Annexe à la lettre du Secrétaire général de l'Autorité de contrôle prudentiel et de résolution
à la Directrice générale de l'Association française des établissements de crédit et des entreprises d'investissement

Octobre 2015

Rapport sur le contrôle interne

(Rapport établi en application des articles 258 à 266 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)

Sommaire

Préambule

Ce rapport a pour objet de rendre compte de l'activité du contrôle interne au cours de l'exercice écoulé et de retracer les dispositifs de mesure, de surveillance, d'encadrement des risques auxquels l'établissement est exposé et de diffusion d'information à leur sujet.

Les éléments ci-après mentionnés le sont à titre indicatif dans la mesure où ils s'avèrent pertinents au vu de l'activité et de l'organisation de l'établissement. Ils sont complétés par toute autre information de nature à permettre une appréciation du fonctionnement du système de contrôle interne et une évaluation des risques effectifs de l'établissement.

Le présent document s'appuie sur une version « fusionnée » des rapports établis en application des articles 258 à 266 de l'arrêté du 3 novembre 2014. Toutefois, les établissements qui le souhaitent peuvent continuer de remettre des rapports distincts dès lors que ces derniers couvrent l'ensemble des éléments mentionnés ci-après.

Les derniers documents transmis par les dirigeants effectifs à l'organe de surveillance et, le cas échéant, au comité des risques, en application de l'article 253 de l'arrêté du 3 novembre 2014, sur l'analyse et le suivi des risques auxquels l'établissement est exposé doivent être inclus dans le présent rapport (tableaux de bord internes).

Par ailleurs, il est précisé que les documents examinés par l'organe de surveillance dans le cadre de l'examen de l'activité et des résultats du contrôle interne, en application des articles 252 et 253 de l'arrêté du 3 novembre 2014, doivent être adressés au Secrétariat général de l'Autorité de contrôle prudentiel et de résolution (SGACPR), ou à la Banque centrale européenne (BCE) selon les cas, sans attendre les extraits des procès-verbaux des réunions au cours desquelles ils sont examinés et qui doivent également être transmis au SGACPR ou à la BCE selon les cas dès qu'ils sont disponibles.

La rédaction est en français. Par exception, les rapports des établissements soumis à la supervision directe de la BCE peuvent être rédigés en anglais, à l'exception des parties relevant des champs de compétence en propre de l'ACPR (parties 7, 8, 12, 18, 19, 20, 21 et annexe 3).

N.B. : lorsque l'établissement fait l'objet d'une surveillance sur une base consolidée et/ou d'une surveillance complémentaire au titre des conglomérats financiers, les rapports sur le contrôle interne comprennent une information relative aux conditions dans lesquelles le contrôle interne est assuré au niveau de l'ensemble du groupe et/ou du conglomérat. Lorsque le dispositif de contrôle interne d'une filiale est totalement intégré au dispositif du groupe, il n'est pas nécessaire de remettre un rapport relatif à l'organisation du contrôle interne pour cette filiale. En revanche les dispositifs de mesure, de surveillance et d'encadrement des risques doivent être exposés pour chaque établissement assujetti.

1. Présentation générale des activités exercées et des risques encourus par l'établissement

1.1. Description des activités :

– description synthétique des activités exercées ;

– cartographie synthétique des activités de négociation sur instruments financiers exercées (pour les établissements assujettis au titre Ier de la loi n°2013-672 du 26 juillet 2013 de séparation et de régulation des activités bancaires) ;

– pour les nouvelles activités :
  - description détaillée des nouvelles activités exercées par l'établissement au cours du dernier exercice (par métiers et/ou zones géographiques et/ou filiales…),
  - présentation des procédures définies pour ces nouvelles activités,
  - description du contrôle interne des nouvelles activités ;

– description des changements organisationnels ou humains importants et des projets significatifs lancés ou menés au cours du dernier exercice.

1.2. Présentation des principaux risques générés par les activités exercées par l'établissement :

– description, formalisation et mise à jour de la cartographie des risques ;

– description des actions mises en œuvre sur les risques identifiés par la cartographie ;

– présentation des informations quantitatives et qualitatives des risques présentés dans les états de synthèse transmises aux dirigeants effectifs, à l'organe de surveillance, et le cas échéant au comité des risques et au comité *ad hoc* permettant d'expliciter la portée des mesures utilisées pour évaluer le niveau des risques encourus et fixer les limites (cf. article 230 de l'arrêté du 3 novembre 2014).

1.3. Présentation de la stratégie et de la politique en matière de risques :

– description des processus mis en place pour détecter, gérer, suivre et déclarer chaque risque significatif (cf. article L.511-55 du Code monétaire et financier) ;

– préciser le cadre d'appétence pour le risque, ses modalités de définition et de révision (cf. article L.511-93 du Code monétaire et financier).

2. Modifications significatives apportées à l'organisation du dispositif de contrôle interne

Lorsque l'organisation du dispositif de contrôle interne ne présente pas de changements significatifs, elle peut être présentée de manière synthétique dans une annexe ou en communiquant la charte de contrôle interne en vigueur.

***Nota bene** : Pour l'exercice 2015, cette partie devra inclure une description des adaptations prises par l'établissement pour se mettre en conformité avec les nouvelles dispositions introduites par la transposition de la directive CRDIV et par 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'ACPR.*

2.1. Au dispositif de contrôle permanent (y compris l'organisation du contrôle de l'activité à l'étranger et des activités externalisées) :

– description des changements significatifs dans l'organisation du dispositif de contrôle permanent (y compris les principales actions projetées dans le domaine du contrôle permanent, cf. article 259 f) de l'arrêté du 3 novembre 2014) : *préciser notamment l'identité, le rattachement hiérarchique et fonctionnel du responsable de contrôle permanent ainsi que les autres fonctions éventuellement exercées par ce dernier au sein de l'établissement ou au sein d'autres entités du même groupe ;*

- description des changements significatifs dans l'organisation du dispositif de contrôle de la conformité : *préciser notamment l'identité, le rattachement hiérarchique et fonctionnel du responsable de la conformité ainsi que les autres fonctions éventuellement exercées par ce dernier au sein de l'établissement ou au sein d'autres entités du même groupe* ;
- description des changements significatifs dans l'organisation des comités des risques, des nominations et des rémunérations (le cas échéant) : *préciser notamment la date de constitution, la composition, la durée du mandat, les modalités de fonctionnement et les compétences de chaque comité* ;
- description des changements significatifs dans l'organisation du dispositif de lutte contre le blanchiment des capitaux et le financement du terrorisme – LCB/FT ;
- description des changements significatifs dans l'organisation de la fonction de gestion des risques : *préciser notamment l'identité, le positionnement hiérarchique et fonctionnel du responsable de la fonction de gestion des risques ainsi que les autres fonctions éventuellement exercées par ce dernier au sein de l'établissement ou au sein d'autres entités du même groupe* ;
- description synthétique des modifications apportées à l'ensemble du dispositif de contrôle permanent pour assurer le respect du titre Ier de la loi n°2013-672 du 26 juillet 2013 de séparation et de régulation des activités bancaires pour les établissements assujettis.

2.2. Au dispositif de contrôle périodique (y compris l'organisation du contrôle de l'activité à l'étranger et des activités externalisées) :

- identification, rattachement hiérarchique et fonctionnel du responsable de contrôle périodique ;
- description des changements significatifs dans l'organisation du dispositif d'audit interne ;
- principales actions projetées dans le domaine du contrôle périodique (plan d'audit… cf. article 259 f) de l'arrêté du 3 novembre 2014).

3. Gouvernance

***Nota bene** : Pour l'exercice 2015, cette partie devra inclure une description des adaptations prises par l'établissement pour se mettre en conformité avec les nouvelles dispositions introduites par la transposition de la directive et par 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'ACPR.*

3.1. Implication des organes dirigeants dans le contrôle interne

3.1.1. Modalités d'information de l'organe de surveillance et, le cas échéant, du comité des risques :

- modalités d'information de l'organe de surveillance ainsi que, le cas échéant, du comité des risques sur les mesures prises pour assurer le contrôle des activités externalisées et des risques en résultant (cf. article 253 c) de l'arrêté du 3 novembre 2014) ;
- modalités d'approbation des limites par l'organe de surveillance ainsi que, le cas échéant, par le comité des risques (cf. article 224 de l'arrêté du 3 novembre 2014) ;
- modalités d'information de l'organe de surveillance, de l'organe central, ainsi que, le cas échéant, du comité des risques en cas de survenance d'incidents significatifs au sens de l'article 98 (cf. article 245 de l'arrêté du 3 novembre 2014) ;
- modalités d'information de l'organe de surveillance, de l'organe central et, le cas échéant, du comité des risques sur les anomalies significatives détectées par le dispositif de suivi et d'analyse en matière de LCB/FT ainsi que sur les insuffisances de ce dispositif (cf. article 246 de l'arrêté du 3 novembre 2014) ;
- si nécessaire, modalités d'information de l'organe de surveillance, ou le cas échéant du comité des risques, par le responsable de la fonction de gestion des risques, en précisant les sujets concernés (cf. article 77 de l'arrêté du 3 novembre 2014) ;

- modalités d'information de l'organe de surveillance et, le cas échéant, du comité des risques, par les responsables du contrôle périodique, de l'absence d'exécution des mesures correctrices décidées (cf. article 26 b) de l'arrêté du 3 novembre 2014) ;
- conclusions des contrôles effectués portés à la connaissance de l'organe de surveillance ainsi que, le cas échéant, du comité des risques, et en particulier éventuelles défaillances relevées, et mesures décidées pour y remédier (cf. article 243 de l'arrêté du 3 novembre 2014).

3.1.2. Modalités d'information des dirigeants effectifs :

- modalités d'information des dirigeants effectifs en cas de survenance d'incidents significatifs au sens de l'article 98 de l'arrêté du 3 novembre 2014 (cf. article 245 de l'arrêté du 3 novembre 2014) ;
- modalités d'information des dirigeants effectifs sur les anomalies significatives détectées par le dispositif de suivi et d'analyse en matière de LCB/FT ainsi que sur les insuffisances de ce dispositif (cf. article 246 de l'arrêté du 3 novembre 2014) ;
- modalités d'information par le responsable de la fonction de gestion des risques de l'exercice de ses missions aux dirigeants effectifs (cf. article 77 de l'arrêté du 3 novembre 2014) ;
- modalités d'alerte des dirigeants effectifs, par le responsable de la fonction de gestion des risques, de toute situation susceptible d'avoir des répercussions significatives sur la maîtrise des risques (cf. article 77 de l'arrêté du 3 novembre 2014).

3.1.3. Diligences effectuées par les dirigeants effectifs et l'organe de surveillance :

- description des diligences effectuées par les dirigeants effectifs et l'organe de surveillance pour vérifier l'efficacité des dispositifs et procédures de contrôle interne (cf. articles 241 à 243 de l'arrêté du 3 novembre 2014).

3.1.4. Traitement des informations par l'organe de surveillance :

- modalités d'examen du dispositif de gouvernance et d'évaluation périodique de son efficacité (cf. article L.511-59 du Code monétaire et financier) ;
- modalités d'approbation et de révision régulière des stratégies et politiques en matière de risques (cf. article L.511-60 du Code monétaire et financier) ;
- modalités de détermination des orientations et du contrôle de la mise en œuvre des dispositifs de surveillance afin de garantir une gestion efficace et prudente de l'établissement (cf. article L.511-67 du Code monétaire et financier) ;
- modalités d'adoption et de révision des principes généraux de la politique de rémunération et de sa mise en œuvre (cf. article L.511-72 du Code monétaire et financier) ;
- dans le cadre de l'examen par l'organe de surveillance des incidents significatifs révélés par les procédures de contrôle interne, principales insuffisances constatées, enseignements tirés de l'analyse et mesures prises le cas échéant pour y remédier (cf. article 252 de l'arrêté du 3 novembre 2014) ;
- dates auxquelles l'organe de surveillance a examiné l'activité et les résultats du contrôle interne au cours de l'exercice écoulé ;
- dates d'approbation des limites globales de risques par l'organe de surveillance, après consultation le cas échéant du comité des risques (cf. article 224 de l'arrêté du 3 novembre 2014).

3.2. Politique et pratiques de rémunération (y compris pour les filiales et succursales situées à l'étranger)

***Nota bene** : Pour l'exercice 2015, cette partie devra inclure une description des adaptations prises par l'établissement pour se mettre en conformité avec les nouvelles dispositions introduites par la transposition de la directive et par 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'ACPR.*

Cette partie ne concerne pas les établissements de paiement et les établissements de monnaie électronique (cf. article 273 de l'arrêté du 3 novembre 2014).

Cette partie peut faire l'objet d'un rapport distinct.

3.2.1. Gouvernance de la politique de rémunération :

- date de constitution, composition, durée du mandat, modalités de fonctionnement et compétences du comité de rémunération visé à l'article L.511-102 du Code monétaire et financier ;
- description des principes généraux de la politique de rémunération définie en application de l'article L. 511-72 du Code monétaire et financier (modalités et date d'adoption, date de mise en œuvre, modalités de revue) ainsi que, le cas échéant, l'identité des consultants externes dont les services ont été utilisés pour définir la politique de rémunération (cf. article 266 de l'arrêté du 3 novembre 2014) ;
- date et relevé des conclusions de l'évaluation interne destinée à s'assurer du respect de la politique et des procédures en matière de rémunérations adoptées par l'organe de surveillance (cf. article L.511-74 du Code monétaire et financier).

