutions

[25] Cf. former Article L. 563-3 of the MFC which stipulated that: "*Any major transaction concerning sums where the unit or total amount is greater than a sum set by Decree in the Conseil d'État [former Article R. 563-2 of the MFC: 150,000 euros] and which, without falling within the scope of application of Article L. 562-2, occurs in unusually complex conditions and does not seem to display any economic justification or licit objective, must be subjected to specific scrutiny on the part of the financial institution or the person indicated in Article L. 562 […].*".

[26] Cf. also the guidelines and sectorial principles of application for the insurance sector of the ACP concerning third-party introduction published on the AML/CFT page of the ACP website.

concerned to ensure that the exchanges between the commercial teams and the units responsible for the compliance control system are formalised and kept in the customer files; that the history and content of the cases processed by the units responsible for the compliance control system are also formalised and kept (including the customer files for which the alerts were filed with no follow-up, as well as the information justifying the closure of a business relationship). In six of the financial institutions examined, insufficient human and technical compliance management resources proved to have a negative impact on the quality of the alert processing operations (cf. *infra*).

3.3.4 Monitoring cash transactions

42. **Monitoring cash withdrawals and/or deposits was an integral part of the monitoring system. Most of the financial institutions had implemented alert mechanisms to this end in order to identify transactions exceeding a given threshold, whether for individual transactions or, less frequently, grouped transactions.** One financial institution had submitted cash transactions exceeding a given thresholds value to the approval of operatives in the units responsible for the compliance control system. Furthermore, three financial institutions had either prohibited certain cash transactions (deposits) or limited their number (primarily by requesting supporting documents from a relatively low threshold). **The monitoring systems nevertheless demonstrated failings with regard to**:

- **the information and supporting documents used to record the transactions and analyse the alerts** (cf. §38 to 41);
- **the alert tool settings** (no justification and inappropriate thresholds adopted, which appeared highly heterogeneous, the kind of customers or activities offering no valid rationale – from 500 euros to 150,000 euros – application, even, of the former threshold of 150,000 euros);
- **the monitoring scope applied** (cash withdrawals abroad not covered by the monitoring system).

The ACP asked the financial institutions concerned to formalise and implement a monitoring system for all transactions, including cash transactions. More particularly, the ACP asked them to produce a formal analysis of customer requests concerning the regular provision of cash, to collect the information and supporting documents stipulated by the regulations with regard to transactions subject to enhanced scrutiny, and to implement *a posteriori* monitoring of high-value transactions.

3.3.5 Enhanced scrutiny

43. Due to the aforementioned failings (cf. §38 to 42), **several financial institutions were unable to satisfactorily detect or handle those transactions subject to enhanced scrutiny. In particular, since 2009, one financial institution no longer kept the information relating to these transactions in the files provided for this purpose. More generally speaking, either the files were poorly formalised or they did not contain the information and supporting documents required to analyse the transactions, or they were handled late, sometimes by up to several months**. The ACP asked the financial institutions concerned to improve the timeframe for handling files and the justification of transactions subject to enhanced scrutiny (obligatory nature of the information and documents mentioned in Article R. 561-31 of the MFC).

4 Suspicious transactions reporting mechanism[27]

The ACP expects the financial institutions to declare to Tracfin, within a reasonable time frame, the sums recorded in their books or transactions relating to sums which they know, suspect or have good reason to suspect are derived from a predicate offence punishable by a term of imprisonment lasting more than one year or contribute to terrorism financing.

4.1 Obligation to report suspicious transactions

44. **All the financial institutions had adopted a mechanism for reporting suspicious activity to Tracfin. The annual volume of reports varied considerably from one financial institution to another and was not necessarily proportional to the number of accounts open or to the value of managed assets. The customer characteristics and in particular the different levels of sensitivity with regard to the risk of money laundering and terrorism financing which existed between the customer categories could not justify these differences in volume.** These differences seemed in part to reflect the failure to apply the obligations of identification and oversight identified previously. **One financial institution in particular did not require its chargés d'affaires to inform the Tracfin reporting officer of customer files for which entry into a business relationship had been refused, meaning that the Tracfin reports authority was not in a position to complete, if necessary, a suspicious activity report**. The ACP asked the financial institutions concerned to ensure the strict application of the report obligations and to inform it of the follow-up relating to the files which should, according to the on-site supervisory mission, have been the subject of a suspicious transactions report. In particular, the ACP asked them to list the customers for which an entry into a business relationship had been refused, indicate the reasons for refusal, define the conditions for information feedback to the Tracfin reporting officer, examine the cases of refusal to open an account during the years 2010 and 2011 and, where necessary, prepare a suspicious transaction report.

