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

Juillet ~~2023~~2024

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 modifié relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution)

Sommaire

Préambule

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

Les éléments ci-après mentionnés le sont à titre indicatif dans la mesure où ils s'avèrent pertinents au vu de l'activité et de l'organisation de l'établissement[1]. 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 modifié. 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 modifié, 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 modifiée, 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 modifié 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 modifiée, 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 modifiée.

À cet égard, il est rappelé que les différentes annexes[2] du rapport de contrôle interne listées ci-dessous, constituent des documents bureautiques autonomes qui doivent être télétransmis indépendamment du corps du rapport de contrôle interne :

- annexe relative à la sécurité des moyens de paiement scripturaux ;
- annexe relative aux mesures mises en œuvre en faveur des clients en situation de fragilité financière ;
- annexe listant les opérations conclues avec les dirigeants effectifs, les membres de l'organe de surveillance et, le cas échéant, avec les actionnaires principaux ;
- annexe précisant les méthodes mises en œuvre, y compris les simulations de crise, pour appréhender les risques liés à l'utilisation des techniques de réduction du risque de crédit reconnues pour l'application du règlement CRR ;
- annexe (pour les sociétés de financement) relative à l'identification, la mesure, la gestion et le contrôle du risque de liquidité et qui décrit les hypothèses utilisées pour établir le tableau de trésorerie prévisionnelle ;

[1] Il est rappelé que les EI de classe 2 et 3 sont tenues de décrire les systèmes de surveillance et de maîtrise des risques auxquels elles sont exposées, notamment concernant les risques de crédit et de contrepartie, résiduel, de concentration, de marché, d'intermédiation, de règlement-livraison, de liquidité, le risque opérationnel, le risque de sécurité et les risques pour les clients, les risques pour le marché et les risques pour l'entreprise au sens du règlement (UE) n° 2019/2033 du Parlement européen et du Conseil du 27 novembre 2019.

[2] Ces annexes sont à remettre en fonction de la nature, des activités et des risques encourus par l'établissement.

- annexe décrivant les hypothèses et les principes méthodologiques retenus ainsi que les résultats des simulations de crise relatives au risque de crédit conformément à l'article 177 du règlement CRR ;
- annexe décrivant les hypothèses et les principes méthodologiques retenus ainsi que les résultats des simulations de crise relatives aux risques de marché conformément au point g) du paragraphe 1 de l'article 368 du règlement CRR ;
- annexe décrivant les hypothèses et les principes méthodologiques retenus, ainsi que les résultats des simulations de crises relatives au risque de crédit de contrepartie conformément aux articles 286 et 290 du règlement CRR ;
- annexe relative aux informations sur le cantonnement de fonds clientèles conformément à l'arrêté du 06 septembre 2017.

Point d'attention : Compte tenu de l'entrée en vigueur le 17 janvier 2025 du règlement européen 2022/2554 sur la résilience opérationnelle numérique du secteur financier, dit « règlement DORA », le Secrétariat général de l'ACPR a décidé d'ajouter au sein de ce canevas, une annexe dédiée aux technologies de l'information et de la communication (TIC), distincte du corps du rapport de contrôle interne, pour mieux préciser la nature des informations attendues par le superviseur en la matière.

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.

Point d'attention : Compte tenu des travaux européens encore en cours, la nouvelle annexe ajoutée suite à la mise en place du règlement DORA sera communiquée à l'automne prochain pour une première remise attendue exceptionnellement pour le 30 juin 2025 au plus tard. Il est rappelé toutefois aux établissements l'importance de procéder sur l'exercice 2024 aux ultimes adaptations nécessaires pour se conformer à ce nouveau règlement.

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 18, 19, 22 et annexe 2).

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 : intégration des membres du conseil d'administration à jour (date de début et fin des mandats) et de l'organisation du directoire ;

– description 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 modifié) ;

– pour les entreprises d'investissement soumises à la règlementation IFR, identification et justification des facteurs k concernés par les activités de l'établissement (cf. tableau descriptif des facteurs k en annexe) ;

– pour les entreprises d'investissement soumises à la règlementation IFR, identification des activités de l'établissement qui ne sont captées par aucun facteur k.

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. articles L.511-55 ou L. 533-29 du Code monétaire et financier) ;

- préciser le cadre d'appétence pour le risque, ses modalités de définition et de révision (cf. articles L.511-93 ou L. 533-31-2 du Code monétaire et financier) ;

- description des politiques régissant la gestion, la qualité et l'agrégation des données sur les risques à différents niveaux dans l'établissement, y compris pour l'activité à l'étranger et les activités externalisées : *mise en place, selon des modalités adaptées à la taille, la nature et à la complexité de l'activité de l'établissement, d'une structure de données uniforme ou homogène permettant d'identifier sans équivoque les données sur les risques ainsi que des mesures permettant d'assurer l'exactitude, l'intégrité, l'exhaustivité et la disponibilité en temps utile des données sur les risques, définition d'un processus de gouvernance du dispositif d'agrégation des données sur les risques* (cf. article 104 de l'arrêté du 3 novembre 2014 modifié) ;

- pour les entreprises d'investissement soumises à la règlementation IFR, présentation succincte du dispositif de fermeture ordonnée : *descriptif du raisonnement et des impacts généraux dans des circonstances de fermeture ordonnée de l'établissement*.

