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

Juillet 2018

Rapport sur le contrôle interne
Établissements de crédit, sociétés de financement et entreprises d'investissement

(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 2

1. Présentation générale des activités exercées et des risques encourus par l'établissement 3
2. Modifications significatives apportées à l'organisation du dispositif de contrôle interne 3
3. Gouvernance 4
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) 8
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) 8
6. Processus d'évaluation de l'adéquation du capital interne 8
7. Risque de non conformité (hors risque de blanchiment des capitaux et de financement du terrorisme) 9
9. Risque de crédit et de contrepartie (cf. articles 106 à 121 de l'arrêté du 3 novembre 2014) 11
10. Risques associés aux contrats dérivés de gré à gré 16
11. Risques de marché 17
12. Risque opérationnel 18
13. Risque comptable 21
14. Risque de taux d'intérêt global 21
15. Risque d'intermédiation des prestataires de services d'investissement 23
16. Risque de règlement/livraison 24
17. Risques de liquidité 24
18. Risque de levier excessif 27
19. Dispositif de contrôle interne des dispositions relatives à la protection des fonds de la clientèle des entreprises d'investissement 27
20. Dispositions de séparation bancaire 28
21. Politique en matière d'externalisation 29
22. Informations spécifiques demandées aux conglomérats financiers 30
23. Annexe relative à la sécurité des moyens de paiement scripturaux mis à disposition ou gérés par l'établissement 32

Annexe 1 61

Annexe 2 63

Annexe 3 65

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 rappelé que conformément aux dispositions de l'article 4 de l'instruction n°2017-I-24, 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 ainsi que les extraits des procès-verbaux des réunions au cours desquelles ils sont examinés, doivent être adressés, de façon trimestrielle, au Secrétariat général de l'Autorité de contrôle prudentiel et de résolution (SGACPR).

Ces documents ainsi que le rapport de contrôle interne doivent être, conformément aux dispositions des articles 12 et 13 de l'instruction n°2017-I-24, communiqués au SGACPR **par télétransmission sous format bureautique**, selon des modalités techniques définies par l'ACPR **et signés électroniquement** selon les modalités définies par l'instruction n° 2015-I-19 modifiée et par l'annexe I de l'instruction n°2017-I-24.

Le rapport de contrôle interne doit être remis au SGACPR au plus tard :

- le 31 mars suivant la fin de chaque exercice pour les groupes et les établissements soumis à la supervision directe de la Banque centrale européenne, à l'exception de la partie relative à la politique et aux pratiques de rémunération qui peut être remise au plus tard le 30 avril suivant la fin de chaque exercice ;
- le 30 avril suivant la fin de chaque exercice pour les autres assujettis, y compris la partie relative à la politique et aux pratiques de rémunération pour les établissements qui y sont soumis.

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, 19, 20, 23 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 ;

– 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) ;

– description du cadre et du processus utilisés pour collecter, stocker et agréger les données sur les risques à différents niveaux dans l'établissement, y compris pour l'activité à l'étranger et les activités externalisées.

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.

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 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 2018, cette partie devra inclure une description des adaptations prises par l'établissement pour se mettre en conformité avec les nouvelles dispositions introduites par les orientations de l'ABE sur la gouvernance interne, qui entrent en vigueur à compter du 30 juin 2018.*

3.1. Principes généraux de gouvernance

- description de la politique de « *culture du risque* » déployée au sein de l'établissement : présentation synthétique des procédures de communication et des programmes de formation du personnel sur le profil de risque et leur responsabilité en matière de gestion des risques… ;
- présentation des normes éthiques et professionnelles promues par l'établissement *(indiquer s'il s'agit de normes élaborées en interne ou si application de normes publiées par des associations/organismes externes)*, description du dispositif mis en œuvre pour s'assurer de leur bonne application en interne, du processus mis en œuvre en cas de manquement et des modalités d'information aux instances dirigeantes… ;
- description des procédures mises en place pour identifier, gérer et prévenir les conflits d'intérêts au sein de l'établissement, modalités d'approbation et de révision de ces dernières.

3.2. Implication des organes dirigeants dans le contrôle interne

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

- 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) ;

- 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) ;
- modalités d'information de l'organe de surveillance concernant l'évaluation périodique effectuée par le Comité des nominations sur les connaissances, les compétences et l'expérience des membres de l'organe de surveillance, tant individuellement que collectivement (cf. article L. 511-100 du Code monétaire et financier). Communiquer au SGACPR les conclusions de cette évaluation.

3.2.2. 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 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).

3.2.3. 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).

3.2.4. 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).

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

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

3.3.1. 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 et à la partie 2.4.2 des Orientations ABE ;
- 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) ;
- description du rôle des fonctions risques, conformité et support dans la conception et la mise en œuvre de la politique de rémunération (cf. paragraphes 30, 32 à 35, 54 à 56 des Orientations ABE) ;
- 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).

3.3.2. 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 (relatifs, absolus, quantitatifs, qualitatifs) utilisés pour mesurer la performance et ajuster la rémunération au risque (cf. paragraphe 194 des Orientations ABE),
  - des critères (relatifs, absolus, quantitatifs, qualitatifs) définis pour définir le lien entre rémunération et performance (cf. paragraphe 194 des Orientations ABE),
  - 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,
  - des critères utilisés pour déterminer les montants en cas de résiliation anticipée du contrat de travail, sous réserve des dispositions applicables du code du travail (cf. paragraphe 144 des Orientations),
  - de la politique en place pour prévenir le contournement de la réglementation par le personnel à travers les mécanismes de couverture individuelle (cf. partie 10.1 des Orientations).
- le cas échéant, description, périmètre et justification des exemptions prévues aux articles 198 et 199 de l'arrêté du 3 novembre 2014 appliquées par l'établissement ;
- 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 et parties 12 et 14.1.3 des Orientations ABE) ;
- 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 et paragraphes 202, 218 des Orientations ABE) ainsi que l'impact de la politique de rémunération sur le capital et la liquidité (cf. paragraphes 109 et 111 des Orientations ABE) ;

– 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 (*pour rappel, l'assemblée générale compétente pour les employés d'une filiale est celle de la filiale et non pas celle de l'entreprise-mère*) 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 et de la section 2.3 des Orientations ABE, et mention de toute éventuelle réduction du plafond en application du paragraphe 43 des Orientations ABE.

3.3.3. 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) ;

– la rémunération totale de chaque dirigeant effectif ainsi que celle du responsable de la fonction de gestion des risques et, le cas échéant, du responsable de la conformité (cf. article 266 de l'arrêté du 3 novembre 2014).

3.3.4. 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 et partie 4 des Orientations de l'ABE).

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)

- planning des missions (risques et/ou entités ayant fait l'objet d'une vérification du contrôle périodique au cours de l'exercice écoulé), état d'achèvement et ressources allouées en jour-homme ;
- 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, dirigeant ou membre de l'organe de surveillance –, 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, des dirigeants effectifs et des membres de l'organe de surveillance, 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 du périmètre des activités pertinentes pour l'étude de l'adéquation du capital interne, et de l'approche utilisée pour déterminer la matérialité des risques ;
- description des méthodologies employées pour la mesure, l'évaluation et l'agrégation des risques pour quantifier le capital interne (horizons d'analyse, approche par la valeur économique, description des modèles et paramètres de calcul…). Cette description doit inclure des explications concernant les limites ou faiblesses de la méthodologie de calcul employée, ainsi que la façon dont ces éléments sont gérés, voire corrigés dans l'étude d'adéquation du capital interne ;
- 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) ;