45. **The number of reports relating to tax fraud was limited. Automatic reports based on predetermined criteria** (e.g. the presence of a special-purpose fund, statement of professional activity, etc.) **were carried out by one financial institution.** The ACP required that any atypical transactions observed be subject to systematic analysis, possibly leading to a suspicious transaction report being sent to Tracfin.

4.2 Timeframe for suspicious transactions reporting

46. **While the general quality of the information contained in the suspicious transactions reports sent to Tracfin did not give rise to any particular remark, several failings were observed relating to the method of transmitting the reports, in particular report timeframes which can be very long (ranging from a few months to a few years)**. These timeframes would appear to be the result of the previously-mentioned failings concerning the application of due diligence obligations and, for one financial institution, the practice of combining all suspicious transaction reports on a single customer but relating to transactions staggered over time.

[27] Cf. joint ACP and Tracfin guidelines concerning suspicious activity reporting published on the AML/CFT page of the ACP website.

5 Asset freezing mechanism

The ACP expects the financial institutions to:

- *adopt operational mechanisms adapted to their activities enabling them to detect and block any transaction to the advantage of a person or entity whose funds, financial instruments and economic resources have been frozen;*
- *promptly update the lists of people and entities subject to asset-freezing measures;*
- *adjust the detection devices so that spelling variations are taken into account ("partial match" function);*
- *implement, if justified by the activities, an automated detection device on customers and transactions when entering into a business relationship and for the entire duration thereof;*
- *ensure that the units responsible for the compliance control system satisfactorily process and monitor the alerts generated by the detection devices in a limited time frame and that the French Treasury General Directorate can, when necessary, be alerted as quickly as possible.*

47. **Generally speaking, the financial institutions had implemented detection devices. Only one financial institution had not adopted such a device** and the ACP requested its setting-up.

48. **The mechanisms implemented by several financial institutions demonstrated failings, in particular with regard to**:
    - **the content of the procedures** (general terms of the asset freezing obligation without any operational adaptation):
    - **the list update timeframe** (up to twenty days);
    - **the detection tool settings** (e.g. restrictive spelling settings ("exact match" function), no automatic filtering when entering into a business relationship, long scanning intervals, etc.);
    - **the detection scope** (e.g. detection concerning solely the names mentioned in the orders of the French Minister for the Economy[28], failure to take these names into account in the detection device, customer databases not scanned during the business relationship, manual scanning of the customer databases only during the periodic review of customer files or several months after the publication of the lists, failure to screen transactions, manual screening of in-payments, etc.);
    - **the blockage of transactions** (no automatic blockage of transactions which triggered an alert).

49. **Furthermore, these failings had not been identified by all the financial institutions due to a lack of permanent second-level control** on the quality of the detection device for transactions to the profit of a person or entity whose funds, financial instruments and economic resources have been frozen, or due to inappropriate configuration settings on the device.

50. **In general, alerts were handled directly by operational staff within the units responsible for the compliance control system. This mechanism demonstrated occasional failings, for example with regard to the timeframe for handling alerts which could take up to one month**. The ACP asked the financial institutions concerned to implement a second-level control function specialized in terrorism financing fight.

51. The ACP asked the financial institutions concerned to swiftly implement a system for screening customer databases and transactions on a regular basis, as part of the fight against terrorism financing,

[28] Cf. article L. 562-1 and thereafter of the MFC.

and to block the transactions. The configuration settings of the detection device must be sufficiently flexible to accept different spellings of the same name.