3.2.2. Principales caractéristiques de la politique de rémunération :

- description de la politique de rémunération de l'établissement notamment (cf. article 266 de l'arrêté du 3 novembre 2014) :
  - des critères utilisés pour mesurer la performance et ajuster la rémunération au risque,
  - des critères définis pour définir le lien entre rémunération et performance,
  - de la politique en matière d'étalement des rémunérations,
  - de la politique de rémunérations variables garanties exceptionnellement accordées dans les conditions prévues à l'article L.511-77 du Code monétaire et financier,
  - des critères utilisés pour déterminer la proportion des montants en espèces par rapport à d'autres formes de rémunération ;
- description de la politique de rémunération des personnels des unités chargées de la validation et de la vérification des opérations (cf. articles 15 de l'arrêté du 3 novembre 2014, L. 511-71 et L. 511-75 du Code monétaire et financier) ;
- modalités de prise en compte de l'ensemble des risques dans la détermination de l'assiette de rémunération variable (y compris des risques de liquidité inhérents aux activités concernées ainsi que du capital nécessaire eu égard aux risques encourus) (cf. articles L. 511-76, L.511-77, L. 511-82 et L. 511-83 du Code monétaire et financier) ;
- date de la communication à l'ACPR, ou à la BCE selon les cas, du plafond de la part variable proposé à l'assemblée générale compétente et liste des personnes concernées par le plafonnement de la part variable de la rémunération et justification des choix, en application de l'article L.511-78 du Code monétaire et financier.

3.2.3. Informations relatives aux rémunérations des dirigeants effectifs et des personnes dont les activités professionnelles ont une incidence significative sur le profil de risque de l'entreprise (cf. articles 202 ou, le cas échéant, 199, et au 5°) de l'article 266 de l'arrêté du 3 novembre 2014, ainsi qu'à l'article R.511-18 du Code monétaire et financier) :

Indiquer :

- les catégories de personnels concernés ;
- les montants globaux des rémunérations correspondant à l'exercice, répartis entre part fixe et part variable, et le nombre de bénéficiaires, indiquer également ces informations par domaine d'activités ;
- les montants globaux et forme des rémunérations variables, répartis entre paiements en espèces, en actions et droits de propriété équivalents, et autres instruments mentionnés aux articles 52 ou 63 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 ou autres instruments susceptibles d'être totalement convertis en instruments de fonds propres de base ou amortis *(indiquer la période d'acquisition ou de durée de détention minimale des titres*) (cf. articles L. 511-81, R.511-22 et R. 511-23 du Code monétaire et financier) ;
- les montants globaux des rémunérations différées, réparties entre rémunérations acquises et non acquises (cf. article R.511-18 du Code monétaire et financier) ;
- les montants globaux des rémunérations différées attribués au cours de l'exercice, versés ou réduits, après ajustements en fonction des résultats (cf. article R.511-18 du Code monétaire et financier) ;
- les paiements au titre de nouvelles embauches ou indemnités de licenciement et le nombre de bénéficiaires (cf. article R.511-18 du Code monétaire et financier) ;
- les garanties d'indemnités de licenciement accordées au cours de l'exercice, le nombre de bénéficiaires et la somme la plus élevée accordée à ce titre à un seul bénéficiaire (cf. article R.511-18 du Code monétaire et financier) ;
- les méthodes employées pour les calculs d'actualisation (cf. articles 203 à 210 de l'arrêté du 3 novembre 2014).

3.2.4. Transparence et contrôle de la politique de rémunération :

- modalités de vérification de l'adéquation entre la politique de rémunération et les objectifs de maîtrise des risques, notamment compte tenu de la taille et de l'importance systémique de l'établissement ainsi que de la nature, l'échelle et de la complexité de ses activités, en tenant compte du principe de proportionnalité (cf. article 4 de l'arrêté du 3 novembre 2014) ;
- modalités de publication des informations relatives à la politique et aux pratiques de rémunération prévues par l'article 450 du règlement 575/2013 du Parlement européen et du Conseil du 26 juin 2013 (cf. articles 267 et 268 de l'arrêté du 3 novembre 2014).

4. Résultats des contrôles périodiques effectués au cours de l'exercice écoulé (cf. article 17 de l'arrêté du 3 novembre 2014) (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 présent 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.

5. Recensement des opérations avec les dirigeants effectifs, les membres de l'organe de surveillance et les actionnaires principaux (cf. articles 113 et 259 g) de l'arrêté du 3 novembre 2014)

Joindre une annexe comprenant :

– **caractéristiques des engagements ayant fait l'objet d'une déduction des fonds propres prudentiels** : identité des bénéficiaires, type de bénéficiaires – personne physique ou personne morale, actionnaire ou dirigeant –, nature des engagements, montant brut, déductions éventuelles et pondération, date de leur mise en place et date d'échéance ;

– **nature des engagements envers des actionnaires principaux et des dirigeants, n'ayant pas fait l'objet d'une déduction** en raison soit des dates auxquelles ont été conclus ces engagements, soit de la notation ou de la cotation attribuée aux bénéficiaires des engagements. Néanmoins, il n'apparaît pas nécessaire de mentionner les engagements dont le montant brut n'excède pas 3 % des fonds propres de l'établissement.

6. Processus d'évaluation de l'adéquation du capital interne

Ce dispositif n'est pas obligatoire pour les établissements inclus dans une consolidation et qui sont exonérés de l'assujettissement aux ratios de gestion sur base sociale ou sous consolidée.

– description des systèmes et procédures mis en place pour s'assurer que le montant et la répartition du capital interne sont adaptés à la nature et au niveau des risques auquel l'établissement est exposé *(avec un accent particulier sur les risques non pris en compte par le pilier 1)* (cf. article 96 de l'arrêté du 3 novembre 2014) ;

– niveau de capital interne alloué aux risques pour l'exercice écoulé et pour l'exercice à venir ;

– simulations de crise réalisées aux fins d'évaluation de l'adéquation du capital interne : description des hypothèses et principes méthodologiques retenus ainsi que des résultats obtenus ;

– modalités de contrôle prévues afin de vérifier que ces systèmes et procédures demeurent adaptés à l'évolution du profil de risques de l'établissement.

7. Risque de non conformité (hors risque de blanchiment des capitaux et de financement du terrorisme)

7.1. Formation du personnel aux procédures de contrôle de la conformité et information immédiate du personnel concerné des modifications pouvant intervenir dans les textes applicables aux opérations réalisées (cf. articles 39 et 40 de l'arrêté du 3 novembre 2014)

7.2. Évaluation et maîtrise du risque de réputation

7.3. Autres risques de non-conformité (déontologie bancaire et financière…)

7.4 Procédures permettant le signalement des manquements, infractions et dysfonctionnements

Indiquer :

– les procédures mises en place pour permettre au personnel de signaler aux responsables et comités compétents de leur entreprise ainsi qu'à l'ACPR (ou à la BCE selon les cas) les manquements ou

infractions à la réglementation prudentielle commis au sein de l'établissement ou susceptibles de l'être (cf. article L.511-41 du Code monétaire et financier) ;

– les procédures mises en place pour permettre à tout dirigeant ou préposé de faire part, au responsable de la conformité de l'entité ou de la ligne métier à laquelle ils appartiennent, ou au responsable mentionné à l'article 28 de l'arrêté du 3 novembre 2014, de ses interrogations sur d'éventuels dysfonctionnements concernant le dispositif de contrôle de la conformité (cf. article 37 de l'arrêté du 3 novembre 2014).

7.5. Centralisation et mise en place de mesures de remédiation et de suivi

Indiquer :

– les procédures mises en place pour centraliser les informations relatives aux dysfonctionnements éventuels dans la mise en œuvre des obligations de conformité (cf. articles 36 et 37 de l'arrêté du 3 novembre 2014) ;

– les procédures mises en place pour suivre et évaluer la mise en œuvre effective des actions visant à remédier aux dysfonctionnements dans la mise en œuvre des obligations de conformité (cf. article 38 de l'arrêté du 3 novembre 2014).

7.6. Description des principaux dysfonctionnements identifiés au cours de l'exercice

7.7. Résultats des contrôles permanents menés en matière de risque de non-conformité :

– 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 présent rapport ;

– modalités de suivi des recommandations résultant des contrôles permanents *(outils, personnes en charge)* ;

– modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein des entreprises, par les personnes compétentes (cf. articles 11 f) et 26 a) de l'arrêté du 3 novembre 2014).

8. Risque de blanchiment des capitaux et de financement du terrorisme

8.1. Classification des risques (LCB/FT) (cf. articles 57 à 60 de l'arrêté du 3 novembre 2014) :

– description, formalisation, mises à jour et présentation des analyses sur lesquelles cette classification est fondée.

8.2. Procédures (LCB/FT) (cf. articles 61 à 70 de l'arrêté du 3 novembre 2014) :

– description, formalisation et date(s) de mise à jour des procédures sur lesquelles s'appuie le dispositif de LCB/FT en faisant ressortir les modifications significatives intervenues au cours de l'exercice notamment sur les procédures relatives :
  - à l'identification des nouveaux clients et des bénéficiaires effectifs,
  - à l'identification des clients occasionnels,
  - à la connaissance des clients,
  - aux modalités de mise en conformité des dossiers clients existants avec les obligations de vigilance constante ;

– description des modalités de mise en œuvre des obligations de vigilances allégées, complémentaires et renforcées ;

– description des modalités de mise en œuvre des obligations en matière de virements de fonds (en tant que prestataire de paiement du donneur d'ordre, prestataire de paiement intermédiaire, prestataire de paiement du bénéficiaire) ;

- le cas échéant, modalités de circulation au sein du groupe des informations nécessaires à l'organisation de la lutte contre le blanchiment des capitaux et le financement du terrorisme : description des procédures existantes sur les échanges d'informations relatives à l'existence et au contenu des déclarations ;
- modalités de définition des critères et seuils de significativité des anomalies en matière de LCB/FT.

8.3. Résultats des contrôles permanents menés en matière de risque de blanchiment des capitaux et de financement du terrorisme :

- 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 présent rapport ;
- modalités de suivi des recommandations résultant des contrôles permanents *(outils, personnes en charge) ;*
- modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein des entreprises, par les personnes compétentes (cf. articles 11 f) et 26 a) de l'arrêté du 3 novembre 2014*).*

8.4. Principales insuffisances du dispositif relevées notamment par les autorités de contrôle nationales et étrangères et mesures correctrices décidées

9. Risque de crédit et de contrepartie [1] (cf. articles 106 à 121 de l'arrêté du 3 novembre 2014)

***Nota bene** : pour les prestataires de services d'investissement (PSI), le cas particulier des **opérations de service à règlement-livraison différé (SRD)**, est traité dans ce chapitre avec notamment des éléments d'information sur la sélection des clients pour lesquels ce type d'ordre est autorisé, sur les limites d'intervention fixées et sur la gestion du risque (couverture initiale, maintien de cette couverture, suivi des prorogations, provisionnement des créances douteuses).*

9.1. Dispositif de sélection des opérations :

- critères prédéfinis de sélection des opérations ;
- éléments d'analyse de la rentabilité prévisionnelle des opérations de crédit pris en compte lors des décisions d'engagement : *méthodologie, données prises en compte (sinistralité, etc.)* ;
- description des procédures d'octroi de crédit, incluant le cas échéant un dispositif de délégation ;
- politique d'octroi des crédits à l'habitat à la clientèle française, notamment en ce qui concerne les critères relatifs à la charge de remboursement en fonction du revenu disponible des emprunteurs, au rapport entre le montant des prêts accordés et la valeur des biens financés et à la durée des crédits.

9.2. Dispositif de mesure et de surveillance des risques :

- *stress scenarii* utilisés pour mesurer le risque encouru, hypothèses retenues, résultats et description de leur intégration opérationnelle ;
- description synthétique des limites d'engagement fixées en matière de risque de crédit – par bénéficiaire, par débiteurs liés, etc. *(préciser le niveau des limites par rapport aux fonds propres et par rapport aux résultats)* ;
- modalités et périodicité de la révision des limites fixées en matière de risque de crédit *(indiquer la date de la dernière révision)* ;

1. Les établissements de paiement qui effectuent des opérations de crédit sont également concernés par ce point.

- dépassements éventuels de limites observés au cours du dernier exercice *(préciser les causes, les contreparties concernées, le montant de l'engagement total, le nombre des dépassements et leur montant)* ;
- procédures suivies pour autoriser ces dépassements ;
- mesures mises en œuvre pour régulariser ces dépassements ;
- identification, effectifs et positionnement hiérarchique et fonctionnel de l'unité chargée de la surveillance et de la maîtrise des risques de crédit ;
- modalités et périodicité de l'analyse de la qualité des engagements de crédit et des garanties qui y sont attachées ; indication des éventuels reclassements des engagements au sein des catégories internes d'appréciation du niveau de risque, ainsi que les affectations dans les rubriques comptables de créances douteuses ou dépréciées ; indication de l'ajustement éventuel du niveau de provisionnement ; date à laquelle cette analyse est intervenue au cours du dernier exercice ;
- présentation du système de mesure et de gestion des risques de crédit mis en place afin de détecter, gérer les crédits à problème, d'apporter les corrections de valeurs adéquates et d'enregistrer des provisions ou des dépréciations de montants appropriés (cf. article 115 de l'arrêté du 3 novembre 2014) ;
- modalités et périodicité de l'analyse des risques de perte de valeur des actifs loués (opérations de location à caractère financier) ;
- modalités, périodicité et résultats de l'actualisation et de l'analyse des dossiers de crédit (au moins pour les contreparties dont les créances sont impayées ou douteuses ou dépréciées ou qui présentent des risques ou des volumes significatifs) ;
- répartition des engagements par niveau de risque (cf. articles 106 et 253 a) de l'arrêté du 3 novembre 2014) ;
- modalités d'information des dirigeants effectifs (via des états de synthèse), de l'organe de surveillance et le cas échéant du comité des risques sur le niveau des risques de crédit (cf. article 230 de l'arrêté du 3 novembre 2014) ;
- rôles des dirigeants effectifs, de l'organe de surveillance et le cas échéant du comité des risques dans la définition, le contrôle et la révision de la stratégie globale en matière de risques de crédit et de l'appétence pour les risques de crédit actuels et futurs de l'établissement (cf. articles L.511-92 et L.511-93 du Code monétaire et financier), et dans la fixation des limites (cf. article 224 de l'arrêté du 3 novembre 2014) ;
- éléments d'analyse de l'évolution des marges, notamment sur la production au cours de l'année écoulée : *méthodologie, données prises en compte, résultats* :
  - communication des éléments détaillés du calcul des marges : produits et charges pris en compte ; s'il est tenu compte du besoin de refinancement, indication du montant de la position nette emprunteuse et du taux de refinancement retenu ; s'il est tenu compte des gains liés au placement des fonds propres alloués aux encours, communication des montants et du taux de rémunération,
  - identification des différentes catégories d'encours (clientèle de particuliers par exemple avec mise en évidence des prêts à l'habitat) ou des lignes de métier pour lesquelles les marges sont calculées,
  - mise en évidence des évolutions constatées à partir d'un calcul sur la base des encours (à la fin de l'exercice et à des échéances antérieures), et le cas échéant sur la base de la production de l'année écoulée ;
- modalités, périodicité et résultats de l'analyse par les dirigeants effectifs de la rentabilité des opérations de crédit *(indiquer la date de la dernière analyse)* ;
- modalités et périodicité d'information de l'organe de surveillance sur l'exposition de l'établissement au risque de crédit (joindre le dernier tableau de bord destiné à l'information de l'organe de surveillance) ;
- modalités de suivi des critères d'octroi des crédits à l'habitat à la clientèle française ;
- modalités d'approbation par l'organe de surveillance des limites proposées par les dirigeants effectifs, assisté le cas échéant du comité des risques (cf. article 253 de l'arrêté du 3 novembre 2014) ;

– modalités d'approbation et de révision par l'organe de surveillance des stratégies et politiques régissant la prise, la gestion, le suivi et la réduction des risques de crédit (cf. article L.511-60 du Code monétaire et financier).