- description de l'élaboration et de la mise à jour d'un plan de capitalisation en vue de s'assurer du maintien d'un montant de capital réglementaire et interne suffisant sur une durée d'au moins 3 ans, même dans des circonstances adverses (simulation de crise) :
    - niveau et définition du capital interne alloué par type de risques pour l'exercice écoulé en expliquant les principales différences entre le capital interne et le capital réglementaire, ainsi que les méthodes et hypothèses utilisées pour l'allocation du capital au sein de l'établissement,
    - prévisions du niveau de capital interne
- 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, description du champ d'application et du processus d'élaboration ainsi que de sa prise en compte dans les processus de décision managériale ;
- modalités de contrôle prévues afin de vérifier que ces systèmes et procédures demeurent adaptés à l'évolution du profil de risques de l'établissement ;
- documentation formalisant le process d'élaboration et de validation de l'adéquation du capital interne, des hypothèses, du plan de capitalisation, des simulations de crise et des méthodologies utilisées dans le process, notamment la répartition des rôles ainsi que l'information et l'implication des organes de gestion et/ou de surveillance dans la validation ;
- documentation formalisant l'intégration de ce process dans la stratégie globale de l'établissement, notamment par l'intégration des problématiques de capital interne et d'appétit au risque dans les process de prises de décisions managériales via des reportings appropriés ;
- les établissements soumis à CRR et ne se trouvant pas sous la supervision directe de la BCE, doivent remettre un « manuel du lecteur », élaboré comme un document global facilitant l'évaluation de la documentation justifiant de leur adéquation en capital. À cet effet, le «manuel du lecteur» doit fournir une vue d'ensemble de tous les documents communiqués aux autorités compétentes sur ce sujet, ainsi que de leur statut (nouveau, non modifié, modifié avec des corrections mineures, etc.). Le «manuel du lecteur» doit essentiellement fonctionner comme un index reliant les éléments d'information spécifiques prévus pour le rapport de contrôle interne aux documents fournis à l'autorité compétente concernant l'évaluation de son adéquation en capital. Le «manuel du lecteur» doit également comporter des renseignements concernant les modifications significatives apportées aux informations par rapport à celles communiquées précédemment, les éléments éventuellement exclus des informations communiquées, ainsi que toute autre information qui pourrait être utile à l'autorité compétente en vue de l'évaluation. En outre, le «manuel du lecteur» doit contenir des références à toutes les informations rendues publiques par l'établissement sur son adéquation en capital ;
- les établissements soumis à CRR et ne se trouvant pas sous la supervision directe de la BCE, doivent formaliser et remettre les conclusions des évaluations de l'adéquation du capital interne ainsi que leur incidence sur la gestion du risque et sur la gestion globale de l'établissement.

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

Nota bene : *À compter de l'exercice 2018, les informations relatives au risque de blanchiment des capitaux et de financement du terrorisme sont à remettre dans un rapport annuel de contrôle interne dédié, prévu aux articles R.561-38-6, R.561-38-7 et R.562-1 du code monétaire et financier. Les modalités de remise de ce rapport seront précisées par un futur arrêté prévu pour l'automne 2018.*

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) ;
- les procédures mises en place pour permettre au personnel de signaler à l'ACPR tout manquement aux obligations définies par les règlements européens et par le Code monétaire et financier (cf. article L. 634-1 et L. 634-2 du Code monétaire et financier).

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 crédit et de contrepartie (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).*

***Nota bene** : Pour l'exercice 2018, cette partie devra inclure une description synthétique des adaptations prises par l'établissement pour se mettre en conformité avec les nouvelles dispositions introduites par les orientations de l'ABE sur les pratiques de gestion du risque de crédit et à la comptabilisation des pertes de crédit attendues, qui sont entrées en vigueur depuis le 1er janvier 2018.*

8.1. 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, d'escalade et/ou de limites ;
- 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.

8.2. 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, par secteurs d'activité 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)* ;
- 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 ;
- description des dispositifs de suivi des indicateurs avancés du risque (préciser les principaux critères de placement des contreparties sous watch-list) ;
- modalités et périodicité de l'analyse de la qualité des engagements de crédit ; 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 ;
- modalités et périodicité de la réévaluation des garanties et collatéraux, ainsi que les principaux résultats des contrôles réalisés dans l'année le cas échéant ;

- 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) ;
- description du processus d'évaluation comptable des pertes de crédit attendues (méthodes utilisées, facteurs et hypothèses pris en compte dans les modèles internes développés, périodicité de revue…) ;
- modalités et périodicité des décisions de provisionnement, incluant le cas échéant un dispositif de délégation et/ou d'escalade ;
- modalités et périodicité des exercices de back-testing des modèles de provisionnement collectif et statistique, ainsi que les principaux résultats de l'année le cas échéant ;
- modalités et périodicité de l'analyse des risques de perte de valeur des actifs loués (opérations de location à caractère financier) ;
- modalités et périodicité de l'analyse des risques de perte de valeur des actifs immobiliers financés (y compris les actifs financés en crédit-bail) ;
- 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 ;
- répartition des engagements de crédits à l'habitat par type de garantie (caution, hypothèques, etc.) ;

- présentation de la LTV sur crédits à l'habitat par type de garantie (à l'origination, en moyenne et après réévaluation des collatéraux) ;
- 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) ;
- le cas échéant, modalités et périodicité de l'analyse, de la mesure et de la surveillance du risque lié aux opérations intragroupe (risque de crédit et risque de crédit de contrepartie).

Éléments spécifiques au risque de crédit de contrepartie :

- description des métriques de risque employées pour mesurer le risque de crédit de contrepartie ;
- description de l'intégration du suivi du risque de crédit de contrepartie dans le dispositif global de suivi du risque de crédit.

8.3. Risque de concentration

8.3.1. Risque de concentration par contrepartie :

- outil de suivi du risque de concentration par contrepartie y compris les contreparties centrales et les entités du système bancaire parallèle : agrégats éventuellement définis, description du dispositif de mesure des engagements sur un même bénéficiaire (cadre prudentiel applicable aux contreparties considérées, situation financière de la contrepartie et du portefeuille, vulnérabilité à la volatilité du prix des actifs notamment pour les entités du système bancaire parallèle, 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 et les entités du système bancaire parallèle.

8.3.2. Risque de concentration sectorielle :

- outil de suivi du risque de concentration sectorielle (notamment pour le système bancaire parallèle) : agrégats éventuellement définis, modèle économique et profil de risque, dispositif de mesure des engagements sur un même secteur d'activité (notamment l'interconnexion des contreparties), 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 *(montant des expositions, 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 (notamment pour le système bancaire parallèle).

8.3.3. 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.

8.4. 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).

8.5. 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.

8.6. 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[1].

– 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.

8.7. 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)* ;

– 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).

8.8. 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) ;

– synthèse des incidents intervenus au cours de l'année le cas échéant (appels de garanties refusés, nantissements non réalisés etc.).

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

8.9. 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.

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

9. Risques associés aux contrats dérivés de gré à gré

9.1. Techniques d'atténuation des risques pour les contrats dérivés de gré à gré non compensés par une contrepartie centrale :

- description des procédures et des dispositifs permettant d'assurer la confirmation rapide des termes des contrats dérivés de gré à gré non compensés par une contrepartie centrale, de rapprocher les portefeuilles, de gérer le risque associé, de déceler rapidement les éventuels différends entre parties et de les régler, et de surveiller la valeur des contrats en cours (cf. paragraphe 1 de l'article 11 du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux) ;
- description des procédures de valorisation des contrats dérivés de gré à gré non compensés par une contrepartie centrale (cf. paragraphe 2 de l'article 11 du règlement (UE) n° 648/2012) ;
- description des procédures de gestion des risques de contrepartie et d'échange de garanties (collatéral) sur les contrats dérivés de gré à gré non compensés par une contrepartie centrale (cf. paragraphe 3 de l'article 11 du règlement (UE) n° 648/2012) ;
- description des procédures de calcul et de collecte des marges de variation ;
- description des procédures de calcul et de collecte des marges initiales ;
- description des modèles utilisés pour le calcul des marges initiales ;
- description des critères utilisés pour la sélection du collatéral échangé ;
- description des méthodes d'évaluation du collatéral ;
- description des procédures opérationnelles et de la documentation contractuelle utilisées pour les échanges de collatéral ;
- description du nombre, du volume, et de l'évolution des litiges observés (« collateral dispute ») avec les contreparties avec lesquelles des garanties sont échangées, ainsi que des procédures de résolution de ces litiges ;
- description des modalités et fréquences de calcul du capital alloué à la gestion du risque non couvert par un échange approprié de garanties (collatéral) (cf. paragraphe 4 de l'article 11 du règlement (UE) n° 648/2012).

