GP Banque

L'audit des prestations essentielles externalisées

2017

Cahier Professionnel du Groupe Banque

GP Banque

Ce document est le fruit d'une initiative des membres du Groupe Professionnel Banque de l'Ifaci. Les Groupes Professionnels de l'Ifaci ont pour objectif d'échanger sur des thématiques spécifiques d'un secteur d'activité, d'un domaine, ou d'une fonction. Ces échanges peuvent, le cas échéant, faire l'objet de publications destinées aux auditeurs et contrôleurs internes du secteur concerné. Ces publications sont réalisées sous la responsabilité des membres du Groupe de travail, et leur contenu technique n'engage ni les établissements auxquels appartiennent les participants de ce Groupe, ni l'Ifaci.

Ce « Cahier Professionnel » a été rédigé par les membres du Groupe Professionnel Banque de l'Ifaci assistés par le Cabinet Regulation Partners.

Groupe Professionnel Banque

SOMMAIRE

Préface 7

Introduction 10

Rappel du contexte 12

1- Définition, formes et obligations réglementaires de l'externalisation 14

1.1 Définitions 14
1.2 Types et exemples de prestations essentielles externalisées 17
1.3 Formes et périmètre de l'externalisation 20
1.4 Obligations réglementaires en matière d'externalisation 22
1.4.1 Obligations en matière d'externalisation d'activités au titre de l'arrêté du 3 novembre 2014 22
1.4.2 Obligations en matière de prestations de services d'investissement au titre du règlement général de l'AMF 26
1.4.3 Obligations en matière d'externalisation au titre de la Postion n°2013- P-01 de l'ACPR « relative à l'application du règlement CRBF n° 97-02[1] modifié à l'intermédiation en opérations de banque et en services de paiement » du 13 novembre 2013 30
1.4.4 Livre blanc Internet de la Commission Bancaire 31
1.4.5 Rapport annuel sur le contrôle interne en application des articles 258, 259, 262 à 264 et 266 de l'arrêté du 3 novembre 2014. 32
1.5 Enseignements tirés des sanctions récentes liées aux Prestations de Services Essentielles Externalisées (PSEE) 33

2. Réglementations étrangères 36

2.1 Les principes de base posés par le CEBS (Committee of European Banking Supervisors) 36
2.2 Les spécificités réglementaires par pays 38
2.2.1 Agrément ou décision préalable 38
2.2.2 Formalisation contractuelle 40
2.2.3 Droit de suite du superviseur 41
2.3 Contrôle du délégataire – identification de responsables dédiés 42
2.4 Plans d'urgence et de poursuite de l'activité (ex PCA) relatifs au activités externalisées 43

1. Le règlement CRBF 97-02 a été remplacé par l'arrêté du 3 novembre 2014.

3. Audit chez le délégant 46

3.1 Audit du processus d'approbation et de mise en place des prestations externalisées 46
3.1.1 Une organisation dédiée 48
3.1.2 Une grille d'analyse des risques 50
3.1.3 La vérification de l'agrément du délégataire 51
3.1.4 L'audit des contrats existants 51
3.1.5 La revue de la conformité des contrats 52
3.1.6 La vérification des bonnes conditions de conservation des contrats 55
3.1.7 La conformité de l'externalisation aux conditions définies 56
3.1.8 La pertinence et l'efficacité du contrôle permanent sur le processus d'approbation et le suivi des décisions 56
3.2 Audit du processus de supervision des prestations externalisées 56
3.2.1 La structure de gouvernance et le pilotage de la relation 56
3.2.2 Les outils et les moyens de suivi, le pilotage des opérations 58
3.2.3 Le rôle des acteurs opérationnels 62
3.2.4 La pertinence et l'efficacité du Contrôle Permanent sur le dispositif de supervision / pilotage des prestations externalisées 63
3.2.5 Vérification de l'évaluation des risques au sein de l'entreprise délégante par l'audit 64

4 Audit chez le délégataire 69

4.1 Préparation de la mission d'audit 72
4.1.1 Documentation à réunir chez le délégant 73
4.1.2 Documentation à obtenir du délégataire en début de mission 74
4.1.3 Cadrage de la mission d'audit 74
4.1.3.1 Contexte de réalisation de la mission d'audit 74
4.1.3.2 Modalités d'accès à l'information chez le délégataire 75
4.2 Audit de la conformité de la prestation 76
4.2.1 Auditabilité de la prestation 77
4.2.1.1 Documentation du processus de traitement 77
4.2.1.2 Ségrégation des univers clients par délégant 78
4.2.2 Reporting de production et contrôles chez le délégataire 78
4.2.3 Incidents de traitement 79
4.2.4 Situation financière 80
4.2.5 Plan d'urgence et de poursuite d'activité (ex PCA) 81
4.2.6 Obligations réglementaires du contrat 82
4.2.7 Obligations générales du contrat 83
4.3 Autres thèmes du programme d'audit chez le délégataire 84
4.3.1 Organisation constatée chez le délégataire 84
4.3.2 Système d'information du délégataire 84
4.3.3 Sécurité des systèmes d'information du délégataire 86
4.3.4 Dispositif de contrôle interne chez le délégataire 87

4.4 Rapport de la mission : débriefing et diffusion..... 88
4.4.1 Débriefing 88
4.4.2 Diffusion du rapport..... 88
4.5 Suite de la mission d'audit 89

5. IOBSP (Intermédiaires en Opérations de Banque et Services de Paiement 90

5.1 Une approche par les risques pour préparer les contrôles des mandataires PSEE 92
5.1.1 Mise en place d'indicateurs de risques par les établisse ments assujettis..... 92
5.1.2 Contrôle des mandats..... 93
5.1.2.1 Le mandat des mandataires exclusifs ou non exclusifs..... 93
5.1.2.2 Le suivi des Courtiers en Opérations de Banque et Services de Paiement (non PSEE) 95
5.2 Des contrôles sur pièces et/ou sur place 96
5.2.1 Les modalités de contrôle 96
5.2.1.1 Les contrôles sur pièces à distance..... 98
5.2.1.2 Les contrôles sur place..... 100
5.2.2 Le nécessaire déploiement des contrôles en interne par les IOBSP..... 101

Annexes 104

Annexe 1 : Clause à insérer dans les contrats portant sur les prestations de services essentielles ; 105

Annexe 2 : Références des réglementations étrangères et textes internationaux ; 107

Annexe 3 : Dispositions du RG AMF applicables aux SGP ;..... 109

Annexe 4 : Addendum « Audit des prestations informatiques » ;..... 113

PRÉFACE

Je suis heureux de préfacer ce Cahier professionnel du Groupe Banque de l'Ifaci, qui me paraît montrer tout l'intérêt d'une réglementation telle que l'arrêté du 3 novembre 2014, pour assurer la convergence des objectifs des banques et des superviseurs. Il est en effet un très bon exemple de la manière dont l'expérience concrète des pratiques du contrôle interne peut s'appuyer sur un texte réglementaire : c'est là précisément l'objectif poursuivi par le contrôle bancaire en France, qui a insisté sur le renforcement de ces pratiques professionnelles, depuis au moins le Règlement du comité de la réglementation bancaire et financière n°97-02 du 21 février 1997 relatif au contrôle interne.

Alors que beaucoup considéraient à l'origine que le contrôle interne, précisément parce qu'il devait trouver sa place dans chacune des organisations particulières des établissements bancaires, ne devait pas faire l'objet de réglementations prescriptives externes, la conviction partagée en France est qu'une accroche réglementaire est un moyen puissant de promouvoir et de faire converger les bonnes pratiques. La généralisation par ce moyen du schéma des trois lignes de défense (opérationnelle, contrôle permanent et périodique) est ainsi l'un des atouts qui à mon sens a concouru à la solidité de notre système bancaire avant et après la grande crise de 2008.

Cet atout doit bien entendu être mis au service des nouveaux défis qui surgissent des évolutions du métier bancaire. Or nul ne doute, vu les contraintes que la situation économique fait peser sur la rentabilité des banques, et l'impérieux besoin d'intégrer les bénéfices de l'innovation technologique, que le recours à l'externalisation ne soit appelé à se développer, en tant qu'un des moyens d'assurer le meilleur service au meilleur coût. Son contrôle, tout particulièrement par les audits des établissements, est donc un enjeu majeur des développements à venir pour assurer que ces

évolutions puissent se faire dans de bonnes conditions de sécurité pour les établissements et leur clientèle. Dans ce contexte, le caractère très précis et complet de ce document devrait apporter une aide très utile pour contribuer à assurer la convergence des pratiques vers les hauts standards professionnels que j'appelle de mes vœux.

Du point de vue du contrôleur externe, et dans le cadre des compétences nationales que l'ACPR continue à exercer directement, je voudrais souligner l'intérêt de l'accent mis sur le contrôle des différents intervenants dans la chaîne de distribution des produits. La diversité des cadres applicables aux différents types d'intermédiation ne doit pas en effet faire obstacle à l'efficacité des contrôles internes dont dépend la réputation des établissements, dans un contexte où le renforcement de ces règles de conduite tant en ce qui concerne la protection du consommateur que les dispositions plus régaliennes comme la lutte contre le financement du terrorisme, va intervenir prochainement.

Édouard Fernandez-Bollo
Secrétaire général de l'ACPR - Autorité de Contrôle Prudentiel et de Résolution

PARTICIPANTS AU GROUPE DE RECHERCHE

GROUPE BANQUE

Jean-François Couturier	**Responsable adjoint de l'Inspection Générale** *BNP Paribas*
Christiane Legat	**Directrice de l'Inspection Générale et de l'Audit Interne |** *Crédit Immobilier de France*
Marianne Louradour	**Directrice de l'Audit du Groupe** *Caisse des dépôts*
Christian Mascle	I**nspecteur Principal Direction Inspection Générale** *Groupe BPCE*
Emmanuel Rousseau	**Responsable de l'Audit Interne du Groupe** *Edmond de Rothschild*
Anne-Marie Schricke	**Responsable relations régulateurs à l'Inspection Générale |** *Crédit Agricole CIB*
Beatrice Vedrenne-Robson	**Country Lead Barclays Internal Audit** *Barclays*
Marie-Agnès Nicolet	**Présidente** *Regulation Partners*
Pierre Caillieret	**Inspecteur** *BPCE*
Catherine Foillard	**Inspection Générale** *BNP Paribas*
Jean-Philippe Leyrat	**Auditeur** *Caisse des dépôts et consignations*
Cindy Rubal	**Consultante Manager** *Regulation Partners*

INTRODUCTION

Au cours de ces dernières années, le développement de l'activité des établissements financiers dans de multiples directions et le souci d'en améliorer constamment les performances financières ont contribué à accélérer le recours à l'externalisation de tâches nombreuses et variées.

Cette évolution, source d'opportunités mais également de risques, a conduit les établissements financiers à renforcer leurs modalités de surveillance des opérations concernées.

Les dispositions prises par la plupart des régulateurs, dans un certain nombre de textes récents, constituent de surcroît une incitation claire à mieux définir et structurer l'environnement de contrôle et, plus précisément, les interventions de l'audit interne.

Après un bref rappel des évolutions constatées, ce cahier développe les trois points suivants :

1. Définition et formes de l'externalisation, en s'appuyant notamment sur les textes des principaux régulateurs ;
2. Audit de l'externalisation chez le délégant, élément indispensable à la sécurisation de l'environnement de contrôle ;
3. Audit chez le délégataire des activités externalisées, son périmètre et ses modalités spécifiques.

Cet ouvrage comporte également un focus particulier sur les IOBSP considérés comme des PSEE lorsqu'ils sont mandataires des établissements.

L'ambition de ce document est de proposer un cadre d'intervention au contrôle périodique du secteur bancaire et financier mais également à l'ensemble des auditeurs internes qui peuvent être amenés à réaliser une mission sur ce sujet.

Il peut également être utilement consulté par les managers et les acteurs des fonctions de contrôle de l'organisation.

Ce document propose des orientations en termes d'organisation des entreprises, de conduite et de contenu des missions d'audit. Ces orientations sont à interpréter comme des bonnes pratiques que chacun devra adapter en fonction de sa propre situation.

RAPPEL DU CONTEXTE

Dans le paysage bancaire, le recours à l'externalisation n'est plus une exception même si le développement de ce mode de production a été très progressif et demeure toujours en retrait par rapport aux pratiques des entreprises non financières. Le processus trouve son origine dans les années 1970, les établissements assujettis procédant alors progressivement à l'externalisation de leurs activités administratives (imprimerie et stockage de données en particulier).

Au cours des deux décennies suivantes, l'externalisation s'est développée à la faveur des stratégies de recentrage sur le cœur de métier mises en place par les principaux établissements bancaires. Ces logiques de spécialisation, menées dans un but d'efficience, se sont traduites notamment par la cession des activités non stratégiques et/ou par le recours accru à l'externalisation pour les activités dites périphériques.

Aujourd'hui, l'externalisation est utilisée de façon croissante pour des opérations telles que le développement, la maintenance et l'exploitation de logiciels, les back-office, les centres d'appels, ainsi que la plupart des processus de paiement et de transaction.

Pourquoi a-t-on recours à l'externalisation ?

Les principales raisons qui poussent les établissements bancaires à externaliser leurs activités sont variées :

> l'optimisation des investissements et le renforcement de l'efficacité opérationnelle des activités jugées prioritaires ;

> le maintien d'une expertise, son actualisation et l'accès aux nouvelles technologies ;

> l'amélioration de la qualité de service ;

> la flexibilité des moyens de production et organisationnels ; l'externalisation étant alors un moyen de lisser les pointes d'activité et de préserver l'emploi.

Toutefois, le recours à l'externalisation présente un certain nombre de risques qu'il convient de citer :

> la perte de connaissances et de compétences en interne ;

> la dépendance vis-à-vis des délégataires externes ;

> la dégradation de la qualité de service ou la moindre adaptation aux évolutions des besoins de la clientèle ;

> la sous-estimation des coûts induits ou des coûts cachés de l'externalisation ou encore la perte de l'avantage de coûts quand un même délégataire fournit plusieurs services ou détient une position dominante sur le marché (rapport de force) ;

> la perte de contrôle des activités externalisées (chaîne d'externalisation);

> l'augmentation de l'exposition au risque opérationnel.

Dans son bulletin de novembre 2004, la Commission bancaire indiquait que : « les risques de perte de contrôle et ceux liés à l'accroissement des risques opérationnels étaient des risques prioritaires » et soulignait « que l'externalisation était porteuse d'un autre risque important, à savoir les difficultés accrues pour le superviseur d'accéder à l'information pertinente à des fins de contrôle de l'activité des établissements. » Face à l'ensemble de ces risques, le dispositif de supervision français devait rapidement évoluer. C'est chose faite puisque la réglementation sur le contrôle interne intègre depuis une dizaine d'années des exigences spécifiques pour les établissements qui externalisent des activités proches de leur cœur de métier ou susceptibles d'avoir un impact sur leur clientèle ou présentant des risques pour l'organisation.

1| DEFINITION, FORMES ET OBLIGATIONS RÉGLEMENTAIRES DE L'EXTERNALISATION

1.1 Définitions

Le Petit Robert indique que le mot « externaliser » est un verbe apparu dans la langue française en 1989 sur le modèle du terme anglais « to externalize » et en donne la définition suivante : « confier à une entreprise extérieure une tâche, une activité secondaire».

Le dictionnaire Hachette encyclopédique mentionne le transfert « à l'extérieur de certaines activités de l'entreprise » tandis que le Larousse illustré propose la définition suivante : « pour une entreprise, confier une partie de sa production ou de ses activités (comptable, gardiennage, etc.) à des partenaires extérieurs ».

Alors que la notion de sous-traitance est définie par la Loi n°75-1334 du 31 décembre 1975[2] « opération par laquelle une entreprise confie par un sous-traité et sous sa responsabilité (…) à une autre personne appelée sous-traitant, l'exécution de toute ou partie du contrat d'entreprise ou du marché public conclu avec le maître d'ouvrage », aucune loi ne définit l'externalisation.

> Pour les établissements assujettis à l'arrêté du 3 novembre 2014 (notamment établissements de crédit, entreprises d'investissement, sociétés de financement, établissement de paiement, établissements de monnaie électronique…), la définition des activités externalisées est celle fournie par l'article 10 q de l'arrêté du 3 novembre 2014 : « les activités pour lesquelles l'entreprise assujettie confie à un tiers, de manière durable et à titre habituel, la réalisation de prestations de services ou d'autres tâches opérationnelles essentielles ou importante par sous-traitance au sens de la loi no 75-1334 du 31 décembre 1975, par démarchage au sens des articles L. 341-1 et L. 341-4 du code monétaire et financier susvisé, par le recours à des personnes en vue de distribuer de la monnaie électronique pour le compte de l'entreprise assujettie au sens des articles L. 525-8 et suivants du même code, par le recours aux agents liés définis aux articles L. 545-1 et suivants du même code, par le recours aux agents définis aux articles L. 523-1 et suivants du même code ou par toute autre forme ».

2.Loi n°75-1334 relative à la sous-traitance du 31 décembre 1975 publiée au Journal Officiel du 3 janvier 1976, version consolidée au Journal Officiel du 27 juillet 2005.

Les prestations de services ou autres tâches opérationnelles essentielles ou importantes, définies au sens de l'article 10 r, s'entendent par :

> les opérations de banque au sens de l'article L. 311-1 du code monétaire et financier susvisé, l'émission et la gestion de monnaie électronique au sens de l'article L. 315-1 du même code, les services de paiement au sens du II de l'article L. 314-1 du même code et les services d'investissement au sens de l'article L. 321-1 du même code, pour lesquels l'entreprise assujettie a été agréée ;

> les opérations connexes mentionnées aux paragraphes 1, 2, 3, 7 et 8 du I de l'article L. 311-2, aux paragraphes 1, 2, 5 et 6 de l'article L. 321-2 et aux articles L. 522-2 et L. 526-2 du code monétaire et financier susvisé ;

> les prestations participant directement à l'exécution des opérations ou des services mentionnés aux deux premiers tirets ci-dessus ;

ou toute prestation de services lorsqu'une anomalie ou une défaillance dans son exercice est susceptible de nuire sérieusement à la capacité de l'entreprise assujettie de se conformer en permanence aux conditions et obligations de son agrément et à celles relatives à l'exercice de son activité, à ses performances financières ou à la continuité de ses services et activités.

Cependant, à la lecture de ces différents articles, les notions d'externalisation et de prestations de services essentielles peuvent encore être précisées pour bon nombre d'établissements financiers de la place.

D'ailleurs, Danièle Nouy, lorsqu'elle était Secrétaire Générale de la Commission Bancaire indiquait[3]: « ...La définition de l'externalisation est à la fois extensive et sélective. Extensive, parce qu'elle veut couvrir l'ensemble des situations et des activités, quelle que soit la forme juridique retenue par les établissements qui y font appel : sous-traitance, délégation... Sélective, avec trois niveaux de sélectivité.

- *Le premier niveau est celui des prestations essentielles, celles qui requièrent un agrément, un agrément de banque ou d'entreprise d'investissement. Dans ce cas-là, on peut externaliser, mais uniquement au profit d'un*

3.Propos tenus par Danièle Nouy lors de la troisième rencontre avec la Commission Bancaire organisée par l'Ifaci le 23/11/05

établissement qui a lui-même un agrément. Evidemment, cela implique un certain nombre de diligences supplémentaires. La possibilité d'externaliser est limitée.

- Le deuxième niveau d'externalisation possible concerne les autres prestations essentielles. Ce sont celles qui participent non pas à la décision de traiter une opération qui requiert un agrément, mais à l'exécution matérielle d'une opération qui demanderait un agrément.
- *Le troisième niveau de prestation, ne requiert pas forcément un contrôle interne renforcé des diligences particulières. »*

En mars 2011, l'ACP (aujourd'hui ACPR-Autorité de Contrôle Prudentiel et de Résolution) s'est également exprimée sur la notion d'externalisation, notamment pour la distinguer de la tierce introduction aux termes des « Lignes directrices relatives à la tierce introduction » en matière de lutte contre le blanchiment et contre le financement du terrorisme (LCB-FT), « quand bien même le tiers serait lui-même un assujetti en application de l'article L.561-2 du CMF ».

En effet, en matière d'externalisation, le prestataire agit au nom et pour le compte de l'organisme financier. La mise en œuvre de la prestation par le prestataire « est nécessairement soumise aux procédures et au dispositif de contrôle interne » de l'organisme financier qui a recours à l'externalisation[4]. En revanche, dans le cas de la tierce introduction, le tiers introducteur applique ses propres procédures afin de se conformer à ses obligations de vigilance à l'égard du client car il est considéré comme réalisant des diligences équivalentes.

Les lignes directrices rappellent que cette tierce introduction est très limitée

« Les obligations de vigilance dont la mise en œuvre peut être confiée à un tiers introducteur sont celles prévues :

– au 1er alinéa de l'article L. 561-5 du CMF, à savoir l'identification et la vérification de l'identité du client, et, le cas échéant, du bénéficiaire effectif de la relation d'affaires ; et

– au 1er alinéa de l'article L. 561-6 du même code, à savoir la connaissance de l'objet et de la nature de la relation d'affaires.

4. 1, b, point n°3 des lignes directrices de l'ACP relatives à la tierce introduction.

Il ne peut être recouru à la tierce introduction pour la mise en œuvre des obligations prévues au 2e alinéa de l'article L. 561-6 du CMF. »

Les contrôles à réaliser vis-à-vis d'un tiers introducteur ne sont donc pas les mêmes que vis-à-vis d'un PSEE.

Il est à noter que l'établissement financier qui a recours à un prestataire (externalisation) de même que celui qui fait appel à un tiers introducteur demeurent responsables du respect de leurs propres obligations de vigilance en matière de LCB-FT.

La définition réglementaire laisse une réelle marge d'interprétation aux établissements, aussi le groupe de travail a-t-il entrepris de clarifier la notion de prestations essentielles et de les classer dans le but de mieux cerner le périmètre à auditer.

1.2 Types et exemples de prestations essentielles externalisées

Le tableau[5] ci-après propose une liste, non exhaustive, des types de prestations externalisées que le groupe de place a identifiés comme étant visés par les dispositions de l'arrêté du 3 novembre 2014.

Type de prestation de services essentielles	Libellé de la prestation externalisée
*Les opérations de banque au sens de l'article **L. 311-1** du code monétaire et financier susvisé, l'émission et la gestion de monnaie électronique au sens de l'article L. 315-1 du même code, les services de paiement au sens du II de l'article L. 314-1 du même code et les services d'investissement au sens de l'article **L. 321-1** du même code, pour lesquels l'entreprise assujettie a été agréée*	> Ouverture de compte, octroi de crédit ; > Fabrication et personnalisation de cartes bancaires ; > Fabrication/personnalisation, acheminement de chéquiers ; > Traitement des chèques et de monnaie électronique ; > Gestion de la caisse centrale (espèces) ; > Gestion des automates bancaires (DAB, GAB) ; > Gestion relation clients (« call centers ») ; > Prestations de banque à distance ;

5. Tableau établi par un groupe de place composé des établissements suivants : HSBC, Banques Populaires, Calyon, Société Générale et BNP Paribas et enrichi par le Groupe de travail Banque de l'Ifaci.