9.3. Risque de concentration

9.3.1. Risque de concentration par contrepartie :

– outil de suivi du risque de concentration par contrepartie y compris les contreparties centrales : agrégats éventuellement définis, description du dispositif de mesure des engagements sur un même bénéficiaire (précisions sur les procédures d'identification des bénéficiaires liés (définition d'un seuil quantitatif au-delà duquel cette recherche est systématique ...) ; l'utilisation de l'approche par transparence notamment en matière d'expositions sur des organismes de placement collectif, des titrisations ou le refinancement de créances commerciales (affacturage, …) ainsi que sur l'inclusion des techniques d'atténuation du risque de crédit), modalités d'information des dirigeants effectifs et de l'organe de surveillance ;

– dispositif de limites d'exposition par contrepartie : description synthétique du système de limite par contrepartie *(préciser leur niveau par rapport aux résultats et aux fonds propres)*, modalités et périodicité de la révision des limites, dépassements éventuellement constatés, modalités d'implication des dirigeants effectifs dans la détermination des limites et d'information sur leur suivi ;

– montant des engagements sur les principales contreparties ;

– conclusion sur l'exposition au risque de concentration par contrepartie y compris les contreparties centrales.

9.3.2. Risque de concentration sectorielle :

– outil de suivi du risque de concentration sectorielle : agrégats éventuellement définis, dispositif de mesure des engagements sur un même secteur d'activité, modalités d'information des dirigeants effectifs et de l'organe de surveillance ;

– dispositif de limites d'exposition sectorielle : description synthétique du système de limite sectorielle *(préciser leur niveau par rapport aux résultats et aux fonds propres)*, modalités et périodicité de la révision des limites, dépassements éventuellement constatés, modalités d'implication des dirigeants effectifs dans la détermination des limites et d'information sur leur suivi ;

– répartition des engagements par secteurs ;

– conclusion sur l'exposition au risque de concentration sectorielle.

9.3.3. Risque de concentration géographique :

– outil de suivi du risque de concentration par zone géographique : agrégats éventuellement définis, dispositif de mesure des engagements sur une même zone géographique, modalités d'information des dirigeants effectifs et de l'organe de surveillance ;

– dispositif de limites d'exposition par zone géographique : description synthétique du système de limite par zone géographique *(préciser leur niveau par rapport aux résultats et aux fonds propres)*, modalités et périodicité de la révision des limites, dépassements éventuellement constatés, modalités d'implication des dirigeants effectifs dans la détermination des limites et d'information sur leur suivi ;

– répartition des engagements par zones géographiques ;

– conclusion sur l'exposition au risque de concentration géographique.

9.4. Exigences liées à l'utilisation des systèmes de notations internes pour le calcul des exigences en fonds propres au titre du risque de crédit :

– contrôles ex-post et comparaisons avec des données externes afin de s'assurer de l'exactitude et de la cohérence du ou des systèmes de notations internes, des procédés et des paramètres utilisés ;

– contenu et périodicité de contrôle des systèmes de notations dans le cadre du contrôle permanent et dans le cadre du contrôle périodique ;

- description de l'insertion opérationnelle des systèmes de notation : utilisation effective des paramètres issus des systèmes de notation dans l'approbation des crédits, la tarification, la gestion du recouvrement, le suivi des risques, la politique de provisionnement, l'allocation du capital interne et le gouvernement d'entreprise (tableaux de bord à destination des dirigeants effectifs / des organes de surveillance, notamment) ;
- modalités d'implication des dirigeants effectifs dans la conception et la mise à jour du ou des systèmes de notations internes : notamment approbation des principes méthodologiques, vérification de la bonne maîtrise de la conception et du mode de fonctionnement du ou des systèmes, modalités selon lesquelles ils sont informés de son/leur fonctionnement ;
- démonstration que les méthodes internes d'évaluation du risque de crédit ne reposent pas exclusivement ou mécaniquement sur un système de notation externe du risque (cf. article 114 de l'arrêté du 3 novembre 2014).

9.5. Risques liés aux opérations ou montages de titrisation :

- présentation de la stratégie en matière de titrisation et de transfert du risque de crédit ;
- présentation des politiques et des procédures internes mises en place afin de s'assurer avant d'investir de la connaissance approfondie des positions de titrisation concernées et du respect de l'obligation de rétention de 5% d'intérêt économique net par les établissements agissant en qualité d'*originateur*, de sponsor ou de prêteur initial ;
- modalités d'évaluation, de suivi et de maîtrise des risques liés aux montages ou opérations de titrisation (et notamment analyse de leur substance économique) pour les établissements *originateurs*, *sponsors* ou investisseurs y compris via des scénarios de crise (hypothèses, périodicité, conséquences) ;
- pour les banques originatrices, description du processus interne d'évaluation des transactions déconsolidantes prudentiellement, étayée par une piste d'audit et modalités de suivi du transfert de risque sur la durée à travers une revue périodique.

9.6. Risque de crédit intra-journalier :

Risque encouru dans le cadre de l'activité de conservation par les établissements qui octroient à leur client un crédit en cours de journée, en espèces et/ou en titres, pour faciliter l'exécution des opérations de titres[2].

- description de la politique appliquée par l'établissement pour la gestion du risque de crédit intra-journalier ; description des limites (modalités de définition et de suivi) ;
- présentation du système de mesure des expositions et de suivi des limites sur une base intra-journalière (y compris la gestion des éventuels dépassements de limites) ;
- modalités des décisions d'octroi d'un crédit intra-journalier ;
- modalités d'évaluation de la qualité des sûretés réelles ;
- description des reportings à destination des dirigeants effectifs et des organes de surveillance ;
- conclusion sur l'exposition au risque de crédit intra-journalier.

9.7. Résultats des contrôles permanents menés sur les activités de crédit :

- 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 présent rapport *;*
- modalités de suivi des recommandations résultant des contrôles permanents *(outils, personnes en charge)* ;

2. Le risque de crédit intra-journalier recouvre également le risque de crédit *overnight* pour les opérations dont le règlement intervient pendant la nuit.

– modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein des entreprises, par les personnes compétentes (cf. articles 11 f) et 26 a) de l'arrêté du 3 novembre 2014).

9.8. Risques liés à l'utilisation des techniques d'atténuation du risque de crédit :

Joindre une annexe comprenant :

– description du dispositif mis en œuvre pour identifier, mesurer, et surveiller le risque résiduel auquel est exposé l'établissement au titre de l'utilisation des techniques d'atténuation du risque de crédit ;

– description synthétique des procédures destinées à s'assurer, lors de leur mise en place, que les techniques d'atténuation du risque de crédit utilisées sont juridiquement valables, que leur valeur n'est pas corrélée à celle du débiteur et qu'elles sont dûment documentées ;

– présentation des modalités d'intégration du risque de crédit associé à l'utilisation des techniques d'atténuation du risque de crédit dans le dispositif général de gestion du risque de crédit ;

– description des simulations de crise relatives aux techniques d'atténuation du risque de crédit (hypothèses et principes méthodologiques retenus ainsi que résultats obtenus).

9.9. Simulations de crise relatives au risque de crédit :

Joindre une annexe comprenant la description des hypothèses et principes méthodologiques retenus (notamment modalités de prise en compte des effets de contagion à d'autres marchés) ainsi que des résultats obtenus.

9.10. Conclusion synthétique sur l'exposition au risque de crédit

10. Risques de marché

Description de la politique conduite par l'établissement en matière d'activités de marché réalisées pour compte propre.

10.1. Dispositif de mesure des risques de marché :

– enregistrement des opérations de marché ; calcul des positions et des résultats *(préciser la périodicité) ;*

– rapprochements entre les résultats de gestion et les résultats comptables *(préciser la périodicité) ;*

– évaluation des risques résultant des positions du portefeuille de négociation *(préciser la périodicité) ;*

– modalités selon lesquelles les différentes composantes du risque (y compris le risque de base et le risque de titrisation) sont prises en compte (notamment pour les établissements disposant de volumes significatifs effectuant une mesure globale du risque) ;

– champ de la couverture des risques (différentes activités et portefeuilles, au sein des différentes implantations géographiques).

10.2. Dispositif de surveillance des risques de marché :

– rôles des dirigeants effectifs, de l'organe de surveillance et le cas échéant du comité des risques dans la définition de la stratégie globale en matière de risques de marché et de l'appétence pour les risques de marché actuels et futurs de l'établissement (cf. articles L.511-92 et L.511-93 du Code monétaire et financier), et dans la fixation des limites (cf. article 224 de l'arrêté du 3 novembre 2014) ;

– identification, effectifs et positionnement hiérarchique et fonctionnel de l'unité chargée de la surveillance et de la maîtrise des risques de marché ;

– contrôles réalisés par cette unité, et en particulier contrôle régulier de la validité des outils de mesure globale des risques (back-testing) ;

- description synthétique des limites fixées en matière de risques de marché *(préciser le niveau des limites, par type de risques encourus, par rapport aux fonds propres et par rapport aux résultats)* ;
- périodicité de la révision des limites fixées en matière de risques de marché *(indiquer la date à laquelle est intervenue cette révision au cours du dernier exercice)* ; organe en charge de décider le niveau des limites ;
- dispositif de surveillance des procédures et des limites ;
- dépassements éventuels de limites observés au cours du dernier exercice *(préciser les causes des dépassements, leur nombre et leur montant) ;*
- procédures suivies pour autoriser ces dépassements et mesures mises en œuvre pour régulariser ces dépassements ;
- procédures d'information sur le respect des limites *(périodicité, destinataires) ;*
- modalités, périodicité et conclusions de l'analyse transmise aux dirigeants effectifs et à l'organe de surveillance des résultats des opérations de marché *(indiquer la date de la dernière analyse)* ainsi que du niveau des risques portés, notamment au regard du montant des fonds propres alloués et du niveau de capital interne permettant de couvrir les risques de marché significatifs non soumis à des exigences de fonds propres (cf. articles 130 à 133 de l'arrêté du 3 novembre 2014) :
  - joindre un exemple des documents transmis aux dirigeants effectifs lui permettant d'apprécier les risques de l'entreprise, notamment par rapport à ses fonds propres et ses résultats.

10.3. Résultats des contrôles permanents menés sur les risques de marché :

- 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 présent rapport ;
- modalités de suivi des recommandations résultant des contrôles permanents *(outils, personnes en charge) ;*
- modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein des entreprises, par les personnes compétentes (cf. articles 11 f) et 26 a) de l'arrêté du 3 novembre 2014).

10.4. Simulations de crise relatives aux risques de marché :

Pour les établissements utilisant leurs modèles internes pour le calcul des exigences en fonds propres, joindre une annexe comprenant la description des hypothèses et principes méthodologiques retenus ainsi que des résultats obtenus.

10.5. Conclusion synthétique sur l'exposition aux risques de marché

11. Risque opérationnel

Description synthétique du cadre général de détection, de gestion, de suivi et de déclaration du risque opérationnel, en lien avec la complexité des activités, le profil de risque et la tolérance au risque de l'établissement *(préciser le périmètre des entités et opérations prises en compte, le rôle des dirigeants effectifs et des organes de surveillance et la répartition des compétences en matière de gestion du risque opérationnel).*

11.1. Identification et évaluation du risque opérationnel

- description des types de risques opérationnels auxquels l'établissement est exposé ;
- description du système de mesure et de surveillance du risque opérationnel *(préciser la méthode utilisée pour le calcul des exigences en fonds propres)* ;

- description synthétique des reportings utilisés pour la mesure et la gestion du risque opérationnel *(préciser notamment la périodicité et les destinataires des reportings, les zones de risques couvertes, la présence ou non d'indicateurs d'alerte mettant en évidence le cas échéant des pertes potentielles futures)* ; documentation et communication des procédures relatives à la surveillance et à la gestion du risque opérationnel ;
- description des procédures spécifiques pour la maîtrise du risque de fraude interne et externe au sens de l'article 324 du règlement (UE) n°575/2013 du Parlement européen et du Conseil du 26 juin 2013 ;
- pour les établissements utilisant l'approche standard, procédures et critères retenus pour la mise en correspondance de l'indicateur pertinent pour les lignes d'activité, procédures de révision en cas de lancement d'une nouvelle activité ou de modification d'une activité existante ;
- pour les établissements utilisant une approche de mesure avancée, description de la méthodologie retenue *(y compris des facteurs relatifs au contrôle interne et à l'environnement dans lequel ils opèrent)* et des évolutions le cas échéant apportées au cours de l'exercice, description des procédures de vérification de la qualité des données historiques ;
- description synthétique des techniques d'assurance éventuellement utilisées.

11.2. Intégration du dispositif de mesure et de gestion du risque opérationnel dans le dispositif de contrôle permanent :

- description des modalités d'intégration de la surveillance du risque opérationnel, incluant notamment les risques liés à des événements de faible occurrence mais à fort impact, les risques de fraudes interne et externe définis à l'article 324 du règlement (UE) n°575/2013 et les risques liés au modèle, dans le dispositif de contrôle permanent ;
- description des principaux risques opérationnels avérés au cours de l'exercice (incidents de règlement, erreurs, fraudes…) et des enseignements qui en ont été tirés.