9.2. Procédures de gestion et de contrôle des risques des transactions intragroupe :

- description des procédures centralisées d'évaluation, de mesure et de contrôle des risques associés aux transactions intragroupe mentionnées aux paragraphes 2. a) et d) de l'article 3 du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux ;
- description des procédures de gestion des risques associés aux transactions intragroupe bénéficiant des dérogations prévues aux paragraphes 6, 8 ou 10 de l'article 11 du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux ;

- description des changements significatifs pouvant affecter la fluidité des transferts de fonds propres ou de remboursements rapides de passifs entre les contreparties qui bénéficient des dérogations prévues aux paragraphes 6, 8 ou 10 de l'article 11 du règlement (UE) n°648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux. Inclure le détail des observations ou anticipations relatives aux pays dont la situation a significativement évolué à cet égard ;
- informations relatives aux transactions intragroupe réalisées au cours de l'année bénéficiant des dérogations prévues aux paragraphes 6, 8 ou 10 de l'article 11 du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux (cf. article 20 du règlement délégué n° 149/2013 de la Commission du 19 décembre 2012 complétant le règlement (UE) n° 648/2012).

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) ;*
- rapprochements entre la valorisation prudente, telle que définie dans le règlement délégué 2016/101 du 26 Octobre 2015, et la valorisation comptable, du portefeuille enregistré comptablement en juste valeur par résultat ;
- 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 ; cette annexe devra rappeler de manière exhaustive les changements de modèle effectués durant l'année écoulée, en distinguant ceux reconnus comme matériels, de ceux reconnus comme non matériels, selon les définitions du règlement délégué 2015/942 du 4 mars 2015, et expliquer en quoi le contrôle interne a ou n'a pas été à l'origine de tels changements.

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

11. Risque opérationnel

11.1. Gouvernance et organisation du 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 ;
- gouvernance : description de la gouvernance déployée pour la gestion du risque opérationnel et de la gouvernance du modèle s'il y a lieu, rôle et missions des différents comités mis en place, décisions structurantes prises au cours de l'exercice en matière de risque opérationnel ;
- organisation : présentation des différentes équipes en charge du contrôle permanent du risque opérationnel par métiers et par zones géographiques (nombre d'ETP prévu et réel, missions, rattachement des équipes), objectifs des différentes équipes de contrôle permanent, actions menées au cours de l'exercice et état d'avancement des projets de réorganisation en fin d'année, contraintes

rencontrées et solutions envisagées/mises en place lors de la mise en œuvre de ces projets de réorganisation, objectifs à atteindre et délais prévus pour un déploiement total de l'organisation cible ;

- périmètre des entités : entités intégrées et méthodes (en nombre et en proportion des actifs), traitement des entités entrées dans le périmètre de consolidation prudentiel au cours des 2 derniers exercices, entités éventuellement exclues et motifs d'exclusion, opérations prises en compte.

11.2. 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)* ;
- dispositif de surveillance déployé pour assurer la prise en compte dans les calculs des exigences en fonds propres de l'exhaustivité des incidents à recenser, notamment au titre des risques juridique et de non–conformité ; identification des risques nécessitant un perfectionnement du dispositif de surveillance en cours et actions correctives prises ;
- présentation de la cartographie des risques avec identification des métiers/risques non (encore) couverts par la cartographie déployée à la fin de l'exercice ;
- 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 ;
- état des lieux des réflexions en cours sur les évolutions que l'établissement doit anticiper concernant les modalités de calcul des exigences réglementaires au titre du risque opérationnel.

11.3. 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, cybersécurité, …) et des enseignements qui en ont été tirés.

11.4. 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]).

11.5. Risques liés aux technologies de l'information et de la communication (TIC) :

- présentation de la stratégie de l'établissement concernant ses TIC (organisation, objectifs prioritaires fixés, cadre d'appétence pour les risques liés aux TIC, budget alloué, procédures mises en place, date de dernière mise à jour…) ;
- 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 TIC ;
- objectifs de la politique de sécurité des systèmes d'information (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 des tests d'intrusion effectués au cours de l'exercice ;
- nom du responsable de la sécurité des systèmes d'information ;
- description synthétique du cadre général de la détection, de l'évaluation, de la gestion et de la surveillance des risques liés aux TIC *(préciser le rôle des dirigeants effectifs et de l'organe de surveillance et la répartition des compétences en matière de pilotage des risques liés aux TIC, les outils utilisés, les ressources déployées…)* ;
- description du dispositif de contrôle permanent et périodique des systèmes d'information et synthèse des constatations des contrôles effectués (voir 11.6) ;
- présentation de la cartographie des risques liés aux TIC incluant notamment les risques pour la disponibilité et la continuité des TIC, la sécurité des TIC, l'intégrité des données et le risque lié au changement de TIC (identifiant en particulier quels systèmes et services sont essentiels au bon fonctionnement, à la disponibilité, à la continuité et à la sécurité des activités de l'établissement) ;
- modalités et périodicité d'information de la direction générale et de l'organe de surveillance sur l'exposition de l'établissement aux risques liés aux TIC (joindre le dernier tableau de bord destiné à les informer) ;
- 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.

11.6. Résultats des contrôles permanents menés en matière de risque opérationnel y compris des risques liés aux TIC :

- 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).

11.7. 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.

- présentation des modifications intervenues dans le périmètre de consolidation le cas échéant (entrées et sorties).

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) ;
- présentation du dispositif de prévention du risque comptable, y compris le risque de défaillance des systèmes informatiques (sites de repli…).

13. Risque de taux d'intérêt global

- 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 activités de couverture: *préciser les différents instruments mis en œuvre et les contrôles menés sur ces activités ;*
- 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 interne 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

- 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, et les liens de financement intragroupe, 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) ;
- pour les établissements de crédit et succursales d'établissements de crédit ayant leur siège dans un pays tiers, 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).

16.1. 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 systèmes d'information, 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* ;
- les sociétés de financement 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.
- 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 en lien avec le dispositif de limites en matière de risque de liquidité ;
- 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 ;
- description de la méthodologie utilisée en matière d'évaluation régulière, conformément à l'article 23 du règlement délégué (UE) 2015/61 sur l'exigence de couverture des besoins de liquidité pour les établissements de crédit (*Liquidity Coverage Ratio – LCR*), de la probabilité et du volume potentiel, sur 30 jours calendaires, des sorties de trésorerie liées aux produits ou services qui ne relèvent pas des articles 27 à 31 du LCR. Le cas échéant, information sur l'existence de sorties de trésorerie réelles qui ne seraient pas envisagées par la Décision 2016-C-26 de l'ACPR ;
- 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 ;
- modalités de prise en compte, de mesure, de suivi et d'encadrement du risque de liquidité intra-journalier ;
- 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 en intégrant également la dimension du risque de liquidité intra-journalier le cas échéant) : *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 et justifier 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)* ;
- procédure et périodicité de la révision des limites fixées en matière de risques de liquidité *(indiquer la date de la dernière révision les intervenants, les modalités suivies)* ;
- 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 et description des dispositifs de mesure et suivi des actifs grevés et non grevés ;
- 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).
- les établissements soumis à CRR et ne se trouvant pas sous la supervision directe de la BCE, doivent remettre un « manuel du lecteur », élaboré comme un document global facilitant l'évaluation de la documentation justifiant de leur adéquation en liquidité. À cet effet, le «manuel du lecteur» doit fournir une vue d'ensemble de tous les documents communiqués aux autorités compétentes sur ce sujet, ainsi que de leur statut (nouveau, non modifié, modifié avec des corrections mineures, etc.). Le «manuel du lecteur» doit essentiellement fonctionner comme un index reliant les éléments d'information spécifiques prévus pour le rapport de contrôle interne aux documents fournis à l'autorité compétente concernant l'évaluation de son adéquation en liquidité. Le «manuel du lecteur» doit également comporter des renseignements concernant les modifications significatives apportées aux informations par rapport à celles communiquées précédemment, les éléments éventuellement exclus des informations communiquées, ainsi que toute autre information qui pourrait être utile à l'autorité compétente en vue de l'évaluation. En outre, le «manuel du lecteur» doit contenir des références à toutes les informations rendues publiques par l'établissement sur son adéquation en liquidité.