*Les opérations connexes mentionnées aux paragraphes 1, 2, 3, 7 et 8 du I de l'article **L. 311-2**, aux paragraphes 1, 2, 5 et 6 de l'article **L. 321-2** du code monétaire et financier susvisé et aux articles L. 522-2 et L. 526-2 du code monétaire et financier ;*	> Délivrance de devises ;
Les prestations participant directement à l'exécution des opérations ou des services mentionnés aux deux premiers tirets ci-dessus ;	> Centre d'opposition sur moyens de paiement ; > Terminaux de paiement par carte (maintenance uniquement); > Gestion relation clients (centres d'appels) ; > Exploitation informatique (paramétrage et supervision métiers des traitements) ; > Back office, post-marché ; > Éditique (relevés de comptes etc…) ; > Conservation de titres vis à viss des teneurs de comptes conservateurs (Cf. 1.4.2) ; > Sous-conservation de titres chez des dépositaires étrangers notamment ;
Les autres opérations connexes mentionnées aux articles L. 311-2 et L. 321-2 du code monétaire et financier susvisé ;	> Conseil et assistance en matière de gestion de patrimoine (produits d'épargne bancaire et produits d'épargne financière) ; > Conseil et assistance en matière de gestion financière, ingénierie ; > Opérations de location simple de biens mobiliers ou immobiliers ; > Location de coffres-forts ;

6. Commission des sanctions ACP, 27/11/2012, BANK TEJARAT PARIS, Grief 6.

Toute prestation de services lorsqu'une anomalie ou une défaillance dans son exercice est susceptible de nuire sérieusement à la capacité de l'entreprise assujettie de se conformer en permanence aux conditions et obligations de son agrément et à celles relatives à l'exercice de son activité, à ses performances financières ou à la continuité de ses services et activités,	> Moyens relatifs au plan de continuité des activités ; > Infogérance et exploitation informatique ; >Traitements comptables pour compte propre et reportings réglementaires ; > Stockage et archivage ; > Recouvrement de créances ; >Transport de valeurs autres que des fonds ;
LCB-FT1 *(Sanction ACP 2012 articles 237 à 240 de l'arrêté du 3 novembre 2014)*	> Détection des opérations concernées par le gel des avoirs ou détection automatisée d'alertes au sens de la LCB/FT ; > Paramétrage des outils d'alerte et de filtrage ;
Contrôle interne[7] *(Sanction ACP 2012, articles 237 à 240 de l'arrêté du 3 novembre 2014)*	> Contrôle permanent ; > Contrôle périodique ;

Certaines de ces activités peuvent être réalisées par démarchage. Par conséquent, cette modalité d'exercice de ladite activité rentre bien dans le cadre de la définition des prestations essentielles externalisées. En outre, ces distinctions par type de prestations fournies doivent permettre d'identifier les prestations qui concourent de façon substantielle à la décision engageant l'entreprise vis-à-vis de sa clientèle à conclure une opération. (voir 1.4.1).

Afin de permettre à chaque établissement de définir le champ de ses prestations essentielles, le Groupe de travail a également décidé de lister un certain nombre de prestations :

- qui peuvent être incluses dans les prestations essentielles uniquement si leur profil de risque « présente un effet significatif sur la maîtrise des risques de l'établissement » : fabrication des moyens des cartes bancaires et chéquiers,

7. Commission des sanctions ACP, 27/11/2012, BANK TEJARAT PARIS, Grief 28.

transport de fonds, développements informatiques durables liés aux applications bancaires ou réglementaires, sécurité et gardiennage par exemple ;
- qui ne sont pas visées par l'arrêté du 3 novembre 2014 : service de paie, maintenance du matériel bureautique classique, traduction d'un contrat, par exemple.

Par ailleurs, dans l'esprit même de la règlementation, certaines autres prestations peuvent être importantes ou stratégiques pour l'établissement sans pour autant relever de la définition réglementaire des prestations de services essentielles externalisées. Dès lors, l'établissement doit s'assurer que les risques liés à ces prestations sont gérés, suivis et contrôlés dans le cadre des risques opérationnels. A ce titre, il est rappelé que l'établissement demeure responsable de l'activité externalisée.
Prestations n'entrant pas dans le champ de l'externalisation dès lors qu'elles n'ont pas vocation à être exercées directement par l'établissement et donc ne sont pas susceptibles d'être confiées à un tiers :

- Information financière (ex. Reuters, Bloomberg…) ;
- Fournisseurs Energie, Réseaux (ERDF, France TELECOM ORANGE…) ;
- Systèmes de paiement de place : Swift, TARGET 2, CORE, Europay ;
- Système de négociation, compensation et règlement titres (Euroclear, Clearnet, Euronext, …).

1.3 Formes et périmètre de l'externalisation

Selon une étude du BSC (le Comité de Surveillance Bancaire) de la Banque Centrale Européenne, les banques européennes utilisent différents modèles stratégiques pour leurs politiques d'externalisation, à savoir :

- des modèles intra-groupes sous la forme de filiales ;
- des entités non financières domestiques ou européennes ou situées dans un autre pays ;
- des joints ventures et GIE ;
- des alliances entre banques.

Selon l'activité considérée et l'objectif recherché, différentes approches sont possibles afin de tirer pleinement profit des caractéristiques propres à chaque modèle stratégique.

Ainsi, les établissements qui privilégient le contrôle direct sur l'activité ou la confidentialité des données et disposant d'une taille suffisante choisiront davantage le modèle intra-groupe (filialisation). A l'inverse, les banques qui recherchent en priorité la réduction massive des coûts auront plutôt recours à un délégataire extérieur localisé dans un pays en voie de développement.

Quelle que soit la forme d'externalisation retenue, les principes de surveillance de ces activités s'appliquent.

> Distinction entre les notions de contrôle exclusif et contrôle conjoint

Les notions de contrôle exclusif ou conjoint pour l'application de la surveillance consolidée au sens de l'article 6 de l'arrêté du 3 novembre 2014 sont définies par le règlement n°99-07 du comité de la réglementation comptable (§ 1002 et 1003) « sauf pour les établissements assujettis soumis aux normes IFRS pour lesquels ces notions sont définies dans les normes IFRS adoptées » (cf. voir annexe 6 « Définition du périmètre de contrôle interne dans le cadre de la surveillance consolidée »).

Pour les établissements soumis aux normes IFRS, les notions de contrôle exclusif ou conjoint peuvent être définies comme suit :

- Le contrôle exclusif est présumé exister lorsque l'établissement détient directement ou indirectement par l'intermédiaire de filiales, plus de la moitié des droits de vote d'une entité, sauf si dans des circonstances exceptionnelles, il peut être clairement démontré que cette détention ne permet pas le contrôle. Le contrôle exclusif existe également lorsque l'établissement, détenant la moitié ou moins des droits de vote d'une entité dispose de la majorité des pouvoirs au sein des organes de direction ;
- Le contrôle conjoint s'exerce dans les co-entités au titre desquelles deux co-entrepreneurs ou plus sont liés par un apport contractuel établissant un contrôle conjoint.

> Application lorsque le délégataire externe fait partie du groupe de l'entreprise assujettie

Les dispositions réglementaires s'appliquent également dans le cas où le délégataire externe fait partie du groupe de l'entreprise assujettie. En effet, l'article 235 précise : « lorsque l'entreprise assujettie recourt à un prestataire externe, auquel sont appliquées les dispositions de l'article 6a du présent arrêté, les dispositions prévues à l'article 234 sont intégrées dans le dispositif de contrôle interne sur base consolidée ».

1.4 Obligations réglementaires en matière d'externalisation

Bien que la notion d'externalisation ne soit pas définie par la loi, les obligations des établissements bancaires en matière d'externalisation sont, en revanche, encadrées par différents textes.

1.4.1 Obligations en matière d'externalisation d'activités au titre de l'arrêté du 3 novembre 2014

Issues de l'article 1er de l'arrêté du 31 mars 2005, ces obligations figurent respectivement aux articles 231 à 232, 234 à 236, 237 à 240, 253 c) et 275 de l'arrêté du 3 novembre 2014. Elles trouvent leur inspiration dans les onze principes relatifs à l'outsourcing énoncés, en avril 2004, par le Comité Européen des Contrôleurs Bancaire (CEBS). Ces principes sont désormais inclus dans des « guidelines on outsourcing », publiés par le CEBS le 14 décembre 2006[8].

> Obligations générales

Ces obligations sont au nombre de trois :

- Les entreprises assujetties doivent, tout d'abord s'assurer (art. 231) que *« toute prestation qui concourt de façon substantielle à la décision engageant l'entreprise vis-à-vis de sa clientèle à conclure une opération mentionnée aux trois premiers tirets de l'article 10r n'est externalisée qu'auprès de personnes agréées ou habilitées selon les normes de leur pays à exercer de*

8. http://www.c-ebs.org/GL02OutsourcingGuidelines.pdf.pdf.

- *telles activités ».* L'expression « *selon les normes de leur pays* » permet de penser que le délégataire étranger doit être habilité, au regard de la réglementation qui lui est applicable, à effectuer de telles opérations. Un assujetti pourra externaliser certaines opérations couvertes en France par un agrément ACPR auprès de délégataires étrangers n'ayant aucun statut particulier dès lors que les opérations en question ne requièrent pas, dans le pays où elles sont exercées, par le délégataire considéré, d'habilitation ou d'agrément spécifique (ex : cas des opérations de crédit-bail ou d'affacturage qui ne nécessitent pas d'agrément spécifique dans certains pays européens.)
- Les entreprises assujetties doivent en deuxième lieu (art. 234, a) s'assurer que « *leur système de contrôle au sens de l'article 11 inclut leurs activités externalisées* ». En clair, il faudra qu'elles intègrent, dans « *leur système de contrôle des opérations et procédures internes* » l'externalisation d'activités.
- Les entreprises assujetties doivent, enfin (art. 234, b) se doter « *de dispositifs de contrôle au sens de l'article 12 de leurs activités externalisées* ». Cela signifie que les dispositifs de contrôle permanent et périodique mis en place devront prendre en compte les activités externalisées visées à l'article 10r. Les entreprises assujetties doivent s'assurer que le contrôle permanent, le contrôle périodique et le contrôle de la conformité incluent ces activités dans leur périmètre. La fréquence et la profondeur des contrôles seront fondées notamment sur les résultats et la qualité du contrôle interne.

> Obligations particulières pesant sur les entreprises assujetties et les délégataires en cas d'externalisation de prestations de services essentielles

L'article 237 dispose, en préambule, que « *les entreprises assujetties qui externalisent des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes à leurs activités au sens du q) et r) de l'article 10, demeurent pleinement responsables du respect de toutes les obligations qui leur incombent*».

L'article 238 prévoit, que les entreprises assujetties doivent :

- Formaliser la relation avec les délégataires. L'article 238 a) dispose, en effet, que l'externalisation d'activité au sens de l'arrêté du 3 novembre 2014 doit donner lieu à un contrat écrit entre le prestataire externe et l'entreprise assujettie.
- Se doter d'une procédure d'habilitation et de contrôle des délégataires choisis. L'article 238 b) indique très précisément que l'externalisation d'activité au sens de l'arrêté du 3 novembre 2014 doit « *s'inscrire dans le cadre d'une politique formalisée de contrôle des prestataires externes définie par l'entreprise assujettie* ».

L'article 239 prévoit que les entreprises assujetties doivent s'assurer, dans leurs relations avec leurs prestataires externes, que ces derniers :

1. s'engagent sur un niveau de qualité répondant à un fonctionnement normal du service et qu'ils ont bien mis en place des mécanismes de secours appropriés (en cas de difficulté grave affectant la continuité du service) ou, à défaut, prévoir dans leur propre plan de continuité d'activité le risque de défaillance du délégataire ;
2. ne peuvent imposer une modification substantielle de la prestation qu'ils assurent sans l'accord préalable de l'entreprise assujettie ;
3. se conforment aux procédures définies par l'entreprise assujettie concernant l'organisation et la mise en œuvre du contrôle des services qu'ils fournissent ;
4. leur permettent, chaque fois que cela est nécessaire, l'accès, le cas échéant sur place, à toute information sur les services mis à leur disposition, dans le respect des réglementations relatives à la communication d'informations. C'est-à-dire que l'entreprise française assujettie qui externalise des activités auprès d'un prestataire externe devra pouvoir procéder à des contrôles chez ce prestataire. Dès lors, les contrats passés avec les prestataires devront, comporter une « clause d'audit » ;

5. leur rendent compte de façon régulière de la manière dont est exercée l'activité externalisée ainsi que leur situation financière ;
6. acceptent que l'ACPR, ou toute autre autorité étrangère équivalente au sens des articles L 632-7, L. 632-12 et L. 632-13 du Code monétaire et financier (il s'agit des autorités compétentes des autres Etats partie à l'Espace Économique Européen et de celles, hors EEE, avec lesquelles l'ACPR a conclu un accord bilatéral de coopération), ait accès aux informations sur les activités externalisées nécessaires à l'exercice de sa mission, y compris sur place (art 239 f). Les contrats conclus avec les prestataires devront, en conséquence, comporter une clause permettant l'accès de l'ACPR (ou de ses homologues) chez les intéressés lorsque les besoins de l'enquête le justifieront. Il s'agit là de l'instauration d'un « droit de suite » contractuel au profit de l'ACPR qui ne devrait, selon toute vraisemblance, être utilisé que très exceptionnellement par cette dernière lorsqu'elle n'aura pas réussi à obtenir de l'entreprise assujettie toutes les assurances voulues.

Ces dispositions particulières ont donné lieu à la proposition, par le Groupe de place précédemment cité, d'une clause à insérer dans les contrats (voir annexe 1 « Clause à insérer dans les contrats portant sur les prestations de services essentielles »).

> Obligations de reporting à l'organe de surveillance concernant l'externalisation

Conformément aux dispositions du nouvel article 253 alinéa 1, c) de l'arrêté du 3 novembre 2014, les dirigeants effectifs de l'entreprise assujettie sont tenus d'informer régulièrement, au moins une fois par an, l'organe de surveillance (le Conseil d'administration ou le Conseil de surveillance dans une société anonyme) et, le cas échéant, le comité des risques, « *des mesures prises pour assurer le contrôle des activités externalisées et des risques éventuels qui en résultent pour l'entreprise assujettie* », étant précisé que : « l*es prestations de services*

ou autres tâches opérationnelles essentielles ou importantes relevant des trois premiers tirets de l'article 10 r) doivent être distinguées dans cette information ». On constate donc qu'une distinction est opérée entre les opérations de banque et services d'investissement, celles qui leur sont étroitement liées et les autres, pour lesquelles le degré d'exigence en matière de reporting est moindre. Cette information spécifique sur les activités externalisées donnée à l'organe de surveillance devra, par ailleurs, figurer dans le rapport annuel sur la mesure et la surveillance des risques prévu à l'article 262.

L'article 238 de l'arrêté du 3 novembre 2014 exige que l'externalisation d'activités « *s'inscrive dans le cadre d'une politique formalisée de contrôle des prestataires externes* ». La question se pose de ce que doit contenir une telle politique.

1.4.2 Obligations en matière de prestations de services d'investissement au titre du règlement général de l'AMF

Les prestations de services d'investissement sont considérées comme des prestations de services essentielles au sens de l'arrêté du 3 novembre 2014. Toutefois, certaines dispositions du règlement général de l'AMF définissent des diligences particulières en matière de contrôle concernant ces prestations. Au demeurant, l'articulation entre les deux dispositifs réglementaires est clairement assurée, l'article 19 de l'arrêté du 3 novembre 2014 prévoyant, en particulier, que les fonctions relatives au contrôle permanent peuvent être confiées aux personnes en charge des contrôles prévus par le règlement général de l'AMF.

Concernant la Tenue de Compte de Conservation (TCC), l'Article 322-35 renvoie à l'article 313-75 et prévoit **d'évaluer les moyens et procédures des délégataires à qui le TCC a confié sa conservation.** « *Quand il recourt à un tiers, en application de l'article 322-33, et hormis les cas où il conserve les avoirs correspondant aux titres de ses clients dans un ou plusieurs comptes ouverts auprès d'un dépositaire central ou d'un émetteur,* **le teneur de compte-conservateur applique les dispositions des articles 313-14 à 313-16 et 313-72 à 313-75.**

La responsabilité du teneur de compte-conservateur vis-à-vis du titulaire du compte-titres n'est pas affectée par le fait qu'il recourt à un tiers mentionné à

l'article 322-33. Toutefois, lorsqu'un teneur de compte-conservateur conserve pour le compte d'un client professionnel des titres financiers émis sur le fondement d'un droit étranger, il peut convenir d'une clause totalement ou partiellement exonératoire de sa responsabilité avec ce client professionnel. »

« Article 313-14 : Lorsqu'il recourt à un tiers pour détenir les instruments financiers de ses clients, le prestataire de services d'investissement agit avec toute la compétence, le soin et la diligence requis dans la sélection, la désignation et l'examen périodique de ce tiers et des dispositions prises par celui-ci concernant la détention de ces instruments financiers.

Le prestataire de services d'investissement prend en compte l'expertise et la réputation dont jouit le tiers concerné sur le marché, ainsi que toute exigence légale ou réglementaire ou pratique de marché liée à la détention de ces instruments financiers de nature à affecter négativement les droits des clients. »

« Article 313-15 : Lorsque, pour la détention des instruments financiers de ses clients, le prestataire de services d'investissement recourt à un tiers situé dans un autre État qui dispose d'une réglementation et d'une surveillance spécifiques en matière de détention d'instruments financiers pour le compte d'un client, il choisit ce tiers parmi ceux soumis à cette réglementation et à cette surveillance spécifiques et agit conformément aux dispositions de l'article 313-14. »

« Article 313-16 : Pour la détention des instruments financiers de ses clients, le prestataire de services d'investissement ne peut recourir à un tiers situé dans un État non partie à l'accord sur l'Espace économique européen dans lequel aucune réglementation ne régit la détention d'instruments financiers pour le compte d'une autre personne que si l'une des conditions suivantes est remplie :

1° La nature des instruments financiers ou des services d'investissement liés à ces instruments financiers exige de les détenir auprès d'un tiers dans cet État non partie à l'accord sur l'Espace économique européen ;

2° Si la détention des instruments financiers est assurée pour le compte d'un client professionnel, ce client a demandé par écrit au prestataire de services d'investissement qu'ils soient détenus par un tiers dans cet État non partie à l'accord sur l'Espace économique européen. »

Les sociétés de gestion (dont certaines sont filiales de groupes bancaires) ont également des dispositions réglementaires à appliquer en cas d'externalisation de certaines de ses activités (voir annexe 3 « Dispositions du RG AMF applicables aux SGP). La position AMF 2012-17 sur la fonction de conformité applicable à l'ensemble des Prestataires de Services d'Investissement (PSI) rappelle également quelques éléments clés concernant l'externalisation de cette fonction de vérification de la conformité.

10.1. Orientation générale n°10 :

Les PSI doivent s'assurer que toutes les exigences applicables à la fonction de vérification de la conformité sont satisfaites lorsque tout ou partie de cette fonction est externalisée.

10.2. Orientations complémentaires :

Les exigences de la directive MIF concernant l'externalisation de fonctions essentielles ou importantes s'appliquent en totalité à l'externalisation de la fonction de vérification de la conformité.

Les exigences qui s'appliquent à la fonction de vérification de la conformité demeurent inchangées, que tout ou partie de cette dernière soit ou non externalisée ; la responsabilité du respect des exigences en vigueur relève des instances dirigeantes du PSI.

Le PSI doit mener une évaluation avec la vigilance qui s'impose avant de choisir un prestataire de services, afin de garantir que les critères visés aux articles 6 et 14 de la directive portant mesures d'exécution de la directive MIF soient satisfaits.

Le PSI doit s'assurer que le prestataire de services dispose de l'autorité, des ressources et de l'expertise nécessaires et d'un accès à toutes les informations pertinentes pour exercer efficacement les missions de vérification de la conformité externalisées.

L'étendue de cette évaluation menée avec un soin approprié dépend de la nature, de l'échelle et de la complexité des responsabilités et des procédures qui sont externalisées, ainsi que des risques liés.

Les PSI doivent également s'assurer que lorsque tout ou partie de la fonction de vérification de la conformité est externalisée, celle-ci demeure par nature

permanente, c'est-à-dire que le prestataire de services à qui cette fonction est externalisée doit être en mesure d'exercer la fonction en permanence et pas seulement dans des circonstances spécifiques.

Les PSI doivent contrôler que le prestataire de services exerce ses responsabilités de manière adéquate, ce qui inclut le contrôle de la qualité et de la quantité des services fournis. Les instances dirigeantes sont chargées de la surveillance et du contrôle permanents de la fonction externalisée et doivent disposer des ressources et de l'expertise nécessaires pour être en mesure d'exercer cette responsabilité. Les instances dirigeantes peuvent désigner une personne spécifique pour surveiller et contrôler pour leur compte la fonction externalisée.

L'externalisation de la fonction de vérification de la conformité au sein d'un groupe ne minimise en rien la responsabilité des instances dirigeantes de chacun des PSI au sein du groupe. En revanche, une fonction de vérification de la conformité centralisée au niveau du groupe peut parfois faciliter l'accès du responsable de la vérification de la conformité aux informations et renforcer l'efficacité de la fonction, en particulier lorsque les PSI partagent les mêmes locaux.

Si un PSI, en raison de la nature, du volume et de l'échelle de ses activités, est dans l'incapacité de garantir l'indépendance du personnel chargé de la vérification de la conformité vis-à-vis de l'exécution des services qu'il doit contrôler, alors l'externalisation de la fonction de vérification de la conformité constitue vraisemblablement une solution appropriée.