6 Internal control

6.1 Permanent control system

The ACP expects the financial institutions to:

- *implement a permanent independent control system;*
- *provide the units responsible for permanent control with sufficient human resources (staff, staff qualifications) and technical resources (off-site monitoring tools, on-site visits) with regard to the activities and geographical presence of the financial institution;*
- *perform regular AML/CFT intelligence (legal developments, information communicated by the relevant national and international authorities, etc.);*
- *implement formal monitoring of the control activities.*

6.1.1 Independent permanent control

52. **In addition to the chargé d'affaires, the permanent control of the AML/CFT system was carried out by the units responsible for the compliance control system. Nevertheless, several financial institutions did not have staff within these units dedicated exclusively to control missions**. The ACP asked the financial institutions concerned to implement an independent control of the AML/CFT system, in particular with regard to the conditions for closing alerts.

6.1.2 Permanent control missions

53. **The missions entrusted to the units responsible for the compliance control system were extensive**, in particular covering all or part of the following aspects: drafting and validating procedures, regulatory intelligence, processing high-risk files when entering into a business relationship and for the duration thereof, monitoring external services and controlling intermediaries. **One financial institution had not implemented any regulatory intelligence in the field of AML/CFT**. The ACP asked this financial institution to implement a structured compliance control system including a regulatory intelligence service.

6.1.3 Oversight on internal control

54. **In several financial institutions, the control activities undertaken by the units responsible for the compliance control system demonstrated a number of failings linked to:**

- **the lack of formalisation of the control procedures**;
- **the exclusion of certain transactions from the scope of the transactions supervised** (e.g. the early repayment of credit, transactions performed by non-high-risk customers, transactions in foreign currencies, cash withdrawals of more than 150,000 euros, partial and early surrender of life insurance contracts, no control of anomalies detected by the control systems concerning information on the instructing party in the event of a funds transfer, etc.);

- **the absence of regular monitoring of the controls performed** (e.g. the absence of a file recording the controls carried out, imprecise knowledge of the exact number of files inspected, etc.).

The requests made by the ACP to the financial institutions concerned primarily referred to: updating and completing procedures related to internal control work specifying the operating mode; improving the means of disseminating these procedures; ensuring the exhaustiveness of the controls; mapping compliance control combined with a management chart allowing users to periodically check the execution of the controls, to see the main results and to monitor the progress of the allied action plans.

6.1.4 Control resources

55. **The resources allocated to the units responsible for the compliance control system were satisfactory in most financial institutions. Several supervisory reports nevertheless noted a lack of**:

– **human resources** (allocation of too few people in light of the total staff and the nature of the activity);

– **technical resources** (e.g. a lack of monitoring tools for customer files' reviews, lack of monitoring tools for customer files under surveillance, insufficient number of on-site visits – no on-site visits to subsidiaries or branches where the AML/CFT system demonstrates significant failings, on-site visits made a long time after the failings were detected–).

This prevented these units from completing their missions satisfactorily.

The ACP asked the financial institutions concerned to provide the units responsible for the compliance control system with sufficient qualified staff to enable them to complete all the tasks entrusted to them in a satisfactory manner.

6.2 Periodic control system

The ACP expects the financial institutions to:

– *adopt a periodic control system independent from the operational activities and, if relevant to the size of the financial institution, from the permanent control activities;*

– *perform controls of the permanent control and AML/CFT systems at appropriate intervals;*

– *implement a formal monitoring of these controls in order to check that the recommendations are correctly implemented within the timeframes indicated.*

6.2.1 Independent periodic control

56. **In general, the financial institutions had adopted an independent periodic control system, entrusted either to operatives of the financial institution or the parent company, or to an external agency. Three financial institutions had not implemented a periodic control system distinct from the permanent control system at the time of the on-site supervisory missions**. The ACP asked the financial institutions concerned to implement such a system as quickly as possible. **Furthermore, one of the financial institutions had not taken the money laundering and financing of terrorism risk classification into account when defining the periodic control schedule and was therefore unable to adapt the frequency of the controls to the level of risk.** The ACP asked that the periodic control schedule be communicated together with the explanation of the criteria adopted in defining the schedule, issuing a reminder that the periodic control schedule must cover a full cycle of investigations for as small a number of financial years as possible.