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. 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).

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

- les établissements soumis à CRR et ne se trouvant pas sous la supervision directe de la BCE, doivent formaliser et remettre les conclusions des évaluations de l'adéquation de la liquidité interne ainsi que leur incidence sur la gestion du risque et sur la gestion globale de l'établissement.

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 à la protection des fonds de la clientèle des entreprises d'investissement

- mode d'organisation de la gestion des comptes espèces de la clientèle et articulation (permettant de retracer de manière chronologique les différents flux) avec l'exécution des services d'investissement ou de compensation ;
- présentation de la méthode mise en œuvre pour assurer la protection des fonds reçus de la clientèle et description de l'outil de calcul du montant des fonds reçus des clients et à cantonner ;
- pour les établissements assurant la protection des fonds reçus en les plaçant dans un ou plusieurs comptes ouverts spécialement à cet effet auprès d'un établissement de crédit : communication de toute modification apportée à la convention de compte de cantonnement, description des procédures prévues pour assurer le placement des fonds ;

- pour les établissements assurant la protection des fonds reçus au moyen d'une garantie : communication de toute modification apportée au contrat de garantie ou de cautionnement et de tout élément relatif à l'actualisation du montant de la couverture constituée en lien avec l'évolution du volume d'activité ;
- présentation des procédures mises en place pour veiller au respect des dispositions relatives à la protection des fonds de la clientèle des entreprises, des vérifications associées et présentation des éventuels incidents ou insuffisances mis en évidence par ces vérifications ;
- communication du rapport des commissaires aux comptes sur l'adéquation des dispositions mises en place en application des dispositions réglementaires relatives au cantonnement.

19. Dispositions de séparation bancaire

Nota bene : Cette partie concerne l'application du titre Ier de la loi de séparation et de régulation bancaire n°2013-672 du 26 juillet 2013 (Loi SRAB). Il est rappelé que les mandats des unités internes mentionnés dans la cartographie doivent être transmis au SGACPR en parallèle de la transmission du rapport de contrôle interne.

19.1. Cartographie des activités de négociation sur instruments financiers

- communication de la cartographie actualisée des unités internes chargés des opérations sur instruments financiers telle que mentionnée à l'article 1 de l'arrêté du 9 septembre 2014 au niveau du plus petit échelon organisationnel, avec identification des regroupements réalisés. La cartographie devra mentionner a minima les éléments suivants :
    - le nom littéral du plus petit échelon organisationnel,
    - une description synthétique des activités menées,
    - la (les) catégorie(s) d'exemption de séparation afférente telle que mentionnée à l'article L.511-47 du Code monétaire et financier,
    - le nombre de traders,
    - le PNB généré sur l'année,
    - les principales limites de risque (VaR, autres mesures internes), leur consommation moyenne et maximale sur l'année ;
- description des évolutions de la cartographie ;
- description des principales nouvelles activités et des activités arrêtées.

19.2. Indicateurs de suivi

- 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 et des analyses réalisées sur l'année écoulée (avec identification des desks atypiques).

19.3. Bilan des activités avec les fonds à effet de levier au sens de la loi SRAB :

- description des activités ;
- bilan des résultats et des risques générés (risques de marché, de crédit et de contrepartie) ;
- description des dispositifs de maîtrise des risques précités et contrôles afférents.

19.4. Résultats des contrôles

- 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. Politique en matière d'externalisation

– présentation de la stratégie de l'établissement ou du groupe en matière d'externalisation, incluant notamment la description des dispositions existantes pour éclairer la prise de décision d'externalisation avant que celle-ci ne soit effective ;

– description des activités externalisées[2] (au sens des paragraphes q) et r) de l'article 10 de l'arrêté du 3 novembre 2014) et proportion par rapport à l'activité globale de l'établissement *(dans son ensemble et domaine par domaine)* ;

– description des activités essentielles ou importantes (au sens de l'article 10 de l'arrêté du 3 novembre 2014) pour lesquelles l'établissement a prévu de les externaliser en ayant recours à un prestataire de services en nuage (*cloud computing*) et proportion par rapport à l'activité globale de l'établissement ;

– description des conditions dans lesquelles a lieu le recours à l'externalisation : nom du fournisseur de services, pays d'implantation, agrément et surveillance prudentielle des prestataires externes, procédures mises en place en vue de s'assurer de l'existence d'un contrat écrit et de sa conformité avec les exigences de l'article 239 de l'arrêté du 3 novembre 2014, y compris celle permettant à l'Autorité de contrôle prudentiel et de résolution, ou la BCE selon les cas, de se rendre sur place au sein du prestataire extérieur, etc. ;

– pour le cas particulier d'activités externalisées par le recours à un fournisseur de services en nuage (*cloud computing*), description des conditions dans lesquelles a lieu le recours à l'externalisation : le modèle de services en nuage (public/privé…), les dates de début et d'expiration des services fournis, le nom des éventuels sous-traitants de « nième rang » et une indication sur le caractère substituable du fournisseur de services (facile/difficile/impossible) ;

– description du dispositif de contrôle permanent et périodique des activités externalisées ;

– description du dispositif d'identification, de gestion et de suivi des risques associés à l'externalisation ;

– description des dispositifs mis en œuvre par l'établissement pour conserver l'expertise nécessaire afin de contrôler effectivement les activités externalisées et gérer les risques associés à l'externalisation ;

– 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) ;

– description des diligences effectuées par les dirigeants effectifs pour vérifier l'efficacité des dispositifs et procédures de contrôle interne des activités externalisées (cf. articles 242 de l'arrêté du 3 novembre 2014) ;

– description, formalisation et date(s) de mise à jour des procédures sur lesquelles s'appuie le contrôle permanent et périodique des activités externalisées (dont les procédures d'examen de la conformité) ;

– résultats des contrôles permanents menés sur les activités externalisées : principales insuffisances relevées et mesures correctives engagées pour y remédier (date de réalisation prévisionnelle et état

[2] En précisant celles qui le sont par recours à un prestataire de services en nuage (*cloud computing*)

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)* ;

– résultats des contrôles périodiques menés sur les activités externalisées : principales insuffisances relevées et mesures correctives engagées pour y remédier (date de réalisation prévisionnelle 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.

21. 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.

21.1. 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.