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

Lorsque l'organisation du dispositif de contrôle interne qui contient les trois lignes de défense correspondant aux niveaux de contrôle décrits ci-dessous, ne présente pas de changements significatifs, elle peut être présentée de manière synthétique dans une annexe (cf. canevas en annexe 1 du présent document) ou en communiquant la charte de contrôle interne en vigueur.

2.1. Au dispositif de contrôle permanent « 1er et 2ème niveaux de contrôle » (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 qui correspond aux premier et deuxième niveaux de contrôle tel que défini à l'article 12 de l'arrêté du 3 novembre 2014 modifié (y compris les principales actions projetées dans le domaine du contrôle permanent, cf. articles 259 f) ou 259 bis d) dudit arrêté) : *préciser notamment l'identité, le rattachement hiérarchique et fonctionnel du ou des responsable(s) de contrôle permanent ainsi que les autres fonctions éventuellement exercées par ce(s) dernier(s) au sein de l'établissement ou au sein d'autres entités du même groupe, préciser les unités en charge du contrôle de deuxième niveau, l'identité, pour chacune d'elles, de leur responsable ;*
- description des changements significatifs dans l'organisation de la fonction de vérification de la conformité : *préciser notamment l'identité et le rattachement hiérarchique et fonctionnel du responsable de la fonction de vérification 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 procédures internes mises en place pour encadrer la désignation et la révocation du responsable de la fonction de vérification de la conformité (cf. article 28 de l'arrêté du 3 novembre 2014 modifié) ;
- 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* ;
- identification du dirigeant effectif en charge de la cohérence et de l'efficacité du contrôle permanent de 2ème niveau.

2.2. Au dispositif de contrôle périodique « 3ème niveau de contrôle » assuré par la fonction d'audit interne (y compris l'organisation du contrôle de l'activité à l'étranger et des activités externalisées) :

- identification du responsable de la fonction d'audit interne en charge du troisième niveau de contrôle tel que défini à l'article 12 de l'arrêté du 3 novembre 2014 modifié ;
- identification du dirigeant effectif en charge de la cohérence et de l'efficacité du contrôle périodique ;
- description des changements significatifs dans l'organisation de la fonction d'audit interne ;
- principales actions projetées dans le domaine du contrôle périodique (plan d'audit… cf. articles 259 f) ou 259 bis d) de l'arrêté du 3 novembre 2014 modifié) ;
- description des procédures internes mises en place pour encadrer la désignation et la révocation du responsable de la fonction d'audit interne (cf. article 17 de l'arrêté du 3 novembre 2014 modifié) ;

- dispositions prises le cas échéant pour s'assurer que le cycle complet d'investigations de l'ensemble des activités de l'établissement ou le cas échéant du groupe, n'excède pas cinq ans (cf. article 25 de l'arrêté du 3 novembre 2014 modifié) ;
- dispositions prises le cas échéant pour s'assurer que le cycle d'audit est déterminé selon une approche proportionnée aux risques identifiés au sein de l'établissement ou le cas échéant du groupe.

3. Gouvernance

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 (y compris dans le contexte de l'octroi de prêts et de l'exécution d'autres transactions) tant au niveau de l'établissement que ceux concernant son personnel, modalités d'approbation et de révision de ces dernières (cf. article 38 de l'arrêté du 3 novembre 2014 modifié et Orientations n°2021/05 de l'ABE) ;
- description des procédures mises en place pour identifier, gérer et prévenir les discriminations sur la base du genre, de la race, de l'origine sociale ou ethnique, de l'orientation sexuelle, etc. entre les membres du personnel (cf. Orientations n°2021/05 de l'ABE) ;
- description des procédures mises en place pour garantir des opportunités égales entre les membres du personnel sans tenir compte de leur genre, et améliorer la représentation du genre sous-représenté dans l'organe de direction (cf. Orientations n°2021/05 de l'ABE).

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 modifié) ;
- 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 (hors incidents informatiques) au sens de l'article 98 (cf. article 245 de l'arrêté du 3 novembre 2014 modifié) ;
- 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 modifié) ;
- modalités d'information de l'organe de surveillance et, le cas échéant, du comité des risques, par le responsable de la fonction d'audit interne, de l'absence d'exécution des mesures correctrices décidées (cf. article 26 b) de l'arrêté du 3 novembre 2014 modifié) ;
- modalités d'information par le responsable de la fonction de vérification de la conformité de l'exercice de ses missions à l'organe de surveillance (cf. article 31 de l'arrêté du 3 novembre 2014 modifié) ;

- 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 modifié) ;
- 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 ainsi que le détail du suivi des mesures imposées dans le cadre des procédures d'autorisation des nominations des membres administrateurs et dirigeants effectifs par le superviseur prudentiel.

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 modifié (cf. article 245 de l'arrêté du 3 novembre 2014 modifié) ;
- 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 modifié) ;
- 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 modifié).

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 modifié).