6.2.2 Periodic control of the AML/CFT system

57. **In general, the control of the AML/CFT systems was satisfactory. The AML/CFT systems were generally subject to regular** (18-24 months) **and in-depth controls** (analysis of the procedures and examination of a relevant sample of files). **Nevertheless, four financial institutions did not satisfy these requirements, either because they had never performed a periodic control of the AML/CFT systems or because they had not performed a periodic control in this field over the past three years, or because the controls performed lacked depth** (e.g. a limited sample of transactions controlled, etc.). The ACP asked the financial institutions concerned to incorporate AML/CFT into the scope of the periodic control system and to perform, in the near future, a periodic control mission to check the compliance of the customer files (e.g. process of updating the information on the identity and knowledge of the customers, justification of the source of assets, etc.) and of the transactions (e.g. transfers of funds).

6.2.3 Follow-up to the recommendations

58. **Several financial institutions did not correctly follow-up on the recommendations formulated within the periodic control framework.** The ACP asked them to formalise the results of the periodic control, the recommendations issued, the corrective actions identified, and the implementation thereof.

7 Staff training

The ACP expects the financial institutions to:

- *train their staff concerned by the field of AML/CFT both before they take up their posts and during the course of their work;*
- *provide operational training adapted to the activities of the financial institutions;*
- *perform formal follow-up to the training actions implemented.*

59. **Training the staff concerned by the field of AML/CFT fell under the aegis of the units responsible for the permanent control system in all the financial institutions. It was organised using IT media** (e-learning) **and/or materials provided directly by the financial institutions** (by individuals working within the units responsible for the compliance control system in collaboration with the chargé d'affaires or, in the case of one small-scale financial institution, members of the executive board) **or by external consulting agencies**. **In 2009 and 2010, the training actions focused on the presentation of the new AML/CFT obligations** introduced into French law in 2009. **They were intended both for staff members working in the commercial teams and executive or management personnel with, in some financial institutions, a strong adaptation of the training themes according to the activity and level of responsibility required.** In general, the training was intended for both new and existing staff members. The frequency and duration of the training courses varied considerably (e.g. ranging from several sessions a year to one session every two years for operatives already working in the field in question).

60. **In five financial institutions, the training actions proved to be insufficient with regard to the following elements**:

    - **the scope of the staff concerned** (e.g. the exclusion of some sites or activities, absence of training once operational, etc.);
    - **the training content** (e.g. too general – in particular in one financial institution which only provided its staff with the following three documents without any additional explanations or operational

adaptations: a note written by a professional association dated February 2009, Order No. 2009-104 dated 30 January 2009, and a Tracfin document concerning the types of tax fraud appended to the joint ACP and Tracfin guidelines concerning suspicious activity reporting – training courses focusing on only some of the AML/CFT obligations – presentation of the process for entering into a business relationship without any particular details concerning high-risk cases, new regulatory obligations not taken into account – training ill-adapted to the activities and levels of responsibility involved, etc.);

- **the frequency and duration of the training courses** (e.g. one single training course in two years, limited duration of the training – one hour only – on AML/CFT before taking up a post, etc.);
- **follow-up on the training actions** (e.g. the absence of a list of trained-up staff).

The ACP asked the financial institutions concerned to implement an operational training system, in particular to ensure that staff knowledge remained up to date and adapted to the nature of their activities and their responsibilities in the field of AML/CFT.

Conclusion

61. **The main expectations of the ACP in relation to the implementation of AML/CFT obligations in the field of wealth management focus on the following points**:
    - stronger governance and more specifically coherence of the group-wide internal control and AML/CFT systems;
    - the detection of high-risk customers and the introduction of appropriate due diligence mechanisms;
    - improved knowledge of the business relationship and the customer when entering into a relationship and for the duration thereof;
    - improved automated monitoring systems concerning the business relationships;
    - compliance with the Tracfin reporting obligations, in particular reducing the declaration timeframe;
    - improved detection devices with regard to the assets-freeze lists;
    - increased human and technical resources allocated to the units responsible for the compliance control system.