21.2. 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).*

21.3. 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 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 …)

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

SOMMAIRE

Introduction

I. Présentation des moyens de paiement et des risques de fraude associés

1. Carte de paiement et assimilée
   1.1. Présentation de l'offre
   1.2. Organisation opérationnelle de l'activité carte et assimilée
   1.3. Grille d'analyse des risques et principaux incidents de fraude

2. Virement (SEPA et autres)
   2.1. Présentation de l'offre
   2.2. Organisation opérationnelle de l'activité virement
   2.3. Grille d'analyse des risques et principaux incidents de fraude

3. Prélèvement
   3.1. Présentation de l'offre
   3.2. Organisation opérationnelle de l'activité prélèvement
   3.3. Grille d'analyse des risques et principaux incidents de fraude

4. Lettre de change (LCR) et billet à ordre relevé (BOR)
   4.1. Présentation de l'offre
   4.2. Organisation opérationnelle de l'activité LCR et BOR
   4.3. Grille d'analyse des risques et principaux incidents de fraude

5. Chèque
   5.1. Présentation de l'offre
   5.2. Organisation opérationnelle de l'activité chèque
   5.3. Présentation des principaux incidents de fraude

6. Monnaie électronique
   6.1. Présentation de l'offre
   6.2. Organisation opérationnelle de l'activité monnaie électronique
   6.3. Présentation des principaux incidents de fraude

7. Services d'information sur les comptes et d'initiation de paiement
   7.1. Présentation de l'offre
   7.2. Organisation opérationnelle de l'offre
   7.3. Présentation des mesures de protection des données de paiement sensibles

II. Présentation des résultats du contrôle périodique (sur le périmètre des moyens de paiement scripturaux)

III. Évaluation de la conformité aux recommandations d'organismes externes en matière de sécurité des moyens de paiement

IV. Annexes

1. Matrice de cotation des risques de fraude de l'établissement
2. Glossaire

INTRODUCTION

Rappel du cadre règlementaire

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.

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.

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

Cette annexe a pour objet d'apprécier le niveau de sécurité atteint par l'ensemble des moyens de paiement scripturaux émis ou gérés par l'établissement.

Cette annexe comporte 4 parties :

- une partie portant sur la présentation de chaque moyen de paiement, des risques de fraude associés et des dispositifs de maitrise des risques mis en place (I) ;
- une partie consacrée aux résultats du contrôle périodique sur le périmètre des moyens de paiement scripturaux (II) ;
- une partie destinée à recueillir l'auto-évaluation de la conformité de l'établissement aux recommandations d'organismes externes en matière de sécurité des moyens de paiement scripturaux (III) ;
- une annexe comprenant la matrice de cotation des risques de fraude et un glossaire pour la définition des termes techniques/acronymes utilisés par l'établissement dans l'annexe (IV).

Concernant la partie I, l'analyse des risques de fraude de chaque moyen de paiement est réalisée à partir des données de fraude telles que déclarées par l'établissement auprès de la Banque de France dans le cadre de la collecte statistiques « Recensement de la fraude sur les moyens de paiement scripturaux »[3]. En conséquence, cette analyse s'effectue :

- sur la fraude brute et couvre à la fois la fraude interne et la fraude externe ;
- et, sur la base des définitions et typologie de fraude retenue pour la déclaration statistique auprès de la Banque de France (cf. supra).

[3] Cf. Guide de remplissage de la fraude : https://www.banque-france.fr/stabilite-financiere/securite-des-moyens-de-paiement-scripturaux/oscamps/documentation-des-collectes

Pour ce faire, des grilles d'analyse des risques de fraude spécifiques à chaque moyen de paiement scriptural, présentées dans l'annexe, sont à compléter en fonction des offres propres à chaque établissement. Toutefois, s'agissant du chèque, les établissements ayant répondu au questionnaire d'évaluation du « Référentiel de la sécurité du chèque » (RSC) de la Banque de France, sont dispensés de produire cette analyse mais doivent néanmoins faire état des principaux incidents de fraude rencontrés au cours de l'exercice sous revue. Il en est de même pour la monnaie électronique dans la mesure où la fraude de ce moyen de paiement ne fait pas l'objet d'une collecte spécifique.

La liste de recommandations liées à la sécurité des moyens de paiement émises par des organismes externes, présentée dans la partie III de l'annexe, tient compte de l'entrée en application, le 13 janvier 2018, de la 2ème directive européenne sur les services de paiement. Il est demandé de fournir des commentaires explicatifs pour les recommandations pour lesquelles la pleine conformité de l'établissement n'est pas assurée.

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) :

- pour la partie portant sur la présentation de chaque moyen de paiement (I), l'établissement affilié est tenu de présenter son offre de produits et services ainsi que l'organisation opérationnelle de l'activité. En revanche, il est dispensé de produire la grille d'analyse des risques et principaux incidents de fraude et doit mentionner « qu'il se réfère à ce qui a été décrit par l'organe central dans sa propre annexe ».

- concernant la partie consacrée à la présentation des résultats du contrôle périodique (II), si celui-ci est effectué sous la responsabilité de l'organe central et décrit par lui, seuls les contrôles propres à l'établissement affilié doivent être fournis par ce dernier.

- pour la partie destinée à recueillir l'auto-évaluation de la conformité aux recommandations d'organismes externes en matière de sécurité des moyens de paiement scripturaux (III), l'établissement affilié en est dispensé et doit mentionner « qu'il se réfère à ce qui a été décrit par l'organe central dans sa propre annexe ».

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 est tenu de renseigner l'annexe dans son intégralité et pour la partie consacrée à la présentation des résultats du contrôle périodique (II), il 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).

Définition des principaux termes utilisés dans l'annexe

Termes	Définitions
Canal d'initiation	Selon les différents services et moyens de paiement, la notion de canal d'initiation correspond : - pour la carte, au canal d'utilisation de la carte : paiement point de vente, retrait, paiement à distance, sans contact, enrôlement dans des *wallets* internet ou des solutions de paiement mobile ; - pour le virement, au canal de réception de l'ordre de virement : guichet,

	espace de banque en ligne, solution de télétransmission… ; - pour le prélèvement, au canal de réception des ordres de prélèvement ; - pour le chèque, au canal de remise du chèque : courrier, automate… - pour les services d'information sur les comptes et d'initiation de paiement au moyen de connexion : site web, application mobile, protocole dédié…
Fraude externe	Dans le domaine des moyens de paiement, détournement de ces derniers, par des actes de tiers, au profit d'un bénéficiaire illégitime.
Fraude interne	Dans le domaine des moyens de paiement, détournement de ces derniers, par des actes de tiers et impliquant au moins un membre de l'entreprise, au profit d'un bénéficiaire illégitime.
Fraude brute	Au sens de la collecte statistiques « Recensement de la fraude sur les moyens de paiement scripturaux » de la Banque de France, la fraude brute correspond au montant nominal des transactions de paiement autorisées ayant fait l'objet d'un rejet a postériori pour motif de fraude. Elle ne tient donc pas compte des fonds qui ont pu être recouvrés après traitement du contentieux.
Risque brut	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.
Risque résiduel	Risque subsistant après prise en compte des mesures de couverture.
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.

I - PRÉSENTATION DES MOYENS DE PAIEMENT ET DES RISQUES DE FRAUDE ENCOURUS PAR L'ÉTABLISSEMENT

1. Carte et assimilée

1.1. Présentation de l'offre

a. Description de l'offre de produits et de services

Produit et/ou service	Caractéristiques, ancienneté et fonctionnalités proposées	Clientèle concernée	Canal d'initiation	Commentaires sur l'évolution de la volumétrie d'activité	Commentaires sur les évolutions d'ordre technologique, fonctionnel et sécuritaire
En tant qu'établissement émetteur					
*Ex : **Carte de paiement** : carte internationale,…*	*Ex : -Maturité -Date de commercialisation -Équipée de la fonction sans contact par défaut - Enrôlement dans un dispositif d'authentification -Service carte virtuelle…*	*Ex : Particuliers*	*Ex : Au point de vente ou sur automate, paiement à distance,…*	*Préciser les facteurs explicatifs des variations significatives de l'activité (nombre et montant)*	*Indiquer les évolutions intervenues au cours de l'exercice sous revue Ex : réalisation de pilote, mise en place d'alertes SMS pour les transactions des cartes haut de gamme à l'international,…*
*Ex : **Carte de retrait***					
Ex : Enrôlement dans des wallets					
En tant qu'établissement acquéreur					
Ex : Offre d'acceptation des paiements par carte en proximité					
Ex : Offre d'acceptation des paiements par carte en VAD					

b. Projets envisagés de l'offre de produits et de services

Décrire les projets de commercialisation de nouveaux produits/services ou d'évolution de l'offre existante d'ordre technologique, fonctionnel et sécuritaire prévus à court et moyen terme.