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. articles L.511-60 ou L. 533-29-1 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. articles L.511-72 ou L. 533-30-1 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 modifié) ;
- 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 modifié).

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 ou L. 533-31-4 du Code monétaire et financier et à la partie 2.4.2 des Orientations ABE n°2021/04 ou à la partie 2.3.2 des Orientations ABE n°2021/13 ;

– description des principes généraux de la politique de rémunération définie en application de l'article L. 511-72 ou L. 533-30 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 modifié) ;

– description du rôle des fonctions risques, conformité et support dans la conception et la mise en œuvre de la politique de rémunération (cf. paragraphes 36, 38 à 41, 60 à 62 des Orientations ABE n°2021/04 ou paragraphes 35, 37 à 40, 56 à 58 des Orientations ABE n°2021/13) ;

– 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 ou L. 533-30-2 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 modifié) :

- des critères (relatifs, absolus, quantitatifs, qualitatifs) utilisés pour mesurer la performance et ajuster la rémunération au risque (cf. paragraphe 215 des Orientations ABE n°2021/04 ou paragraphe 209 des Orientations ABE n°2021/13),
- des critères (relatifs, absolus, quantitatifs, qualitatifs) définis pour définir le lien entre rémunération et performance (cf. paragraphe 215 des Orientations ABE n°2021/04 ou paragraphe 209 des Orientations ABE n°2021/13),
- 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 ou L. 533-30-8 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 162 des Orientations n°2021/04 ou paragraphe 155 des Orientations ABE n°2021/13),
- 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 ABE n°2021/04 ou n°2021/13),
- des écarts de rémunération entre les femmes et les hommes : détail du dispositif permettant de réaliser un suivi des écarts de rémunération pour la population concernée[3] (cf. article 511-71 du Code monétaire et financier, article 266 de l'arrêté du 3 novembre 2014 modifié et paragraphes 63, 64 et 65 des Orientations ABE n°2021/04 ou paragraphes 59, 60 et 61 des Orientations ABE n°2021/13).

[3] À savoir les preneurs de risque, à l'exclusion des membres de l'organe de direction, les membres de l'organe de direction dans sa fonction exécutive, les membres de l'organe de surveillance et les autres membres du personnel (cf. paragraphe 101 des Orientations ABE n°2021/05 ou paragraphe 92 des Orientations ABE n°2021/14).

- le cas échéant, description, périmètre et justification des exemptions prévues aux articles 198 et 199 de l'arrêté du 3 novembre 2014 modifié appliquées par l'établissement ;
- dans le cas d'un groupe bancaire soumis à la surveillance sur base consolidée, description du dispositif mis en place le cas échéant au sein des filiales sociétés de gestion de portefeuille ou entreprises d'assurance ou réassurance pour les personnels dont l'activité peut avoir une incidence significative directe sur le profil de risque ou les activités des établissements de crédit, des entreprises d'investissement et des sociétés de financement du groupe (cf. article 200 de l'arrêté du 3 novembre 2014 modifié) ;
- 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 modifié, L. 511-71 et L. 511-75 ou L. 533-30 et L.533-30-3 du Code monétaire et financier et parties 12 et 14.1.3 des Orientations ABE n°2021/04 ou n°2021/13) ;
- 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 ou L. 533-30-5, L. 533-30-8 et L. 533-30-12 du Code monétaire et financier et paragraphes 223, 239 des Orientations ABE n°2021/04 ou paragraphes 217 et 234 des Orientations ABE n°2021/13) ainsi que l'impact de la politique de rémunération sur le capital et la liquidité (cf. paragraphes 123 et 125 des Orientations ABE n°2021/04 ou paragraphes 118 et 120 des Orientations ABE n°2021/13) ;
- 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 modifié, ainsi qu'à l'article R.511-18 ou R. 533-19 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, L. 533-30-11, R.511-22 et R. 511-23, R. 533-21 et R. 533-21-2 du Code monétaire et financier) ;
- les montants globaux des rémunérations différées, réparties entre rémunérations acquises et non acquises (cf. article R.511-18 ou R. 533-19 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 ou R. 533-19 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 ou R. 533-19 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 ou R. 533-19 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 modifié) ;
- 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 fonction de vérification de la conformité (cf. article 266 de l'arrêté du 3 novembre 2014 modifié).

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 modifié) ;
- 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. article 268 de l'arrêté du 3 novembre 2014 modifié et partie 20 des Orientations de l'ABE n°2021/04) ;
- modalités de publication des informations relatives à la politique et aux pratiques de rémunération prévues par l'article 51 du règlement 2019/2033 du Parlement européen et du Conseil du 27 novembre 2019 (cf. partie 20 des Orientations de l'ABE n°2021/13).

4. Résultats des contrôles périodiques effectués au cours de l'exercice écoulé (cf. article 12 de l'arrêté du 3 novembre 2014 modifié) (y compris pour les activités à l'étranger)

- programme des missions (risques et/ou entités ayant fait l'objet d'une vérification de la fonction d'audit interne au cours de l'exercice écoulé), état d'achèvement et ressources allouées en jour-homme, si recours à un prestataire externe : fréquence d'intervention et dimension de l'équipe ;
- 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 la fonction d'audit interne 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) ou 259 bis e) de l'arrêté du 3 novembre 2014 modifié)

Pour les sociétés de financement, joindre une annexe comprenant :

– **caractéristiques des engagements ayant fait l'objet d'une déduction des fonds propres prudentiels** conformément à l'article 5 de l'arrêté du 23 décembre 2013 relatif au régime prudentiel des sociétés de financement : 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.