62. **These expectations are not specific to the activities of wealth management. They also apply to the other activities of the financial institutions under the supervision of the ACP,** such as retail banking, market operations, life insurance, etc.

63. In undertaking this appraisal, the ACP wanted to draw lessons from thematic on-site supervision of wealth management with regard to AML/CFT. Following this appraisal, and with a view to consolidating its explanatory and preventive action, **the ACP will revise the Banking Commission guidelines on wealth management in cooperation with the professionals on the Combating Money Laundering Advisory Board** attached to the College.

64. Furthermore, when revising the instructions concerning the money laundering questionnaires for financial institutions in the banking and insurance sectors, for which work has already been launched within the Combating Money Laundering Advisory Board, the ACP will specify its requests on feedback communication. These may notably focus on governance issues and the implementation of AML/CFT obligations within a group, involving oversight of compliance with these obligations by the head offices with regard to their branches and by parent companies with regard to their subsidiaries.

Enclosures:

Annex 1: Methodology of the on-site supervisory missions in the banking sector
Annex 2: Statistical data relating to the follow-up to the on-site supervisory missions

Annex 1

Methodology of the on-site supervisory missions in the banking sector[29]

1. **Whether it takes the form of a general investigation or a thematic mission concerning AML/CFT, the on-site supervision of a financial institution allows in-depth investigations to be carried out in order to ensure the effective implementation of compliant and relevant mechanisms resulting from Order No. 2009-104 of 30 January 2009.** Thanks to their complete and multi-format design, on-site supervisory missions allow investigators to collect detailed information and precise explanations while performing direct controls, thereby enabling the Inspectorate to obtain probative corroboration of the information received from the establishments by the off-site control divisions of the ACP through the regulatory submission of the annual statements, referred to as "BLANCHIMT statuses", as well as the annual report on internal control and risk monitoring, the periodic interviews and any on-site visits conducted.

2. In real terms, with regard to the activity of wealth management, just like any other business line, the methodology adopted by the on-site supervision teams on AML/CFT involves reviewing various sources of information and talking to the people responsible for the processes concerned in order to associate the compliance controls with the essential appraisal of the effectiveness and the coherence of the approach adopted by each establishment according to its exposure to the risks of money laundering. **This approach combines an analysis of written documentation, an examination of the transaction monitoring system, quality control of the data stored in the databases, and direct review of a sample of customer files and transactions:**

   - **Analysis of the written documentation relating to AML/CFT institution and implementation**, in particular the internal procedures; training media; summaries and permanent control of the activity of the AML/CFT function; related audit, control and advisory reports; the minutes of corporate bodies and operational committees' meetings dealing with AML/CFT, etc. Analysing this documentation gives knowledge on whether or not the AML/CFT policy is implemented entirely and forcefully in its different operational aspects, and whether the managers responsible and the governing corporate bodies are sufficiently involved.

   - **Examination of the characteristics of the transaction monitoring system**, serving to detect irregular transaction patterns from a standpoint of money laundering as well as politically exposed persons or parties included on the official lists of people subject to asset freezing. The design, functions and security of the IT tool dedicated to alerts is examined in order to assess the relevance of its configuration settings and the use made of it.

   - **Quality control of the data stored in the databases.** By consulting the customer, transaction and alerts databases, the Inspectorate is able to undertake computerised analyses using objective risk indicators (country of residence, classification of transactions by combining the type of transaction and the amount involved, etc.) intended to demonstrate the areas of sensitivity to the risk of money laundering, to compare them with the establishment's risk classification and to use them to create a sample of files to be examined. These analyses also make it possible to list information of unreliable quality with regard to identification and knowledge of the customers (name, address, activity, financial profile, etc.) and compliance with the European requirements concerning the information to be included on funds transfers.

[29] The on-site supervision methodology used by Anti-money laundering Mission for the insurance sector is similar.