Dans son « Guide relatif à l'organisation du dispositif de maîtrise des risques au sein des Sociétés de Gestion de Portefeuille (SGP)» [9] diffusé le 1er août 2014, l'AMF rappelle un élément essentiel :

Lorsque la SGP confie l'exercice de la fonction de RCCI (responsable de la conformité et du contrôle interne) à un prestataire externe ou à un salarié d'une autre entité de son groupe, elle doit en permanence s'assurer que le temps consacré à l'exercice de la fonction de RCCI soit suffisant au regard de l'activité et de la taille de la société. La fonction de conformité doit demeurer permanente. »

Dans le cas de l'appartenance à un groupe, les services d'audit interne du groupe

9. Position-Recommandation de l'AMF du 1er août 2014 (DOC-2014-06)

peuvent effectuer des missions de contrôle périodique au sein de la SGP.
Lorsqu'en application du principe de proportionnalité, le responsable de la conformité et du contrôle interne est également en charge du contrôle des risques, il n'est pas souhaitable que le contrôle périodique soit exercé par le RCCI. La SGP devrait confier à un prestataire externe le contrôle périodique de l'établissement.
Les contrôles réalisés par la fonction de contrôle périodique peuvent être effectués sur une base annuelle ou pluriannuelle. »

1.4.3. Obligations en matière d'externalisation au titre de la Position n°2013-P-01 de l'ACPR « relative à l'application du règlement CRBF 97-02 modifié à l'intermédiation en opérations de banque et en services de paiement » du 13 novembre 2013

De nombreux établissements de crédit ou de paiement font appel à des intermédiaires notamment pour la conclusion de contrats de crédit avec des clients, élément essentiel de l'activité bancaire.
Par sa Position n°2013-P-01, l'ACPR considère que les IOBSP, Intermédiaires en Opérations de Banque et Services de Paiement, (activité régie par les article L519-1 et suivants du Code Monétaire et Financier) disposant, pour l'activité d'intermédiation, d'un mandat d'un établissement de crédit ou de paiement, doivent être considérés comme des « prestataires de services ou d'autres tâches opérationnelles essentielles ou importantes » au sens de l'article 10 q) de l'arrêté du 3 novembre 2014.

Cette Position implique que les établissements rationalisent les contrôles de l'activité confiée à ces prestataires. Ils mettent donc en place des indicateurs de risques appliqués à chaque IOBSP. Le résultat de cette « approche par les risques » permet de cibler les IOBSP qui seront contrôlés en priorité.

Le superviseur distingue également les IOBSP mandatés par l'établissement assujetti et les courtiers. Alors que les premiers sont bien des PSEE compte tenu

du mandat qui leur est confié par l'établissement assujetti, les seconds ne sont pas des PSEE car ils agissent en vertu d'un mandat confié par le client et non pas par la banque. Cette question spécifique est développée au chapitre [5] de ce document.

1.4.4. Livre blanc Internet de la Commission Bancaire

La Banque de France et le Secrétariat général de la Commission bancaire ont publié en décembre 2000 un livre blanc sur les conséquences prudentielles de l'utilisation d'Internet.

Ce document constitue un recueil de bonnes pratiques en matière de contrôle interne, de lutte contre le blanchiment et de sécurisation des opérations bancaires et financières en ligne.

Voici un extrait de l'avant-propos : « *[…] Internet favorise le recours de plus en plus poussé à l'externalisation. Les établissements doivent être en mesure de contrôler ce type de situation, en prévoyant notamment des clauses d'audit précises dans les contrats de sous-traitance.* »

La troisième partie de ce document portant sur la maîtrise des risques, développe les considérations suivantes : « *Le choix du délégataire externe devrait [...] s'effectuer sur la base de critères tels que* :

- *son expérience ;*
- la clarté des responsabilités juridiques des conventions [...], en continuité d'exploitation mais aussi en cas de liquidation du délégataire ;
- la possibilité de se désengager de ces accords, sous quel délai et à quels coûts ?
- les plans de continuité des services offerts par le délégataire externe ;
- le degré de transparence du délégataire permettant à l'établissement contractant d'évaluer périodiquement les systèmes de contrôles internes [..];
- le degré de sécurité offert par le délégataire externe en termes de respect du secret professionnel.

En parallèle, l'établissement devrait se poser les questions suivantes :

- *comment l'établissement va-t-il mesurer son degré de dépendance vis-à-vis du délégataire [..] ?*
- *l'implication du management est-elle suffisante pour [..] réexaminer périodiquement [..] si la solution de la prestation [..] est toujours adaptée aux besoins [..] et si le choix du délégataire est pertinent [..] ? »*

1.4.5 Rapport annuel sur le contrôle interne en application des articles 258 à 259, 262 à 264 et 266 de l'arrêté du 3 novembre 2014

Le contenu du sommaire détaillé recommandé par l'ACPR pour l'élaboration du rapport sur le contrôle interne, illustre l'intérêt particulier accordé par le superviseur aux activités externalisées. Les établissements assujettis sont invités à expliciter les dispositifs liés au contrôle des prestations externalisées :

- « Résultats des contrôles périodiques effectués au cours de l'exercice écoulé (**y compris pour les activités à l'étranger et les activités externalisées)**»
  - › risques et/ou entités ayant fait l'objet d'une vérification du contrôle périodique au cours de l'exercice écoulé ;
  - › principales insuffisances relevées ;
  - › mesures correctives engagées pour remédier aux insuffisances relevées, date de réalisation prévisionnelle de ces mesures et état d'avancement de leur mise en œuvre à la date de rédaction du […] rapport ;
  - › modalités de suivi des recommandations résultant des contrôles périodiques (outils, personnes en charge) et résultats du suivi des recommandations ;
  - › enquêtes réalisées par le corps d'inspection de la maison-mère, des organismes extérieurs (cabinets extérieurs, etc.), résumé des principales conclusions et précisions sur les décisions prises pour pallier les éventuelles insuffisances relevées.

Par ailleurs, les informations attendues dans l'annexe de présentation du rapport de contrôle interne, prévu à l'article 258 de l'arrêté du 3 novembre, comprennent notamment la présentation synthétique du dispositif de contrôle interne avec :

- « description du contrôle des activités externalisées (au sens des q et r de l'article 10 de l'arrêté du 3 novembre 2014) et des conditions dans lesquelles a lieu le recours à l'externalisation : pays d'implantation, agrément et surveillance prudentielle des prestataires externes, rédaction d'un contrat (description des principales dispositions)» […];
- Les mesures prises en cas de transfert de données (le cas échéant auprès de prestataires externes) dans un pays n'offrant pas une protection considérée comme adéquate.

De même, la description du dispositif de contrôle permanent (y compris le dispositif de contrôle de la conformité) inclut :

- La « description, formalisation et date(s) de mise à jour des procédures sur lesquelles s'appuie le contrôle permanent y compris pour l'activité à l'étranger et les activités externalisées (dont les procédures d'examen de la conformité) ».

1.5. Enseignements tirés des sanctions récentes liées aux PSEE

Le 27 novembre 2012, une sanction de 300 000€ avec blâme a été prononcée par la Commission des sanctions de l'ACP à l'encontre d'une banque[10]. Deux des griefs sont relatifs à une lacune en matière de délégation de prestation de service essentielle.

A travers cette sanction, le superviseur souligne plusieurs points relatifs à l'externalisation d'activités essentielles ou importantes :

- Les missions de contrôle confiées à des prestataires externes par les établissements assujettis à l'arrêté du 3 novembre 2014 doivent être considérées comme des PSEE. Les clauses de suivi obligatoire des PSEE doivent être insérées dans les contrats.

10. Commission des sanctions ACP, 27/11/2012, BANK TEJARAT PARIS.

- Il est reproché à l'établissement de crédit de ne pas avoir intégré dans le contrat liant l'établissement à un prestataire chargé de missions de contrôle périodique, les mentions (explicites) relatives au contrôle des PSEE (la seule référence à l'article 37-2 du CRBF 97-02 étant considérée comme insuffisante) et permettant de satisfaire aux exigences de niveau de qualité, protection des informations confidentielles, accès de l'ACP aux informations. Le grief est ainsi rédigé :

[…] Considérant que l'article 37-2 du CRBF 97-02 relatif à l'externalisation des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes par les banques, leur impose dans son paragraphe 3 de s'assurer que ces prestataires s'engagent sur un niveau de qualité répondant à un fonctionnement normal du service et, en cas d'incident, conduisant à recou- rir à des mécanismes de secours, qu'ils assurent la protection des informations confidentielles ayant trait à l'entreprise assujettie et à ses clients, et acceptent que l'ACP ait accès aux informations sur les activités externalisées nécessaires à l'exercice de sa mission, y compris sur place ;

« […] La commission estime que, quelle que soit la notoriété de ce cabinet, la simple mention de l'article l'article 37 du CRBF 97-02 dans la lettre par laquelle BTP lui confiait la responsabilité de son audit interne ne suffisait pas à garantir le respect de toutes les dispositions de ce règlement, dès lors qu'il n'y est fait référence que pour rappeler la possibilité de cette externalisation ; que ce document ne peut donc être regardé comme permettant à BTP de satisfaire aux exigences ci-dessus rappelées (niveau de qualité, protection des informations confidentielles, accès de l'ACP aux informations), alors qu'aucune mention de ces obligations n'y figure ; que, bien que formel, le grief 28 est établi […] »

- Les établissements délégants sont responsables de l'activité essentielle externalisée : « *[…] Considérant que, selon le grief 6, les paramétrages du logiciel » installé par un prestataire de BTP (la société A1) pour détecter les opérations concernées par le gel des avoirs n'étaient pas performants,*

en raison du recours à des critères orthographiques trop restrictifs et de l'absence de maîtrise de ces paramétrages ; que BTP invoque en défense, d'une part, le fait que le rapport n'a relevé aucune violation de la réglementation imputable aux prétendues déficiences de ce logiciel et, d'autre part, la responsabilité de la société A1, chargée de mettre en place ce logiciel, de le paramétrer et de former ses agents ; que, comme le représentant du collège,[…] La commission estime que BTP ne peut se décharger sur son fournisseur de sa responsabilité, alors que, selon l'article 37-2 du règlement n°97-02 les banques qui externalisent ce type de prestation « demeurent pleinement responsables du respect de toutes les obligations qui leur incombent » et doivent « conserver l'expertise nécessaire pour contrôler effectivement les prestations ou les tâches externalisées et gérer les risques associés à l'externalisation » ; que les carences du dispositif relevées par le rapport établissent donc le grief 6 […] ».

2| RÉGLEMENTATIONS ÉTRANGÈRES

Les exigences réglementaires françaises s'inscrivent dans le cadre de standards internationaux (Comité de Bâle, le Joint Forum, IOSCO[11]).

Si les grands principes sont identiques dans les différents pays, quelques différences sensibles existent, notamment dans le niveau d'exigences des textes, par exemple la nécessité ou non de demander un accord préalable au superviseur, le besoin de recourir pour certaines activités à des institutions agréées ou encore la prise en compte dans les contrats d'externalisation de la sous-délégation. Le paragraphe suivant a pour objet de mettre en exergue quelques prises de position issues de réglementations étrangères paraissant intéressantes pour le groupe de travail.

2.1 Les principes de base posés par le CEBS (Committee of European Banking Supervisors)

Le CEBS a énoncé en avril 2004 plusieurs grands principes afin d'aider les établissements financiers et les régulateurs des états membres de l'Union Européenne dans leurs pratiques et leurs approches de l'Outsourcing :

> Principes à l'attention des établissements financiers

1. L'externalisation ne doit jamais porter ou conduire à la délégation des responsabilités de management des activités externalisées ;
2. La responsabilité finale de la bonne gestion des risques associés à l'outsourcing incombe à la direction de l'institution procédant à l'externalisation ;
3. Une attention particulière doit être portée dès lors que l'entité externalise des activités stratégiques, i.e. activités d'une telle importance que tout

11. Le Joint Forum a été créé en 1996 sous l'égide du Comité de Bâle relatif à la supervision bancaire, de l'IOSCO et de l'association internationale des régulateurs du secteur Assurance. Il a pour objet de traiter les sujets relatifs aux secteurs bancaires, Assurance ainsi que ceux relatifs aux marchés de valeurs.
L'IOSCO (International Organization of Securities Commission) rassemble les régulateurs des marchés de valeurs. L'IOSCO Technical Committee Standing Committee on the Regulation of Market Intermediaries (SC3) a publié une consultation en août 2004 "Consultation Report on Principles on Outsourcing of Financial Services for Market Intermediaries". Le document a été actualisé en janvier 2005

problème dans la fourniture de ces activités pourrait avoir un effet significatif sur la capacité de l'institution à satisfaire aux exigences réglementaires, voire poursuivre son activité ;

4. Il ne devrait y avoir aucune restriction quant à l'externalisation d'activités non stratégiques ;
5. L'externalisation doit s'inscrire dans une politique identifiée, incluant des plans d'urgence et des stratégies de sortie ;
6. Les stratégies d'externalisation des institutions devraient leur permettre de faire face aux risques associés ;
7. Tout accord d'externalisation devrait être l'objet d'un contrat officiel et détaillé ;
8. Dans la gestion de ses relations avec le délégataire de service, l'institution devrait s'assurer de la mise en place d'un Service Level Agreement (SLA) ;

> Trois principes à l'attention des superviseurs

9. Les autorités de supervision doivent avoir pour objectif d'établir un droit à l'information et à conduire, ou ordonner, des inspections sur place auprès des délégataires de service ;
10. Les autorités de supervision devraient prendre en compte le risque de concentration (quand un délégataire fournit ses services à plusieurs institutions)
11. Les autorités de supervision devraient prendre en compte les risques associés aux «chaînes» d'externalisation (lorsqu'un délégataire sous-traite une partie des activités externalisées à d'autres délégataires).

En Décembre 2006, le CEBS a publié une actualisation de ses principes.

Le CEBS et le Committee of European Securities Regulators (CESR) ont travaillé ensemble sur ce projet afin que les principes soient cohérents par rapport au cadre réglementaire défini par la MiFid pour les établissements de crédit.

2.2. Les spécificités réglementaires par pays

Les développements suivants visent à présenter les grands traits des réglementations locales sans prétendre à l'exhaustivité. Pour plus de détails, nous vous recommandons de vous reporter aux textes réglementaires postés sur les sites (voir annexe 2 « Références des réglementations étrangères et textes internationaux ») »

2.2.1 Agrément ou décision préalable

Certaines réglementations vont plus loin que les principes de base et sont plus exigeantes que la réglementation française.

Luxembourg

L'établissement qui a l'intention d'externaliser une activité matérielle doit obtenir une autorisation préalable de la CSSF.

Concernant les services de gestion/d'opération des systèmes informatiques, les établissements peuvent recourir contractuellement à des services de gestion d'opérations de leur système :

- au Luxembourg, uniquement auprès d'un Etablissement de crédit ou d'un professionnel financier disposant d'un agrément de « PSF de support » ;
- dans le cadre d'une externalisation auprès d'une entité du Groupe au Luxembourg ou à l'étranger, l'établissement devra s'assurer que les systèmes externalisés ne contiennent aucune donnée confidentielle lisible concernant les clients autres que les clients institutionnels, sauf s'il existe un consentement explicite du client ou du propriétaire des données.

Suisse

C'est la même exigence de garantir le secret bancaire qui a poussé le superviseur Suisse à légiférer de manière assez drastique.

Les principes de sécurité informatique et notamment la confidentialité des données clientèle prennent une place importante. L'information des clients (principe 6) est un principe assez dissuasif sur la sous-traitance des activités à l'étranger.

Cette possibilité de transfert à l'étranger n'est possible que si le droit de suite du superviseur est pratiqué dans le pays d'accueil.

Par ailleurs, les clients doivent être informés du transfert de données les concernant :

- l'information doit être préalable et comporter des indications détaillées ;
- en cas de transfert à l'étranger, le client doit être informé par courrier spécial et de la possibilité de mettre fin sans préjudice aux relations contractuelles doit lui être offerte.

Au-delà des activités qui demandent un agrément spécifique, la réglementation suisse a précisé, dans une annexe non exhaustive, à la circulaire de la FINMA, des exemples pratiques de prestations soumises à la circulaire.

Cette distinction s'avère très utile pour l'ensemble des établissements désireux d'établir le périmètre précis de ces activités.

Hong Kong

La réglementation de Hong Kong oblige les établissements à obtenir des autorités de contrôle une autorisation préalablement à la mise en œuvre de leur projet d'externalisation.

Singapour

Les réglementations du MAS (Monetary Authority of Singapore) contiennent des pratiques prudentielles sur la gestion des risques de l'outsourcing. Leur application par un établissement doit être proportionnée à la nature de l'outsourcing et à l'ampleur des risques encourus.

Le MAS vérifiera l'application de ces directives pour évaluer la qualité du dispositif de gestion des risques.

2.2.2 Formalisation contractuelle

Sous-délégation

Certaines réglementations, notamment celles du Royaume-Uni et du Luxembourg, indiquent que les conditions de sous-délégation doivent être prévues dans le contrat initial si elles constituent un élément majeur de modification des conditions d'exercice du délégataire.

Pour d'autres pays, par exemple la France, ces mentions relèvent de bonnes pratiques.

Convention de Services (Service Level Agreement- SLA)

Parmi les points que l'on retrouve dans l'ensemble des réglementations, figure notamment l'exigence de rédaction d'une convention de services (SLA).

Ces conventions doivent être régulièrement revues (par exemple annuellement) afin d'évaluer s'il est nécessaire de les réécrire pour les mettre en conformité avec les standards du marché, les évolutions réglementaires ou encore les changements de stratégies commerciales.

La **réglementation Britannique** ("FCA Handbook- Integrated Prudential sourcebook for banks") définit cette convention comme « un accord négocié entre le délégataire et la banque sur les niveaux de service offerts », et précise qu'une banque devrait toujours avoir un SLA écrit si le délégataire n'exerce pas ses activités dans les locaux du groupe. Le SLA doit également fournir des reportings périodiques et des solutions appropriées si des dysfonctionnements apparais--sent. »

L'Australie prévoit même de faire figurer un « modèle de performance qui non respecté peut occasionner l'application de pénalités ».

La réglementation de **Hong Kong** ("Seventh Schedule to the banking Ordinance") précise que la nature et le niveau de services à fournir ainsi que les responsabilités contractuelles et les engagements du fournisseur de service doivent être

clairement présentés dans un contrat de service entre l'établissement et le fournisseur de service.

Concernant les clauses contractuelles, la réglementation de Singapour indique que la fin du contrat doit être prévue dans le cas où le fournisseur devient insolvable, change d'actionnaire, est en liquidation ou si la sécurité et la confidentialité se sont détériorées. Par ailleurs, le contrat de service doit définir les fonctions, obligations et responsabilités de chacune des parties, et doit être contrôlé par l'autorité compétente.

Les accords doivent ensuite être revus régulièrement pour que le niveau de contrôle de l'activité sous-traitée soit approprié.

Par ailleurs, la réglementation de **Taiwan** ("Outsourcing Guidelines for Financial Institutions") inclut la réglementation anti-blanchiment dans les textes de référence à rappeler dans les contrats.

2.2.3 Droit de suite du superviseur

Les réglementations prévoient généralement la possibilité pour le superviseur d'exercer un contrôle sur l'activité déléguée.

Six principes énoncés dans le rapport du IOSCO

1. Le régulateur, (…) doit avoir accès aux documents et enregistrements du fournisseur de service relatifs aux activités externalisées ;
2. Le régulateur doit être capable d'obtenir rapidement, sur demande, les informations concernant des activités régulées ;
3. Le régulateur peut obtenir, sans délai, les documents détenus par le délégant ou le délégataire ;
4. L'accès à ces documents, par le régulateur, peut être direct ou indirect, bien que le délégant doive toujours maintenir un accès direct à ces documents et enregistrements ;
5. Le délégant doit faciliter au régulateur l'accès aux documents, au moyen de dispositions contractuelles : pour garantir l'accès du délégant aux informations du délégataire (y inclus si nécessaire des inspections sur site) et

inciter le délégataire à transmettre des reportings adaptés aux demandes du régulateur ;

6. Le régulateur doit évaluer ces mesures et peut si nécessaire : 1) prendre des mesures contre le délégant pour ne pas avoir fourni les documents demandés dans sa juridiction; 2) imposer des conditions spécifiques pour l'accès aux documents du délégataire.

2.3 Contrôle du délégataire – identification de responsables dédiés

Sur le contrôle du délégataire, les réglementations sont tout aussi précises.

Luxembourg

La réglementation exige que, pour chaque activité sous-traitée, le délégant désigne parmi ses employés une personne qui aura la responsabilité de la gestion de la relation avec le sous-traitant.

Australie

La réglementation australienne (Guidance Note AGN 231.1) indique que des procédures doivent être mises en place par l'établissement financier pour contrôler le risque de sous-traitance en accord avec la politique définie par le conseil d'administration.

Une structure, composée de salariés spécialisés dans l'activité à sous-traiter, doit être spécifiquement constituée pour prendre en charge la gestion des accords conclus avec les sous-traitants, évaluer les risques et émettre des recommandations à l'attention de la direction Générale et du conseil d'administration.

Singapour - Taïwan

Les obligations réglementaires prévoient que le délégant mette en place une équipe dédiée au contrôle de l'Outsourcing, qui devra organiser des points réguliers avec le fournisseur de services afin de vérifier le bon déroulement de l'Outsourcing. Au-delà, la réglementation de Taiwan prévoit que cette structure peut engager des audits réguliers ou inopinés du délégataire. Conformément

aux "Procedures for the Outsourcing of Financial Institution Operation", amendée en mai 2014, une liste limitative d'activités pouvant être externalisées est présentée (article 3). De plus, certaines activités doivent faire l'objet d'un accord préalable du régulateur ("collection of debts", commercialisation de crédits à la consommation sauf crédit automobile…).

La loi met l'accent sur la nécessaire protection de l'intérêt du client et son information en matière d'externalisation lorsque l'externalisation intègre des données de clients. A ce titre, le transfert de données personnelles du client au sous-traitant est strictement encadré.

2.4 Plans d'urgence et de poursuite de l'activité (PUPA) relatifs aux activités externalisées

La problématique PCA, Plan de Continuité des Activités, est assez généralement traitée dans l'ensemble des réglementations.

USA - Australie

Ces deux réglementations précisent que l'institution doit prévoir un plan de continuité des activités externalisées au sein même de l'entreprise, ou chez un autre délégataire, au cas où le fournisseur initial ne serait plus capable d'assurer le contrat de service.

Hong Kong

La réglementation de Hong Kong va au-delà des deux réglementations précédemment citées et précise que l'établissement financier doit régulièrement examiner le PCA du délégataire et s'assurer qu'il est adapté à une défaillance grave affectant la continuité du service ou que son propre plan de continuité tient compte de l'impossibilité pour le délégataire externe d'assurer sa prestation.

Singapour

Dans le même ordre d'idée, l'établissement délégant doit s'assurer que son propre PCA n'est pas compromis par l'externalisation. Le MAS a en effet publié des standards à utiliser, pour évaluer l'impact de l'externalisation sur l'efficacité d'un Plan de Continuité d'Activité.

L'institution doit :

- Déterminer si le fournisseur de services a mis en place un PCA, proportionné à l'externalisation ;
- S'assurer que le fournisseur de services teste régulièrement son PCA, et que ce dernier valide la capacité à réaliser les opérations ;
- S'assurer que le fournisseur est capable d'isoler et d'identifier les informations, documents et enregistrements de l'institution ;
- Etablir son propre PCA selon les pires scénarios, comme par exemple une fin anticipée de l'externalisation ou une liquidation du fournisseur de services.

Taïwan

La réglementation indique que les activités de la banque commerciale ou que les intérêts des clients de la banque ne doivent pas être affectés par une qualité réduite de services, voire d'une cessation d'activités partielle ou totale du sous-traitant.