1.2. Organisation opérationnelle de l'activité

Présenter de manière synthétique le processus de traitement du moyen/service de paiement depuis son émission/réception jusqu'à sa remise aux systèmes d'échange/imputation en compte en précisant en particulier les traitements externalisés (y compris auprès d'entités du groupe) et ceux mutualisés avec d'autres établissements. Un schéma organisationnel peut-être inséré si nécessaire.

Acteurs	Rôles
Activité d'émission et de gestion	
Directions, services, prestataires,…	
Activité d'acquisition	

Décrire les changements et/ou projets organisationnels lancés ou menés au cours de l'année sous revue ou envisagés à court et moyen terme.

1.3. Grille d'analyse des risques et principaux incidents de fraude

a. Rappel de la typologie de fraude applicable

Typologie de fraude	Description
Vol/perte de la carte	Le fraudeur utilise une carte de paiement obtenue suite à une perte ou à un vol.
Carte non parvenue	La carte a été interceptée lors de son envoi entre l'émetteur et le titulaire légitime. Ce type d'origine se rapproche de la perte ou du vol. Cependant, il s'en distingue dans la mesure où le porteur peut moins facilement constater qu'un fraudeur est en possession d'une carte lui

	appartenant et où il met en jeu des vulnérabilités spécifiques aux procédures d'envoi des cartes.
Carte falsifiée ou contrefaite	Une carte de paiement authentique est falsifiée par modification des données magnétiques, d'embossage ou de programmation ; une carte contrefaite est réalisée à partir de données recueillies par le fraudeur.
Numéro de carte usurpé ou numéro de carte non affecté	-Le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage » (à l'aide de générateurs aléatoires de numéros de carte) et utilisé en vente à distance. -Utilisation d'un PAN (*Personal Account Number*) cohérent mais non attribué à un porteur, puis généralement utilisé en vente à distance.

b. Cotation globale du risque de fraude sur la carte et assimilée

La matrice de cotation utilisée par l'établissement pour évaluer le risque de fraude est à communiquer dans la partie IV de la présente annexe.

Risque brut *(Risque inhérent avant les mesures de couverture)*	
Risque résiduel *(Risque subsistant après les mesures de couverture)*	

c. Mesures de couverture du risque de fraude

Décrire les mesures de couverture en précisant en gras d'une part, celles déployées durant l'exercice sous revue et d'autre part, celles envisagées en indiquant dans ce cas leur échéance de mise en œuvre.

En tant qu'établissement émetteur :

Typologie de fraude	Canal d'initiation	Mesures de couverture
Vol/perte de la carte	*Ex : au point de vente*	
Carte non parvenue		
Carte falsifiée ou contrefaite		
Numéro de carte usurpé ou numéro de carte non affecté		

En tant qu'établissement acquéreur :

Typologie de fraude	Canal d'initiation	Mesures de couverture
Vol/perte de la carte		
Carte non parvenue		
Carte falsifiée ou contrefaite		
Numéro de carte usurpé ou numéro de carte non affecté		

d. Évolution de la fraude brute au cours de la période sous revue

En tant qu'établissement émetteur :

Typologie de fraude	Canal d'initiation	Description des principaux cas de fraude rencontrés (eu égard à leur montant et/ou fréquence)
Ex : numéro de carte usurpé	*Ex : paiement à distance*	*Ex : attaques par skimming, détournement de cartes SIM,…*

En tant qu'établissement acquéreur :

Typologie de fraude	Canal d'initiation	Description des principaux cas de fraude rencontrés (eu égard à leur montant et/ou fréquence)

e. Présentation des risques de fraude émergents

Décrire les nouveaux scénarios de fraude rencontrés au cours de l'exercice sous revue.

2. Virement

2.1. Présentation de l'offre

a. Description de l'offre de produits et de services

Produit et/ou service	Caractéristiques, ancienneté et fonctionnalités proposées	Clientèle concernée	Canal d'initiation	Commentaires sur l'évolution de la volumétrie d'activité	Commentaires sur les évolutions d'ordre technologique, fonctionnel et sécuritaire
En tant qu'établissement du donneur d'ordre					

b. Projets envisagés de l'offre de produits et de services

Décrire les projets de commercialisation de nouveaux produits/services ou d'évolution de l'offre existante d'ordre technologique, fonctionnel et sécuritaire prévus à court et moyen terme.

2.2. Organisation opérationnelle de l'activité virement

Présenter de manière synthétique le processus de traitement du moyen/service de paiement depuis son émission/réception jusqu'à sa remise aux systèmes d'échange/imputation en compte en précisant en particulier les traitements externalisés (y compris auprès d'entités du groupe) et ceux mutualisés avec d'autres établissements. Un schéma organisationnel peut-être inséré si nécessaire.

Acteurs	Rôles
Activité d'émission et de gestion	

Décrire les changements et/ou projets organisationnels lancés ou menés au cours de l'année sous revue ou envisagés à court et moyen terme.

2.3. Grille d'analyse des risques et principaux incidents de fraude

a. Rappel de la typologie de fraude applicable

Typologie de fraude	Description
Faux ordre de virement	-Le fraudeur émet un faux ordre de virement (y compris lorsque celui-ci a été effectué sous la contrainte par le titulaire légitime). -Usurpation des identifiants de la banque en ligne du donneur d'ordre légitime (y compris lorsque les identifiants ont été obtenus sous la contrainte ou via des procédés tels que le *phishing* ou l'ingénierie sociale).
Falsification de l'ordre de virement	L'ordre de virement est intercepté et modifié par le fraudeur.
Détournement	Le payeur émet un virement à destination d'un RIB/IBAN qui n'est pas celui du bénéficiaire légitime. Fait typiquement suite à une usurpation d'identité du bénéficiaire (ingénierie sociale par exemple).

b. Cotation globale du risque de fraude sur le virement

La matrice de cotation utilisée par l'établissement pour évaluer le risque de fraude est à communiquer dans la partie IV de la présente annexe.

Risque brut *(Risque inhérent avant les mesures de couverture)*	
Risque résiduel *(Risque subsistant après les mesures de couverture)*	

c. Mesures de couverture du risque de fraude

Décrire les mesures de couverture en précisant en gras d'une part, celles déployées durant l'exercice sous revue et d'autre part, celles envisagées en indiquant dans ce cas leur échéance de mise en œuvre.

Typologie de fraude	Canal d'initiation	Mesures de couverture
Faux ordre de virement		
Falsification de l'ordre de virement		
Détournement		
Autres		

d. Évolution de la fraude brute au cours de la période sous revue

Typologie de fraude	Canal d'initiation	Description des principaux cas de fraude rencontrés (eu égard à leur montant et/ou fréquence)

e. Présentation des risques de fraude émergents

Décrire les nouveaux scénarios de fraude rencontrés au cours de l'exercice sous revue.

3. Prélèvement

3.1. Présentation de l'offre

a. Description de l'offre de produits et de services

Produit et/ou service	Caractéristiques, ancienneté et fonctionnalités proposées	Clientèle concernée	Canal d'initiation	Commentaires sur l'évolution de la volumétrie d'activité	Commentaires sur les évolutions d'ordre technologique, fonctionnel et sécuritaire
En tant qu'établissement du débiteur					
En tant qu'établissement du créancier					

b. Projets envisagés de l'offre de produits et de services

Décrire les projets de commercialisation de nouveaux produits/services ou d'évolution de l'offre existante d'ordre technologique, fonctionnel et sécuritaire prévus à court et moyen terme.