11.3. Plan d'urgence et de poursuite d'activité :

- définitions retenues et objectifs du (ou des) plan(s) d'urgence et de poursuite d'activité, scénarios retenus, architecture globale (un plan unique ou un plan par métier, cohérence globale en cas de plans multiples), responsabilités *(nom, coordonnées (adresse électronique, numéro de portable si possible) et positionnement des différents responsables en charge de la gestion du (ou des) plan(s) d'urgence et de poursuite d'activité et de leur déclenchement (RPUPA), nom, coordonnées et positionnement du ou des responsables de la gestion de la crise s'ils sont différents des RPUPA…)*, périmètre des activités couvertes par le (ou les) plan(s) d'urgence et de poursuite d'activité, activités traitées en priorité en cas de crise, risques résiduels non couverts par le plan d'urgence et de poursuite d'activité, délais de mise en œuvre du plan d'urgence et de poursuite d'activité ;
- formalisation des procédures, description synthétique des sites de secours informatique et de repli ;
- tests du plan d'urgence et de poursuite d'activité (objectifs, périmètre, fréquence, résultats), mise à jour du plan d'urgence et de poursuite d'activité (fréquence, critères), outil de gestion du plan d'urgence et de poursuite d'activité (logiciel, développement informatique), reporting à la direction (sur les tests, les modifications) ;
- audit du plan d'urgence et de poursuite d'activité et résultats des contrôles permanents ;
- activation du ou des plan(s) d'urgence et de poursuite d'activité et gestion des crises rencontrées au cours de l'exercice (exemple : grippe A [H1N1]).

11.4. Sécurité des systèmes d'information :

- nom du responsable de la sécurité des systèmes d'information ;
- identification et réévaluation de la cartographie des risques informatiques ;
- objectifs de la politique de sécurité informatique (et en particulier modalités de préservation de l'intégrité et de la confidentialité des données, ainsi que mesures spécifiques mises en place pour l'activité de banque en ligne) ;

– description du contrôle permanent du niveau de sécurité des systèmes d'informations et de ses résultats ;

– description des procédures mises en place en cas de cyber-attaque (c'est-à-dire un ou plusieurs évènements indésirables ou inattendus fortement susceptibles de compromettre la sécurité des informations et d'affaiblir ou de nuire à l'activité de l'établissement), notamment pour les incidents majeurs c'est-à-dire ceux dont l'impact financier dépasse soit 25 millions d'euros soit 0,5% du CET1 de l'établissement.

11.5. Résultats des contrôles permanents menés en matière de risque opérationnel :

– 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 présent rapport ;

– modalités de suivi des recommandations résultant des contrôles permanents *(outils, personnes en charge)* ;

– modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein des entreprises, par les personnes compétentes (cf. articles 11 f) et 26 a) de l'arrêté du 3 novembre 2014).

11.6. Conclusion synthétique sur l'exposition au risque opérationnel

12. Risque comptable

12.1. Modifications significatives apportées à l'organisation du dispositif comptable

Lorsque l'organisation du dispositif comptable ne présente pas de changements significatifs, elle peut être présentée de manière synthétique dans une annexe.

12.2. Résultats des contrôles permanents menés en matière de risque comptable :

– 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 présent rapport ;

– modalités de suivi des recommandations résultant des contrôles permanents *(outils, personnes en charge)* ;

– modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein des entreprises, par les personnes compétentes (cf. articles 11 f) et 26 a) de l'arrêté du 3 novembre 2014).

13. Risque de taux d'intérêt global

***Nota bene** : pour l'exercice 2015, cette partie devra inclure une description des éventuelles adaptations prises ou à entreprendre par l'établissement pour se mettre en conformité avec les nouvelles dispositions introduites par les orientations de l'EBA sur le risque de taux d'intérêt dans le portefeuille bancaire, dont l'entrée en vigueur est prévue au 1er janvier 2016.*

– description synthétique du cadre général de la détection, de l'évaluation et de la gestion du risque de taux d'intérêt global *(préciser le périmètre des entités et opérations prises en compte en justifiant le recours au principe de proportionnalité en cas de gestion sur base consolidée, le rôle des dirigeants effectifs et des organes de surveillance et la répartition des compétences en matière de pilotage du risque de taux d'intérêt global).*

13.1. Dispositif de mesure et de suivi (et méthodologie) du risque de taux d'intérêt global :

- description des outils et de la méthodologie utilisée en matière de gestion du risque de taux d'intérêt global *(préciser les indicateurs utilisés par l'établissement notamment gaps statiques ou dynamiques, calcul de sensibilité des résultats, calcul de valeur actualisée nette, hypothèses et résultats des stress scenarii, impact des variations du risque de taux d'intérêt global sur l'activité de l'établissement pour l'année écoulée, en cas d'exposition dans différentes devises, la méthodologie utilisée pour l'agrégation des expositions)* ;
- présentation des conventions d'écoulement utilisées par l'établissement *[préciser le périmètre couvert, les principales hypothèses retenues, le traitement de la production nouvelle, des produits ne portant pas intérêts (tels que les fonds propres), des options explicites, implicites et comportementales, notamment le traitement des dépôts non-échéancés (présentation de la méthodologie utilisée pour la segmentation des dépôts par catégories, l'identification des dépôts stables) et des produits d'épargne réglementée]* ;
- présentation des résultats des indicateurs de mesure de risque de taux d'intérêt global utilisés par l'établissement : *préciser le niveau des gaps statiques ou dynamiques, les résultats des calculs de sensibilité des revenus, des calculs de valeur actualisée nette et des stress scenarii* ;
- présentation des résultats d'un choc uniforme correspondant au niveau le plus élevé entre i) +/- 200 bp et ii) les 1er et 99ème centiles des variations journalières de taux d'intérêt observées sur un historique de cinq ans, et mises à l'échelle d'une année de 240 jours. Le choc uniforme est appliqué à la hausse et à la baisse, dans les limites d'un taux d'intérêt positif, sur le PNB courant à horizon situé entre un et cinq ans et sur la valeur économique de l'établissement, en tenant compte uniquement des activités autres que de négociation. Le calcul des résultats du choc uniforme est effectué selon deux méthodologies distinctes :
    - i) en excluant les fonds propres des éléments du passif et en plafonnant la duration moyenne des dépôts à vue à 5 ans,
    - ii) selon les hypothèses retenues par l'établissement pour sa gestion interne du risque de taux d'intérêt global. Présentation des hypothèses retenues et justification des éventuelles différences avec les hypothèses normalisées décrites au i).

L'annexe 1 au présent document décrit, à titre d'exemple, pour les établissements qui ne disposeraient pas de méthodologie propre, les méthodes susceptibles d'être utilisées pour calculer les résultats d'un choc uniforme de 200 bp. L'impact du choc sur la valeur économique est rapporté au niveau de fonds propres règlementaires de l'établissement ;

- sensibilité des résultats du choc à une modification des hypothèses retenues *(préciser l'impact d'un mouvement non-parallèle de la courbe des taux, des décalages entre références de taux (risque de base) et d'une modification des hypothèses et conventions d'écoulement retenues)* ;
- présentation du capital économique alloué au regard du risque de taux d'intérêt global encouru par l'établissement ;
- présentation des scénarios de taux alternatifs utilisés par l'établissement (par exemple, des scénarios d'aplatissement, de pentification, d'inversion, de choc sur les taux courts, etc.) et des résultats sur la valeur économique et les revenus.

13.2. Dispositif de surveillance du risque de taux d'intérêt global :

- pour l'approche par les revenus et l'approche par la valeur économique des capitaux propres, description synthétique des limites fixées en matière de risque de taux d'intérêt global *(indiquer la nature et le niveau des limites mises en place, par exemple en termes de gap, de sensibilité par rapport aux résultats ou aux fonds propres, indiquer la date à laquelle la révision des limites est intervenue au cours du dernier exercice, préciser la procédure de suivi des dépassements)* ;
- description synthétique des reportings utilisés pour la gestion du risque de taux d'intérêt global *(préciser notamment la périodicité et les destinataires des reportings)* ;
- rôles des dirigeants effectifs, de l'organe de surveillance et le cas échéant du comité des risques dans la définition de la stratégie globale en matière de risque de taux d'intérêt global et de l'appétence pour les risques de taux actuels et futurs de l'établissement (cf. articles L.511-92 et L.511-93 du Code monétaire et financier), et dans la fixation des limites (cf. article 224 de l'arrêté du 3 novembre 2014).

13.3. Dispositif de contrôle permanent de la gestion du risque de taux d'intérêt global :

– préciser s'il existe une unité en charge de la surveillance et de la gestion du risque de taux d'intérêt global et de manière plus générale comment cette surveillance s'inscrit dans le dispositif de contrôle permanent.

13.4. Résultats des contrôles permanents menés en matière de risque de taux d'intérêt global :

– 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 présent rapport ;

– modalités de suivi des recommandations résultant des contrôles permanents *(outils, personnes en charge)* ;

– modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein des entreprises, par les personnes compétentes (cf. articles 11 f) et 26 a) de l'arrêté du 3 novembre 2014).

13.5. Conclusion synthétique sur l'exposition au risque de taux d'intérêt global

14. Risque d'intermédiation des prestataires de services d'investissement

– relevés de la répartition globale des engagements par ensemble de contreparties et de donneurs d'ordres (par notation interne, par instrument financier, par marché ou par tout autre critère significatif dans le cadre des activités exercées par l'établissement) ;

– éléments d'information sur la gestion du risque (prises de garantie, appels de couverture des positions, collatéraux,…) et sur les procédures suivies en cas de défaillance d'un donneur d'ordre (couverture insuffisante des positions, refus de l'opération) ;

– description synthétique du dispositif de limites d'engagement fixées en matière de risque d'intermédiation – par bénéficiaire, par débiteurs liés, etc. *(préciser le niveau des limites par rapport au volume d'opérations des bénéficiaires et par rapport aux fonds propres)* ;

– modalités et périodicité de la révision des limites fixées en matière de risque d'intermédiation *(indiquer la date de la dernière révision)* ;

– dépassements éventuels de limites observés au cours du dernier exercice *(préciser les causes, les contreparties concernées, le montant de l'engagement total, le nombre des dépassements, leur durée et leur montant)* ;

– procédures suivies pour autoriser ces dépassements et mesures mises en œuvre pour régulariser ces dépassements ;

– éléments d'analyse retenus pour apprécier le risque sur les donneurs d'ordres pris en compte lors des décisions d'engagement *(méthodologie, données prises en compte)* ;

– typologie des erreurs intervenues au cours de l'exercice dans la prise en charge et l'exécution des ordres *(modalités et périodicité de l'analyse des erreurs par le responsable du contrôle interne, seuil retenu par les dirigeants effectifs pour documenter ces erreurs)* ;

– résultats des contrôles permanents menés en matière de risque d'intermédiation ;

– principales conclusions de l'analyse du risque encouru.

15. Risque de règlement/livraison

- description du système de mesure du risque de règlement/livraison *(mise en évidence des différentes phases du processus de règlement, prise en compte des nouvelles opérations venant s'ajouter aux opérations en cours…)* ;
- description synthétique des limites fixées en matière de risque de règlement/livraison *(préciser le niveau des limites, par type de contrepartie, par rapport au volume d'opérations de ces contreparties et par rapport aux fonds propres)* ;
- périodicité de la révision des limites fixées en matière de risque de règlement/livraison *(indiquer la date de la dernière révision)* ;
- dépassements éventuels de limites observés au cours du dernier exercice *(préciser les causes des dépassements, leur nombre, leur durée et leur montant)* ;
- procédures suivies pour autoriser ces dépassements et mesures mises en œuvre pour régulariser ces dépassements ;
- analyse des suspens en cours *(préciser leur antériorité, leurs causes, le plan d'action pour leur apurement)* ;
- résultats des contrôles permanents menés en matière de risque de règlement/livraison ;
- principales conclusions de l'analyse du risque encouru.

Pour les prestataires de services d'investissement qui apportent leur garantie de bonne fin :

- description des différents instruments traités et de chaque système de règlement utilisé avec identification des différentes phases du processus de règlement livraison ;
- modalités de suivi des flux de trésorerie et de titres ;
- modalités de suivi et de traitement des suspens ;
- modalités de mesure des ressources, titres ou espèces facilement mobilisables pour assurer le respect des engagements vis-à-vis des contreparties.

16. Risques de liquidité [3]

***Nota bene** : Pour l'exercice 2015, cette partie devra inclure une description des adaptations prises par l'établissement pour se mettre en conformité avec les nouvelles dispositions introduites par la transposition de la directive et par 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'ACPR.*

- description synthétique du cadre général de la détection, de la mesure, de la gestion et du suivi des risques de liquidité: *préciser le périmètre des entités et opérations prises en compte, en tenant compte des expositions hors bilan, le rôle des dirigeants effectifs et des organes de surveillance et la répartition des compétences en matière de pilotage des risques de liquidité, le profil de risque et le niveau de tolérance au risque (cf. articles 181 et 183 de l'arrêté du 3 novembre 2014)* ;
- informations sur la diversification de la structure de financement et des sources de financement : description de la structure de financement et des sources de financement auxquelles l'établissement a recours *(préciser les différents canaux, les montants, les maturités, les principales contreparties, le recours aux instruments d'atténuation des risques de liquidité),* description des indicateurs utilisés pour mesurer la diversification des sources de financement (cf. article 160 de l'arrêté du 3 novembre 2014).

3. Les succursales des établissements ayant leur siège social dans un autre État membre de l'Union européenne ou partie à l'accord sur l'Espace économique européen doivent adresser un rapport sur la mesure et la surveillance des risques de liquidité jusqu'à la date à laquelle l'exigence des besoins de liquidité est applicable, conformément à l'acte délégué adopté en vertu de l'article 460 du règlement (UE) n°575/2013 du Parlement européen et du Conseil du 26 juin 2013 (cf. article 271 de l'arrêté du 3 novembre 2014).