Article 8 « Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation »[12]: les procédures de contrôle interne de l'établissement financier délégant doivent prévoir un plan d'intervention d'urgence (plan de continuité d'activité).

Article 18 « Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation » : une banque nationale qui répond aux exigences de qualification peut externaliser ses opérations de saisie de données, de traitement, et les résultats du système d'information liés aux services financiers de détail à un fournisseur de services offshore, à condition qu'il soit dûment approuvé par la Commission de supervision financière

12. Texte de février 2012 avec amendements apportés le 9 mai 2014 (www.banking.gov.tw)

après que la banque ait soumis notamment les documents suivants :

- Un rapport d'inspection, émis par une tierce partie indépendante spécialisée dans les technologies de l'information, indiquant que le système d'information du fournisseur de services offshore n'est pas en dessous des normes de sécurité de l'information.
- Un plan d'urgence au cas où le système d'information offshore ne parvient pas à fournir des services et un rapport d'évaluation émis par une tierce partie indépendante spécialisée dans les technologies de l'information indiquant que ce plan répond aux exigences suivantes :
  - La banque doit assurer les opérations fonctionnelles de dépôt, de retrait et de paiement des transactions de clients existants dans les quatre heures suivant l'échec du système d'information offshore à fournir des services, et doit assurer la bonne gestion des risques financiers et commerciaux ;
  - La banque doit assurer les opérations fonctionnelles de crédit et d'autres activités majeures à Taïwan dans les sept jours suivant l'incident, grâce à l'activation du système de sauvegarde, l'installation du serveur d'information (temporaire) ou d'autres moyens, à condition qu'il ait été évalué que le système d'information offshore ne pourrait pas être fonctionnel dans un laps de temps rapide en raison d'une catastrophe naturelle.

3| AUDIT CHEZ LES DÉLÉGANTS

En amont des contrôles qui seront organisés chez le délégataire, l'audit interne du processus chez le « délégant » répond à un double objectif :

- Fournir l'assurance que la décision d'externaliser une activité essentielle est entourée d'un cadre de procédures sécurisé et répond bien aux objectifs fixés par le management ;

- Vérifier par la suite que la supervision des prestations externalisées est correctement organisée et permet un degré de maîtrise suffisant des opérations par le délégant.

3.1 Audit du processus d'approbation et mise en place des prestations externalisées

L'audit du processus d'approbation des prestations externalisées débute par une revue des politiques et procédures afin de s'assurer que les principes régissant le recours à l'externalisation sont définis et qu'une structure décisionnaire ad hoc a été désignée.

En effet, au regard des enjeux stratégiques, des conséquences organisationnelles et des risques encourus, la décision d'externaliser des activités essentielles est un processus « sensible » qui devrait être encadré par une politique, des procédures formalisées et une organisation dédiée.

L'auditeur débutera donc sa mission par la collecte et la revue des documents qui décrivent et régissent ce processus (politique et procédures d'externalisation) et par l'interview des personnes qui participent ou devraient participer systématiquement à la décision d'externaliser une activité essentielle.

Les principaux prérequis indispensables à la mise en place des prestations externalisées et donc à ce titre propres à servir de socle à l'audit sont les suivants :

- une politique et des procédures formalisées et diffusées : afin de donner au processus d'externalisation des prestations un cadre sécurisé ;
- des définitions claires : permettant de distinguer les prestations essentielles des autres, en fonction de la nature des activités et/ou de leur importance/ enjeu pour l'établissement. Les personnels qui étudient la possibilité d'une externalisation doivent être en mesure d'identifier très en amont si la pestation entre dans le cadre du processus d'approbation ou non ;
- une identification des personnels concernés : Il s'agira le plus souvent du service en charge du contact avec les délégataires extérieurs pour mener les études de faisabilité et de coûts et/ou pour organiser les appels d'offres ;
- une intégration des exigences spécifiques de l'arrêté du 3 novembre 2014 dans la démarche de négociation : pour permettre la qualification de la prestation et pour intégrer dans les contrats la dimension de contrôle requise réglementairement (via notamment la clause FBF -voir annexe 1 bis-, ou par exemple des précisions contractuelles concernant la supervision des prestations et l'organisation par le délégant de missions d'audit) ;
- une information des délégataires du caractère « essentiel » de la prestation au sens réglementaire du terme[13], ce qui implique que son externalisation ne pourra s'opérer définitivement qu'après accord d'un comité d'approbation.

L'ensemble des dispositions ci-dessus doit faire l'objet d'un cadre homogène sous forme d'une politique d'externalisation et de procédures. Ces documents doivent définir notamment les principes généraux et les critères de décision validés par la direction générale en matière d'externalisation (Cf. 238-b de l'arrêté du 3 novembre 2014 indiquant que l'externalisation d'activités s'inscrit dans le cadre d'une politique formalisée de contrôle des prestataires externes définie par l'entreprise assujettie). Ces documents devront également préciser les critères et modalités permettant de définir la prestation comme étant PSEE ou non.

13. Art. 10r de l'arrêté du 3 novembre 2014

L'entreprise assujettie à la surveillance organisée de ses prestataires externes doit formaliser l'organisation qu'elle retient. Il importe que cette politique, soumise à l'approbation de l'organe de surveillance, donne le cadre :

- des fonctions ou activités qui peuvent être externalisées et sur quels critères ; des exigences à remplir par le délégataire dans le cadre obligatoire d'un contrat. Le contrat, outre la description des résultats à fournir et des clauses obligatoires (voir annexe 1 « Clause à insérer dans les contrats portant sur les prestations de services essentielles ») doit imposer :
  - L'existence de reporting réguliers sur le niveau de service avec une liste d'indicateurs convenus ;
  - L'organisation d'échanges formalisés et réguliers avec le PSEE permettant de remédier aux incidents et aux non conformités constatés dans le cadre de la réalisation de la prestation et de tenir informé chacun des co-contractants des évolutions organisationnelles et techniques le concernant.
- d'une liste actualisée des prestations considérées comme essentielles ou importantes et du service en charge de la tenue de cette liste ;
- de l'intégration dans la cartographie des risques auditables des PSEE ;
- de la possibilité ouverte ou non au délégataire de sous-traiter la prestation à la condition que le sous-traitant effectue sa prestation dans les mêmes conditions d'encadrement et de contrôle et sous réserve de l'accord préalable du délégant ;
- des responsabilités de suivi du prestataire en matière de contrôle permanent et de contrôle périodique au sein de l'entreprise assujettie ;

3.1.1 Une organisation dédiée

Comme indiqué précédemment, l'approbation de la décision d'externalisation d'une prestation par une structure ad hoc faisant office de comité de sélection et approbation des projets d'externalisation constitue un élément clé du processus d'externalisation.

Cette structure peut revêtir la forme d'un comité spécifique, d'une fonction

spécialisée ou bien encore s'intégrer dans la procédure « Comité Nouveaux Produits » existante dans la plupart des établissements, sans d'ailleurs que l'une des solutions soit exclusive de l'autre.

Il convient à ce titre de rappeler que l'article 35 de l'arrêté du 3 novembre 2014 oblige les entreprises à prévoir « des procédures spécifiques d'examen de la conformité, notamment des procédures d'approbation préalable systématique, incluant un avis écrit du responsable en charge de la conformité […], pour les produits nouveaux ou pour les transformations significatives apportées aux produits préexistants». Conformément à l'article 221 de l'arrêté du 3 novembre 2014, les établissements doivent analyser en amont et de manière prospective les risques encourus lorsqu'ils décident de réaliser des opérations portant sur de nouveaux produits (le concept de nouveaux produits comprenant l'externalisation des activités).

Le recours à l'externalisation (d'activités essentielles ou non) peut être considéré comme entrant dans ce cadre et, au-delà, il est clair que l'existence d'une structure ad hoc peut largement contribuer à formaliser le processus de décision aboutissant à l'externalisation.

En l'espèce, si une telle structure a été mise en place pour autoriser les externalisations, l'audit devra vérifier que :

- L'instance considérée dispose bien de l'expertise nécessaire, par la présence de représentants au moins des fonctions juridiques, Conformité, Risque opérationnel, achats, des opérationnels concernés et de toute autre fonction impliquée dans l'activité externalisée ;
- Le pouvoir de décision de cette instance est clairement établi ;
- Enfin, l'audit devra vérifier que le management au plus haut niveau, voire l'organe de surveillance de l'entreprise (conseil d'administration ou de surveillance), a bien été informé des décisions d'externalisation de prestations essentielles, à tout le moins pour les plus importantes d'entre elles d'un point de vue économique ou stratégique ;

3.1.2 Une grille d'analyse des risques

Pour être valides et éclairer le processus d'approbation, les dossiers d'externalisation devront démontrer que l'ensemble des risques a bien été identifié et que les objectifs sont clairement définis.

L'audit devra ainsi vérifier que les dossiers comportent au moins les éléments suivants :

- un «plan stratégique» avec un budget énumérant et chiffrant les sources d'économies, les dépenses nouvelles pour opérer l'externalisation, le montant de charges annuelles une fois l'externalisation effectuée, des indicateurs de retour sur investissement etc. ;
- la liste des services/départements/directions concernés directement ou indirectement par l'externalisation ;
- le calendrier du projet d'externalisation ;
- une description détaillée des activités et processus opérationnels à externaliser avec une définition précise d'indicateurs et d'objectifs de niveau de service ;
- l'analyse des risques inhérents au transfert de l'activité vers le prestataire avec des scenarii évaluant autant que possible les impacts en termes de coûts ;
- l'analyse des risques inhérents à l'activité externalisée ;
- la prise en compte des aspects PCA/PUPA ;
- la description du dispositif de contrôle interne à mettre en place sur l'activité externalisée.

L'analyse des risques inhérents à l'exécution du projet d'externalisation portera au moins sur :

- le risque opérationnel[14] en cas de défaillance du sous-traitant, ou de défaut de qualité ou de sécurité de la prestation ;
- le risque juridique lié au contrat ;
- le risque de réputation vis-à-vis notamment des clients ;

14. Compris au sens de l'article 10 j) de l'arrêté du 3 novembre 2014

- le risque de non-conformité ;
- Les modalités d'une ré-internalisation éventuelle de l'activité (ou de transfert de l'activité vers un autre prestataire) devront être documentées.

3.1.3 La vérification de l'agrément du délégataire

Certaines activités nécessitent selon les pays où elles sont exercées un agrément des autorités locales. La possibilité de donner délégation à un tiers pour exercer certaines de ces activités pour lesquelles une entreprise a été habilitée est diversement encadrée selon les législations.

Ainsi, selon les articles 231 et 232 de l'arrêté du 3 novembre 2014, les opérations nécessitant un agrément sont les opérations de banque, les opérations connexes aux opérations de banque, les services d'investissement et services connexes aux services d'investissement.

Dans le cadre des établissements de paiement et établissements de monnaie électronique, l'audit s'assurera que l'ACPR a été informée préalablement à l'externalisation des fonctions opérationnelles des services de paiement ou d'émission et de gestion de monnaie électronique.

L'audit s'assurera prioritairement que la prestation externalisée a été correctement qualifiée afin d'identifier la législation dont elle relève. Ensuite, il conviendra de vérifier qu'un avis juridique a été formalisé sur les obligations réglementaires des pays du délégant et du délégataire pour notamment se prononcer sur la nécessité d'un agrément du délégataire par les autorités compétentes.

Enfin, si un tel agrément est nécessaire, l'audit examinera la conformité du document reçu.

3.1.4 L'audit des contrats existants

Le recensement des contrats d'externalisation

Dans certains établissements, les contrats peuvent être conservés ou déclarés de manière centralisée, cette situation ne se retrouve cependant pas dans l'ensemble des groupes.

Dans l'hypothèse d'une gestion centralisée, le système d'information dédié à la gestion, à la conservation ou simplement au recensement des contrats devrait permettre d'identifier rapidement :

- les contrats relatifs à l'externalisation de prestations essentielles ;
- les contrats ayant reçu l'approbation formalisée d'un comité « nouveaux produits / nouvelles activités ».

L'audit évaluera aussi le dispositif de contrôle permanent en place dans l'entité en charge de la centralisation des contrats. Ce dispositif devrait viser à détecter les contrats qui porteraient sur une activité essentielle qui n'aurait pas été identifiée comme telle et/ou qui n'aurait pas reçu l'approbation par le comité ad hoc. Dans l'hypothèse d'une gestion non centralisée, l'audit pourra établir un questionnaire qui sera adressé à des départements susceptibles de conclure des contrats d'externalisation. Ce questionnaire visera à tester l'exhaustivité de la base d'information sur les contrats quand elle existe ou à constituer la population de contrats auditables en l'absence de système d'information centralisé.

3.1.5 La revue de la conformité des contrats

Le principe de l'établissement d'un contrat entre le prestataire externe et l'entreprise délégante est rendu obligatoire par l'article 238 de l'arrêté du 3 novembre 2014 qui précise plusieurs dispositions contractuelles.

En France, une clause « standard » (voir annexe 1 section 1 bis « Clause à insérer dans les contrats portant sur les prestations de services essentielles ») a été élaborée par la FBF en octobre 2005 et mise à jour au 20 septembre 2009. Elle reprend les exigences des articles 238 et 239. Les éléments qui la constituent devraient figurer dans un contrat d'externalisation sous une forme ou une autre.

La clause précise en premier lieu que les « prestations de services faisant l'objet du contrat sont considérées comme des prestations de services essentielles à l'activité du client (au sens de l'article 10r de l'arrêté du 3 novembre 2014) »

Elle précise ensuite que conformément au règlement, le délégataire s'engage au moins sur quatre points :

1. **« respecter les dispositions du présent contrat, de ses annexes et avenants concernant :**
   - le niveau de qualité attendu de ses prestations pour répondre à un fonctionnement normal du service ;
   - la mise en œuvre, en cas d'incident, de difficulté grave ou de force majeure, des mécanismes de secours permettant au client de bénéficier de la continuité du service ;
   - les procédures définies par le client concernant l'organisation et la mise en œuvre du contrôle des prestations qu'il fournit au titre du présent contrat ;
   - le compte-rendu régulier de la manière dont est exercée l'activité qui lui est confiée et de sa situation financière ;
   - La protection en termes d'intégrité et de confidentialité des informations traitées».

Ce premier point reprend les alinéas a), b), c), e) et g) de l'article 239. Il implique que dans le contrat (ou ses annexes, par exemple le cahier des charges) soient précisément définis :

› le niveau de qualité attendu ;

› les instructions pour agir en cas de difficultés graves pouvant perturber la continuité du service ;

› les procédures pour la réalisation de la prestation.

Pour appliquer la disposition relative au PCA, il est recommandé que le contrat contienne une clause obligeant le prestataire à envoyer chaque année à l'établissement délégant le résultat des tests menés en matière de PCA/PUPA.

L'auditeur veillera donc au moins à s'assurer que le contrat comporte une partie dédiée à chacun de ces sujets, partie qui aura été validée par des « experts » au service du délégant indépendant du délégataire.

2. **« accepter l'accès, à chaque fois que le client l'estimera nécessaire, au client ou à ses délégataires le cas échéant sur place, à toute information relative aux prestations fournies, dans le respect des réglementations relatives à la communication d'informations » (voir annexe 1 section 1 bis « Clause à insérer dans les contrats portant sur les prestations de services essentielles ») ;**

Ce deuxième point reprend l'alinéa e) de l'article 239. Il permettra, dans les faits, au délégant de mener directement des audits relatifs à l'activité externalisée chez le délégataire.

L'auditeur sera particulièrement vigilant quant à toute clause qui limiterait, de manière anormale, l'exercice du droit d'audit indépendamment des interventions d'autres départements ; par exemple : nombre de jours, conditions d'accès aux locaux, aux informations et aux interlocuteurs chez le prestataire, facturation par le prestataire de la charge de travail induite. Le cas échéant, l'audit pourra être amené à demander une modification du contrat.

3. **« accepter que l'ACPR ait accès, y compris sur place, aux informations nécessaires à sa mission et portant sur les prestations faisant l'objet du présent contrat » ;**

Ce troisième point reprend l'alinéa h) de l'article 239. Il a pour objet de préciser la nature du « droit de suite » de l'ACPR (ou, le cas échéant, de la BCE) qui lorsqu'elle contrôle un établissement assujetti à son autorité doit avoir la possibilité de poursuivre ses investigations chez ses délégataires. Cette clause donne un droit d'accès de principe au superviseur pour effectuer des investigations directement chez le délégataire.

4. **« recueillir l'accord exprès et écrit du client » :**

- avant de procéder à toute modification des prestations faisant l'objet du présent contrat ;
- avant de déléguer tout ou partie des prestations faisant l'objet du présent contrat à un tiers, ou de conclure avec un tiers un contrat de prestation de

services ou de sous-traitance touchant à ces activités. Ce contrat devra inclure l'ensemble des engagements résultant de la présente clause ».

Ce dernier point encadre le droit du délégataire à modifier la prestation (par rapport aux dispositions dont il est question au point 1) ou à la sous-traiter.

En plus de la conformité aux réglementations, l'audit s'assure de la conformité des contrats aux procédures internes de sélection des délégataires et fournisseurs.

Ainsi, le respect de l'ensemble des règles internes applicables aux contrats en général et pas seulement aux contrats d'externalisation est à vérifier. Par exemple, les établissements ont pour la plupart constitué des listes de délégataires / fournisseurs habilités par les directions « Achats ». Un contrôle standard consiste à s'assurer que les délégataires auprès desquels sont externalisées des activités remplissent les critères de sélection ou d'habilitation en vigueur de l'établissement et que lorsqu'ils ne sont pas habilités, l'interdiction n'est pas contournée par la signature d'un contrat avec une autre société habilitée.

3.1.6 La vérification des bonnes conditions de conservation des contrats

La problématique de la bonne conservation des contrats n'est évidemment pas spécifique aux seuls contrats régissant les prestations externalisées.

Il appartient à l'audit de contrôler systématiquement que les originaux sont inventoriés et conservés dans un lieu sécurisé (coffre/armoire ignifugée ou site sécurisé concernant les contrats dématérialisés) facilement et rapidement accessible. Les originaux devraient en principe être gérés de manière centralisée et les entités opérationnelles devraient donc plutôt disposer de copies fiables et à jour.

Si les originaux sont conservés par un délégataire externe, cette prestation de conservation doit être elle-même clairement précisée dans un contrat qui mentionne aussi les conditions de communication des originaux ; en outre,

l'établissement doit pouvoir s'assurer des conditions de sécurité qui régissent la conservation de ces contrats.

3.1.7 La conformité de l'externalisation aux conditions définies

L'audit peut intervenir dès la prise d'effet du contrat ou une fois l'activité réellement externalisée. L'objectif, quel que soit le moment de l'intervention, est de s'assurer que les éléments qui composent le dossier projet présenté au comité ad hoc sont bien repris de manière conforme dans le dispositif mis en place.

3.1.8 La pertinence et l'efficacité du contrôle permanent sur le processus d'approbation et le suivi des décisions

L'audit vérifiera que le système de contrôle permanent couvre le processus d'approbation et de suivi des décisions (en particulier les conditions fixées lors de l'approbation du dossier d'externalisation) et qu'il a été élaboré suivant une démarche d'évaluation des risques.

3.2. Audit du processus de supervision des prestations externalisées

Une fois que l'audit se sera assuré que l'externalisation est dûment validée et que les clauses du contrat sont considérées comme conformes à la réglementation et aux instructions internes, il devra alors vérifier que :

- la supervision de la relation avec le délégataire est organisée ;
- des outils de suivi sont disponibles ;
- le pilotage de la relation est efficace ;
- les acteurs opérationnels sont bien définis et leurs responsabilités précisées ;
- le contrôle permanent du délégant est présent et actif sur le dispositif de supervision.

3.2.1 La structure de gouvernance et le pilotage de la relation

Vérifier que les responsabilités du délégant sont spécifiées

Quels que soient l'importance et l'enjeu de l'activité externalisée ou l'organisation

du délégant, il convient de s'assurer que les responsabilités de la relation avec le délégataire sont attribuées et effectives au sein de l'organisation délégante.
La désignation d'un responsable est une étape indispensable en tant que pilote de la relation. Il peut s'avérer que certains sujets nécessitent une responsabilité partagée entre plusieurs personnes ou services ; dans ce cas, il convient de s'assurer que la responsabilité de l'activité externalisée n'est pas diluée et que cette collégialité fonctionne de manière efficace par rapport aux objectifs définis (positionnement du responsable, moyens alloués…).
De plus, il convient de veiller à ce que des back-up soient prévus pour ces postes.

Evaluer l'organisation et la structure du pilotage

› **en matière de gouvernance**

Il s'agit ici de vérifier que les décisions structurantes, le suivi et l'évolution des objectifs stratégiques, la gestion des transitions, le changement de délégataire sont traités, décidés au bon niveau dans l'organisation du délégant et suivis d'effets.
Le respect et la conformité des dispositions contractuelles, le respect du contrat de service (SLA), la qualité des reportings et la nature des prestations par rapport au contrat sont également appréciés par ce comité.
L'audit s'assurera que la structure de gouvernance est destinataire des résultats des missions d'audit interne ou externe ayant eu lieu ou planifiées chez le délégataire et du suivi de la mise en œuvre des recommandations émises lors de ces missions.

› **en matière de suivi opérationnel**

Le suivi opérationnel et technique ainsi que le pilotage de la performance peuvent être traités par un comité avec une fréquence plus régulière.
L'audit s'assurera que l'organisation opérationnelle prévoit une répartition claire des responsabilités. Il vérifiera également l'existence d'un organigramme mis à jour régulièrement et communiqué à l'ensemble du personnel.
Il contrôlera que :

- les rattachements sont appropriés ;

- les responsabilités permanentes et les fiches de fonctions sont établies ;
- chaque intervenant a les compétences et/ou l'autorité nécessaire(s) ;
- en cas de défaillance d'un intervenant un back-up est prévu ;
- le temps alloué et consacré au sujet est suffisant.

La comparaison de cette structure avec celle mise en place chez le délégataire est également un axe de travail qui permet de vérifier que les interlocuteurs, contacts et circuits de communication sont clairement identifiés et opérants.

Enfin, l'audit vérifiera l'existence de comptes rendus formels de ces comités (responsabilité de rédaction, responsabilité de validation) et évaluera le suivi des décisions et leur bonne communication aux opérationnels.

3.2.2 Les outils et les moyens de suivi, le pilotage des opérations

L'objectif est de s'assurer que :

- l'ensemble des moyens à disposition permet un suivi efficace en accord avec les éléments contractuels et réglementaires du sujet traité et qu'ils sont utilisés à bon escient ;
- des indicateurs conformes à leur description au sein du contrat de service existent chez le délégataire mais également chez le délégant afin que l'auditeur soit en mesure de réaliser des rapprochements et assurer l'efficacité des échanges et des moyens.
- dans le cas où le contrat prévoit des pénalités en cas de non-respect des indicateurs, la clause relative à ces pénalités a bien été activée le cas échéant. Dans le cas contraire, l'auditeur vérifiera les raisons pour lesquelles la clause n'a pas été activée.