Pour les établissements de crédit et les entreprises d'investissement, joindre une annexe comprenant **les caractéristiques des engagements envers des actionnaires principaux, des dirigeants effectifs et des membres de l'organe de surveillance** : 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.

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 modifié) ;

– 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 du champ d'application et du processus d'élaboration des simulations de crise : *périmètre (entités et risques pris en compte), fréquence d'application, outils utilisés, unité(s) en charge de leur élaboration, implication des instances dirigeantes dans le processus de validation…,*
- description des hypothèses et principes méthodologiques retenus ainsi que des résultats obtenus,
- description du processus de prise en compte des simulations de crise dans les processus de décision managériale notamment en matière d'appétence pour les risques, de planification du capital et de fixation des limites ;

– 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 ;

– les entreprises d'investissement de classe 2 doivent formaliser un rapport en application de l'article L533-2-2 du Code monétaire et financier pour rendre compte du dispositif ICAAP mis en place par l'entreprise d'investissement et justifier de l'effectivité de l'adéquation entre ses fonds propres internes disponibles et les risques auxquels elle est exposée, de manière dynamique et dans le temps, dans des conditions de marché normales et tendues. Un canevas présentant à titre indicatif la liste des informations essentielles à fournir par l'entreprise d'investissement dans ce rapport est mis à disposition par le SGACPR sur le site internet de l'ACPR[4].

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

Rappel : *Les informations relatives au risque de blanchiment des capitaux et de financement du terrorisme sont à remettre dans le rapport sur l'organisation des dispositifs de contrôle interne de LCB-*

[4] Canevas disponible à partir de la page suivante : Communication à la profession | ACPR (banque-france.fr)

FT et de gel des avoirs, prévu aux articles R.561-38-6 et R.561-38-7 du Code monétaire et financier, selon les modalités définies dans l'arrêté du 21 décembre 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 modifié)

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 fonction de vérification 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 modifié, 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 modifié) ;
- 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 Procédures lors d'opérations relatives à de nouveaux produits, de croissance externe et interne

- présentation des procédures d'examen de la conformité mises en œuvre lors de la réalisation d'opérations relatives à des nouveaux produits ou services, à des changements significatifs de ces derniers ou des systèmes associés aux produits, lors d'opérations de croissance externe et interne ou de transactions exceptionnelles : *avis requis, par écrit et de façon systématique, du responsable de la fonction de vérification de la conformité préalablement à l'exécution de ces opérations* (cf. articles 35 et 221 1er alinéa de l'arrêté du 3 novembre 2014 modifié).

7.6. 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 modifié) ;
- 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 modifié).

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

7.8. Résultats des contrôles permanents de 2ème niveau 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 modifié).

8. Risque de crédit et de contrepartie (cf. articles 106 à 121 de l'arrêté du 3 novembre 2014 modifié)

***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).*

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 modifié) ;
- pour les établissements de crédit et les entreprises d'investissement présentant un niveau de prêts non performants supérieur à 5% : présentation de la stratégie de gestion et de réduction des expositions non-performantes poursuivie *(plan d'action et calendrier, évaluation de l'environnement opérationnel, objectifs quantitatifs, objectifs d'atteinte à court, moyen et long terme, objectifs par principaux portefeuilles, objectifs par options de mise en œuvre …)* et description du dispositif de mise en œuvre opérationnelle *(plan opérationnel approuvé par l'organe de direction, unités impliquées, outils utilisés, fréquence des états de reporting instaurés, implication des instances dirigeantes…)* ;
- pour les établissements de crédit et les entreprises d'investissement : présentation du processus de restructuration des expositions *(critères pris en compte dans la décision de restructuration, délais appliqués, procédures de contrôle mises en place pour s'assurer de la viabilité de la mesure de restructuration prise…)* et modalités de suivi des expositions restructurées, notamment par des indicateurs clés de performance *(paramètres des expositions non performantes, activités de renégociation, activités de liquidation, promesse de paiement de l'emprunteur et la collecte de liquidités…)* ;
- 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 modifié) ;
- 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 modifié) ;
- 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 ou L. 533-31-1 et L. 533-31-2 du Code monétaire et financier), et dans la fixation des limites (cf. article 224 de l'arrêté du 3 novembre 2014 modifié) ;

– 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 modifié) ;

– 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 modifié) ;

~~– description des mesures mises en œuvre par l'établissement pour se mettre en conformité avec d'une part les Orientations de l'ABE sur les estimations de probabilité de défaut (PD), les estimations de perte en cas de défaut (LGD) et sur le traitement des expositions sur lesquelles il y a eu défaut (EBA/GL/2017/16) et d'autre part les Orientations de l'ABE sur les estimations de LGD en cas de ralentissement économique (EBA/GL/2019/03).~~

~~– description des mesures mises en œuvre par l'établissement pour se mettre en conformité avec les Orientations de l'ABE sur l'atténuation du risque de crédit pour les établissements appliquant l'approche NI avec leurs propres estimations de LGD (EBA/GL/2020/05).~~

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[5].