16.1. Dispositif de mesure (et méthodologie utilisée) des risques de liquidité :

- description des outils et de la méthodologie utilisée en matière de gestion des risques de liquidité : *préciser les hypothèses retenues et les échéances prises en compte pour le calcul des indicateurs utilisés par l'établissement (cf. article 156 de l'arrêté du 3 novembre 2014), en lien avec la complexité des activités, le profil de risque et la tolérance au risque de l'établissement, déclinaison des outils et indicateurs utilisés pour chaque devise dans laquelle l'établissement développe une activité importante, préciser les scénarios alternatifs tels que prévus à l'article 168 de l'arrêté du 3 novembre 2014* ;
- le cas échéant, description et justification des scénarios spécifiques à certaines implantations étrangères, entités juridiques ou lignes d'activité (cf. article 171 de l'arrêté du 3 novembre 2014) ;
- informations sur les dépôts et leur diversification (en nombre de déposants) ;
- description des hypothèses retenues pour constituer le stock d'actifs liquides ;
- description des moyens mis en œuvre pour connaître en permanence le stock d'actifs liquides nécessaires et des hypothèses d'ajustement aux différents horizons considérés ;
- modalités de prise en compte du coût interne de la liquidité et analyse de l'évolution des indicateurs de coût de la liquidité au cours de l'exercice ;
- description des plans de financement : modalités d'évaluation de la capacité à lever des fonds auprès des sources de financement de l'entreprise en temps normal et en période de stress sur toutes les maturités envisagées et par devise (*hypothèses et résultats des tests effectués*…), modalités de prise en compte du risque de réputation, modalités de distinction des actifs grevés et non grevés disponibles à tout moment notamment en situation d'urgence et modalités de prise en compte des limitations d'ordre juridique, règlementaire et opérationnel aux éventuels transferts de liquidité et d'actifs non grevés entre les entités, modalités de prise en compte des possibles décotes en cas de cession d'actifs dans des délais brefs ;
- description des *stress scenarii* utilisés pour mesurer le risque encouru en cas de forte variation des paramètres de marché (indiquer les hypothèses retenues ainsi que leur périodicité de révision et décrire le processus de leur validation ; indiquer le résultat de la simulation et les modalités de sa communication à l'organe de surveillance), ainsi que les principales conclusions de l'analyse du risque encouru en cas de forte variation des paramètres de marché ;
- description des plans d'urgence mis en place pour faire face à une crise de liquidité (le plan doit prendre en compte à la fois le risque propre de refinancement, le risque d'assèchement des marchés et les interactions entre les deux risques) : *préciser notamment les procédures mises en place (identité et niveau hiérarchique des personnes concernées, solutions d'accès à la liquidité envisagée, communication au public, tests réguliers des plans d'urgence…)* ;
- description des plans de rétablissement de la liquidité fixant les stratégies et mesures de mise en œuvre afin de remédier aux éventuels déficits de liquidité et devant être testés régulièrement : *préciser notamment les mesures opérationnelles adoptées garantissant une mise en œuvre immédiate de ces plans de rétablissement (détention de sûretés immédiatement disponibles…)*.

16.2. Dispositif de surveillance des risques de liquidité :

- description synthétique des limites fixées en matière de risques de liquidité ainsi que du niveau de tolérance aux risques de liquidité *(préciser les niveaux, par type d'activité, par devise, par type de contrepartie, par rapport au volume d'opérations de ces contreparties et par rapport aux fonds propres)* ;
- périodicité de la révision des limites fixées en matière de risques de liquidité *(indiquer la date de la dernière révision)* ;
- périodicité de la révision des critères d'identification, de valorisation, de liquidité, de disponibilité des actifs et de prise en compte des instruments d'atténuation des risques de liquidité *(indiquer la date de la dernière révision)* ;
- périodicité de la révision des hypothèses et hypothèses alternatives liées à la situation de financement, aux positions de liquidité et aux facteurs d'atténuation du risque *(indiquer la date de la dernière révision)* ;

- dépassements éventuels de limites observés au cours du dernier exercice *(préciser les causes des dépassements, leur nombre et leur montant)* ;
- procédures suivies pour autoriser ces dépassements et mesures mises en œuvre pour régulariser ces dépassements ;
- description synthétique des reportings utilisés pour la gestion des risques de liquidité (*préciser notamment la périodicité et les destinataires des reportings)* ;
- description des incidents rencontrés au cours du dernier exercice ;
- description des dispositifs de mesure et de gestion de la qualité et de la composition des coussins de liquidité ;
- procédures de contrôle par la fonction de gestion des risques des actifs définis comme liquides ;
- modalités d'approbation et de révision par l'organe de surveillance des stratégies et politiques régissant la prise, la gestion, le suivi et la réduction des risques de liquidité (cf. article L.511-60 du Code monétaire et financier).

16.3. Dispositif de contrôle permanent de la gestion des risques de liquidité :

- présentation de l'environnement de contrôle de la gestion des risques de liquidité *(préciser le rôle du contrôle permanent).*

16.4. Pour les établissements de crédit (et les succursales d'établissements de crédit ayant leur siège à l'étranger) :

- modalités de prise en compte du coût interne de la liquidité et analyse de l'évolution des indicateurs de coût de la liquidité au cours de l'exercice ;
- dans le cadre de l'approche standard des risques de liquidité, les établissements élaborent une annexe au rapport :
  - décrivant les caractéristiques et hypothèses utilisées pour établir le tableau de trésorerie prévisionnelle et les modifications intervenues au cours de l'exercice,
  - comportant une analyse de l'évolution des impasses calculées dans les tableaux de trésorerie établis au cours de l'exercice ;
- pour les établissements utilisant l'approche avancée des risques de liquidité, préciser comment la méthodologie interne tient compte des répercussions systémiques pouvant résulter de l'importance de l'établissement sur son marché, notamment dans chacun des États membres de l'Union européenne où il exerce son activité (cf. article 150 de l'arrêté du 3 novembre 2014).

16.5. Résultats des contrôles permanents menés en matière de risques de liquidité :

- 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 présent rapport ;
- modalités de suivi des recommandations résultant des contrôles permanents *(outils, personnes en charge)* ;
- modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein des entreprises assujetties, par les personnes compétentes (cf. articles 11 f) et 26 a) de l'arrêté du 3 novembre 2014).

16.6. Conclusion synthétique sur l'exposition aux risques de liquidité

17. Risque de levier excessif

Cette partie ne s'applique pas aux sociétés de financement (cf. article 213 de l'arrêté du 3 novembre 2014).

- description des politiques, processus et indicateurs (incluant le ratio de levier et les asymétries entre actifs et obligations) utilisés pour détecter, gérer et suivre le risque de levier excessif de façon prudente (cf. article 211 de l'arrêté du 3 novembre 2014) ;
- cible de ratio de levier fixée par l'établissement ;
- *stress scenarii* utilisés pour évaluer la résistance de l'établissement en cas de diminution de ses fonds propres en raison de pertes attendues ou réalisées (cf. article 212 de l'arrêté du 3 novembre 2014), incluant des plans de renforcement des fonds propres en situation de crise.

18. Dispositif de contrôle interne des dispositions relatives au cantonnement des fonds de la clientèle des entreprises d'investissement, des établissements de paiement et des établissements de monnaie électronique

- description de l'outil de calcul du montant des fonds des clients, des procédures prévues pour leur placement et des vérifications associées (cf. notamment article 255 g) de l'arrêté du 3 novembre 2014) ;
- communication du rapport des commissaires aux comptes sur l'adéquation des dispositions mises en place en application des dispositions réglementaires relatives au cantonnement.

19. Dispositif de contrôle interne des dispositions de séparation bancaire

- description des indicateurs mis en place pour permettre le contrôle du respect du titre Ier de la loi n°2013-672 du 26 juillet 2013 de séparation et de régulation bancaire, notamment ceux relatifs aux activités de tenue de marché (cf. article 6 de l'arrêté du 9 septembre 2014 portant application du titre Ier de la loi de séparation bancaire) ;
- description synthétique des résultats des indicateurs mis en place ;
- résultats du contrôle permanent relatif aux exigences prévues à l'article 2 de l'arrêté du 9 septembre 2014 portant application du titre Ier de la loi n°2013-672 du 26 juillet 2013 de séparation et de régulation des activités bancaires, actions et mesures correctives engagées pour remédier aux insuffisances relevées ;
- résultats du contrôle périodique du respect du titre Ier de la loi n°2013-672 du 26 juillet 2013 de séparation et de régulation bancaire, actions et mesures correctives engagées pour remédier aux insuffisances relevées.

20. Informations spécifiques demandées aux conglomérats financiers

- total de bilan du groupe et total de bilan respectif du secteur bancaire, du secteur des assurances et du secteur non financier.

20.1. Dispositif de contrôle interne et d'évaluation des risques appliqué à l'ensemble des entités appartenant au conglomérat financier :

- présentation des conditions dans lesquelles les activités des entités d'assurance sont prises en compte dans le système de contrôle interne du conglomérat ;
- présentation des procédures anticipant l'impact des stratégies de développement sur le profil des risques et les exigences complémentaires en matière de fonds propres ;

– présentation des procédures permettant d'identifier, de mesurer, de surveiller et de maîtriser les transactions entre les différentes entités du conglomérat ainsi que la concentration des risques ;

– résultats des contrôles permanents menés sur les entités d'assurance.

20.2. Informations sur les risques liés aux entités du secteur des assurances :

– description des risques portés par les entités du secteur des assurances et qui sont de même nature que les risques liés aux activités bancaires et financières ;

– description des risques spécifiques attachés aux activités d'assurance *(il conviendra notamment de préciser quels risques sont gérés de façon centralisée, selon quelles procédures, ceux qui restent décentralisés).*

20.3. Informations sur les transactions intra-groupe :

– informations relatives aux transactions intragroupe réalisées au cours de l'année entre les entités du conglomérat ayant une activité bancaire ou de services d'investissement d'une part et celles ayant une activité d'assurance d'autre part dès lors qu'elles font au moins l'objet d'une influence notable :

- description de celles-ci, notamment en différenciant les différentes catégories définies à l'article 4 de l'instruction 2005-04 de la Commission bancaire et en soulignant le degré d'interdépendance des activités au sein du conglomérat,
- pour chaque type de transaction, le sens dans lequel elle est réalisée dans la majorité des cas (d'une entité ayant une activité bancaire ou de services d'investissement vers une entité ayant une activité d'assurance ou l'inverse), et les objectifs poursuivis,
- modalités de tarification interne de ces transactions ;

– information quantitative sur toute transaction intragroupe dont le montant excède 5 % de la somme des exigences de solvabilité applicables aux différents secteurs, calculée sur la base de l'arrêté annuel précédent :

- dès lors qu'ils sont supérieurs au seuil : le montant nominal cumulé des transactions donnant lieu à des versements de flux financiers hors opérations de marché (prêts, garanties, ventes d'actifs…) le montant global des commissions versées, et pour les opérations sur instruments financiers à terme, l'équivalent risque de crédit global (ou à défaut le montant notionnel global),
- pour chaque transaction, lorsqu'il est supérieur au seuil, le montant nominal de la transaction et la date de conclusion de celle-ci. Les conglomérats financiers donnent, de surcroît, une description de la transaction, en précisant l'identité des contreparties, le sens dans lequel elle est réalisée et les objectifs poursuivis, selon le modèle ci-après :

Type de transaction	Date de la conclusion de l'opération	Montant nominal pour les éléments du bilan, le montant notionnel et l'équivalent risque de crédit pour les instruments financiers à terme.	Description de l'opération (contreparties, sens, objectifs poursuivis …)

21. Annexe relative à la sécurité des moyens de paiement scripturaux mis à disposition ou gérés par l'établissement

Document à transmettre en double exemplaire.

Contexte

Cette annexe est consacrée à la sécurité des **moyens de paiement scripturaux** définis à l'article L. 311-3 du Code monétaire et financier, émis ou gérés par l'établissement.
Sont considérés comme moyens de paiement tous les instruments qui permettent à toute personne de transférer des fonds, quel que soit le support ou le procédé technique utilisé.

L'annexe est transmise par le Secrétariat général de l'Autorité de contrôle prudentiel et de résolution à la Banque de France pour l'exercice de sa mission définie au I de l'article L. 141-4 du Code monétaire et financier.

Les établissements gestionnaires de moyens de paiement sans être pour autant leurs émetteurs doivent renseigner cette annexe. Les établissements qui n'émettent ou ne gèrent aucun moyen de paiement portent la mention : « l'établissement n'émet ou ne gère aucun moyen de paiement au titre de son activité ».

Caractéristiques et contenu de l'annexe

L'annexe étant principalement destinée à la Banque de France, elle constitue un document autonome du reste des rapports établis en vertu des articles 258 à 266 de l'arrêté du 3 novembre 2014.

À travers cette annexe, les « établissements concernés » présentent **l'évaluation, la mesure et le suivi de la sécurité des moyens de paiement** qu'ils émettent ou qu'ils gèrent au regard de leurs procédures internes et des recommandations d'organismes externes telles que celles mentionnées dans la liste fournie en annexe.

Les informations attendues par la Banque de France se concentrent autour des 4 points suivants :

- identification des moyens de paiement émis ou gérés par l'établissement ;
- procédures et mesures mises en œuvre pour maîtriser les risques liés aux processus opérationnels associés aux moyens de paiement émis ou gérés ;
- types de contrôles axés sur la sécurité des moyens de paiement mis en place par l'établissement ;
- évolutions prévues dans le paysage des moyens de paiement émis ou gérés par l'établissement.

Cette annexe est composée :

- d'une **partie descriptive** récapitulant les quatre points évoqués ci-dessus et qui est détaillée dans la méthodologie de remplissage de l'annexe ;
- d'une **partie d'évaluation**, qui permet à l'établissement d'apprécier la qualité de ses réponses en fonction des objectifs de sécurité définis (Appendice A).

Sont exclues du champ de cette annexe toutes les données concernant les statistiques de fraude pour l'ensemble des moyens de paiement, lesquelles sont désormais communiquées via le questionnaire intitulé « Recensement de la fraude sur les moyens de paiement scripturaux » (site ONEGATE/OSCAMPS).