› **Les outils et les moyens de suivi**

Indicateurs de qualité

Il convient de vérifier qu'ils existent, mais aussi de s'assurer qu'ils sont en adéquation avec les termes du contrat de service. Leur description détaillée ainsi que leur fréquence de production doivent donc être formalisées, validées et approuvées par toutes les parties.

A titre d'exemple, dans le cadre de l'externalisation d'une activité de passage d'ordres de bourse (notamment en ligne), ces indicateurs devront mentionner le volume moyen d'ordres passés dans un laps de temps donné et figurer dans la partie du contrat où le délégataire doit s'engager. L'auditeur vérifiera également la pertinence des indicateurs de qualité définis.

Indicateurs de production

Ils permettent de vérifier le respect des engagements du délégataire vis-à-vis de son client (volumes, coûts de production…).

Afin de suivre les différents critères de décision qui ont amené à procéder à l'externalisation d'une activité, il est nécessaire d'être à même de comparer la production sous-traitée à la production réalisée avant externalisation.

Suivi et recensement des incidents et des non-conformités

L'audit s'assure qu'une base permet d'enregistrer les différents événements affectant la prestation. Elle comporte a minima un certain nombre d'éléments comme la date, l'heure, la nature, la durée, le coût estimé de l'incident ou des non conformités... tous les critères permettant une appréciation objective à comparer aux engagements mentionnés dans le contrat de service.

L'audit devra également contrôler que ces incidents et ces non conformités sont portés à la connaissance du responsable et examinés. Cet examen doit donner lieu à des mesures correctrices formalisées. Un suivi régulier sera opéré.

Un circuit formalisé et disponible de remontée des incidents et des non conformités à un comité est à prévoir via la formalisation d'un compte rendu. Les incidents dépassant les seuils prévus à l'article 98 de l'arrêté du 3 novembre 2014 font l'objet d'un reporting aux dirigeants effectifs et à l'organe de surveillance.

Ressources affectées à l'externalisation

Dans le cadre de certaines activités, le contrôle de l'adéquation des moyens humains est prévu par la réglementation (conservation de titres).

D'une manière générale, le délégant pourrait être amené à s'assurer :

- du profil professionnel des ressources mobilisées par le délégataire en cas de haute technicité de la tâche ;
- de la mise à niveau du personnel par des programmes de formation.

Il peut également demander des indicateurs sur des points spécifiques tels que le turnover par exemple.

Plan de continuité d'activité (PCA) / Plan d'Urgence et de Poursuite d'Activités (PUPA)

L'auditeur interne devra s'assurer que le contrat d'externalisation prévoit :

- un plan de continuité d'activité/plan d'urgence et de poursuite d'activités ;
- les tests de ce plan de continuité ;
- une information systématique relative à tout changement significatif de système ou d'organisation ;
- un reporting annuel sur les tests réalisés et une information relative aux mesures correctrices mises en place suite à ces tests.

› **Le contrat de service (Service Level Agreement)**

L'audit interne s'assure de :

- l'existence d'un contrat de service qui reprend les différents éléments précédemment cités ;
- sa connaissance par les collaborateurs concernés ;
- sa mise à la disposition des personnes impliquées, d'une part les gestionnaires de l'activité concernée et d'autre part les personnes en charge de sa validation et de sa signature.

Pour s'assurer que les engagements de production ou de réalisation en termes de quantités, qualités et délais, sont tenus, l'audit vérifiera que tous les éléments concernant la supervision et le pilotage sont mentionnés avec précision (détail des différents indicateurs et fréquence de leur diffusion).

Lorsqu'un processus d'externalisation existe depuis déjà quelques années, il

conviendra de vérifier qu'il a bien fait l'objet des avenants ou mises à jour requises le cas échéant. La non présence de ces pièces complémentaires implique de mener des investigations sur le sujet afin de garantir qu'il ne s'agit pas d'une omission mais d'une absence de mise à jour.

Au rythme de l'évolution des outils (matériels ou logiciels), il apparaît toutefois peu probable que ceux utilisés dans le cadre de l'externalisation ne subissent pas de modifications. Il convient donc de veiller à ce que ces mises à jour soient impérativement reportées dans les contrats ou tout autre document concerné, relatifs aux modalités d'exécution des prestations.

Enfin, il est nécessaire de vérifier que la couverture des sujets traités dans le contrat de service est globale (opérationnelle et réglementaire). Il est primordial de s'assurer que tous ces points sont pris en compte, que les exigences de chaque partie ont été exprimées, étudiées et arbitrées. Le contrat n'est pas un document unilatéral, il doit être compris et assimilé par toutes les parties concernées et surtout validé par les personnes compétentes et responsables.

› **Le pilotage des opérations**

L'objectif est de s'assurer, une fois les responsabilités définies, que l'ensemble des moyens mis à disposition permet un suivi efficace en accord avec les éléments contractuels et réglementaires du sujet traité et qu'ils sont utilisés de manière adéquate.

- **L'utilisation des outils et des moyens**

Elle doit être réalisée à bon escient, les outils doivent être documentés et leurs utilisateurs convenablement formés.

Il conviendra de s'assurer que la consolidation générale des résultats fournis par les outils et les moyens est cohérente, pertinente et non redondante.

- **La qualité des informations recueillies pour alimenter les indicateurs**

Chaque donnée et chaque circuit de données sont validés par les responsables des outils.

A cet effet, la cohérence et la fiabilité des données en entrée doivent être vérifiées.

- **Tableaux de bord**

Différents types d'indicateurs sont utilisés pour alimenter des tableaux de bord à destination du comité ad hoc. Le pilote a pour responsabilité, en collaboration avec les responsables opérationnels de commenter les écarts éventuels par rapport aux engagements contractuels/ exigences réglementaires afin d'éclairer les décisions du comité.

3.2.3 Le rôle des acteurs opérationnels

Dans ce cadre, il convient de vérifier que les acteurs opérationnels sont référencés comme faisant partie d'une équipe dédiée au suivi de la relation ou en cas d'organisation non dédiée, sont référencés au sein d'un organigramme complet et à jour. Leurs responsabilités, fonctions et compétences requises pour l'exercice de leur activité sont formalisées au sein d'une fiche de fonction et de responsabilités permanentes. Cette fiche a été au préalable validée par un membre du management et transmise à la Direction des Ressources Humaines. Cette équipe est au fait des conditions du contrat de service. Ceci afin de vérifier, grâce à leur suivi au jour le jour, la réalisation des engagements contractuels et l'atteinte ou non des objectifs fixés dans les termes du contrat.

Dans certains cas prédéfinis ou à la demande de son responsable, cette équipe peut être chargée de rédiger des expressions de besoins complémentaires sur une partie de l'activité externalisée, de suivre les évolutions apportées ou de proposer les actions correctives nécessaires.

La principale mission des premiers acteurs de la délégation est, outre leur activité opérationnelle, de remonter au pilote leur appréciation factuelle sur la performance opérationnelle, i.e. sur la prestation rendue tant au niveau de la production que de la qualité de service. Un moyen efficace consiste à mettre en place des indicateurs « jumeaux » de ceux fournis par le délégataire. La comparaison sera plus facile et surtout moins contestable. Ces acteurs connaissent et maîtrisent la teneur du contrat de service, notamment sur les engagements quantitatifs et qualitatifs du délégataire à leur égard.

Ils ont également la responsabilité d'alimenter et de tenir à jour la base des incidents et des non conformités et surtout de remonter toutes les informations susceptibles d'alimenter le pilote quant à l'atteinte ou non des différents objectifs fixés, notamment ceux définis dans le cadre du contrat de service. D'une manière générale, toute information susceptible de remettre en cause le bon fonctionnement de l'externalisation ou allant à l'encontre de ses caractéristiques ou motivations doit être remontée au pilote.

Il convient de s'assurer que les acteurs du contrôle permanent sont identifiés au sein de la structure et que leurs contrôles dans le cadre de l'externalisation sont exhaustifs.

3.2.4 La pertinence et l'efficacité du Contrôle Permanent[15] sur le dispositif de supervision/ pilotage des prestations externalisées

› **L'existence effective d'un dispositif relevant du contrôle permanent**

L'audit a pour objectif de vérifier que le dispositif de supervision/pilotage est correctement couvert par le contrôle permanent.

Il vérifiera que les responsabilités ont été établies, que les fiches de postes sont formalisées et exhaustives. Il contrôlera que les plans de contrôle mettent en évidence la périodicité des contrôles et les livrables attendus.

› **Evaluation des risques**

L'audit interne s'assurera que le plan de contrôle mis en place par le contrôle permanent découle bien des résultats de ce "Risk assessment".

15. Selon l'article 12 de l'arrêté du 3 novembre 2014, « Les entreprises assujetties disposent, selon des modalités adaptées à leur taille, à la nature et à la complexité de leurs activités, d'agents réalisant les contrôles, permanent ou périodique.
Selon l'article 13 : « Le contrôle permanent de la conformité, de la sécurité et de la validation des opérations réalisées et du respect des autres diligences liées aux missions de la fonction de gestion des risques est assuré, avec un ensemble de moyens adéquats, par :
– Certains agents, au niveau des services centraux et locaux, exclusivement dédiés à cette fonction ;
– D'autres agents exerçant des activités opérationnelles ».
Et enfin selon l'article 17 : « Le contrôle périodique de la conformité des opérations, du niveau de risque effectivement encouru, du respect des procédures, de l'efficacité et du caractère approprié des dispositifs mentionnés à l'article 13 est assuré au moyen d'enquêtes par des agents au niveau central et, le cas échéant, local, autres que ceux mentionnés audit article ».

› **Référentiel de contrôle et plan de contrôles de la prestation**

L'objectif est de vérifier que le contrôle permanent dispose d'un référentiel de contrôle sur son périmètre.

L'audit contrôlera son existence, sa couverture et sa bonne application. Il est utile et opportun de s'assurer que ce référentiel est cohérent avec celui édité par le délégataire, ceci, afin de garantir une communication sur des bases communes et une bonne compréhension mutuelle.

Une fois les responsabilités connues, le contrôle permanent disposera également d'indicateurs clés de suivi de la qualité et de la performance, et d'indicateurs clés de risques. Il convient de s'assurer que le contrôle permanent a donc à sa disposition les indicateurs de contrôle à même de lui permettre d'évaluer de manière récurrente le dispositif.

L'audit est en charge de vérifier qu'une analyse pertinente de ces indicateurs de contrôle est effectuée par le contrôle permanent.

Cette analyse pourra prévoir des données de pilotage (coûts et bénéfices réels par rapport aux bénéfices attendus, risques). Cette aide à la décision fera l'objet d'un reporting qualitatif et quantitatif à destination du comité ad hoc.

L'audit vérifie ensuite l'existence de points de contrôles formalisés et documentés couvrant le périmètre, ainsi que la pertinence des critères retenus pour ces points de contrôle.

Enfin, l'audit contrôlera que des tableaux de bord sont disponibles et que la problématique du PUPA est traitée.

3.2.5 Vérification par l'audit de l'évaluation des risques au sein de l'entreprise délégante

L'exercice de l'évaluation des risques a pour objectif final de fournir des éléments objectifs pour la construction du plan d'audit et de déterminer la fréquence à laquelle chaque activité externalisée devra être revue[16].

16. Selon les bonnes pratiques professionnelles, le plan d'audit prévoit que l'ensemble des activités d'une structure ou d'une entité soit audité sur un cycle de temps raisonnable, indépendamment du risque déterminé par le résultat du Risk Assessment.

L'évaluation des risques consiste à :

- décrire l'univers auditable ;
- hiérarchiser les entités en fonction de leur niveau de risque global.

› **Décrire l'univers auditable**

- Un domaine auditable constitue le niveau élémentaire sur lequel le risque doit être évalué dans le cadre de l'évaluation des risques. Décrire l'univers auditable consiste donc à lister les « domaines auditables » ;
- Trois types d'audit peuvent être conduits : des audits sur le processus d'approbation des activités externalisées, sur la supervision de ces activités et enfin sur le délégataire (audit sur place) ;
- Le processus d'approbation peut être appréhendé en tant que tel dans l'exercice de l'évaluation des risques et donc être considéré comme un « domaine » auditable à part entière ;
- La supervision/le pilotage des activités externalisées pourront être considérés comme un ou plusieurs domaines auditables. On pourra définir un domaine « auditable » par couple délégataire/activité externalisée ;
- Le principal enjeu à ce stade de l'exercice est de garantir l'exhaustivité des « domaines auditables » et donc ici principalement de la liste des couples délégataires/activités externalisées. Le recensement des activités externalisées sera d'autant plus facile que la gestion des contrats d'externalisation est centralisée. Dans le cas d'une organisation décentralisée, l'audit envoie un questionnaire ou organise des interviews avec les responsables des différentes activités de l'établissement sur base déclarative pour s'assurer que toutes les activités externalisées ont été prises en compte.

› **Hiérarchiser les entités en fonction de leur niveau de risque global**

Les entités sont hiérarchisées par application d'une matrice.

A titre d'exemple, il est proposé ci-dessous une liste de types de risques à évaluer inspirée notamment des catégories de risques opérationnels « Bâle II ».

Type de risque	Exemple
Risque commercial	> mauvaise qualité de la prestation délivrée aux clients du délégant
Risque de non conformité	> organisation ou fonctionnement de l'externalisation non-conforme aux règlements ou lois applicables au délégant et/ou au délégataire
Risque d'erreur d'exécution	> le délégataire n'est pas correctement organisé pour garantir la sécurité et la qualité d'exécution de la prestation
Risque de fraude ou autres activités criminelles	> détournement de l'information destinée au délégataire
Risque de perte des moyens d'exploitation	> Perte de données informatiques lors de transfert entre la société délégante et le délégataire
Risque de défaillance des systèmes d'information	> Intrusion dans le système d'information du délégataire > rupture dans la continuité d'exploitation
Risque stratégique	> l'activité externalisée pourrait être gérée dans un objectif non-conforme aux objectifs stratégiques du délégant > échec dans la mise en place de la supervision de l'activité externalisée et perte de compétence
Risque de réputation	> comportements ou pratiques du délégataire irréguliers ou non-conformes aux standards éthiques du délégant

Risque de contrepartie	>capacités financières du délégataire insuffisantes pour remplir ses obligations ou remédier à une défaillance
Risque pays	> une évolution « politique » du pays dans lequel est externalisée la prestation empêche l'accès aux informations ou la fourniture de la prestation
Risque contractuel	> une interprétation du contrat différente entre le délégant et le délégataire ne peut être arbitrée suffisamment rapidement pour ne pas nuire à l'exécution de la prestation
Risque de concentration	> le délégant externalise plusieurs activités chez le même délégataire
Risque systémique	> le même délégataire est utilisé par plusieurs établissements significatifs de la même « industrie »
Risque de diffusion d'information confidentielle	> transmission de données non sécurisées entre le délégataire et le délégant
Risque sur le personnel	> turn-over élevé et perte de compétence > délit de marchandage

› **Critères de hiérarchisation**

L'échelle de risque du plus catastrophique au plus insignifiant sera fonction notamment de la taille, de l'activité et de l'organisation des établissements. L'évaluation du risque prend en compte la probabilité d'occurrence du risque (qui peut être exprimée en fréquence d'apparition dans le temps) et son impact financier direct (lié à l'arrêt ou à un incident de la production) ou indirect

(lié au risque d'image par exemple) estimé pour l'établissement. Hiérarchiser les domaines auditables permettra de planifier les missions à conduire en adaptant la fréquence et la profondeur en fonction des risques dans le cadre d'un cycle d'audit pluriannuel.

4| AUDIT CHEZ LE DÉLÉGATAIRE

L'audit chez le délégataire participe de l'objectif d'entière maîtrise des activités externalisées par les délégants, visé par l'arrêté du 3 novembre 2014. Le contrôle périodique des prestations confiées à des tiers « de manière durable et à titre habituel » intervient en complément des dispositifs de contrôle permanent des risques et de la conformité mis en œuvre chez le délégant.

L'audit des délégataires suppose comme préalable l'existence d'un cadre contractuel, qui définit les prestations, encadre la relation, fixe les obligations des parties, et prévoit une clause d'audit dûment inscrite.

Pour le délégant, il a pour finalité de s'assurer que la prestation externalisée est conforme aux spécifications stipulées dans le contrat, tant du point de vue des résultats mesurables du service ou produit livré que de celui des moyens mis en œuvre par le délégataire.
Ce contrôle périodique repose sur les obligations stipulées dans la documentation contractuelle, qui comprend le contrat mais également tous les documents annexes précisant ce dernier : convention de service (Service Level Agreement) ou annexes spécifiques au contrat consacrées aux tarifs, délais de livraison, indicateurs de qualité de service, PUPA…

L'audit des délégataires consiste à évaluer, sur pièces et sur place chez le délégataire, l'ensemble des éléments qui concourent à la conformité réglementaire, à la sécurité, à la qualité et à la pérennité de la prestation, telle qu'elle est définie dans le contrat. Il porte principalement sur les produits ou services livrés, les reportings adressés au délégant et les processus de traitement mis en œuvre par le délégataire.

L'audit des délégataires vise à mettre en évidence les améliorations à apporter

en vue de renforcer le dispositif de contrôle interne des activités externalisées par le délégant.

L'évolution des exigences des délégants vis-à-vis des délégataires a conduit ces derniers à promouvoir l'émission organisée de reportings et de rapports destinés à combler voire à limiter le besoin de contrôle sur place de la part des délégants. La mise en avant de l'organisation du prestataire, de son dispositif de contrôle et de la mise en œuvre de ce dernier s'illustre particulièrement au travers du développement de l'utilisation des rapports rédigés par des auditeurs certifiés en référence à la norme ISAE 3402.

La norme ISAE 3402 a été développée par l'AICPA (American Institut of Certified Public Accountants). Elle tend à s'imposer dans le cadre général des relations liant un prestataire à son client. Bien que la norme ait une vocation générale et s'impose internationalement, il y a lieu de préciser sa portée exacte de façon à ce que le rapport ISAE 3402 s'insère au niveau qui est le sien dans un dispositif de contrôle des prestations essentielles externalisées. La pertinence du rapport ISAE 3402 de type 1 ou de type 2 dans le cadre du contrôle des prestations essentielles externalisées est un sujet central. Le rapport de type 1 donne une description du système de contrôle, des objectifs qui lui sont assignés et des contrôles eux-mêmes.

Le rapport ISAE de type 2 a pour objectif de donner l'opinion d'un auditeur certifié en référence aux normes spécifiques ISAE sur la description du système de contrôle du prestataire, les objectifs de contrôle et sur la réalisation effective des contrôles.

L'opinion émise au titre du rapport de type 2 couvre le caractère adéquat de la conception des contrôles pour atteindre les objectifs spécifiques qui lui ont été assignés et l'efficacité des contrôles sur une période donnée. Le rapport de type 2 comprend de surcroît une description des tests effectués pour asseoir l'opinion de l'auditeur.

On comprend donc que le rapport est émis en référence aux objectifs de contrôle que s'est assignés l'entité faisant l'objet du rapport. Elle ne peut donc être

présentée comme une certification de qualité du contrôle interne. Il s'agit d'une opinion émise en référence à une norme sur l'atteinte des objectifs de contrôle. Elle rentre, à ce titre, dans le faisceau d'éléments à disposition du contrôleur périodique sur le délégataire.

Elle ne dispense pas ce dernier de l'exercice de sa démarche de contrôle périodique autonome, que celle-ci soit mise en œuvre par lui-même ou par un tiers qu'il aura choisi, afin de vérifier la conformité aux engagements contractuels et exigences réglementaires.

L'avancée réelle que constitue la généralisation des rapports émis en référence aux normes ISAE 3402, ne permet pas au délégant de justifier à lui seul de la mise en œuvre de ses diligences de contrôles. Son obtention et son analyse en référence au contrat de prestation sont des points de passage obligés auxquels doivent s'ajouter des travaux complémentaires à adapter en fonction de la qualité des rapports produits.

L'audit des prestations peut revêtir différentes formes : cet audit peut être réalisé directement par l'établissement financier délégant. Il peut également être réalisé par plusieurs établissements mutualisant leur mission de contrôle, ce qui permet de diminuer les coûts de l'audit mais également d'optimiser le temps et les ressources du prestataire.

L'audit peut être réalisé par les services d'audit et d'inspection des établissements délégants mais peut également être externalisé à des cabinets de conseil ou d'audit externes spécialisés, sous la responsabilité du contrôle périodique des délégants ou sous l'égide de comités regroupant les inspections générales de plusieurs établissements[17]. Cette solution est en général retenue dans les cas suivants :

- *prestation similaire fournie à plusieurs établissements ;*
- *prestation nécessitant des compétences d'expertise dans un domaine spécifique (prestataire de traitement des chèques ou de fabrication / personnalisation des cartes bancaires, prestataire informatique…).*

17. Existence de Groupes de place en la matière (Comité Inter Inspections générales (CIIG), OCBF).

Dans le cas des groupes bancaires, pour lesquels plusieurs établissements du groupe sous-traitent une partie de leur activité à une société du groupe (exemple conservation titres, prestation informatique…), l'audit peut être réalisé par l'Inspection de la maison mère ou de l'organe central dans le cadre des groupes mutualistes, pour le compte de l'ensemble des établissements délégants.
Dans l'ensemble de ces cas de figure, l'essentiel est que les établissements délégants puissent a minima recevoir les conclusions de l'audit réalisé, avec une bonne vision de l'étendue des travaux réalisés et des investigations menées et demander le cas échéant des investigations complémentaires aux entités en charge de l'audit.

4.1 Préparation de la mission d'audit

La préparation de la mission recouvre principalement la collecte d'informations sur le processus à auditer et le cadrage de la mission.

Plus encore que dans les missions de contrôle périodique classiques, la phase de préparation des missions d'audit chez le délégataire est cruciale, parce qu'elle permet de limiter la durée du séjour sur site et d'éviter de perturber le fonctionnement normal de la prestation. La mission doit donc réunir et analyser un maximum d'informations avant de se rendre sur site.

Le cadrage de la mission d'audit doit prendre en compte les différentes situations de l'audit des prestations externalisées : audit réalisé pour compte propre ou plusieurs délégants, délégataire intra-groupe ou délégataire externe…

Dans tous les cas, la préparation de la mission d'audit s'appuiera sur la cartographie des risques élaborée par le délégant (cf. supra « Organisation du Risk Assessment des prestations externalisées ») et mettra un accent particulier sur les occurrences de risque propres à la phase d'exécution de la prestation :

- inadéquation de la prestation aux besoins de l'entreprise ;
- défaillance ou instabilité du délégataire ;

- non réalisation ou réalisation partielle de la prestation ;
- non qualité i.e. non-conformité de la prestation aux spécifications du délégant ;
- dérapage des coûts de la prestation ;
- perte de compétence en interne sur le processus externalisé ;
- dépendance vis-à-vis du délégataire ;
- non-respect des seuils de risques et des niveaux de sécurité fixés ;
- matérialisation de risques réglementaires, fiscaux et juridiques.