3.2. Organisation opérationnelle de l'activité prélèvement

Présenter de manière synthétique le processus de traitement du moyen/service de paiement depuis son émission/réception jusqu'à sa remise aux systèmes d'échange/imputation en compte en précisant en particulier les traitements externalisés (y compris auprès d'entités du groupe) et ceux mutualisés avec d'autres établissements. Un schéma organisationnel peut-être inséré si nécessaire.

Acteurs	Rôles
Activité d'émission et de gestion	

Décrire les changements et/ou projets organisationnels lancés ou menés au cours de l'année sous revue ou envisagés à court et moyen terme.

3.3. Grille d'analyse des risques et principaux incidents de fraude

a. Rappel de la typologie de fraude applicable

Typologie de fraude	Description
Faux prélèvement	Prélèvement émis par un créancier sans avoir d'autorisation de prélèvement licite du débiteur. Exemple 1 : le fraudeur émet massivement des prélèvements vers des RIB/IBAN dont il a obtenu illégalement la liste et sans aucune autorisation ou réalité économique sous-jacente. Exemple 2 : le créancier émet des prélèvements non autorisés après avoir obtenu les coordonnées bancaires du débiteur grâce à un produit d'appel servant « d'hameçon » (seulement un débit autorisé).
Détournement	-Modification par le fraudeur du numéro de compte à créditer associé

	à des fichiers de prélèvement. -Le créancier émet sciemment un prélèvement dont le montant est très largement supérieur au montant dû (par exemple : le créancier obtient la signature du mandat de prélèvement pour une prestation donnée servant « d'hameçon » et se sert de ce mandat pour extorquer de manière manifeste des fonds au débiteur). Les litiges commerciaux sont exclus. -Émetteur usurpant un identifiant créancier (NNE/ICS) qui n'est pas le sien.
Rejeu	Le créancier émet sciemment des prélèvements déjà émis (qui ont soit déjà été réglé, soit ont fait l'objet de rejets pour opposition du débiteur par exemple).

b. Cotation globale du risque de fraude sur le prélèvement

La matrice de cotation utilisée par l'établissement pour évaluer le risque de fraude est à communiquer dans la partie IV de la présente annexe.

Risque brut *(Risque inhérent avant les mesures de couverture)*	
Risque résiduel *(Risque subsistant après les mesures de couverture)*	

c. Mesures de couverture du risque de fraude

Décrire les mesures de couverture en précisant en gras d'une part, celles déployées durant l'exercice sous revue et d'autre part, celles envisagées en indiquant dans ce cas leur échéance de mise en œuvre.

En tant qu'établissement du débiteur :

Typologie de fraude	Canal d'initiation	Mesures de couverture
Faux prélèvement		
Détournement		
Rejeu		
Autres		

En tant qu'établissement du créancier :

Typologie de fraude	Canal d'initiation	Mesures de couverture
Faux prélèvement		
Détournement		
Rejeu		
Autres		

d. Évolution de la fraude brute au cours de la période sous revue

En tant qu'établissement du débiteur :

Typologie de fraude	Canal d'initiation	Description des principaux cas de fraude rencontrés (eu égard à leur montant et/ou fréquence)

En tant qu'établissement du créancier :

Typologie de fraude	Canal d'initiation	Description des principaux cas de fraude rencontrés (eu égard à leur montant et/ou fréquence)

e. Présentation des risques de fraude émergents

Décrire les nouveaux scénarios de fraude rencontrés au cours de l'exercice sous revue.

4. Lettre de change (LCR) et du billet à ordre relevé (BOR)

4.1. Présentation de l'offre

a. Description de l'offre de produits et des services

Produit et/ou service	Caractéristiques, ancienneté et fonctionnalités proposées	Clientèle concernée	Canal d'initiation	Commentaires sur l'évolution de la volumétrie d'activité	Commentaires sur les évolutions d'ordre technologique, fonctionnel et sécuritaire

b. Projets envisagés de l'offre de produits et de services

Décrire les projets de commercialisation de nouveaux produits/services ou d'évolution de l'offre existante d'ordre technologique, fonctionnel et sécuritaire prévus à court et moyen terme.

4.2. Organisation opérationnelle de l'activité LCR et BOR

Présenter de manière synthétique le processus de traitement du moyen/service de paiement depuis son émission/réception jusqu'à sa remise aux systèmes d'échange/imputation en compte en précisant en particulier les traitements externalisés (y compris auprès d'entités du groupe) et ceux mutualisés avec d'autres établissements. Un schéma organisationnel peut-être inséré si nécessaire.

Acteurs	Rôles
Activité du tiré	
Activité du remettant	

Décrire les changements et/ou projets organisationnels lancés ou menés au cours de l'année sous revue ou envisagés à court et moyen terme.

4.3. Grille d'analyse des risques et principaux incidents de fraude

a. Rappel de la typologie de fraude applicable

Typologie de fraude	Description
Vol, perte (faux, apocryphe)	Effet perdu ou volé, revêtu d'une fausse signature
Contrefaçon	Effet créé de toute pièce par le fraudeur
Falsification	Altération d'un effet valablement émis
Détournement, rejeu	Présentation d'un effet déjà payé

b. Cotation globale du risque de fraude sur les LCR et BOR

La matrice de cotation utilisée par l'établissement pour évaluer le risque de fraude est à communiquer dans la partie IV de la présente annexe.

Risque brut *(Risque inhérent avant les mesures de couverture)*	
Risque résiduel *(Risque subsistant après les mesures de couverture)*	

c. Mesures de couverture du risque de fraude

Décrire les mesures de couverture en précisant en gras d'une part, celles déployées durant l'exercice sous revue et d'autre part, celles envisagées en indiquant dans ce cas leur échéance de mise en œuvre.

Typologie de fraude	Canal d'initiation	Mesures de couverture
Vol, perte (faux, apocryphe)		
Contrefaçon		
Falsification		
Détournement, rejeu		

d. Évolution de la fraude brute au cours de la période sous revue

En tant qu'établissement du tiré :

Typologie de fraude	Canal d'initiation	Description des principaux cas de fraude rencontrés (eu égard à leur montant et/ou fréquence)

En tant qu'établissement du remettant :

Typologie de fraude	Canal d'initiation	Description des principaux cas de fraude rencontrés (eu égard à leur montant et/ou fréquence)

e. Présentation des risques émergents

Décrire les nouveaux scénarios de fraude rencontrés au cours de l'exercice sous revue.

5. Chèque

5.1. Présentation de l'offre

a. Description de l'offre de produits et de services

Produit et/ou service	Caractéristiques, ancienneté et fonctionnalités proposées	Clientèle concernée	Canal d'initiation	Commentaires sur l'évolution de la volumétrie d'activité	Commentaires sur les évolutions d'ordre technologique, fonctionnel et sécuritaire

b. Projets envisagés de l'offre de produits et des services

Décrire les projets de commercialisation de nouveaux produits/services ou d'évolution de l'offre existante d'ordre technologique, fonctionnel et sécuritaire prévus à court et moyen terme.

5.2. Organisation opérationnelle de l'activité chèque

Présenter de manière synthétique le processus de traitement du moyen/service de paiement depuis son émission/réception jusqu'à sa remise aux systèmes d'échange/imputation en compte en précisant en particulier les traitements externalisés (y compris auprès d'entités du groupe) et ceux mutualisés avec d'autres établissements. Un schéma organisationnel peut-être inséré si nécessaire.

Acteurs	Rôles
Activité d'émission	
Activité du remettant	

Décrire les changements et/ou projets organisationnels lancés ou menés au cours de l'année sous revue ou envisagés à court et moyen terme.