Le contenu doit être :

- exhaustif : toute information nécessaire à une correcte appréciation des moyens de paiement ;
- délimité : uniquement des informations concernant les moyens de paiement scripturaux.

Les établissements concernés peuvent également consulter une liste de questions les plus fréquemment posées, régulièrement mise à jour sur le site Internet de l'ACPR.

Méthodologie de remplissage de l'annexe

Le présent guide de remplissage détaille chacun des points évoqués précédemment et définit les termes employés. Sauf contrainte interne, les éléments devront être communiqués en respectant le formalisme du tableau fourni dans ce document.

Les établissements ayant répondu au questionnaire d'évaluation du « Référentiel de la sécurité du chèque » (RSC) de la Banque de France au titre de l'exercice sous revue, sont dispensés de suivre le plan d'analyse proposé pour le chèque, tout comme de transmettre la déclaration RSC dans l'annexe moyens de paiements scripturaux du rapport annuel.

Les établissements membres du GIE Cartes Bancaires pourront utilement s'inspirer du format de réponse proposé par le GIE Cartes Bancaires pour la carte bancaire « CB » qui devra être impérativement complété de leurs caractéristiques propres et pour chaque risque brut identifié, du risque résiduel subsistant après application des mesures de couverture.

Ceci ne dispense pas les déclarants de remplir le tableau fourni en annexe pour les autres cartes interbancaires (VISA-only, Mastercard-only…) et les cartes privatives qu'ils émettent ou gèrent.

I. Identification des moyens de paiement émis ou gérés par l'établissement

Fournir pour chaque moyen de paiement émis ou géré, une description synthétique (ex : SDD, SCT, etc.), la clientèle concernée (particuliers, professionnels…) ainsi que ses caractéristiques (phase dans le cycle de vie[4], modalités de fonctionnement pour les nouveaux moyens de paiement[5], etc.).

Un établissement doit fournir au moins une fois les caractéristiques détaillées de l'ensemble des moyens de paiement qu'il émet ou qu'il gère. Lors des exercices ultérieurs, seuls les nouveaux moyens de paiement innovants ou incorporant de nouvelles fonctionnalités font l'objet d'une description plus détaillée.

II. Procédures et mesures mises en place pour maîtriser les risques liés aux processus opérationnels des moyens de paiement émis ou gérés

Pour chaque moyen de paiement :

- identifier de façon synthétique les principaux risques auxquels sont exposés les processus opérationnels liés au moyen de paiement considéré **(risques bruts)**. Il s'agit d'évaluer la probabilité qu'un événement ou une situation se produise et son impact avant la prise en compte des mesures de prévention ou des mesures correctives ;
- indiquer les procédures et mesures prises par l'établissement pour maîtriser les risques identifiés **(mesures de couverture mises en œuvre)**, pouvant inclure les contrôles de premier niveau effectués par les opérationnels et qui ne sont pas du ressort des services de conformité (ces derniers seront décrits dans la partie « III – les différents types de contrôles axés sur les moyens de paiement ») ;
- fournir des éléments d'information sur la mise en œuvre des recommandations d'organismes externes en matière de sécurité des moyens de paiement (cf. appendice B).

Suite aux solutions mises en place en matière de maîtrise des risques, décrire de manière succincte les risques subsistant après l'application des mesures de couverture précédemment décrites **(risques résiduels)**.

La Banque de France s'attend à une certaine cohérence entre la fraude effectivement constatée par l'établissement et l'estimation des risques résiduels produite.

4. Les phases du cycle de vie : étude, lancement, développement, maturité, déclin, retrait.
5. Détailler ici les différentes versions du moyen de paiement (exemple: cartes de débit, carte de crédit, carte sans contact, paiement mobile…) et expliquer brièvement comment fonctionne ce moyen de paiement.

Cette partie ne doit en aucun cas être confondue avec une description des processus opérationnels mis en place par l'établissement. Elle doit porter exclusivement sur l'analyse, le traitement et le suivi des risques auxquels ces processus sont confrontés.

III. Les différents types de contrôles axés sur les moyens de paiement

Les établissements concernés donnent une description synthétique **des contrôles mis en œuvre en matière de sécurité des moyens de paiement** *(préciser, pour chaque contrôle, si ce dernier est effectué pour un moyen de paiement donné ou de façon transversale pour l'ensemble des moyens de paiement)*, dans le but de s'assurer de leur conformité avec les normes internes et les recommandations externes. Dans cette description l'établissement indique :

– *l'entité de contrôle :*
  - qui a effectué le(s) contrôle(s) (indication du responsable du contrôle),
  - quel est le niveau de rattachement de cette entité (hiérarchique et, le cas échéant, fonctionnel) ? Exemple : le contrôle est effectué par le responsable du Service Inspection Contrôle et Risques, qui est rattaché hiérarchiquement à la Direction Générale, etc.

– *l'objet du contrôle :*
  - quels sont les éléments contrôlés ?
  - à quel niveau du processus a (ont) été effectué(s) ce(s) contrôle(s) ? Il ne s'agit pas ici de décrire l'ensemble des processus, mais d'identifier dans un langage commun, à quelle tâche il est fait référence.

– *la périodicité des contrôles :*
  - s'agissait-il d'un (de) contrôle(s) périodique(s) ou permanent(s) ?
  - quelle a été la fréquence de ce(s) contrôle(s) ?
  - dans le cas du contrôle périodique, quelles ont été les missions concernant les moyens de paiement réalisées au cours de l'année écoulée et quelles sont les missions prévues pour l'année à venir ?

– *les constats du (des) contrôle(s) :*
  - quels ont été les dysfonctionnements constatés suite aux contrôles effectués ?

– *les actions correctives (effectuées ou envisagées) :*
  - suite aux constats précédents, quelles sont les solutions mises en œuvre ou envisagées pour remédier aux dysfonctionnements ? Il est utile de compléter l'information avec le calendrier de mise en œuvre des solutions.

IV. Perspectives et évolutions prévues

Cette partie concerne les évolutions prévues par l'établissement, comme l'émission d'un nouveau moyen de paiement ou toute modification touchant les moyens de paiement émis ou gérés actuellement.

En aucun cas, l'établissement ne doit confondre les **perspectives et évolutions prévues** avec les actions correctrices effectuées ou envisagées dans le cadre des contrôles décrits ci-dessus.

Exemple sur les perspectives et évolutions : La migration vers le format SEPA des virements et prélèvements, lancement d'une carte virtuelle, de cartes prépayées, abandon d'un moyen de paiement, etc.

Remarque importante concernant les groupes mutualistes

- Cas d'une entreprise assujettie affiliée à un organe central qui émet et/ou gère un moyen de paiement scriptural (responsable de l'analyse des risques au niveau global) :
  - l'organe central seul, produit l'analyse de risques dans la présente annexe. L'établissement affilié en est ainsi dispensé. Néanmoins il doit mentionner «qu'il se réfère à ce qui a été décrit par l'organe central, en matière d'analyse des risques et de mesures de couverture mises en place ». Les risques spécifiques à l'établissement lui-même, qui n'ont pas été décrits dans l'analyse fournie par l'organe central, devront néanmoins être précisés par l'établissement affilié.
  - cette remarque s'applique aussi à l'activité de contrôle périodique. Si celle-ci est effectuée sous la responsabilité de l'organe central et décrite par lui dans la partie « contrôle périodique », seuls les contrôles propres à l'établissement affilié doivent être fournis par ce dernier.
  - elle s'applique enfin à la description des évolutions prévues : l'établissement affilié ne doit alors décrire que les évolutions qui lui sont propres et non reprises par l'organe central.

- Cas où l'organe central n'émet ni ne gère de moyens de paiement, mais reste responsable de l'activité de contrôle (notamment les contrôles axés sur les moyens de paiement) :
  - l'établissement affilié doit décrire, de manière claire et précise, l'ensemble des contrôles axés sur les moyens de paiement mis en œuvre par l'organe central et ne doit à aucun moment renvoyer au rapport sur le contrôle interne de l'organe central (lequel ne comporte pas d'annexe relative à la sécurité des moyens de paiement).

Tableau de reporting :

Présentation : Afin de guider le déclarant dans l'élaboration de sa réponse et d'harmoniser les données des différents établissements, l'ensemble des informations peuvent être communiquées à travers le tableau de reporting présenté ci-après. Toutefois et même si ce modèle de reporting est encouragé, l'établissement peut utiliser son propre format de reporting dans la mesure où *a minima* les informations demandées ci-dessous y sont reprises.

Moyen de paiement :		
• **Identification et gestion des risques (par moyen de paiement)**		
Risques **bruts**[6]	**Mesures de couverture** mises en œuvre & Recommandations d'organismes externes	Risques **résiduels**
B) Perspectives et évolutions prévues (par moyen de paiement)		

C) L'activité de contrôle (axée sur les moyens de paiement)				
Entité de contrôle	Objet du contrôle	Périodicité de contrôle	Constats	Actions correctives (effectuées ou envisagées)

[6] Dans le cas où l'établissement n'est pas en mesure de coter ses risques bruts, il doit indiquer la mention « risques bruts non cotés » dans la colonne correspondante.

Terminologie

Moyen de paiement scriptural : instrument de paiement autre que la monnaie fiduciaire, qui permet à toute personne de transférer des fonds, quel que soit le support ou le procédé technique utilisé.

Processus opérationnels : ensemble d'activités corrélées ou qui interagissent, nécessaires à l'exploitation du moyen de paiement.

Risque opérationnel : risque de subir un préjudice en raison d'une inadéquation ou d'une défaillance attribuable aux procédures, aux personnes, aux systèmes ou encore aux événements extérieurs.

Risques bruts : les risques susceptibles d'affecter le bon fonctionnement et la sécurité des moyens de paiement, avant la prise en compte par l'établissement des procédures et mesures pour les maîtriser.

Mesures de couverture : ensemble d'actions mises en place par l'établissement afin de mieux maitriser ses risques, en diminuant leur impact ainsi que leur fréquence de survenance.

Risque résiduel : risque subsistant après prise en compte des mesures de couverture.

Conformité : respect des lois, des réglementations, des codes et des guides de pratiques professionnelles.

Contrôle interne : dispositif consistant à donner une assurance raisonnable quant au respect de la conformité.

Contrôle périodique (ou audit) : contrôle de conformité assuré sous forme d'enquêtes (missions d'audit).

Contrôle permanent : ensemble des procédures, des systèmes et des contrôles mis en œuvre pour vérifier de manière continue le respect des règles, recommandations et codes de bonne conduite édictés en matière de sécurité des moyens de paiement.

Évolution : ensemble des principales modifications technologiques ou organisationnelles pouvant avoir une incidence sur la sécurité des moyens de paiement hormis les actions correctives prises dans le cadre des contrôles permanents ou périodiques.

Appendice A

Grille d'analyse

Préambule

Cette grille d'analyse permet aux établissements assujettis de s'auto-évaluer. Elle complète le tableau de reporting des risques et de contrôle interne axé sur les moyens de paiement scripturaux, mais ne saurait se substituer à lui.

Depuis l'exercice 2011, ces deux documents servent à rendre compte annuellement du degré de maîtrise du moyen de paiement émis ou géré par l'établissement et du niveau de sécurité atteint.

Cette grille d'analyse est consacrée aux objectifs de sécurité. Elle permet à l'établissement de s'évaluer sur une échelle à quatre niveaux en respectant les critères d'appréciation fournis pour chaque objectif.

Elle doit être remplie en fonction des informations fournies dans le tableau de reporting transmis par l'établissement dans le cadre de l'annexe. En effet, ce dernier doit évaluer si les éléments qu'il a fournis dans le tableau de reporting répondent aux objectifs de sécurité énumérés dans le questionnaire.

L'établissement doit cocher la case correspondante et justifier ce choix dans la zone de commentaire associée à chacune des réponses.

Critères d'analyse du contenu des annexes (critères de fond)

Six critères ont été retenus pour permettre l'analyse formalisée du contenu des annexes. Celle-ci vise à déterminer de façon globale le niveau de maîtrise de la sécurité du moyen de paiement par l'établissement et à donner un aperçu de son activité de contrôle dans ce domaine.

1) **Évaluation du système d'identification des risques :** mise en place d'un système visant à recenser et analyser les principaux facteurs internes et externes susceptibles d'atteindre la sécurité du moyen de paiement.

Pas de réponse	
Incorrecte	
Incomplète	
Correcte	

Commentaire sur l'évaluation **:**

Critères d'évaluation :

a) l'établissement dispose d'un référentiel en matière de risque (typologie homogène, critères de recensement, d'analyse et de suivi…) basé sur une méthodologie reconnue et a mis en place un système intégré d'analyse et d'identification des risques ;
b) l'analyse des risques tient compte des évolutions internes et/ou externes à l'établissement ;
c) les risques identifiés sont classés par ordre de priorité (du plus important au plus faible en termes d'impact et de probabilité de survenance).

	Tableau de correspondance
Pas de réponse	Pas de communication de l'établissement concernant l'identification des risques.
Incorrecte	Aucun des critères d'appréciation n'est satisfait.
Incomplète	Satisfaction à au moins un des trois critères.
Correcte	Satisfaction à l'ensemble des critères.

2) <u>Mesures de couverture</u> : mise en œuvre d'une évaluation efficace des risques recensés et de solutions appropriées.

Pas de réponse	
Incorrecte	
Incomplète	
Correcte	

<u>Commentaire sur l'évaluation</u> :

<u>Critères d'évaluation</u> :

a) pour les principaux risques identifiés, l'établissement analyse les incidences potentielles (chiffrées ou non, financière ou non financière) et son degré de maîtrise estimé ;
b) l'analyse des risques donne lieu à des actions spécifiques, dont la responsabilité est clairement définie ;
c) les opérationnels participent au choix des mesures de couverture ;
d) des mesures préventives sont mises en place afin de prévenir les risques non acceptés par l'établissement et susceptibles de porter atteinte à la sécurité des moyens de paiement.

	Tableau de correspondance
Pas de réponse	Pas de communication de l'établissement concernant les mesures de couverture.
Incorrecte	Aucun des critères d'appréciation n'est satisfait.
Incomplète	Satisfaction à au moins un des quatre critères.
Correcte	Satisfaction à l'ensemble des critères.