– 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 de 2ème niveau menés sur les activités de crédit :

– principales insuffisances relevées ;

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

- 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 modifié).

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.).

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 (y compris le risque d'ajustement de l'évaluation de crédit) 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 ou L. 533-31-1 et L. 533-31-2 du Code monétaire et financier), et dans la fixation des limites (cf. article 224 de l'arrêté du 3 novembre 2014 modifié) ;
- 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 modifié :
  - 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 ;

~~– description des mesures mises en œuvre par l'établissement pour se mettre en conformité avec les Orientations de l'ABE sur le traitement des positions structurelles de change (EBA/GL/2020/09).~~

10.3. Résultats des contrôles permanents de 2ème niveau 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 modifié).

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 risque de modèle définis à l'article 4 du règlement délégué (UE) n°2018/959, 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], Covid).~~

~~11.5. Risque informatique :~~

~~*11.5.1. Stratégie informatique et adéquation des ressources informatiques :*~~

- ~~présentation de la stratégie informatique de l'établissement définie en application de l'article 270-1 de l'arrêté du 3 novembre 2014 modifié (organisation, articulation avec la stratégie globale, objectifs prioritaires et plans d'action fixés, cadre d'appétence pour les risques …) et des moyens alloués pour la mettre en œuvre (procédures mises en place pour veiller à son respect, budget alloué et sa procédure de pilotage, nombre et nature des effectifs consacrés à la gestion des opérations informatiques, à la sécurité du système d'information ainsi qu'à la continuité d'activité) ;~~
- ~~présentation du processus de gouvernance (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 informatique).~~

~~*11.5.2. Gestion du risque informatique (cf. article 270-2 de l'arrêté du 3 novembre 2014 modifié) :*~~

- ~~présentation des mesures de réduction des risques informatiques majeurs et de contrôle pour surveiller l'efficacité de ces mesures et description du processus d'information des dirigeants effectifs et de l'organe de surveillance ;~~
- ~~présentation de l'organisation de la gestion du risque informatique (définition des rôles et responsabilités des acteurs[6], dispositif d'évaluation du profil de risque informatique et ses résultats, seuil de tolérance au risque, processus d'audit, modalités et périodicité d'information de la direction générale et de l'organe de surveillance sur l'exposition de l'établissement au risque informatique[7]…) ;~~
- ~~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 du risque informatique incluant notamment le risque pour la disponibilité et la continuité, la sécurité, l'intégrité des données et le risque lié au changement des systèmes informatiques (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)[8].~~

~~*11.5.3 Sécurité du système d'information :*~~

- ~~présentation des objectifs de la politique de sécurité des systèmes d'information (protection de la confidentialité, de l'intégrité et de la disponibilité des informations, des actifs, des services informatiques et des données des clients) et nom du responsable de la sécurité des systèmes d'information ;~~
- ~~description des procédures mises en place pour prévenir et traiter les incidents (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[9] (dispositifs de sécurité physique et logique, de préservation de l'intégrité et de la confidentialité des données, mesures spécifiques mises en place pour l'activité de banque en ligne, description des tests d'intrusion effectués au cours de l'exercice, plan de secours informatique…) ;~~
- ~~présentation de la procédure d'information du superviseur en cas d'incidents majeurs ;~~
- ~~présentation du programme de sensibilisation à la sécurité du système d'information (sensibilisation des collaborateurs et prestataires) et des formations régulières (cf. dernier alinéa de l'article 270-3 de l'arrêté du 3 novembre 2014 modifié).~~

---

[6] ~~Notamment ceux de la fonction informatique.~~

[7] ~~Joindre le dernier tableau de bord destiné à les informer.~~

[8] ~~En particulier, préciser si l'établissement est exposé à des risques particuliers et les mesures spécifiques prises pour les gérer.~~

[9] ~~C'est-à-dire ceux dont l'impact financier dépasse soit 25 millions d'euros soit 0,5% du CET1 de l'établissement. Par exemple, une cyber-attaque.~~

~~***11.5.4 Gestion des opérations informatiques :***~~

~~– description des processus de gestion des opérations informatiques : présentation des procédures couvrant l'exploitation, la surveillance et le contrôle des systèmes et services informatiques ;~~

~~– description du processus de détection et de gestion des incidents opérationnels ou de sécurité (cf. article 270-4 de l'arrêté du 3 novembre 2014 modifié).~~

~~***11.5.5 Gestion du changement et des projets :***~~

~~– description du cadre de conduite des projets et programmes informatiques ;~~

~~– description d'un processus de gestion de l'acquisition, du développement et de l'entretien des systèmes d'information et d'un processus de changements des programmes informatiques : *modalités d'enregistrement, de test, d'évaluation et d'approbation et d'implémentation des modifications apportées au système d'information* (cf. article 270-5 de l'arrêté du 3 novembre 2014 modifié).~~

~~11.6~~11.4. Résultats des contrôles permanents de 2ème niveau menés en matière de risque opérationnel ~~y compris du risque informatique~~ :

– 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 modifié).