5.3. Évolution de la fraude au cours de la période sous revue

a. Rappel de la typologie de fraude applicable

Typologie de fraude	Description
Vol, perte (faux, apocryphe)	Vignette perdue ou volée, revêtue d'une fausse signature
Contrefaçon	Vignette créée de toute pièce par le fraudeur
Falsification	Altération d'une vignette valablement émise
Détournement, rejeu	Présentation d'une vignette déjà payée

b. Principaux cas de fraude rencontrés :

Typologie de fraude	Canal d'initiation	Description des principaux cas rencontrés (eu égard à leur montant et/ou fréquence)

6. Monnaie électronique

6.1. Présentation de l'offre

a. Description de l'offre de produits et de services

Produit et/ou service	Caractéristiques, ancienneté et fonctionnalités proposées	Clientèle concernée	Canal d'initiation	Commentaires sur l'évolution de la volumétrie d'activité	Commentaires sur les évolutions d'ordre technologique, fonctionnel et sécuritaire

b. Projets envisagés de l'offre de produits et de services

Décrire les projets de commercialisation de nouveaux produits/services ou d'évolution de l'offre existante d'ordre technologique, fonctionnel et sécuritaire prévus à court et moyen terme.

6.2. Organisation opérationnelle de l'activité monnaie électronique

Présenter de manière synthétique le processus de traitement du moyen/service de paiement en précisant en particulier les traitements externalisés (y compris auprès d'entités du groupe) et ceux mutualisés avec d'autres établissements. Un schéma organisationnel peut-être inséré si nécessaire.

Acteurs	Rôles

Décrire les changements et/ou projets organisationnels lancés ou menés au cours de l'année sous revue ou envisagés à court et moyen terme.

6.3. Description des principaux incidents de fraude

Principaux cas de fraude rencontrés :

Typologie de fraude	Canal d'initiation	Description des principaux cas rencontrés (eu égard à leur montant et/ou fréquence)

7. Services d'information sur les comptes et d'initiation de paiement

7.1. Présentation de l'offre

a. Description de l'offre de service

Service	Périmètre d'activité	Clientèle concernée	Canal d'initiation	Commentaires sur l'évolution de la volumétrie d'activité	Commentaires sur les évolutions d'ordre technologique, fonctionnel et sécuritaire

b. Projets envisagés de l'offre de service

Décrire les projets d'évolution de l'offre existante d'ordre technologique, fonctionnel et sécuritaire prévus à court et moyen terme.

7.2. Organisation opérationnelle de l'offre

Présenter de manière synthétique le processus d'exécution du service d'information sur les comptes et/ou d'initiation de paiement en précisant en particulier les modalités d'accès aux informations sur les comptes avec les mesures de sécurité associées ainsi que les traitements externalisés (y compris auprès d'entités du groupe) et ceux mutualisés avec d'autres établissements. Un schéma organisationnel peut-être inséré si nécessaire.

Acteurs	Rôles

Décrire les changements et/ou projets organisationnels lancés ou menés au cours de l'année sous revue ou envisagés à court et moyen terme.

7.3. Présentation des mesures de protection des données de paiement sensibles

Décrire les mesures en place pour préserver la confidentialité et l'intégrité des données de paiement sensibles.

II - PRÉSENTATION DES RÉSULTATS DU CONTRÔLE PÉRIODIQUE SUR LE PÉRIMÈTRE DES MOYENS DE PAIEMENT SCRIPTURAUX

Présenter les résultats des missions du contrôle périodique menées au cours de l'année sous revue sur le périmètre des moyens de paiement scripturaux (y compris les missions inter inspections générales conduites auprès des prestataires de service essentielles externalisées).

Intitulé de la mission	Périmètre et objectifs de la mission	Principaux constats et recommandations en termes de sécurité des moyens de paiement scripturaux et échéance de leur mise en œuvre

III - ÉVALUATION DE LA CONFORMITÉ AUX RECOMMANDATIONS D'ORGANISMES EXTERNES EN MATIÈRE DE SÉCURITÉ DES MOYENS DE PAIEMENT

Énoncé de la recommandation	**Organismes émetteurs**	**Réponse de l'établissement**	
		Évaluation de la conformité (oui / partielle / non / N.C.)	**Commentaires sur l'évaluation (en cas de non-conformité ou conformité partielle)**
Mesures de prévention des risques spécifiques			
Les dispositifs d'émission immédiate de cartes en agence ou en magasin ("*Instant issuing*") font l'objet d'une analyse de risques afin d'ajuster leur niveau de sécurité de façon permanente.	OSCP		
Pour les paiements par téléphone mobile et par carte sans contact, une analyse de risques est conduite avant tout déploiement à grande échelle, en vue de garantir un niveau de sécurité global équivalent à celui des paiements de proximité et sur automate.	OSCP		
En cas d'usage de la biométrie comme facteur d'authentification, le prestataire de service de paiement a procédé à une analyse des risques 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 à usage unique pour le paiement à distance).	OSCP		
Les mesures de sécurité PCI sont adoptées et mises en place sur l'ensemble des processus d'acceptation et d'acquisition des cartes de paiement.	OSCP		
Les solutions de type *m-POS* commercialisées par l'établissement doivent respecter les exigences applicables aux terminaux classiques et s'appuyer sur des protocoles de communication entre les différents composants de la solution qui limitent au strict nécessaire la capacité d'accès de l'appareil mobile aux données de transaction.	OSMP		

Authentification forte et enrôlement du client			
L'initiation de paiements (à l'unité ou en masse) sur internet, l'accès aux données sensibles de paiement et la modification de listes de bénéficiaires enregistrés sont protégés par authentification forte.	OSMP		
Pour les paiements par mobile, le code personnel de paiement est 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.	OSCP		
Des règles définissent la période de validité des dispositifs d'authentification (comprenant les mots de passe à usage unique), le nombre maximal d'échecs d'identification/ d'authentification ou de tentatives de connexion ainsi que les délais d'expiration des sessions de services de paiement sur internet.	SecuRe Pay ABE		
L'inscription du client ainsi que la fourniture des outils, logiciels et données d'authentification au client, requis pour l'utilisation des services de paiement (y compris sur internet) est effectuée de manière sécurisée.	SecuRe Pay ABE		
Pour les paiements par téléphone mobile et par carte sans contact, des mesures spécifiques permettent 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.	OSCP		
Gestion des risques opérationnels et de sécurité			
L'établissement a établi un cadre de gestion des risques opérationnels et de sécurité qui définit les mesures de sécurité visant à atténuer ces risques, documenté et réévalué au moins annuellement par un organe de gouverne de haut niveau.	ABE		
En cas d'externalisation, l'établissement veille à ce que le cadre de gestion des risques couvre de manière effective les activités sous-traitées.	ABE		

L'établissement s'assure de la protection des données sensibles de paiement lors de leur stockage, leur traitement et leur transmission.	ABE		
Des mécanismes de suivi des opérations sont mis en place pour prévenir, détecter et bloquer les opérations de paiement suspectes en amont de leur autorisation.	ABE		
L'établissement a mis en place un cadre de gestion de continuité d'activité, visant à assurer sa capacité à fournir des services de paiement sans interruption et à limiter les pertes en cas de perturbation grave. Ce cadre s'appuie sur la définition de scénarios de crise et le test régulier des plans de réponse.	ABE		

IV- ANNEXES

1. Matrice de cotation des risques de fraude

Présenter la méthodologie de cotation des risques de fraude en indiquant en particulier la grille de cotation de la probabilité/fréquence de survenance et impact (financier/non financier (médiatique en particulier) et la grille de cotation globale faisant apparaître les niveaux de criticité.

2. Glossaire

Définir les termes techniques et acronymes utilisés dans l'annexe.

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 [4]

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 ;
- 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 (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. 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.

4. 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)

1.4. 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 *(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 (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[5]

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)

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