4.1.1 Documentation à réunir chez le délégant

La liste précise des documents est variable selon le degré de formalisation du suivi des prestations externalisées par le délégant et selon le détail des exigences exprimées dans la documentation contractuelle. On peut toutefois indiquer les principaux documents suivants, déjà définis dans la partie 3 « Audit chez le délégant » :

- documents de portée générale : politique formalisée de contrôle des délégataires ;
- documents contractuels : contrat (y compris annexes) et convention de service (« Service Level Agreement », qui fait partie du contrat) ;
- documents relatifs au pilotage des prestations externalisées (de niveau Comité de direction): tableau de bord de suivi, comprenant généralement des indicateurs de qualité pour l'ensemble des délégataires ;
- documents relatifs à la gestion de la relation : reportings transmis par le délégataire, comprenant des indicateurs de production et de qualité, les rapports d'erreurs ou incidents éventuels, la correspondance et la situation financière, le cas échéant ;
- documents relatifs au contrôle permanent : cartographie des risques relative aux prestations externalisées (matrice de « Risk Assessment »), référentiel de contrôle de la prestation, résultats des contrôles et plan d'actions correctives en cours de mise en œuvre ;

- rapports d'audit des missions antérieures chez le délégataire ou chez le délégant (vision pilotage) ;
- informations obtenues auprès des utilisateurs de la prestation ou de la mission chez le délégant: questionnaires disponibles ou comptes-rendus d'entretiens réalisés dans le cadre de missions d'audit précédentes.

4.1.2 Documentation à obtenir du délégataire en début de mission

La documentation sur le processus à auditer concerne notamment les éléments suivants :

- documents relatifs à l'organisation et aux processus de traitement concernés ;
- reportings adressés au délégant durant la période sous revue ;
- directives et procédures spécifiées par le délégant en rapport avec la réalisation de la prestation ;
- comptes rendus de réunions et comités ou relevés de décisions ;
- rapports émis par l'audit interne du délégataire traitant du thème de l'audit.

4.1.3 Cadrage de la mission d'audit

Outre les informations habituelles (objet de la mission, champ d'audit, durée …), la note de cadrage de la mission devra spécifier notamment le contexte de réalisation de l'audit et les modalités d'accès aux données.

4.1.3.1 Contexte de réalisation de la mission d'audit

Trois contextes types peuvent être distingués :

1. audit chez le délégataire par un délégant pour son compte propre : c'est le cas général retenu dans ce document pour une mission d'audit de prestation externalisée ;
2. audit chez le délégataire par un ou plusieurs délégants pour le compte de plusieurs délégants : dans cette situation, l'audit peut être réalisé par un délégant pour compte commun, sauf existence de faute lourde, dont le degré reste à définir entre les délégants ;

3. audit chez le délégataire par un cabinet tiers « délégué » pour un ou plusieurs délégants : cette situation est justifiée en particulier lorsque la mission requiert une expertise technique spécifique ou lorsque les ressources d'audit des délégants ne sont pas disponibles au moment de la réalisation de la mission ou encore lorsque le délégataire travaille pour de nombreux délégants ou pour traiter de l'information hautement confidentielle.

Les audits conjoints supposent un consensus des parties prenantes sur un certain nombre de points (thème de la mission, périmètre commun des prestations externalisées à auditer, planning, disponibilité des ressources, méthodes de travail …). Lorsque ce consensus est difficile à obtenir sur les aspects planning, ressources, et méthode d'audit, l'audit par un cabinet tiers constitue une alternative à envisager, notamment si la mission doit être réalisée sans délai (mission de diagnostic consécutive à un dysfonctionnement par exemple).
Chaque établissement devra prévoir, le cas échéant, un contrôle complémentaire sur la partie des prestations externalisées non couverte par le contrôle conjoint (prestations spécifiques).

Les audits conjoints et les audits par un cabinet tiers mandaté appellent la question du partage des coûts de la mission entre les délégants. Par ailleurs, elles impliquent une mutualisation du débriefing et du rapport de mission. D'où la nécessité de prendre en compte ces éléments dans la note de cadrage de la mission.

4.1.3.2 Modalités d'accès à l'information chez le délégataire

La liste des documents, supports des contrôles et tests prévus, est conditionnée par les modalités d'accès au système d'information du délégataire. Sur le modèle des contrôles réalisés par l'administration fiscale française dans le cadre d'une vérification de comptabilité informatisée, il est proposé de retenir les trois modalités pratiques d'intervention suivantes:

- méthode 1 : contrôles réalisés par les auditeurs du délégant sur le système informatique du délégataire ;
- méthode 2 : contrôles réalisés par les collaborateurs du délégataire sur le système informatique du délégataire, sur la base d'un cahier des charges et sous la supervision de l'équipe d'audit du délégant ;
- méthode 3 : contrôles réalisés par les auditeurs du délégant sur des copies de documents, données, traitements ou fichiers du délégataire sur un système informatique n'appartenant pas au délégataire.

Le choix d'une des trois méthodes doit être opéré en fonction de la situation propre du délégataire et des circonstances de la mission ou des contrôles à réaliser. Dans tous les cas, le mode d'accès doit être défini dans la note de cadrage préalable au démarrage de la mission, notamment si l'intervention nécessite l'immobilisation du système informatique du délégataire (méthode 1) ou la mobilisation des ressources humaines et matérielles de celui-ci (méthode 2).

4.2 Audit de la conformité de la prestation

Avertissement

L'audit de la prestation est d'abord et principalement un audit de conformité par rapport au contrat et par rapport à tout document attaché au contrat, quelle que soit la désignation retenue (convention de services, Service Level Agreement, liste d'annexes attachées au contrat…).

Pour autant et au-delà du diagnostic sur le respect du contrat, l'auditeur peut être amené au cours de sa mission à constater le non-respect d'une disposition réglementaire, à laquelle le délégant est assujetti ou qui régit l'activité du délégataire, ou encore à relever des insuffisances par rapport à la maîtrise des risques ou à la performance des processus de traitement en vigueur. Ces deux derniers types de constats (non-conformités réglementaires, points d'améliorations en regard des meilleures pratiques établies) doivent être pris en compte mais identifiés de manière distincte des non-conformités contractuelles (cf. point 4 suite de la mission d'audit).

4.2.1 Auditabilité de la prestation

Le contrôle de l'auditabilité de la prestation vise à s'assurer que le processus de traitement est correctement documenté et que la ségrégation des univers clients dans le système d'information du délégataire permet d'identifier ce qui relève strictement de la prestation du délégant concerné par la mission et garantit de surcroit la confidentialité de ses données.

Si ces points sont définis de manière précise dans la documentation contractuelle, ils peuvent être intégrés dans la revue de conformité de la prestation par rapport au contrat.
Dans le cas contraire, leur examen doit être effectué dans la mesure où la documentation et la ségrégation de l'univers client influent sur le déroulement de la mission d'audit et notamment les modalités d'accès aux données.

4.2.1.1 Documentation du processus de traitement

Afin de s'assurer que la documentation du processus chez le délégataire est conforme à celle définie contractuellement et qu'elle exprime clairement le processus de traitement formalisé par le délégant, la vérification portera sur l'existence des principaux éléments suivants chez le délégataire :

- contrat et convention de service ou annexes attachées au contrat ;
- document attestant de la prise en charge du traitement par le délégataire (par exemple : ordre de mission) ;
- schéma du traitement de la prestation ;
- plan de charge définissant les ressources à affecter à la réalisation de la prestation ;
- modes opératoires de traitement de la prestation.

Les contrôles clés à réaliser sur ces documents portent sur les aspects suivants :

- exhaustivité de ces documents par rapport à la documentation du délégant,
- qualité des principales procédures et modes opératoires: mise à jour, zones de risques non couvertes (incidents, modifications).

4.2.1.2 Ségrégation des univers clients par délégant

En règle générale, les univers clients, et tout particulièrement les données par délégant, doivent être totalement séparés dans le système d'information (au sens général et pas seulement l'informatique) du délégataire, même si certains applicatifs ou traitements sont communs à plusieurs délégants.

Le contrôle de la ségrégation des univers clients vise à s'assurer du degré d'application de cette règle qui garantit la confidentialité des données et à identifier les améliorations à mettre en œuvre lorsque ce principe n'est pas respecté.

Les travaux d'audit porteront sur les points clés suivants :

- organisation du traitement de la prestation dans le système d'information du délégataire ;
- test de vérification de la confidentialité des données.

L'interprétation des résultats des contrôles sera adaptée à la teneur des exigences spécifiées dans le contrat (ségrégation des données et des traitements …).

4.2.2 Reporting de production et contrôles chez le délégataire

Ce contrôle vise à s'assurer de l'exhaustivité des reportings faits par les délégataires, de leur contenu par rapport aux spécifications contractuelles et à vérifier la fiabilité des données mentionnées. Il s'agit également de s'assurer que le délégataire réalise bien les contrôles qui lui sont délégués par le délégant ou qui découlent de la réglementation qui pèse sur le délégant (cf. supra « Respect des obligations réglementaires »).

Les travaux d'audit porteront en particulier sur les différents aspects suivants :

- exhaustivité des reportings ;
- respect de la fréquence des reportings ;
- exhaustivité des indicateurs renseignés ;
- fiabilité des valeurs mentionnées pour les indicateurs retenus ;
- matérialisation des contrôles réalisés par le délégataire.

La liste et la fréquence des reportings définis par le délégant sont stipulées habituellement dans la convention de service ou les annexes attachées au contrat.

Les indicateurs à renseigner recouvrent notamment les informations suivantes : indicateurs de production (volume, montant…), indicateurs de qualité de production (taux d'anomalie plancher, taux de disponibilité des équipements ou services, délais de traitement, de livraison ou de réponse …), moyens à mobiliser (humains, mécaniques ou informatiques), contrôles de production délégués au délégataire.

La fiabilité des valeurs mentionnées pour chacun des indicateurs peut être évaluée par des tests de cohérence entre les différents reportings ou sur l'évolution dans le temps de la valeur d'un indicateur donné.

L'analyse du niveau de service effectivement constaté (i.e. du niveau mesuré par les indicateurs préalablement vérifiés) doit conduire l'audit à porter une opinion sur le respect de ses obligations par le délégataire (défaillances persistantes, ou a contrario dépassement récurrent des objectifs définis dans le document contractuel).

La revue d'audit mettra en évidence les écarts éventuels constatés par rapport aux valeurs de référence de la documentation contractuelle, en particulier s'ils conduisent à l'application de mesures financières (malus ou bonus en fonction des performances réalisées) ou si la convention de service prévoit une résiliation du contrat en cas de non qualité avérée et récurrente (écarts négatifs persistants) ou de défaillance du délégataire.

4.2.3 Incidents de traitement

La notion d'incident désigne ici tout événement nécessitant une correction de la part du délégataire, quelle que soit la dénomination en usage (erreur, litige …). En outre, sont communément qualifiés de problèmes ou d'anomalies, les incidents qui surviennent de manière récurrente.

Le contrôle du reporting des incidents a pour objet de s'assurer que toutes les catégories d'incidents définies contractuellement sont communiquées au

délégant et de vérifier que le délégataire fait diligence pour corriger les incidents.

Le reporting peut faire partie d'un reporting global d'activité ou faire l'objet d'un reporting spécifique adressé par le délégataire.

La revue s'attachera à la vérification des principaux points suivants :

- le respect par le délégataire des critères qualifiant un incident et sa criticité (montant, opération …) ;
- la prise en compte par le délégataire de l'ensemble des incidents impactant la prestation ;
- l'identification des incidents récurrents critiques ;
- la pertinence et le respect de la procédure de communication des incidents par le délégataire ;
- la diligence du délégataire pour corriger les incidents, au regard des exigences du contrat, et la priorisation des plans d'action en fonction de la criticité/récurrence des incidents.

En ce qui concerne l'analyse de la situation des incidents, la revue d'audit s'attachera particulièrement à mettre en évidence des constats et les résultats obtenus, plutôt qu'à procéder à un examen détaillé des moyens mis en œuvre par le délégataire.

4.2.4 Situation financière

Les diligences d'audit concerneront, dans un premier temps, la transmission par le délégataire d'une information sur sa situation financière et, dans un second temps, la fiabilité des données contenues dans le reporting adressé (cohérence avec le rapport annuel) ou la matérialisation d'une certification indépendante des données financières par les commissaires aux comptes, si le rapport annuel n'est pas encore disponible.

L'analyse de la situation financière du délégataire ne vise en aucun cas à refaire le travail des commissaires aux comptes ou à s'immiscer dans la gestion de

l'entreprise du délégataire. Ce contrôle consiste notamment à :

- s'assurer que la situation financière communiquée par le délégataire au délégant est conforme à celle qui a été certifiée par les commissaires aux comptes ou a fait l'objet d'une revue indépendante par ces derniers,
- évaluer le niveau de dépendance économique du prestataire au regard du chiffre d'affaires réalisé avec le délégant,
- s'assurer que la structure financière du groupe auquel appartient le délégataire ne présente pas de risque particulier (exemple : dette importante issue d'une opération de LBO).

En l'absence de documents certifiés, l'analyse portera sur les états de gestion permettant d'évaluer la viabilité du délégataire.

4.2.5 Plan d'Urgence et de Poursuite d'Activités (ex-PCA/PUPA)

L'objectif de ce contrôle est de vérifier qu'il existe des mécanismes de secours de la prestation en cas de difficulté grave affectant la continuité du service concerné et qu'ils sont régulièrement testés.

La revue d'audit vise à couvrir les principaux thèmes suivants :

- existence d'un PCA formalisé et documenté ;
- adéquation des dispositifs constatés par rapport aux spécifications contractuelles en matière de couverture de la prestation ;
- validation formelle du PCA par les parties ;
- test du dispositif effectué selon la fréquence contractuelle (ou moins une fois par an si elle n'est pas stipulée dans le contrat), communication des résultats et des actions correctives ;
- actions de maintien en condition opérationnelle et mise à jour de la documentation relative au PCA.

Il convient de rappeler que l'arrêté du 3 novembre 2014 prévoit l'existence d'un plan de continuité de services de la prestation, qu'il soit assuré par le délégataire ou pris en compte dans le plan de continuité d'activités du délégant.

Cette disposition conduit à trois situations possibles :

- continuité d'activités totalement à la charge du délégataire ;
- continuité d'activités totalement à la charge du délégant ;
- continuité d'activités reposant conjointement sur le délégataire et le délégant.

L'audit doit prendre en compte ces différentes situations, ce qui conduit à réaliser tout ou partie des contrôles chez le délégant dans les deux derniers cas de figure.

Si aucun test n'est intervenu depuis l'homologation du plan de continuité d'activités par les deux parties ou si la fréquence des tests prévus dans le contrat n'est pas respectée, le constat doit être établi et donner lieu à une recommandation de l'Audit.

4.2.6 Obligations réglementaires du contrat

L'activité confiée à un délégataire intègre parfois les obligations réglementaires de l'établissement assujetti (délégant) vis-à-vis du régulateur. Il en est ainsi par exemple des activités telles que le traitement des flux de paiement ou encore la prestation de services d'investissement.

La vérification traitée dans ce paragraphe vise à s'assurer que les contrôles de nature réglementaire délégués par le délégant au délégataire sont exécutés conformément aux spécifications du contrat.

Les principaux points de contrôle de la revue d'audit sont repris ci-après :

- contrôles relatifs au traitement des chèques, virements et espèces ;
- contrôles relatifs aux paiements par monnaie électronique ;
- contrôles délégués relatifs à la lutte contre le blanchiment d'argent (notamment identification des clients) et le financement du terrorisme ;
- contrôles relatifs aux prestations de services d'investissement.

- Il s’agit, pour l’audit interne, de s’assurer de l’adéquation des contrôles avec ceux définis contractuellement.

4.2.7 Obligations générales du contrat

Le contrôle par l’audit de l’application du contrat peut porter également sur les clauses suivantes, les plus fréquentes dans les conventions d’externalisation :

- confidentialité sur la documentation communiquée ;
- subdélégation de la prestation externalisée (autorisée ou non, si oui dans quelles conditions) ;
- obligations découlant de la loi informatique et libertés du 6 janvier 1978 ;
- respect du copyright (en matière informatique notamment) ;
- assurance professionnelle du délégataire ;
- habilitation des délégataires de droit étranger.

La liste précise doit être arrêtée par rapport aux spécifications du contrat relatif à la prestation en revue.
Concernant la subdélégation de la prestation externalisée, l’audit devra s’assurer de l’application des conditions définies dans le contrat : non prévue par le contrat, prévue sur autorisation expresse et conditions du recours à la sous-traitance en cas d’autorisation.

S'agissant des déclarations à la Commission Nationale Informatique et Liberté (CNIL), il convient de noter que la banque, propriétaire des données, est tenue de déclarer les traitements automatisés à la CNIL et que le délégataire a la charge de préserver les données nominatives.

Dans le cadre de l'audit, il conviendra de s'assurer que le délégataire dispose d'une procédure encadrant la transmission des fichiers automatisés à la banque et que cette procédure assure la confidentialité des données transmises quels que soient les moyens utilisés (cryptage des données, anonymisation, code d’accès, etc.).

Pour les délégataires de droit étranger, il est nécessaire de s'assurer que les obligations réglementaires du droit local en matière d'opérations externalisées (respect du secret bancaire, respect des lois locales sur l'environnement, sécurité des données transférées à l'étranger…) sont prises en compte par le délégataire.

4.3 Autres thèmes du programme d'audit chez le délégataire

Les thèmes repris ci-après permettent d'avoir une vue plus complète des processus internes du délégataire et des conditions dans lesquelles la prestation est délivrée.

Ces thèmes concernent notamment l'organisation, le système informatique, la sécurité des systèmes d'information et les systèmes de contrôle interne et qualité constatés chez le délégataire.

4.3.1 Organisation constatée chez le délégataire

L'objet du contrôle consiste à s'assurer que le délégataire dispose d'une organisation et de moyens adaptés à la réalisation des prestations qui lui ont été confiées.

Les travaux d'audit portent sur l'ensemble des procédures organisationnelles permettant de définir les rôles et responsabilités (aux niveaux pilotage, gestion et opérationnel), la composition et l'animation des équipes (comités, tableau de bord, reporting …).

Les contrôles viseront notamment à s'assurer que :

- l'organisation constatée chez le délégataire est compatible avec l'exécution des prestations confiées ;
- l'organisation permet d'assurer une gestion efficace des évolutions dans le temps (absorption des pointes ponctuelles d'activité du délégant sans dégradation des indicateurs de qualité …).

4.3.2 Système d'information du délégataire

Ce paragraphe traite du système d'information, en tant que support technique

et fonctionnel de la majorité des prestations et non des prestations informatiques externalisées (voir annexe 4 « Audit des prestations informatiques »).

L'audit du système d'information du délégataire doit permettre de s'assurer que les applications et les infrastructures informatiques répondent de manière satisfaisante aux besoins du délégant, tant en matière d'automatisation des opérations que de fourniture d'informations de gestion. Ce contrôle vise en outre à vérifier l'existence d'un plan d'évolution du système d'information à même de répondre aux évolutions prévues/prévisibles des conditions de réalisation de la prestation.

L'idée directrice est que le système d'information (matériels et logiciels) ne doit pas constituer un frein au bon fonctionnement actuel et aux évolutions de l'activité (à court et à moyen terme). Le système d'information doit donc contribuer au bon fonctionnement et à la pérennité des processus qu'il supporte et permettre l'évolutivité de la prestation, si nécessaire.

Au plan du matériel informatique, il s'agira de documenter notamment :

- la pérennité des principaux fournisseurs (solidité financière, compétence, notoriété ...) ;
- la pérennité des équipements : collecte des indicateurs permettant de juger de l'espérance de vie des matériels mis en œuvre pour la prestation ;
- la capacité à faire face aux évolutions prévisibles de la prestation : taille mémoire, puissance de traitement pour absorber une croissance de l'activité, maximum potentielle (jusqu'à quel volume d'activité peut-on aller avant de devoir changer de système ?).

Ces informations doivent être recherchées auprès du responsable informatique du délégataire ou s'appuyer sur des audits spécifiques réalisés par le prestataire en interne ou en externe.

Au plan des logiciels, il faut distinguer deux cas avec les contrôles suivants à effectuer:

1. pour les progiciels dont la pérennité et l'évolutivité dépendent essentiellement du fournisseur : solidité financière, volonté de poursuivre ou non la maintenance de l'application, niveau de maîtrise technique du produit par les informaticiens du délégataire (connaissance du langage, de l'architecture du programme, capacité à réaliser des modifications ou des extensions par eux-mêmes, ...) ;

2. pour les logiciels développés en interne pour le compte de l'entreprise délégante, dont la pérennité et l'évolutivité dépendent de la maîtrise des programmes : existence d'une documentation technique à jour, faible dépendance vis à vis de l'informaticien créateur du programme, ...

Dans le cadre de l'audit chez le délégataire, il s'agira de s'assurer que :

- le délégataire dispose des licences et des contrats de maintenance des différents progiciels utilisés ;
- les agents maîtrisent les outils mis à leur disposition en vérifiant par exemple les certifications obtenues par ceux-ci ou en évaluant leur connaissance de l'outil ;
- la revue des incidents informatiques de toutes natures effectuée par le délégataire lui-même conduit à des conclusions qui ne remettent pas en cause l'adéquation du système aux besoins du délégataire ;
- la documentation technique existe et est à jour.

L'audit chez le délégataire peut se reposer sur des référentiels de place dédiés (Norme ISO 27001, COBIT…).

4.3.3 Sécurité des systèmes d'information du délégataire

L'externalisation de prestations sensibles nécessite de s'assurer que ces

18. Telles qu'interprétées dans le livre blanc de la Commission Bancaire sur la sécurité des systèmes d'information.

dernières sont réalisées dans des conditions de sécurité adaptées vis à vis des données et des traitements informatiques.

L'audit s'attachera à vérifier que le plan de sécurité défini dans le contrat de prestation est correctement appliqué en matière de disponibilité des systèmes, d'intégrité des données et des ressources, de conformité aux réglementations[18], de confidentialité des informations et de traçabilité (éléments de preuve).

Au-delà de l'existence et de la pertinence des dispositifs constatés, la revue d'audit pourra également examiner la permanence des mesures conçues et mises en œuvre par le délégataire. Ces évaluations s'appuieront sur les outils ou méthodologies qui font autorité afin de prévenir toute contestation des diagnostics.

4.3.4 Dispositif de contrôle interne chez le délégataire

Si le délégataire est lui-même un établissement bancaire assujetti à l'arrêté du 3 novembre 2014, l'organisation du contrôle interne doit comprendre les trois composantes suivantes :

- un dispositif de contrôle permanent (fonction de contrôle indépendante des opérateurs) ;
- un dispositif de contrôle de la conformité (couvrant notamment la conformité réglementaire) ;
- un dispositif de contrôle périodique (audit).