11.~~7~~5. 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~~.~~ (cf. canevas en annexe 1 du présent document).

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

12.2. Résultats des contrôles permanents de 2ème niveau 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 modifié) ;

– 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 (IRRBB)

~~***Nota bene** : Pour l'exercice 2023, 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 précisant les critères de détection, d'évaluation, de gestion et d'atténuation des risques découlant d'éventuelles variations des taux d'intérêt et de l'évaluation et du suivi du risque d'écart de crédit des activités hors portefeuille de négociation des établissements (ABE/GL/2022/14), en vigueur le 30 juin 2023[10].~~

– 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 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)* ;

– description et justification du recours éventuel au principe de proportionnalité au vu du volume, de la complexité, de l'appétit au risque et du niveau de risque de leurs positions sensibles au risque de taux, ainsi que de la taille, de la stratégie et du modèle d'entreprise de l'établissement, applicable aux exigences suivantes des orientations :

  - calcul et allocation du capital interne au titre du risque de taux (tenant compte à la fois de l'impact sur la valeur économique et sur les produits d'intérêts nets[11]) ;
  - mesure et suivi du risque de taux (notamment avec des scenarios internes de chocs adaptés comme mentionnés aux paragraphes 89 à 102 des Orientations de l'ABE, et l'utilisation des mesures de proportionnalité prévues dans la « matrice de sophistication » à l'annexe II des Orientations de l'ABE) incluant la prise en compte des interactions et effets croisés entre différents types de risques : taux, crédit, liquidité, marché ;
  - dispositifs de surveillance (notamment l'application de limites et de sous-limites uniquement pour les composantes significatives du risque de taux mentionnées aux paragraphes 44(c) et 44(d) des Orientations de l'ABE) ;
  - dispositifs de gouvernance (adaptation des rapports adressés à l'organe de direction en fonction des activités de l'établissement, mentionnée au paragraphe 67 des Orientations de l'ABE).

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 en produits d'intérêts nets, calcul de valeur actualisée nette, hypothèses et résultats des stress scenarii incluant le cas échéant les interactions et effets croisés entre types de risques (taux, crédit, liquidité, marché - paragraphe 97 des Orientations de l'ABE), impact des variations du risque de taux d'intérêt global sur l'activité de l'établissement pour l'année*

~~[10] Sauf les sections 4.5 et 4.6 des Orientations qui s'appliquent au 31 décembre 2023.~~

[11] Comme précisé dans le paragraphe 23 des Orientations ABE (ABE/GL/2022/14), les deux mesures doivent être prises en compte dans le processus d'allocation de capital interne, cependant les établissements ne sont pas censés capitaliser deux fois – au titre de chaque mesure (produits d'intérêts nets et valeur économique)

écoulée, en cas d'exposition dans différentes devises, méthodologie utilisée pour l'agrégation des expositions, impacts des instruments en juste valeur) ;

- 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 automatiques (explicites et implicites) et comportementales, notamment le traitement des dépôts non-échéancés (présentation de la méthodologie utilisée pour la segmentation des dépôts par catégories, de l'identification des dépôts stables, des conventions d'écoulement des différents segments de dépôts non-échéancés), des remboursements anticipés de prêts, des retraits anticipés de comptes à terme, des tirages au hors bilan (e.g. lignes de trésorerie) et des produits d'épargne réglementée]* ;
- présentation des activités de couverture: *préciser la stratégie adoptée, les différents instruments mis en œuvre et les contrôles menés sur ces activités ;*
    - présentation des résultats du « *Supervisory outlier test* » sur la valeur économique des fonds propres selon six scénarios de chocs de taux standardisés ainsi que sur les produits d'intérêts nets selon deux scénarios de chocs de taux standardisés tels que précisés par le ~~standard technique de l'ABE (ABE/RTS/2022/10) en attente de publication par la Commission européenne sous la forme d'un Règlement délégué [publication attendue pour le T3 2023]~~Règlement délégué européen n°2024/856 (RTS) - *hypothèses principales :*
        - Chocs appliqués avec intégration d'un plancher post-choc commençant avec -150 bps (conformément au paragraphe ~~(k)~~7 de l'article ~~4~~3 du ~~standard technique~~RTS susvisé),
        - Exclusion des fonds propres des éléments du passif (instruments CET1 et autres fonds propres permanents sans date d'appel),
        - Se référer à l'article ~~4~~3 du ~~standard technique~~RTS susvisé pour la liste exhaustive des hypothèses de calcul de la sensibilité en valeur économique des fonds propres pour le « *Supervisory outlier test* »,
        - Se référer à l'article ~~5~~4 du ~~standard technique~~RTS susvisé pour la liste exhaustive des hypothèses de calcul de la sensibilité en produits d'intérêts nets pour le « *Supervisory outlier test* ».
- présentation des résultats du « *Supervisory outlier test*» en valeur économique selon les 6 chocs différenciés détaillés dans le ~~standard technique~~RTS susvisé par devises rapportés à 15% des fonds propres de base (TIER 1) de l'établissement ;
- présentation des résultats du « *Supervisory outlier test*» en produits d'intérêts nets selon les 2 chocs prudentiels différenciés détaillés dans le ~~standard technique~~RTS susvisé rapportés à 5% des fonds propres de base (TIER 1) de l'établissement ;
- 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 produits d'intérêts nets, des calculs de valeur actualisée nette et des stress scenarii,*
    - *pour le calcul de la sensibilité en valeur économique et en produits d'intérêts nets, justification des éventuelles différences avec les hypothèses normalisées décrites dans le cadre du « Supervisory outlier test»,*
    - *pour le calcul de la mesure de produits d'intérêts nets, selon les hypothèses internes retenues par l'établissement pour sa gestion interne du risque de taux d'intérêt global, base de projections entre un et cinq ans, utilisant a minima un scénario de base et un scénario de choc ou de tension tel qu'indiqué au paragraphe 15 des Orientations de l'ABE (se référer également à la matrice de sophistication de l'annexe II des Orientations*