- **Direct review of a sample of customer files and transactions.** These controls, established in accordance with the risk parameters identified previously, enable the Inspectorate to test the quality of the implementation of the regulatory due diligence with regard to entering into a relationship with the customer (proof of identity, for example), update knowledge of the customer (domiciliation, financial status of legal persons, etc.) and the transactions' monitoring (collection of supporting information on the transactions which triggered the alert, etc.). Furthermore, particular attention is paid to the quality of the suspicious transactions reporting process in terms of analysis relevance, reactivity, and the clarity of the explanations included in the descriptions provided.

3. **The AML/CFT supervisory missions focusing on financial institutions specialised in wealth management or in business lines within these financial institutions have naturally adapted the general methodological framework to the specific features of this activity** with particular emphasis, within the groups concerned, on the consolidated monitoring system; the keeping of customer files; raising portfolio manager awareness on AML/CFT requirements; the suitability of the alert thresholds; the handling of any conflicts of interest which might exist between asset consulting services and AML/CFT; and the implementation of sixteen criteria on the suspicion of tax fraud stipulated in Article D. 561-32-1 of the MFC.

Annex 2

Appraisal of the follow-up to the on-site supervisory missions

Scope of the study

This annex analyses the twelve follow-up letters issued by the ACP following the analysis of the on-site supervisory reports. The follow-up to the other supervisory reports is not included here.

Main requests formulated by the ACP

The ACP requests concerned the corrective measures to be integrated in the permanent and periodic control systems deployed by several financial institutions (20% of all observations). Remarks were also made with regard to governance (6.1%). The ACP calls on the financial institutions to swiftly implement systems that comply with the legal requirement in these fields.

With regard to the AML/CFT system, significant improvements are expected in terms of customer identification (5.2% of all failings observed), knowledge of customers (5.2%) and the revision of customer files (4.4%). Several requests also concerned the classification of the risks of money laundering and terrorism financing (4.4%) and the creation of business relation profiles, including the detection and oversight of politically exposed persons (9.6%, of which 5.2% concerned devices specifically applicable to politically exposed persons). The ACP draws the attention of the financial institutions to the quality of the business relations monitoring systems (11%) and the enhanced scrutiny of transactions (4.1%). The content of the AML/CFT procedures was also subject to numerous observations (8.1%).

Too often, the information exchanges relating to the organisation of due diligence within the groups for the purposes of AML/CFT as well as the existence and content of the suspicious transaction reports proved to be too limited (5%), and the suspicious transaction reporting mechanisms were sometimes incomplete (3.8%).

Finally, the ACP requested the financial institutions to adopt in a limited time frame asset freezing mechanisms in accordance with the regulations (3.5%).

Other points represent 9.6% of all the observations formulated.

Follow-up on the ACP's requests

Eight of the twelve follow-up letters gave rise to one or more replies sent to the ACP by the financial institutions concerned with a view to specifying the corrective measures adopted or considered in response to the requests formulated by the supervisor. The remaining four follow-up letters have not yet given rise to a reply given that the follow-up letters were only communicated to the financial institutions very recently. For 50% of the financial institutions, the replies were complemented by one or more interviews with the ACP as part of the *ad hoc* or annuals discussions with the financial institutions, in some cases at the very highest level (general management). On-site visits to some financial institutions are also envisaged during the course of 2012 as a complement to the written information concerning the effective implementation of the corrective measures requested.

In light of the latest replies received by the ACP, on average, 82% of the requests formulated by the supervisor have been implemented by the financial institutions. In two cases, all the ACP's requests appeared

to be fully satisfied. A third institution is expected to have implemented all the ACP's requests by the end of the first half of 2012. In three other financial institutions, the rates of progress concerning the ACP's requests are 85%, 80% and 70%, respectively. The last two financial institutions claim to have satisfied 68% and 50% of the ACP's requests, respectively.

In addition to the interviews with the financial institutions, the General Secretariat of the ACP sends further follow-up letters to ensure that matters left pending upon reception of the most recent letters are indeed implemented within the deadlines indicated, which take account of the scope of the corrective measures to be introduced.

All of these elements will be taken into consideration when defining on-site supervisory programmes for the coming years.