Dans le cas contraire (délégataire non agréé en France ou de droit étranger), le dispositif de contrôle interne peut être apprécié par rapport à un référentiel de contrôle interne[19].

L'audit réalisé par le délégant chez le délégataire devra qualifier la situation du délégataire sous la forme d'écarts constatés par rapport à l'arrêté du 3 novembre 2014, à la réglementation bancaire locale ou au référentiel de contrôle interne en vigueur chez le délégataire.

19. COSO, COCO, Turnbull Guidance, Cadre de Contrôle Interne de l'AMF

4.4 Rapport de mission : débriefing et diffusion

Comme pour toute mission d'audit, il convient de s'interroger sur les modalités de conclusion de la mission et notamment sur le débriefing et la diffusion du rapport.

4.4.1 Débriefing

Celui-ci est indispensable à la validation des constats posés et des observations émises. Il se distingue néanmoins des conditions habituelles en ce sens que son contenu est très fortement imprégné de la dimension contractuelle de la relation.

S'il n'a pas pu être obtenu copie des pièces en vue de constituer le dossier d'audit, ce qui est acceptable, l'audit doit veiller à rédiger suffisamment d'éléments permettant de commenter les documents consultés. Une mention particulière en est faite lors du débriefing.

Trois catégories de défauts peuvent être identifiées lors de l'audit :

- Les clauses contractuelles ne sont pas respectées ;
- Les clauses contractuelles sont respectées mais des éléments de fragilité sont détectés (non-conformités réglementaires, continuité d'activité…) ;
- Des axes d'amélioration visant à une meilleure efficacité de la prestation livrée voire à une amélioration de la productivité sont identifiés, bien que le contrat soit respecté.

L'analyse des constats relatifs aux manquements par rapport au contrat est par nature exposée au délégataire.

Le débriefing des points 2 et 3 avec le délégataire sera laissé à l'initiative de chaque délégant

4.4.2 Diffusion du rapport

Une fois le débriefing avec le délégataire mais également avec le délégant donneur d'ordre effectué, le rapport peut être établi et adressé à l'organe ayant

diligenté l'audit.

Ce dernier doit définir le format final du rapport à adresser (recommandations retenues) et le circuit de diffusion interne.

Selon les cas les recommandations seront adressées aux délégataires et/ou aux délégants.

4.5 Suite de la mission d'audit

La diffusion du rapport telle que préconisée facilitera en outre le suivi de la mise en œuvre des recommandations en ce sens qu'il appartiendra au délégant donneur d'ordre de :

- convenir avec le délégataire des modalités de mise en œuvre des recommandations dans le cadre contractuel ; cette action doit être prise en charge par le service gestionnaire de la relation avec le délégataire ou par le contrôle permanent ;
- mettre en place les moyens de contrôle permettant de s'assurer que les actions correctives mises en œuvre pour répondre aux recommandations sont effectives ;
- suivre l'avancement de la résorption des points faibles et des risques associés constatés par la mission d'audit chez le délégataire ;
- rendre compte de la mise en œuvre des recommandations à l'Audit ou au service qualifié pour ce faire et cela conformément aux dispositions prises en la matière par chaque établissement.
- Après la mission d'audit, il est également important de mettre à jour, chez le délégant, l'ensemble des outils et moyens de suivi de la prestation externalisée (cartographie des risques, indicateurs de production et de qualité, bases de recensement des incidents, référentiels et plans de contrôle etc.).

5| IOBSP

Par sa Position n°2013-P-01[20], l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) a mis fin à de nombreux débats et questionnements en confirmant que les Intermédiaires en Opérations de Banque et Services de Paiement (IOBSP) disposant, pour l'activité d'intermédiation, d'un mandat d'un établissement de crédit ou de paiement, doivent être considérés comme des « prestataires de services ou d'autres tâches opérationnelles essentielles ou importantes » (PSEE) au sens de l'article 10 r) de l'arrêté du 3 novembre 2014. Rappelons que les intermédiaires en opérations de banques et services de paiement (IOBSP) ont vu le cadre de leur profession profondément modifiée par le décret 2012-101 du 26 janvier 2012. Les IOBSP qui doivent choisir la catégorie la plus adaptée à leur activité (courtier, mandataire non exclusif, mandataire exclusif ou mandataire d'IOBSP) doivent également respecter des règles de bonne conduite qui sont susceptibles d'être contrôlées par l'ACPR.

Ces IOBSP, pour exercer, doivent être immatriculés auprès de l'ORIAS (Organisme pour le Registre des Intermédiaires en Assurances) qui s'assure au moment de leur immatriculation que les conditions d'honorabilité et de compétence professionnelle des dirigeants sont conformes à la réglementation. L'ORIAS est une association sous tutelle de la Direction du Trésor, créée en 2007 pour homologuer les intermédiaires en assurance.

Son champ d'action s'est élargi à l'immatriculation des IOBSP et des Conseillers en Investissements financiers (CIF) le 1er janvier 2013 ainsi que des IFP et CIP le 1er octobre 2014.). Parmi les IOBSP qui doivent s'immatriculer à l'ORIAS figurent les mutuelles distribuant des produits bancaires. En revanche, une société de financement agréée par l'ACPR pour d'autres activités comme la caution par exemple, peut intermédier des crédits auprès d'autres établissements de crédit ou de financement sans avoir besoin de s'immatriculer à l'ORIAS.

Les conséquences de cette position ACPR pour les établissements assujettis

20. « Position de l'ACPR relative à l'application du règlement n° 97-02 à l'intermédiation en opérations de banque et en services de paiement » du 13 novembre 2013

sont réelles. En effet, pour disposer d'un volume significatif de dossiers de crédit, certains établissements assujettis font appel à de nombreux intermédiaires. Les IOBSP (intermédiaires en opérations de banque et services de paiement) sont souvent de très petites structures, qu'elles soient indépendantes ou qu'elles fassent partie de réseaux de franchises. La principale source d'inquiétude des établissements est le nombre d'IOBSP avec lesquels les établissements ont contracté, car il paraît évidemment très coûteux de tous les contrôler. La Position de l'ACPR permet d'atténuer cette difficulté à deux égards :

- **Les IOBSP ne sont pas tous des PSEE**. C'est parce qu'il existe un mandat[21] entre les mandataires exclusifs ou non-exclusifs et les établissements assujettis pour lesquels ils exercent l'activité d'intermédiation à titre habituel que ces IOBSP sont des PSEE. Ils doivent être contrôlés et traités comme tels par les établissements assujettis. En revanche, en l'absence de mandat d'un établissement assujetti, les courtiers[22] en opérations de banque et services de paiement et leurs sous-mandataires[23] font l'objet de mesures de vigilance de la part de l'établissement assujetti, distinctes de celles qui sont exigées pour les PSEE
- **Les contrôles attendus des établissements assujettis à l'égard de leurs partenaires IOBSP doivent être effectués en suivant une « approche par les risques »**. L'ACPR rappelle que le dispositif de contrôle interne des établissements assujettis doit être cohérent par rapport à la nature de l'intermédiation considérée et à l'importance de la distribution par le

21. Article R519-4 du CMF : **Les mandataires exclusifs** en opérations de banque et en services de paiement (Mandataires exclusifs) exercent l'intermédiation en vertu d'un mandat d'un établissement de crédit ou d'un établissement de paiement et qui sont soumis à une obligation contractuelle de travailler exclusivement avec l'un de ces établissements pour une catégorie déterminée d'opérations de banque ou de services de paiement.
Les mandataires en opérations de banque et en services de paiement exercent l'intermédiation en vertu d'un ou plusieurs mandats non exclusifs (**Mandataires non exclusifs**) délivrés par un ou plusieurs établissements de crédit ou établissements de paiement

22. **Les courtiers en opérations de banque et services de paiement** exercent l'intermédiation en vertu d'un mandat du client, à l'exclusion de tout mandat d'un établissement de crédit ou d'un établissement de paiement, et ne sont pas soumis à une obligation contractuelle de travailler exclusivement avec un établissement de crédit ou un établissement de paiement

23. Il s'agit des mandataires des autres catégories d'IOBSP (Courtiers, mandataires exclusifs ou mandataires non exclusifs). Pour les besoins de nos développements, nous les appellerons les **sous-mandataires**.

canal de l'intermédiation. Les établissements assujettis doivent donc se doter de dispositifs proportionnés de contrôles permanent et périodique de leurs activités confiées à un PSEE (Article 234 de l'arrêté du 3 novembre 2014). Cela implique pour l'établissement assujetti de cibler, grâce à des indicateurs de risques, les IOBSP qui seront contrôlés.

Pour les établissements assujettis à l'arrêté du 3 novembre 2014 qui font appel à des IOBSP, il s'agit de mesurer les conséquences pratiques d'une telle position du régulateur en termes de contrôles.

A cet égard, nous noterons qu'en amont des contrôles, les établissements assujettis mettent en place des indicateurs de risques permettant de contrôler l'activité des IOBSP disposant d'un mandat et de rationaliser la sélection desdits IOBSP qui seront contrôlés par la suite.

Une fois que les IOBSP à contrôler sont sélectionnés, les établissements assujettis effectuent des contrôles sur pièces et/ou sur place, relatifs aux activités déléguées aux mandataires. Nous mettrons donc en exergue les points de contrôles qui peuvent être envisagés et leurs modalités.

5.1 Une approche par les risques pour préparer les contrôles des mandataires, PSEE

Lors de ses contrôles sur pièces et sur place des établissements assujettis, l'ACPR évalue l'adéquation des dispositifs de contrôle interne, y inclus sur base consolidée, au regard de la nature de l'intermédiation considérée ainsi que de l'importance de la distribution par le canal de l'intermédiation. Par conséquent, la mise en d'indicateurs de risques et la délimitation des mandats par les établissements dans leurs relations avec les intermédiaires paraissent déterminantes.

5.1.1 Mise en place d'indicateurs de risques par les établissements assujettis

Les indicateurs de risques mis en place en amont des contrôles par les établissements assujettis permettent de rationaliser les contrôles des mandataires.

Parmi les indicateurs, le régulateur rappelle par exemple la prise en compte :

- du volume des réclamations de la clientèle par mandataire ;

- du taux de défaut des crédits dont le mandataire a été à l'origine ;
- de la qualité de la constitution des dossiers.

Les mandataires contrôlés en priorité par les établissements assujettis sont alors ceux qui présentent un risque plus élevé (ceux pour lequel le volume de réclamations est plus important, ceux qui présentent des dossiers dont la qualité de la constitution est discutable, …). **Evidemment ces critères de risques complètent le premier critère de sélection constitué du volume d'encours des opérations traitées par chaque IOBSP.**

5.1.2 Contrôle des mandats

5.1.2.1 Le mandat des mandataires exclusifs ou non exclusifs

Les contrôles des établissements assujettis et leur responsabilité vis-à-vis des agissements de leurs mandataires sont intrinsèquement liés au périmètre des activités externalisées. Par ailleurs, lorsque l'ACPR effectue des contrôles sur pièce et ou sur place des établissements assujettis, elle peut être amenée à étendre ses contrôles aux PSEE. Le mandat est donc un document clé de la relation contractuelle également pour le régulateur, en cas de contrôle.

A cet égard, il est important que ce document définisse le périmètre de l'externalisation en tenant compte des tâches qui peuvent être prises en charge par le mandataire, de manière effective. En pratique, certains établissements assujettis délèguent par exemple l'authentification des documents d'identité des clients à leurs mandataires (lutte contre le blanchiment de capitaux et contre le financement du terrorisme). Pourtant, ces derniers ne disposent pas des moyens et outils nécessaires à cette authentification (outils coûteux compte tenu de la taille des structures). Une telle pratique est de nature à exposer l'établissement assujetti à un risque de sanction administrative ou d'image.

L'IOBSP peut contrôler les originaux et leur cohérence. Il peut les comparer à l'original qu'il aura vu au préalable. Il lui est même recommandé, compte tenu de ses propres obligations, de contrôler les originaux des documents justificatifs. Le mandat peut donc prévoir ces éléments. Toutefois, il ne pourra pas authentifier ces pièces et garantir qu'il ne s'agit pas de faux.

Autrement dit, le contrôle visuel et de cohérence (absence de ratures, photographies ressemblantes…), qui peut légitimement être exigé de l'IOBSP, (dans le cas où le mandat le prévoit et dans le cas spécifique où l'IOBSP rencontre ses clients en face à face), ne doit pas être confondu avec l'authentification du document qui nécessite des outils adaptés.

Les clauses standards à insérer dans les mandats sont les suivantes:

- la nature et les conditions des opérations que le mandataire est habilité à accomplir pour le compte de l'établissement assujetti ;
- si l'établissement assujetti autorise le mandataire exclusif ou non exclusif à recourir à un sous-mandataire ainsi que, le cas échéant, les modalités de ce recours.

Les clauses prévues par l'arrêté du 3 novembre 2014 :

- niveau de qualité répondant à un fonctionnement normal du service et, en cas d'incident, mécanismes de secours prévus par l'IOBSP ;
- protection des informations confidentielles ayant trait à l'entreprise assujettie et à ses clients ;
- mécanismes de secours en cas de difficulté grave affectant la continuité du service ;
- pas de modification substantielle de la prestation qu'ils assurent sans l'accord préalable de l'entreprise assujettie ;
- conformité aux procédures définies par l'entreprise assujettie concernant l'organisation et la mise en œuvre du contrôle des services qu'ils fournissent ;
- accès, le cas échéant sur place, à toute information sur les services mis à la disposition des établissements, dans le respect des réglementations relatives à la communication d'informations ;
- information de tout événement susceptible d'avoir un impact sensible sur leur capacité à exercer les tâches externalisées de manière efficace et conforme à la législation en vigueur et aux exigences réglementaires ;
- acceptation que l'ACPR ait accès aux informations sur les activités externalisées nécessaires à l'exercice de sa mission, y compris sur place.

5.1.2.2 Le suivi des Courtiers en Opérations de Banque et Services de Paiement (non PSEE)

L'ACPR rappelle que « *Conformément au 1° de l'article R. 519-4 du CMF, le courtier exerce l'intermédiation en vertu d'un mandat du client, à l'exclusion de tout mandat d'un établissement de crédit ou de paiement. Dans ces conditions, l'activité exercée par cette catégorie d'intermédiaires ne saurait relever de l'externalisation telle que définie à l'article 10 r) de l'arrêté du 3 novembre 2014. Il en va de même pour les mandataires auxquels un courtier aurait recours.*
[…]Le courtier et les établissements assujettis peuvent convenir par convention des modalités de mise à disposition de ces informations sur les produits proposés par ceux-ci. En matière d'opération de crédit, une fois que le client a donné son accord sur le produit présenté par le courtier, ce dernier transmet à l'établissement assujetti les informations lui permettant de vérifier notamment la solvabilité du client. »

Bien qu'allégés ou plutôt distincts de ceux prévus pour les PSEE, les contrôles des courtiers par les établissements assujettis ne sont pas pour autant inexistants.
Le régulateur met les établissements assujettis en garde et les encourage à envisager le risque induit par ce canal de distribution dans leur dispositif de contrôle interne (notamment le risque de non-conformité et le risque de crédit).
A minima, il apparaît souhaitable d'apprécier la qualité de ces courtiers selon les mêmes critères de risques (taux de réclamations clientèle, qualité de constitution des dossiers transmis et taux de défaut des opérations traitées). Cette analyse n'est pas forcément un critère de sélection pour le contrôle mais plutôt un suivi des courtiers au titre des contrôles permanents permettant de faire le point avant renouvellement des conventions avec ces courtiers
Ce qui justifie un traitement différencié des courtiers et des mandataires se retrouve dans les obligations complémentaires des courtiers envers leurs clients, permettant de montrer leur indépendance (même si dans l'état actuel des textes, rien n'interdit la rémunération de ces courtiers par les banques à qui les IOBSP ont apporté des dossiers).

Seul le conseil indépendant en matière de crédit immobilier (ou garanti par une hypothèque) ne pourra pas se faire rémunérer par la banque (nouveauté induite par l'ordonnance 2016 -351 du 25 mars 2016 transposant en droit français la directive 2014/17/UE). En effet, les courtiers doivent fonder une analyse objective du marché en se basant sur un nombre suffisant de contrats offerts, fournir au client, y compris au client potentiel, des informations portant sur la description et la comparaison des différents types de contrats disponibles sur le marché pour les opérations et services proposés, de manière personnalisée et adaptée à leur degré de complexité.

Par ailleurs, les courtiers doivent exposer au client les raisons qui motivent ses propositions et indiquer comment il a pris en compte les informations qu'il a recueillies auprès de lui.

Enfin, les courtiers doivent indiquer au client potentiel quels sont ses partenaires bancaires et comment ces partenaires bancaires le rémunèrent.

L'ensemble de ces éléments constituent des règles de bonne conduite applicables aux courtiers et définies dans le décret 2012-101 du 26 janvier 2012.

5.2 Des contrôles sur pièces et/ou sur place

5.2.1 Les modalités de contrôle

Après avoir sélectionné les mandataires qui feront l'objet de contrôles prioritaires (en fonction des indicateurs de risques), les établissements assujettis procèdent à des contrôles sur pièces et/ou sur place. Les contrôles ont pour but de s'assurer du respect du mandat mais également de s'assurer du respect par leurs mandataires du dispositif réglementaire qui leur est applicable.

Il est recommandé aux établissements assujettis de ne pas opter exclusivement pour un type de contrôle plutôt qu'un autre mais de rationaliser le choix entre contrôle sur pièces de certains mandataires et contrôle sur place de certains autres. Ainsi, le contrôle sur place pourrait être privilégié pour les mandataires qui apportent un volume significatif de production et ceux qui présentent un risque plus élevé en fonction des critères de sélection définis plus haut.

Le contrôle sur place peut également être envisagé en complément d'un contrôle sur pièce à la suite duquel le mandataire semble présenter des défaillances significatives (absence de procédures ou de documents justificatifs des conseils apportés au client par exemple).

Globalement, les établissements assujettis devront contrôler :

- le respect par l'intermédiaire de ses **obligations générales** : existence de la société, inscription ORIAS mais aussi honorabilité et capacité professionnelle de ses salariés ;
- la formation du personnel amené à distribuer des crédits, conformément à l'article D311-4-3, III du code de la consommation ainsi que la formation en cas d'évolution réglementaire, sur ce même fondement ;
- le contenu de la **convention signée avec le client** ;
- la documentation commerciale à destination de la clientèle et le site internet (respect des mentions légales) ;
- le processus de traitement des dossiers et l'existence de **procédures écrites** de gestion de la relation clientèle, **conformes à la réglementation**[24] ;
- le respect de la définition légale des différentes catégories d'intermédiaires.
- le respect de l'interdiction du cumul des catégories pour les différentes natures d'activités (crédit à la consommation, regroupement de crédits, crédit immobilier, crédit viager hypothécaire et services de paiement)[25].

A ce titre, **le principe du non cumul doit être effectif**. Cela implique que l'organisation mise en place par l'IOBSP permette au client, au client potentiel mais également au contrôleur d'identifier les activités sans équivoque. Concrètement, le non cumul implique par exemple de distinguer les lieux d'accueil de la clientèle en fonction de l'activité, d'utiliser des adresses faisant apparaître de manière non équivoque la catégorie d'IOSBP, d'utiliser une documentation commerciale/contractuelle permettant au client d'identifier le statut sous lequel intervient son interlocuteur, IOBSP… Cela implique globalement de sensibiliser.

24. R519-20 à R510-26 du CMF
25. R519-4, II du CMF

les collaborateurs sur la transparence dont ils doivent faire preuve face au client Lorsque les IOBSP concernés disposent de sites Internet, ce non cumul doit également être vérifié au travers des informations présentes sur ces sites.

A- Les contrôles sur pièces à distance

Pour tout contrôle sur pièces, il est recommandé au contrôleur de l'établissement assujetti de s'appuyer sur un questionnaire permettant de mieux comprendre l'organisation du mandataire. Ledit questionnaire peut reprendre l'ensemble des obligations du mandataire. Chaque réponse apportée par le mandataire devrait être corroborée par des pièces justificatives.

Aux termes du questionnaire, l'établissement assujetti vérifie les éléments suivants :

- **Existence juridique de l'IOBSP** : coordonnées (adresse, téléphone, le cas échéant le numéro d'immatriculation au RCS, identité des dirigeants). Il convient de demander un extrait Kbis en cas d'immatriculation au RCS ;

- **Enregistrement à l'ORIAS** :
  - immatriculation à l'ORIAS et mise à jour des données: la vérification sur le site de l'ORIAS est facile à mettre en œuvre ;
  - exhaustivité des informations sur les mandats ;
  - exercice de l'activité d'intermédiaire à titre principal ou accessoire et répartition du CA par activité[26] ;
  - catégorie(s) et contrôle de l'interdiction du cumul des catégories. **Le questionnaire comprend alors les questions de nature à évaluer le respect de cette règle par le mandataire**.

- **Conditions d'accès à la profession**[27]
  - existence de justificatifs pouvant attester la capacité professionnelle des salariés dès leur prise de fonction (pour les mandataires sociaux,

26. R519-1 du CMF
27. R519-8 à R519-12 du CMF

cette capacité professionnelle est vérifiée par l'ORIAS au moment de l'immatriculation)

* Le candidat a-t-il un diplôme prévu dans la bonne catégorie du RNCP (Répertoire National des Certifications Professionnelles)?
* Le candidat a-t-il reçu une formation préalable ?
* Le candidat justifie-t-il d'une expérience suffisante ?

› si les salariés n'avaient pas encore la formation suffisante, leur prise de poste a-t-elle été adaptée (vérifier que les salariés en cours de formation n'ont pas eu d'objectifs commerciaux dans le contrat de travail) ;

› existence d'un suivi documenté de la capacité professionnelle:

*Formation continue, notamment en cas d'évolution réglementaire ou d'évolution d'activité

- **Assurance en responsabilité civile[28] et Garantie financière[29]** (si les clients confient des fonds à l'IOBSP). L'IOBSP doit :
  - › pouvoir justifier à tout moment de sa situation en termes de responsabilité civile et de garantie financière ;
  - › adapter sa garantie financière aux montants encaissés. (ce cas se rencontre assez peu pour les IOBSP).

- **Traitement des réclamations :**
  - › existence d'une procédure écrite ? (si oui, demander cette procédure) ; Délais de réponse prévus dans la procédure ? Lorsqu'un numéro de téléphone est proposé, est-il non surtaxé ? Les réponses apportées au client, sont-elles écrites (traçabilité)?