3) <u>Application des principes et recommandations d'organismes externes</u> : mise en œuvre des recommandations exprimées par les organismes externes en matière de sécurité des moyens de paiement (voir la liste indicative de ces recommandations en appendice).

Pas de réponse	
Incorrecte	
Incomplète	
Correcte	

<u>Commentaire sur l'évaluation</u> :

<u>Critères d'évaluation</u> :

a) les recommandations susvisées concernant la sécurité du moyen de paiement sont clairement identifiées et intégrées dans les procédures de l'établissement ;
b) la mise en œuvre des différentes recommandations fait l'objet d'un suivi par le responsable de la conformité ou par un collaborateur en charge de la conformité.

	Tableau de correspondance
Pas de réponse	Pas de communication de l'établissement concernant les mesures de couverture.
Incorrecte	Aucun des critères d'appréciation n'est satisfait.
Incomplète	Satisfaction à un des deux critères.
Correcte	Satisfaction à l'ensemble des critères.

4) <u>L'impact des mesures de couverture et de suivi des risques</u> : les stratégies de couverture adoptées visent à renforcer la sécurité du moyen de paiement et à maîtriser les risques identifiés.

Pas de réponse	
Incorrecte	
Incomplète	
Correcte	

<u>Commentaire sur l'évaluation</u> :

Critères d'évaluation :

a) les mesures mises en place ont contribué au renforcement de la sécurité du moyen de paiement en diminuant l'impact du risque et/ou sa probabilité de survenance ;
b) l'établissement s'assure que les mesures adoptées n'engendrent pas l'apparition d'autres risques ;
c) une veille sur les risques identifiés et leurs évolutions a été instaurée.

	Tableau de correspondance
Pas de réponse	Pas de communication de l'établissement concernant l'organisation des contrôles.
Incorrecte	Aucun des critères d'appréciation n'est satisfait.
Incomplète	Satisfaction à au moins un des trois critères.
Correcte	Satisfaction à l'ensemble des critères.

5) <u>Le dispositif de contrôle :</u> les contrôles mis en place sont appropriés, correspondent à la nature et à la complexité des risques identifiés.

Pas de réponse	
Incorrecte	
Incomplète	
Correcte	

<u>Commentaire sur l'évaluation</u> :

Critères d'évaluation :

a) les activités de contrôle sont proportionnées aux enjeux de chaque risque et conçues pour réduire chacun d'entre eux ;
b) l'établissement veille à ce que son activité de contrôle assure le respect de la conformité et de la réglementation en vigueur ;
c) la mise en œuvre des mesures correctives fait l'objet d'un suivi régulier par les services de contrôle.

	Tableau de correspondance
Pas de réponse	Pas de communication de l'établissement concernant l'organisation des contrôles.
Incorrecte	Aucun des critères d'appréciation n'est satisfait.
Incomplète	Satisfaction à au moins un des trois critères.
Correcte	Satisfaction à l'ensemble des critères.

6) <u>Périodicité des contrôles</u> : le dispositif de contrôle interne relatif aux moyens de paiement scripturaux fait l'objet d'une surveillance permanente.

Pas de réponse	
Incorrecte	
Incomplète	
Correcte	

<u>Commentaire sur l'évaluation</u> :

Critères d'évaluation :

a) existence de contrôles réguliers dans le but de fiabiliser les processus existants et la sécurisation de l'ensemble des activités liées au moyens de paiement ;
b) mise en place de contrôles inopinés pour s'assurer que les principes et procédures de maîtrise de l'activité sont respectés ;
c) mise en place d'indicateurs précis pour définir la fréquence des contrôles ;
d) le dispositif de contrôle périodique couvre tout le périmètre auditable dans un délai raisonnable.

	Tableau de correspondance
Pas de réponse	Pas de communication de l'établissement concernant l'organisation des contrôles.
Incorrecte	Aucun des critères d'appréciation n'est satisfait.
Incomplète	Satisfaction à au moins un des quatre critères.
Correcte	Satisfaction à l'ensemble des critères.

Respect du format de réponse (critères de forme)

Le respect du format de réponse ci-dessous est requis pour permettre à la Banque de France d'obtenir des réponses harmonisées facilement exploitables. Ce respect est noté.

Format de réponse : l'établissement a parfaitement suivi le guide de remplissage et a rempli le tableau de reporting.

Pas de réponse	
Incorrect	
Incomplet	
Correcte	

Commentaire sur l'évaluation :

Critères d'évaluation :

a) le tableau de reporting a été complété par l'établissement ;
b) le tableau de reporting n'est pas suivi par l'établissement pour des raisons internes, qu'il a expressément communiquées.

	Tableau de correspondance
Pas de réponse	Pas d'information concernant cet établissement.
Incorrect	Aucun des critères d'appréciation n'est satisfait.
Incomplet	Satisfaction partielle à un des deux critères (par ex., tableau rempli partiellement ou pas rempli pour l'ensemble des moyens de paiement)
Correcte	Satisfaction aux critères a ou b sans restriction.

Appendice B

Exemples de recommandations

Dans le cadre de l'annexe sur les moyens de paiement prévu à l'article 262 de l'arrêté du 3 novembre 2014, l'établissement indique s'il a pris en compte les recommandations liées à la sécurité des moyens de paiement, émises par des organismes externes. Une liste non exhaustive de ces recommandations est reprise ci-dessous :

A- Les recommandations émises par le Forum européen sur la sécurité des paiements de détail (SecuRe Pay) :

SecuRe Pay a publié son premier rapport sur la sécurité des opérations par Internet le 31 janvier 2013. Ce rapport contient de nombreuses recommandations et bonnes pratiques, dont la mise en œuvre devait intervenir au plus tard au 1er février 2015.

L'intégralité des recommandations est disponible sous le lien suivant :
http://www.ecb.int/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

– Les recommandations sur la gouvernance et l'analyse de risques :

- rédaction d'une politique de sécurité, complète, documentée et régulièrement mise à jour ;
- analyse de risque sur les opérations de paiement par Internet, rédaction d'une procédure de gestion du changement et de gestion des incidents ;
- procédure de reporting des incidents au management et aux autorités compétentes, contrôle des conditions dans lesquelles les commerçants gèrent les données sensibles ;
- mise en place de mesures visant à réduire les risques identifiés, dans le respect de principes de sécurité tels que le « moindre privilège », utilisant des technologies à l'état de l'art et permettant d'assurer une défense en profondeur des systèmes ;
- procédure de continuité d'activité, traçabilité des opérations.

– Les recommandations sur l'identification du client :

- mise en œuvre de procédures de connaissance du client, également présentée sous l'abréviation anglophone KYC (Know Your Customer), information du client sur la sécurité des opérations et les procédures à suivre en cas d'incident.

– Les recommandations sur l'authentification renforcée du client :

- authentification renforcée du client lors du passage d'ordre de virement (sauf si le destinataire a été préalablement enregistré selon la même procédure, en cas de virement de compte à compte ou de virement de faible montant ; les virements au sein du même prestataire de service de paiement doivent faire l'objet d'une analyse de risque) ;
- authentification renforcée du client lors de toute modification de données sensibles (dont celles utilisées pour réaliser cette authentification) ;

- authentification renforcée du client pour les paiements par carte les plus risqués, y compris initiés via des wallets ;
- procédures sécurisées d'enrôlement des clients.

– Les recommandations sur la gestion des sessions :

- définition de règles relatives aux accès et à la durée des sessions ;
- monitoring des transactions, mise en place de systèmes de détection de la fraude ;
- protection des données sensibles.

– Les recommandations sur la communication envers les clients :

- mise en place de canaux sécurisés pour communiquer avec les clients, si nécessaire ;
- procédures d'assistance aux clients ;
- fixation de limites pour les opérations sur Internet, possibilité pour les clients de désactiver la fonctionnalité de paiement en ligne ;
- possibilité pour les clients de vérifier la bonne exécution de la transaction, fourniture de relevés accessibles dans un environnement sécurisé.

B- Les orientations émises par l'Autorité Bancaire Européenne (ABE)

L'ABE a publié le 19 décembre 2014 ses orientations relatives à la sécurité des paiements sur internet, qui définissent des exigences minimales communes pour les services de paiement sur Internet, et dont l'entrée en vigueur était fixée au 1er août 2015. Ces orientations font écho aux recommandations émises par le forum SecuRe Pay.

L'intégralité de ces orientations est disponible sous le lien suivant :
https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_FR+Guidelines+on+Internet+Payments.pdf/

– Les orientations sur la gouvernance et l'analyse de risques :

- rédaction d'une politique de sécurité, complète, documentée et régulièrement mise à jour ;
- analyse de risque sur les opérations de paiement par Internet, rédaction d'une procédure de gestion du changement et de gestion des incidents ;
- procédure de reporting des incidents au management et aux autorités compétentes, contrôle des conditions dans lesquelles les commerçants gèrent les données sensibles ;
- mise en place de mesures visant à atténuer les risques identifiés et permettant d'assurer une défense en profondeur des systèmes ;
- mise en place de systèmes permettant d'assurer la traçabilité complète des opérations et de la cinématique du mandat électronique.

– Les orientations sur les mesures de contrôle et de sécurité :

- mise en œuvre de procédures de connaissance du client, également présentée sous l'abréviation anglophone KYC (Know Your Customer), information du client sur la sécurité des opérations ;

- recours à l'authentification forte du client lors de l'initiation de paiements sur Internet et sur l'accès aux données sensibles de paiement ;
- définition de règles relatives aux accès et à la durée des accès aux services de paiement ;
- sécurisation de la fourniture des outils, logiciels et données d'authentification au client ;
- mise en place de dispositifs de suivi des opérations et de détection des tentatives de fraude ;
- protection des données sensibles de paiement stockées, traitées ou transmises.

– Les orientations relatives à la sensibilisation du client et à la communication :

- procédures d'assistance aux clients ;
- fixation de limites pour les opérations sur Internet, possibilité pour les clients de désactiver la fonctionnalité de paiement en ligne ;
- possibilité pour les clients de vérifier la bonne exécution de la transaction, fourniture de relevés accessibles dans un environnement sécurisé.

C- Les cadres de surveillance de l'Eurosystème pour les instruments de paiement

Ces cadres couvrent le virement, le prélèvement et la carte de paiement et ont été mises à jour au regard des recommandations SecuRe Pay. Ils sont respectivement accessibles en ligne sous les liens suivants :

http://www.ecb.europa.eu/pub/pdf/other/oversightframeworkcredittransferschemes2010en.pdf

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

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

D- Les recommandations de l'Observatoire de la sécurité des cartes de paiement

L'Observatoire de la sécurité des cartes de paiement est une instance destinée à favoriser l'échange d'informations et la concertation entre toutes les parties concernées par le bon fonctionnement de la sécurité des systèmes de paiement par carte. Il émet chaque année des recommandations visant à renforcer cette dernière.

– Paiements par téléphone mobile et cartes sans contact :

- mise en place de mesures permettant, lorsque cela est nécessaire, de s'assurer du consentement du porteur. Par exemple, par la mise à disposition de moyens simples pour activer et désactiver ces nouveaux modes d'initiation, ou pour valider toute transaction ;
- mise en place d'analyses de risques et d'études sécuritaires avant tout déploiement à grande échelle ;
- pour les paiements par téléphone mobile, fourniture d'un code personnel de paiement différent du code PIN de la carte SIM, ainsi que du code confidentiel de la carte de paiement de l'utilisateur ; lorsque ce code personnel est modifiable par l'utilisateur, l'émetteur bancaire doit lui recommander d'en utiliser un différent des autres codes en sa possession ;

- les acteurs impliqués dans l'ensemble des opérations liées au paiement sans contact par téléphone mobile, doivent mettre en œuvre des mesures de protection cryptographiques garantissant l'intégrité et la confidentialité des données échangées entre les systèmes.

– Sécurité des paiements à distance :

- renforcement des méthodes de sécurisation, afin de porter la sécurité des paiements à distance à un niveau équivalent à celui des paiements de proximité et sur automate.
  Exemple : privilégier des méthodes de paiement en vente à distance permettant une authentification forte du porteur afin de permettre au commerçant d'être assuré de l'authenticité de la carte et du porteur, ainsi que du consentement de celui-ci.

- faciliter l'usage des solutions techniques déjà disponibles (code à usage unique, lecteur autonome de carte EMV…), en maîtrisant le coût de leur déploiement et en s'assurant que leur diffusion s'accompagne d'une information et d'une éducation du porteur.

– Usage de la biométrie comme facteur d'authentification lors de paiements par carte :

- nécessité d'une analyse des risques liés à l'usage de l'authentification biométrique afin que le niveau de protection des solutions mises en œuvre soit au moins équivalent à celui offert par les techniques déjà en place (code confidentiel et carte à puce pour le paiement de proximité, code non rejouable pour le paiement à distance).

– Effet du « co-marquage » sur la sécurité des cartes de paiement :

- pour toute nouvelle carte « co-marquée », l'établissement émetteur veille à l'application complète des mesures de sécurité existantes dans l'environnement des cartes de paiement pour le recueil, le stockage et la gestion des données sensibles ;

- dans le cas de co-existence d'applications, les émetteurs choisissent des cartes répondant à un niveau éprouvé et reconnu de protection de l'application de paiement.

– Mesures de sécurité PCI :

- adoption et mise en place des mesures de sécurité PCI par l'ensemble du processus d'acceptation et d'acquisition.

– Conseils de prudence à l'usage des porteurs :

- les conseils de prudence publiés par l'Observatoire doivent faire l'objet d'une communication aux porteurs de cartes, dans le but de les informer sur les bonnes pratiques à adopter et les risques auxquels ils sont confrontés.

– Cartes prépayées :

- la distribution des cartes prépayées doit s'accompagner de mesures visant à protéger les consommateurs, notamment en les informant sur les modes d'utilisation de ces instruments et en assurant la transparence tarifaire ;

- ces cartes présentent un profil de risques similaire à celui des cartes de paiement classiques et doivent donc être soumises aux mêmes mesures de sécurité, tant pour les transactions de proximité que pour les transactions à distance ;

- les cartes prépayées se caractérisent en outre par des risques propres liés au processus de rechargement et au mode de distribution. Elles doivent prévoir des dispositifs de sécurité adaptés afin de s'en prémunir.