ABE). Présentation des hypothèses retenues. Présentation de l'inclusion des instruments à la juste valeur.

L'annexe I des Orientations EBA/GL/2022/14 décrit, à titre d'exemple, pour les établissements qui ne disposeraient pas de méthodologie propre, les méthodes susceptibles d'être utilisées ;

- sensibilité des résultats du choc à une modification des hypothèses retenues *(préciser l'impact des différents mouvements, parallèles et non-parallèles, 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 et de la méthodologie d'allocation choisie ;
- 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 produits d'intérêts nets.

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

- pour l'approche en produits d'intérêts nets et l'approche en valeur économique, 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 modifié).

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 de 2ème niveau 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 modifié).

13.5. Dispositif de surveillance du risque d'écart de crédit issu des activités hors portefeuille de négociation *Credit Spread Risk in the Banking Book* - CSRBB)[~~12~~] :

[~~12~~] ~~Les sections des Orientations ABE/GL/2022/14 concernant le CSRBB ne s'appliquent qu'à compter du 31 décembre 2023.~~

- description synthétique du cadre général de la détection, de l'évaluation et de la gestion du risque CSRBB : *préciser le périmètre des opérations prises en compte et les éventuelles exclusions d'instruments appliquées en les justifiant, description du rôle des dirigeants effectifs et des organes de surveillance et la répartition des compétences en matière de pilotage du risque CSRBB* ;
- description du suivi et de l'évaluation des positions affectées par le risque d'écart de crédit issu des activités hors portefeuille de négociation, via notamment les métriques en valeur économique et produits d'intérêts nets (cf. article 84 paragraphe 2 de la directive 2013/36/UE) : *préciser les indicateurs et outils utilisés, décrire les hypothèses et principes méthodologiques retenus, résultats obtenus ;*
- description synthétique des reportings utilisés pour la gestion du risque CSRBB *(préciser notamment la périodicité et les destinataires des reportings).*

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

- les établissements doivent formaliser et remettre les conclusions des évaluations de leur sensibilité au risque IRRBB et au risque CSRBB, ainsi que leur incidence sur la gestion du risque et sur la gestion globale de l'établissement.

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 modifié)* ;
- 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 modifié) ;
- 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 modifié).

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 modifié), 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 modifié* ;
- 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 modifié) ;
- 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 modifié 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 ;

– les entreprises d'investissement de classe 2 doivent formaliser un rapport en application de l'article L533-2-2 du Code monétaire et financier pour rendre compte du dispositif ILAAP mis en place par l'entreprise d'investissement et justifier de l'effectivité de l'adéquation entre ses actifs liquides disponibles et les risques auxquels elle est exposée, de manière dynamique et dans le temps, dans des

conditions de marché normales et tendues. Un canevas présentant à titre indicatif la liste des informations essentielles à fournir par l'entreprise d'investissement dans ce rapport est mis à disposition par le SGACPR sur le site internet de l'ACPR[13].

16.3. Risque de liquidité et de procyclicité résultant des appels de marges découlant de la compensation centrale par des membres compensateurs et des expositions non-compensées centralement

- présentation des procédures permettant d'éviter que la fourniture de services de compensation centrale aux clients n'entraîne des changements soudains et importants en matière d'appels de marge, de collecte de marge et d'abaissement des notations de crédit ;
- présentation des procédures permettant d'éviter, pour les contrats dérivés de gré-à-gré et des opérations de financement sur titres ne faisant pas l'objet d'une compensation centrale, que les procédures de gestion des risques n'entraîne de changements soudains et importants en matière d'appels de marge, de collecte de marge et d'abaissement des notations de crédit ;
- présentation des procédures permettant de limiter les contraintes de liquidité liées à la collecte des marges (ex : utilisation de l'excédent des garanties de marge initiale plutôt qu'à la collecte de garanties supplémentaires, prise en compte des contraintes opérationnelles des clients).

16.4. 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).*

16.5. Résultats des contrôles permanents de 2ème niveau 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 modifié).

16.6. 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 modifié).