- **Nombre d'acteurs dans la chaîne d'intermédiaires : le Code monétaire et financier interdit la mise en place d'une chaîne de plus de deux intermédiaires consécutifs.** Lorsque le mandataire est autorisé à recourir à un sous-mandataire, il faut vérifier qu'il avait prévenu l'établissement financier avant de contractualiser avec un MIOB, Mandataire d'Intermédiaire en Opérations

28. R519-16 du CMF
29. R519-17 du CMF

de Banque, (si le mandat prévoit cette clause d'information ou accord préalable).
Par ailleurs, lorsqu'un IOBSP recourt à des indicateurs d'affaires, il s'agit de vérifier que l'IOBSP a bien les relations directes avec le client qui lui a été apporté et qu'il mène l'ensemble des diligences envers ce client comme s'il l'avait acquis en direct.

En effet, les décrets du 26 janvier 2012 sur les IOBSP ont distingué clairement l'IOBSP de l'indicateur d'affaires. Ainsi, l'indicateur d'affaires qui intervient contre rémunération ou à titre gratuit, est exclu du champ des obligations applicables aux IOBSP (et donc n'a pas à être immatriculé à l'ORIAS). Son activité doit se restreindre à :

- indiquer un établissement de crédit ou un IOBSP à un client potentiel ou existant ;
- lui transmettre des documents publicitaires ;
- transmettre les coordonnées d'un client potentiel ou existant à un établissement de crédit.

B- Les contrôles sur place

Le contrôle sur place peut être réalisé sous plusieurs formes :

- **la technique du client mystère**. Le contrôleur se présente comme étant un client afin de se rendre compte de l'existence d'une procédure conforme à la réglementation ;
- **le contrôle « classique »**. Dans ce dernier cas, les pièces seront collectées et demandées sur place. Le contrôleur pourra, s'il l'estime utile, assister au traitement d'une demande d'un client par un collaborateur du mandataire.

Lors de ce contrôle, il s'agit de vérifier des éléments tels que :

- l'existence et la conformité des procédures écrites (gestion de la relation clientèle, traitement des réclamations, LCB-FT, …) si elles n'ont pas déjà été analysées dans le cadre d'un contrôle à distance ;

- le respect des procédures et la pertinence de la documentation diffusée au client (par analyse d'un échantillon de dossiers clients par exemple) ;
- les affichages en agence (respect des mentions légales sur les documents publicitaires et affichage des informations dues au client y compris au client potentiel, …) ;
- le respect des règles d'archivage des documents ;
- le cas échéant, les contrôles permanents mis en place en interne (contrôle des MIOBSP - Mandataire d'Intermédiaires en Opérations de Banque et Services de Paiement - ou des franchisés notamment) et le suivi des recommandations issues desdits contrôles (plan de contrôle, formalisation des contrôles internes, …) ;
- lorsque l'IOBSP exerce au titre de plusieurs activités, le contrôleur s'assure que la distinction entre les activités est claire (lieux d'accueil de la clientèle distincts en fonction de l'activité ou bien pancartes et affichages différents, …).

Par ailleurs, lorsque le recours à des sous-mandataires est prévu aux termes du mandat, les établissements assujettis doivent intégrer lesdits sous-mandataires dans leur plan de contrôle (voir §5.2.2. ci-dessous)

Enfin, les contrôles sur pièces et sur place supposent que l'établissement qui contrôle soit mis en mesure de vérifier le respect de la réglementation grâce à des éléments de preuve fournis par les mandataires. Cela implique que lesdits mandataires disposent de procédures et documents probants, formalisés sur support durable (procédures, documents contractuels, documents d'information/conseil[30] …).

C'est pourquoi il est important que les établissements informent et sensibilisent leurs mandataires sur la nature des éléments qu'ils s'attendent à trouver.

5.2.2. Le nécessaire déploiement des contrôles en interne par les IOBSP

Pour se conformer aux exigences du régulateur[31] ou des établissements assu-

30. R519-23 du CMF
31. L'ACPR peut soumettre à contrôle tout IOBSP (II art. L. 612-2 du CMF), qu'il soit mandataire ou courtier

jettis partenaires mais également dans la perspective d'améliorer la qualité du service rendu, il paraît important que les IOBSP accompagnent leurs procédures de dispositifs de contrôles directement au sein de leurs structures.
De nombreux IOBSP font partie de très petites structures et fonctionnent seuls. D'autres IOBSP font le choix d'une organisation en franchises. Enfin de plus en plus d'intermédiaires sont organisés en réseau ou sous une marque commune, notamment pour bénéficier d'un poids plus grand dans les négociations avec les partenaires bancaires ; par ailleurs, certains IOBSP ont eux-mêmes contractualisé avec un nombre important de MIOB. En fonction de la nature de la structure, les contrôles internes des IOBSP peuvent se décliner de la façon suivante :

- **« un contrôle interne standard » attendu de tout IOBSP**

Lorsque la taille de la structure le permet, les IOBSP, toutes catégories confondues, mettent en place un contrôle hiérarchique des actions de leurs collaborateurs. Ils s'assurent que ces derniers se conforment aux procédures internes et aux exigences réglementaires.

- **les réseaux de franchise**

Dans la mesure où la taille de la structure le permet, un contrôle interne standard sera réalisé par chaque franchisé (dirigeant de la franchise par exemple), sur les actions de ses collaborateurs (contrôle interne standard).
Au contrôle interne standard peut s'ajouter un contrôle du franchiseur sur ses franchisés. Compte tenu de l'indépendance des franchises, la supervision par le franchiseur sur les membres de son réseau n'est pas une obligation. Toutefois, elle permettrait au franchiseur de maîtriser le risque d'image en cas de défaillance d'un franchisé. Le cas échéant, cette possibilité de contrôle par le franchiseur peut être intégrée dans le contrat de franchise. Le franchiseur peut également imposer des procédures aux membres de son réseau en prévoyant cette obligation dans le contrat de franchise.
Pour rappel, les franchisés sont des entreprises indépendantes juridiquement[32].

32. Article A441-1 du code de commerce

Elles sont responsables de leurs actions en interne. Elles ne peuvent s'appuyer sur une défaillance de leur franchiseur pour s'exonérer de leurs obligations réglementaires. Dans la mesure où aucune procédure ne serait proposée par le franchiseur ou, lorsque la procédure du franchiseur leur paraît non-conforme, les franchisés apportent les correctifs utiles.

- **les réseaux de MIOB (Mandataire d'intermédiaires en Opérations de Banque)**

Au contrôle interne standard évoqué ci-dessus s'ajoute le contrôle périodique des mandataires exclusifs ou non exclusifs à l'égard de leurs sous-mandataires (MIOB).

L'ensemble des contrôles réalisés par la banque sur ses mandataires doit être transposé vers les MIOB. Chaque établissement doit donc demander à ses mandataires les résultats des contrôles réalisés par le mandataire sur ses sous-mandataires, la formation qu'il leur a dispensée, les procédures qu'il leur demande d'appliquer.

ANNEXES

- Annexe 1 : Clause à insérer dans les contrats portant sur les prestations de services essentielles ;
- Annexe 2 : Références des réglementations étrangères et textes internationaux ;
- Annexe 3 : Dispositions du RG AMF applicables aux SGP ;
- Annexe 4 : Addendum « Audit des prestations informatiques » ;

ANNEXE 1

Clause à insérer dans les contrats portant sur des prestations de services essentielles conclus avec des délégataires par les entreprises assujetties à l'arrêté du 3 novembre 2014

Les prestations de services faisant l'objet du présent contrat sont considérées comme des

prestations de services ou autres tâches opérationnelles essentielles ou importantes à l'activité du client (au sens de l'article 10 r de l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution).

Conformément aux dispositions de l'arrêté du 3 novembre 2014 précité, le délégataire s'engage expressément à :

- respecter les dispositions du présent contrat, de ses annexes et avenants concernant :
  - le niveau de qualité attendu de ses prestations pour répondre à un fonctionnement normal du service ;
  - la mise en œuvre, en cas d'incident, de difficulté grave ou de force majeure, des mécanismes de secours permettant au client de bénéficier de la continuité du service[33] ;
  - les procédures définies par le client concernant l'organisation et la mise en œuvre du contrôle des prestations qu'il fournit au titre du présent contrat ;
  - le compte rendu régulier de la manière dont est exercée l'activité qui lui est confiée et de sa situation financière.
- permettre l'accès, à chaque fois que le client l'estimera nécessaire, au client ou à ses délégataires le cas échéant sur place, à toute information relative

33.Si le prestataire refuse de mettre en place des mécanismes de secours, le client peut l'accepter sous réserve d'avoir prévu, dans son propre plan de continuité d'activité, le risque de défaillance du prestataire.

aux prestations fournies, dans le respect des réglementations relatives à la communication d'informations ;

- accepter que l'ACPR [ou toute autre autorité étrangère équivalente au sens des articles L. 613-12 et L. 613-13 du Code monétaire et financier][34], ait accès, y compris sur place, aux informations nécessaires à sa mission et portant sur les prestations faisant l'objet du présent contrat ;

- recueillir l'accord exprès et écrit du client :
  - avant de procéder à toute modification des prestations faisant l'objet du présent contrat ;
  - avant de déléguer tout ou partie des prestations faisant l'objet du présent contrat à un tiers, ou de conclure avec un tiers un contrat de prestation de services ou de sous-traitance touchant à ces activités. Ce contrat devra inclure l'ensemble des engagements résultant de la présente clause.

Annexe 1 bis

Clause FBF[35] : « Dans le cas où une prestation similaire est rendue à plusieurs établissements bancaires, le prestataire accepte que ces établissements ou leur(s) délégataire(s) puissent conduire des missions d'audit pour compte commun sur les conditions de réalisation de cette prestation et sur sa conformité aux clauses contractuelles ».

34. A ne faire figurer que lorsque le prestataire est situé dans un pays étranger (européen ou extra-européen).
35. Note de la FBF du 29 septembre 2009 présentant le dispositif de contrôle des activités externalisées à des prestataires communs (annexe 8 page 65).

ANNEXE 2

Références des réglementations étrangères et textes internationaux

EBA

https://www.eba.europa.eu/documents/10180/104404/GL02+Outsourcing_+Feedback.pdf

Réglementation luxembourgeoise

Circulaire CSFF 13/563 du 19 mars 2013 (sous-chapitre 7.4)

www.cnpd.lu

Réglementation suisse

Circulaire 2008/7 « Outsourcing - Banques » (Externalisation d'activités dans le secteur bancaire)

https://www.finma.ch/fr/documentation/circulaires/#Adressaten=%7B2C383DE0-169E- 4A28-8ADD- C8A8F6FFC9ED%7D&Order=2

Réglementation britannique

FSA Handbook

www.fsa.gouv.uk

Réglementation américaine

Federal Reserve System

Division of banking supervision and regulation

www.federalreserve.gov

Réglementation australienne

APRA (Australian Prudential Regulation Authority)

Guidance Note AGN .313.1 Managing Outsourcing

www.apra.gouv.au

Réglementation de Singapour

Monetary Authority of Singapour

Guidelines on outsourcing (octobre 2004, actualisées en juillet 2005) (http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing20Guidelines) | www.mas.gov.sg

Réglementation de Hong Kong

Hong Kong Monetary Authority

Supervisory Policy Manual Circular 12/0998 (du 28 décembre 2001)

www.info.gov.hk/hkma

Réglementation de Taiwan

The Bureau of Monetary Affairs (BOMA)

“The outsourcing Guidelines for financial Institution 2005”

"Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation" de février 2012 avec amendements apportés le 9 mai 2014. (http://www.leeandli.com/web/bulletin/artical.asp?id=4767) (http://law.fsc.gov.tw/law/EngLawContent.aspx?id=FL040528)

www.banking.gov.tw

Réglementation indienne

Reserve Bank of India

http://www.rbi.org.in/home.aspx

Réglementation marocaine

Bank Al Maghrib

http://www.bkam.ma/

Norme ISAE 3402 | http://isae3402.com/

Quelques exemples d’outsourcing présenté par FINMA (annexe de la circulaire FINMA 2008/7) http://www.finma.ch/f/regulierung/Documents/finma-rs-2008-07-f.pdf

ANNEXE 3

Dispositions du RG-AMF applicables aux SGP

Article 313-72

Lorsque la société de gestion de portefeuille confie à un tiers l'exécution de tâches ou fonctions opérationnelles essentielles ou importantes pour la fourniture d'un service ou l'exercice d'activités, elle prend des mesures raisonnables pour éviter une aggravation indue du risque opérationnel. L'externalisation de tâches ou fonctions opérationnelles essentielles ou importantes ne doit pas être faite de manière qui nuise sensiblement à la qualité du contrôle interne et qui empêche l'AMF de contrôler que la société de gestion de portefeuille respecte bien toutes ses obligations. Toute externalisation d'une ampleur telle que la société de gestion de portefeuille serait transformée en boîte aux lettres doit être considérée comme contrevenant aux conditions que la société de gestion de portefeuille est tenue de respecter pour obtenir et conserver son agrément.

Article 313-73

L'externalisation consiste en tout accord, quelle que soit sa forme, entre la société de gestion de portefeuille et un prestataire de services en vertu duquel ce prestataire prend en charge un processus, un service ou une activité qui aurait autrement été du ressort de la société de gestion de portefeuille elle-même.

Article 313-74

1. Une tâche ou fonction opérationnelle est considérée comme essentielle ou importante lorsqu'une anomalie ou une défaillance dans son exercice est susceptible de nuire sérieusement soit à la capacité de la société de gestion de portefeuille de se conformer en permanence aux conditions et aux obligations de son agrément ou à ses obligations professionnelles mentionnées au II de l'article L. 621-15 du code monétaire et financier, soit à ses

performances financières, soit à la continuité de ses activités. En particulier, la présente sousection s'applique en cas d'externalisation d'un service d'investissement ;

2. Sans préjudice de l'appréciation de toute autre tâche ou fonction, les tâches ou fonctions suivantes ne sont pas considérées comme des tâches ou fonctions essentielles ou importantes :

- La fourniture au bénéfice de la société de gestion de portefeuille de services de conseil et autres services ne faisant pas partie des services d'investissement, y compris la fourniture de conseils juridiques, la formation du personnel, les services de facturation et la sécurité des locaux et du personnel de la société de gestion de portefeuille ;
- L'achat de prestations standards, y compris des services fournissant des informations de marché ou des flux de données sur les prix.

Article 313-75

1. La société de gestion de portefeuille qui externalise une tâche ou fonction opérationnelle demeure pleinement responsable du respect de toutes ses obligations professionnelles mentionnées au II de l'article L. 621-15 du code monétaire et financier et se conforme en particulier aux conditions suivantes :

- L'externalisation n'entraîne aucune délégation de la responsabilité des dirigeants ;
- L'externalisation ne modifie ni les relations de la société de gestion de portefeuille avec ses clients ni ses obligations envers ceux-ci ;
- L'externalisation n'altère pas les conditions ou les engagements auxquels était subordonné son agrément.

2. La société de gestion de portefeuille agit avec toute la compétence, le soin et la diligence requis lorsqu'elle conclut, applique ou met fin à un contrat d'externalisation d'une tâche ou fonction opérationnelle essentielle ou

importante. La société de gestion de portefeuille est en particulier tenue de prendre toutes les mesures pour que les conditions suivantes soient remplies :

a. Le prestataire de services dispose des capacités, de la qualité et des éventuelles habilitations requises pour exécuter les tâches ou fonctions externalisées de manière fiable et professionnelle ;
b. Le prestataire de services fournit les services externalisés de manière efficace. A cet effet, la société de gestion de portefeuille définit des méthodes d'évaluation du niveau de performance du prestataire de services ;
c. Le prestataire de services surveille de manière appropriée l'exécution des tâches ou fonctions externalisées et gère de manière adéquate les risques découlant de l'externalisation ;
d. La société de gestion de portefeuille prend des mesures appropriées s'il apparaît que le prestataire de services risque de ne pas s'acquitter de ses tâches ou fonctions de manière efficace ou conforme aux obligations professionnelles mentionnées au II de l'article L. 621-15 du code monétaire et financier qui leur sont applicables ;
e. La société de gestion de portefeuille conserve l'expertise nécessaire pour contrôler effectivement les tâches ou fonctions externalisées et gère les risques découlant de l'externalisation, et procède au contrôle de ces tâches et à la gestion de ces risques ;
f. Le prestataire de services informe la société de gestion de portefeuille de tout événement susceptible d'avoir un impact sensible sur sa capacité à exécuter les tâches ou fonctions externalisées de manière efficace et conforme aux obligations professionnelles mentionnées au II de l'article L. 621-15 du code monétaire et financier qui leur sont applicables ;
g. Les modalités de résiliation du contrat d'externalisation à l'initiative de l'une quelconque des parties doivent permettre d'assurer la continuité et la qualité des activités exercées ;
h. Le prestataire de services coopère avec l'AMF pour tout ce qui concerne les tâches ou fonctions externalisées ;

i. La société de gestion de portefeuille, les personnes chargées du contrôle de ses comptes et les autorités compétentes ont un accès effectif aux données relatives aux tâches ou fonctions externalisées et aux locaux professionnels du prestataire de services ;

j. Le prestataire de services assure la protection des informations confidentielles ayant trait à la société de gestion de portefeuille ou à ses clients ;

k. La société de gestion de portefeuille et le prestataire de services établissent, mettent en place et gardent opérationnel un plan d'urgence permettant le rétablissement de l'activité après un sinistre et prévoyant un contrôle régulier des capacités de sauvegarde, dans tous les cas où cela apparaît nécessaire eu égard à la nature de la tâche ou la fonction externalisée.

3. Les droits et obligations respectifs de la société de gestion de portefeuille et du prestataire de services sont clairement définis dans un contrat ;

4. Pour définir les modalités d'application du présent article, lorsque la société de gestion de portefeuille et le prestataire de services appartiennent au même groupe ou relèvent du même organe central, la société de gestion de portefeuille peut prendre en compte la mesure dans laquelle elle contrôle le prestataire de services ou peut exercer une influence sur ses actions ;

5. La société de gestion de portefeuille fournit à l'AMF, à la demande de celle-ci, toutes les informations nécessaires pour lui permettre de vérifier que les tâches ou fonctions externalisées sont effectuées conformément aux exigences du présent livre.

ANNEXE 4

Addendum « Audit des prestations informatiques »

Les prestations informatiques externalisées sont soumises aux mêmes programmes d'audit et objectifs de contrôle que ceux définis dans la partie Audit chez le délégataire de ce cahier de recherche. Toutefois, les prestations informatiques sont caractérisées par le fait qu'elles sont supportées par une documentation spécifique et qu'elles nécessitent des compétences d'audit spécialisées. Par ailleurs, il est nécessaire de circonscrire au préalable, parmi les différentes formes de prestations informatiques, le périmètre des prestations informatiques éligibles à la qualification de prestation informatique externalisée au sens de l'arrêté du 3 novembre 2014.

Cette annexe a précisément pour objet de :

- fournir une typologie des différentes prestations informatiques, mise en perspective avec l'article 10q de l'arrêté du 3 novembre 2014 ;

- détailler les éléments du patrimoine documentaire d'un délégataire informatique à prendre en compte dans le cadre de l'audit ;

- préciser les diligences à mettre en œuvre sur les Plans d'Assurance Qualité (PAQ) des prestations informatiques, ces documents complétant fréquemment les SLA (vue externe du service) des dispositions prises par le délégataire pour satisfaire les exigences définies dans le contrat de prestation.

Périmètre des prestations informatiques externalisées

L'infogérance, qu'elle soit globale ou partielle, rentre naturellement dans le champ des activités externalisées telles que définies par l'article 10q de l'arrêté du 3 novembre 2014. S'agissant de la sous-traitance informatique, le type de recours (durable et habituel, ou au contraire ponctuel) déterminera si la prestation est visée ou non par les dispositions de l'arrêté du 3 novembre 2014 objets de cette analyse. La dernière forme de prestation informatique (apport ponctuel

de ressources) sort quant à elle du champ des activités externalisées définies par l'arrêté du 3 novembre 2014, la mise à disposition de personnel (interne ou externe) étant par essence temporaire et s'exerçant de surcroît sans qu'une réelle autonomie ne soit conférée au délégataire (les collaborateurs concernés étant intégrés au sein des équipes du délégant et supervisés comme tels).

Audit de la prestation chez le délégataire

Auditabilité de la prestation

Outre les documentations listées au paragraphe 4.1.2 de ce document, les sources d'information suivantes peuvent être exploitées avec profit dans le cadre de l'audit d'un délégataire informatique : cahier de charges, procédures organisationnelles et d'exploitation, fiches d'intervention (maintenance corrective), demandes d'évolution (maintenance évolutive), spécifications techniques ou fonctionnelles, Plan d'Assurance Qualité (PAQ), cartographie du système d'information.

Revue de la conformité de la prestation par rapport aux engagements contractuels

Pour les prestations informatiques, et notamment en matière d'infogérance, la convention de services est fréquemment complétée par un plan d'assurance qualité (PAQ), qui comprend les dispositions prises par le délégataire pour satisfaire les exigences définies dans le contrat de prestation.

Les travaux d'audit consisteront à vérifier l'existence, la pertinence et la permanence des dispositions inscrites dans le plan d'assurance qualité du délégataire (si ce dispositif est bien d'application pour la prestation visée).

En premier lieu, l'audit devra s'assurer que l'objectif du plan est clairement défini et applicable au contrat de prestation concerné, et que le patrimoine documentaire[36] du plan est correctement référencé et actualisé selon le cycle de vie de la prestation.

36.Notamment : les procédures, les spécifications, les plannings, …

La définition des rôles et des responsabilités de deux parties (client et fournisseur), l'organisation de l'équipe délégataire ainsi que les modalités de pilotage et de coordination de la prestation doivent également faire l'objet d'une analyse de l'audit, pour s'assurer notamment de la prise en compte dans le plan, de la nécessaire séparation des fonctions entre la maîtrise d'ouvrage et la maîtrise d'œuvre de la prestation (en mode projet), ou entre les équipes de conception, les équipes de développement et les équipes d'exploitation des logiciels supports ou objets de la prestation (en mode production).

La mise en œuvre de la prestation (au sein du plan d'assurance qualité (PAQ) le cas échéant) selon des processus clés permettra par ailleurs à l'audit d'appréhender le niveau de maîtrise de la prestation par le fournisseur du service. A titre d'exemples, les processus suivants ont vocation à être audités: suivi de la production, gestion des évolutions, gestion des incidents, gestion du planning, gestion des sous-traitants, gestion de la communication.

La déclinaison des spécifications du service selon des modalités pratiques de mise en œuvre (standards, méthodes et moyens utilisés par le délégataire pour répondre aux besoins de son client) fera l'objet d'une revue approfondie de la part de l'audit.

De la même façon, le contrôle de la qualité de la prestation par le délégataire (par exemple : détermination d'indicateurs qualité et de tableaux de bord dédiés au suivi de la prestation, contrôle exercé par l'audit interne du délégataire) doit être inclus dans le périmètre de l'audit dans le cadre de sa revue.

Enfin, la revue par l'audit des conditions d'application des processus clés (notamment : situations d'exception pouvant justifier une dérogation à leur application) devra permettre de conclure sur le caractère effectif et fiable de la mise en œuvre de ces processus.