– Mesures de sécurité appliquées aux dispositifs d'émission immédiate de cartes en agence ou en magasin (« Instant issuing ») :

- mise en place d'une analyse de risques et ajustement permanent du niveau de sécurité de ces dispositifs.

E- Les recommandations émises par la Banque de France

La Banque de France a, quant à elle, émis des recommandations concernant la sécurité de la banque en ligne et des paiements par carte en ligne :

– la sécurité de la banque en ligne :

- mise en œuvre de solutions d'authentification « non rejouable », généralisées à l'ensemble de la clientèle utilisant des services de banque en ligne.

– la sécurité des paiements par carte en ligne :

- mise en œuvre de solutions d'authentification « non rejouable » du porteur de la carte pour tout achat en ligne.

Annexe 1

Exemple de méthode de calcul des chocs uniformes de taux sur les activités autres que de négociation

Les établissements assujettis doivent inclure dans leur rapport de contrôle interne les résultats d'un choc uniforme à un an sur le PNB courant et, le cas échéant, les résultats d'un choc uniforme, à la hausse et à la baisse, sur les fonds propres. Ces résultats sont produits sur la base de méthodologies propres à chaque établissement. À titre d'exemple, cette annexe décrit les principales étapes des méthodes de calcul qui pourront être utilisées par les établissements.

Calcul d'un choc uniforme, à la hausse et à la baisse, sur les fonds propres

Dans l'exemple suivant, le choc retenu est de 200 bp. Toutefois, la méthode est analogue pour les chocs correspondant aux 1er et 99ème centiles des variations observées de taux d'intérêt.

1re étape : répartition des lignes de bilan et de hors bilan en bandes de maturité et calcul d'une position nette unique par bande de maturité en euros. Utilisation de la maturité résiduelle.

Les établissements pourront traiter certains actifs et passifs conformément aux éléments suivants :

- inclusion des immobilisations et des fonds propres ;
- traitement des éléments du bilan et de hors bilan à leur valeur comptable. Le traitement du hors bilan peut se limiter aux engagements de financement retenus pour leur valeur nominale ;
- les éléments de bilan et de hors bilan retenus peuvent ne pas tenir compte de données de production nouvelle. Les remboursements anticipés peuvent être pris en compte en fonction des données historiques propres ;
- prise en compte des instruments à taux fixes selon la maturité résiduelle et prise en compte des instruments à taux variable selon la maturité résiduelle jusqu'à la date du prochain fixing ;
- les opérations de grand nombre et petite taille peuvent être estimées statistiquement ;
- calcul des maturités des produits dérivés par rapport à celles des sous-jacents et conversion des produits optionnels en équivalent delta ;
- traitement des futures, forwards, y compris FRA, comme une combinaison d'une position courte et d'une position longue. La maturité d'un future ou d'un FRA peut être définie comme la période jusqu'à l'exercice du contrat plus, le cas échéant, celle de l'instrument sous-jacent ;
- traitement des swaps comme deux positions notionnelles dont on retient les maturités : à titre d'exemple, un swap pour lequel une banque reçoit le variable et paie le fixe peut être traité comme une position longue de maturité équivalente à la période jusqu'au prochain pricing et une position courte d'une maturité équivalente à la durée du swap ;
- écoulement linéaire sur 10 ans des comptes courants débiteurs, livrets ordinaires, livrets jeunes, LEP, CEL, Codevi ou autres livrets et écoulement linéaire sur 8 ans des PEL (les PEL peuvent également faire l'objet de conventions d'écoulement variables selon la génération des contrats).

2e étape : assortir chaque position nette d'un facteur de pondération reflétant la sensibilité de chaque position à une variation donnée de taux d'intérêt. À titre d'exemple, dans le tableau ci-dessous, les facteurs de pondération sont fondés sur les hypothèses d'une hausse et d'une baisse de 200 points de base et d'un proxy de la duration modifiée sur des positions situées au milieu de chaque bande de maturité actualisées au taux de 5 %. 8 bandes de maturité sont ici retenues.

Facteurs de pondération par bande de maturité d'un choc de taux à la hausse et à la baisse

Bande de maturité	Centre de la bande de maturité	Proxy de la duration modifiée	Variation de taux	Facteur de pondération
Moins de 3 mois	1,5 mois	0,12	+ ou - 2%	+ ou - 0,24%
3 à 6 mois	4,5 mois	0,36	+ ou - 2%	+ ou - 0,72%
6 mois à un an	9 mois	0,71	+ ou - 2%	+ ou - 1,43%
1 à 3 ans	2 ans	1,83	+ ou - 2%	+ ou - 3,66%
3 à 5 ans	4 ans	3,55	+ ou - 2%	+ ou - 7,09%
5 à 10 ans	7,5 ans	6,09	+ ou – 2%	+ ou - 12,17%
10 à 15 ans	12,5 ans	8,92	+ ou - 2%	+ ou - 17,84%
Plus de 15 ans	17,5 ans	11,21	+ ou - 2%	+ ou - 22,43%

3e étape : somme des positions pondérées pour conduire à une position nette courte ou longue du portefeuille bancaire (défini comme couvrant les activités autres que de négociation) dans la devise donnée – toute devise constituant plus de 5 % du portefeuille bancaire peut être reportée séparément.

4e étape : calcul de la position pondérée de tout le portefeuille bancaire en sommant les positions des différentes devises.

5e étape : comparaison de la position pondérée du portefeuille avec les fonds propres (Tier 1 et Tier 2).

Calcul d'un choc uniforme de 200 bp à un an sur le PNB courant

1re étape : répartition des lignes de bilan et de hors bilan exposées au risque de taux d'intérêt par bandes de maturité (moins de 3 mois, 3 à 6 mois, 6 mois à un an) en euros jusqu'à un an.

2e étape : calcul des gaps entre actifs et passifs par bande de maturité.

3e étape : (somme des gaps obtenus) × 2 %.

4e étape : comparaison du montant obtenu avec le PNB de l'exercice.

Annexe 2

Informations attendues dans l'annexe de présentation de l'organisation du dispositif de contrôle interne et de l'organisation comptable

1. Présentation synthétique du dispositif de contrôle interne [7]

1.1. Dispositif général de contrôle interne :

– joindre un organigramme faisant apparaître les unités consacrées au(x) contrôle(s) permanent(s) et notamment au contrôle de la conformité, ainsi qu'au contrôle périodique et le positionnement hiérarchique de leurs responsables ;

– coordination prévue entre les différents acteurs du contrôle interne ;

– description du contrôle des activités externalisées (au sens des paragraphes 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)*, etc. ;

– mesures prises en cas d'implantations dans des pays où la réglementation locale fait obstacle à l'application des règles prévues par l'arrêté du 3 novembre 2014 ;

– 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 ;

– modalités de suivi et de contrôle des opérations réalisées dans le cadre de la libre prestation de services.

1.2. Dispositif de contrôle permanent (y compris le dispositif de contrôle de la conformité) :

– description de l'organisation des différents niveaux qui participent au contrôle permanent et au contrôle de la conformité ;

– champ d'intervention du contrôle permanent et du contrôle de la conformité y compris pour l'activité à l'étranger *(activités, processus et entités)* ;

– nombre d'agents affectés au dispositif de contrôle permanent et au contrôle de la conformité (cf. article 13 – 1er tiret – de l'arrêté du 3 novembre 2014) (effectif en équivalent temps plein par rapport à l'effectif total de l'établissement) ;

– 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) ;

– modalités d'information du responsable du contrôle permanent et des dirigeants effectifs en particulier sur l'activité et les résultats du contrôle de la conformité.

1.3. Dispositif de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB/FT) :

– description de l'organisation du dispositif LCB/FT : effectifs, formations dispensées et modalités d'informations du personnel concerné ;

– description du dispositif de suivi et d'analyse mis en place pour détecter les opérations qui constituent des anomalies ;

7. Cette partie peut être adaptée par les établissements en fonction de leur taille, de leur organisation, de la nature et du volume de leurs activités, de leurs implantations et des risques de différentes natures auxquels ils sont exposés (notamment lorsque les responsabilités du contrôle permanent et du contrôle périodique sont confiées, soit à une seule personne, soit aux dirigeants effectifs)

- description du dispositif de suivi et d'analyse mis en place pour détecter les personnes ou entités faisant l'objet d'une mesure de gel des avoirs ;
- modalités de contrôles des obligations de vigilance vis-à-vis des filiales et succursales implantées à l'étranger ;
- conditions de recours à un tiers pour l'identification de la clientèle (cf. articles L. 561-7 et R. 561-13-I du Code monétaire et financier) : *description des conditions dans lesquelles a lieu le recours à un tiers, description des procédures de recours à un tiers et des modalités de contrôle des diligences mises en œuvre par un tiers, préciser le pays d'implantation du tiers, description des principales dispositions du contrat établi le cas échéant* ;
- conditions de recours à des prestataires pour l'identification de la clientèle (cf. article R. 561-13-II du Code monétaire et financier) : *description des conditions dans lesquelles a lieu le recours à un prestataire, description des procédures et du dispositif de contrôle des diligences mises en œuvre par les prestataires, préciser le pays d'implantation du prestataire, description des principales dispositions du contrat* ;
- conditions de recours aux services d'agents (cf. article L. 523-1 du Code monétaire et financier) : *description des procédures et du dispositif de contrôle de la mise en œuvre des obligations de vigilance par les agents, description des principales dispositions du mandat relatives au dispositif LCB/FT.*

1.4. Fonction de gestion des risques :

- organisation de la fonction de gestion des risques *(champs d'intervention, effectifs des unités en charge de la mesure, de la surveillance et de la maîtrise des risques et moyens techniques à disposition)* ;
- pour un groupe, organisation de la fonction de gestion des risques ;
- description des procédures et systèmes mis en place pour le suivi des risques dans le cadre des opérations sur des nouveaux produits, des modifications significatives apportées à un produit préexistant, des opérations de croissance interne et externe et des transactions exceptionnelles (cf. article 221 de l'arrêté du 3 novembre 2014) ;
- description synthétique de l'analyse conduite sur ces nouveaux produits et opérations.

1.5. Dispositif de contrôle périodique :

- description de l'organisation des différents niveaux qui participent à l'organisation du système de contrôle périodique et champ d'intervention du contrôle périodique y compris pour l'activité à l'étranger et les activités externalisées *(activités, processus et entités)* ;
- moyens humains affectés au dispositif de contrôle périodique (cf. article 25 de l'arrêté du 3 novembre 2014) (effectif en équivalent temps plein par rapport à l'effectif total de l'établissement) ;
- description, formalisation et date(s) de mise à jour des procédures sur lesquelles s'appuie le contrôle périodique y compris pour l'activité à l'étranger et les activités externalisées (dont les procédures d'examen de la conformité) en faisant ressortir les modifications significatives intervenues au cours de l'exercice.

2. Présentation synthétique de l'organisation comptable

- description, formalisation et date(s) de mise à jour des procédures relatives à la piste d'audit en ce qui concerne l'information comprise dans les documents comptables ainsi que celles figurant dans les situations destinées à l'Autorité de contrôle prudentiel et de résolution, ou à la BCE selon les cas, et celles nécessaires au calcul des normes de gestion ;
- organisation mise en place afin de garantir la qualité et la fiabilité de la piste d'audit ;
- modalités d'isolement et de suivi des avoirs détenus pour le compte de tiers (cf. article 92 de l'arrêté du 3 novembre 2014) ;
- modalités de suivi et de traitement des écarts entre le système d'information comptable et le système d'information de gestion.

Annexe 3

Mesures mises en œuvre en faveur des clients en situation de fragilité financière (arrêté du 5 novembre 2014 portant homologation de la charte d'inclusion bancaire et de prévention du surendettement)

I. Formation :

1.1 Pourcentage des conseillers clientèle ayant suivi, au cours de l'année sous revue, une formation adaptée sur l'offre spécifique, la clientèle à laquelle elle est destinée et le suivi des clients bénéficiant des services bancaires de base (SBB) : %

1.2 Rappel de formation systématique prévu pour les conseillers ayant déjà suivi la formation : Oui/Non

1.3 Pourcentage des personnels salariés en contact avec la clientèle ayant suivi, au cours de l'année sous revue, une formation sur les dispositifs spécifiques dédiés aux clients en situation de fragilité en place au sein de leur entreprise : %

1.4 Rappel de formation systématique prévu pour les personnes visées au 1.3 ci-dessus ayant déjà suivi la formation : Oui/Non

1.5 Pourcentage de personnes agissant pour le compte de l'entreprise (hors personnel salarié) ayant suivi, au cours de l'année sous revue, une formation sur les dispositifs spécifiques dédiés aux clients en situation de fragilité mis en place : %

1.6 Rappel de formation systématique prévu pour les personnes visées au 1.5 ci-dessus ayant déjà suivi la formation : Oui/Non

II. Contrôle interne[8]

2.1. Le dispositif de contrôle permanent (1er et 2ème niveau) couvre-t-il l'ensemble des mesures relatives :

2.1.1. - au renforcement de l'accès aux services bancaires et services de paiement et à la facilitation de leur usage ? Oui / Non

2.1.2. - à la prévention du surendettement / détection ? Oui / Non

2.1.3. - à la prévention du surendettement / accompagnement ? Oui / Non

2.1.4. - à la formation des personnels et plus particulièrement aux points 1.1 à 1.6 ci-dessus ? Oui / Non

2.2. L'ensemble des points 2.1.1 à 2.1.4 sont-ils couverts sur le cycle de contrôle périodique ? Oui / Non

2.3. Des anomalies significatives ont-elles été détectées à l'occasion des contrôles permanents et le cas échéant périodiques au cours de l'année sous revue ? Oui / Non.
La réponse « Non » dispense de répondre aux questions 2.4 et 2.5

2.4. Si oui, indiquez les principales (dans la limite de 3)

2.5. Les actions correctives nécessaires ont-elles été mises en œuvre ? Oui/ Non

III. Commentaires ou remarques sur la mise en œuvre du dispositif d'inclusion bancaire et de prévention du surendettement (facultatif)

[8] Commentaires explicatifs à apporter en partie III en cas de réponse « non » à l'une des questions ci-dessous.