– 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 modifié) ;

[13] Canevas disponible à partir de la page suivante : Communication à la profession | ACPR (banque-france.fr)

- 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 modifié), 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 conformément à la règlementation en vigueur (i.e. l'arrêté du 6 septembre 2017 relatif au cantonnement des fonds de la clientèle des entreprises d'investissement) 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 la (des) convention(s) de compte(s) de cantonnement ou de toute modification apportée à la convention de compte de cantonnement précédemment transmise, 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 ;
- pour les établissements assurant la protection des fonds reçus auprès d'un établissement de crédit, d'une banque ou d'un fonds du marché monétaire qualifié appartenant au même groupe qu'eux : communication du montant déposé auprès d'une ou de plusieurs entités du groupe par rapport au montant total des fonds des clients à cantonner, justification de la proportion des fonds cantonnés au sein du groupe ;
- 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 responsable unique, disposant des compétences et de l'autorité nécessaires, spécialement chargé des questions relatives au respect par l'entreprise de ses obligations concernant la sauvegarde des instruments financiers et des fonds des clients, conformément à l'article 9 de l'arrêté du septembre 2017 relatif au cantonnement des fonds de la clientèle des entreprises d'investissement ;
- 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. Cette remise, qui peut être effectuée par voie électronique, doit spécifier (i) la liste des unités internes dont l'activité a substantiellement été modifiée depuis la dernière transmission au SGACPR (ii) a minima, les mandats à jour de ces mêmes unités internes. Il est également possible

de transmettre l'intégralité des mandats en mettant en évidence les modifications substantielles depuis la dernière transmission au SGACPR.

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, détaillant notamment les lignes d'activité retenues en interne par l'établissement pour classifier les opérations réalisées avec les organismes de placement collectif (OPC) et autres véhicules similaires ayant recours à l'effet de levier de manière substantielle ;

– recensement des fonds à effet de levier :

	Nombre de fonds
A. OPC ou véhicules étrangers similaires sur lesquels l'établissement est exposé au risque de crédit ou de contrepartie	
A.1. ayant recours directement ou indirectement à un effet de levier de manière substantielle et non explicitement exclus	
A.1.a. ayant recours à l'effet de levier de manière substantielle[14]	
A.1.b. investis ou exposés significativement[15] dans les OPC ou autres véhicules similaires ayant recours à l'effet de levier de manière substantielle	
A.2. n'ayant pas recours à un effet de levier de manière substantielle ou explicitement exclus	
dont: explicitement exclus au titre de l'article 7, paragraphe I, points 1 à 4 de l'arrêté du 9 septembre 2014	

    - préciser selon quelle fréquence les OPC et les véhicules similaires sont recensés et catégorisés dans les classes susmentionnées ;

– bilan des résultats et des risques générés (risques de crédit et de contrepartie) :

[14] au sens de l'article 111 du règlement délégué n° 231/2013 de la Commission du 19 décembre 2012

[15] au-delà du seuil de l'article 7 de l'arrêté du 9 septembre 2014

Nota bene : **Les tableaux et questions ci-dessous précédant la section 19.4 se réfèrent uniquement aux opérations exposant à un risque de crédit ou de contrepartie sur les OPC ou autres véhicules étrangers similaires ayant recours directement ou indirectement à un effet de levier de manière substantielle et non explicitement exclus au titre de l'article 7, paragraphe I, points 1 à 4 de l'arrêté du 9 septembre 2014.**

- synthèse des expositions par nature d'opérations :

KEUR	Valeur comptable brute IFRS	Montant nominal IFRS	Notionnel IFRS	Valeur exposée au risque avant prise en compte des sûretés	Actifs pondérés en risque pour risque de crédit et de contrepartie
A. Opérations ayant pour contrepartie des OPC ou des véhicules similaires					
A.1. Activités de financement hors opérations de marché					
A.1.a. Avances, dont comptes débiteurs					
A.1.b. Prêts hors prises en pension					
A.1.c. Engagements de financement non utilisés					
A.1.d. Engagements de garantie					
A.2. Opérations de marché					
A.2.a. Pensions de titres et prêts-emprunts de titres					
A.2.b. Dérivés					
A.2.b.i. Dérivés à des visées de financement de positions					
A.2.b.ii. Autres dérivés					
A.3. Autres					
B. Investissements dans des OPC ou de véhicules similaires					
B.1. Détention de parts d'OPC ou de véhicules similaires					
B.2. Autres					
Total (A+B)					

- pour les établissements respectant l'une des conditions suivantes à la date d'arrêté :
  - la valeur comptable brute IFRS de la ligne « Total (A+B) » est supérieur à 300 MEUR,
  - la valeur exposée au risque avant prise en compte des sûretés de la ligne « Total (A+B) » est supérieure à 300 MEUR,

- la valeur exposée au risque avant prise en compte des sûretés de la ligne « Total (A+B) » est supérieure à 5% des fonds propres prudentiels :

  - compléter le tableau ci-dessous :

KEUR	Produit net bancaire
A. Opérations ayant pour contrepartie des OPC ou des véhicules similaires	
A.1. Activités de financement hors opérations de marché	
A.2. Opérations de marché	
A.3. Autres	
B. Investissements dans des OPC ou de véhicules similaires	
B.1. Détention de parts d'OPC ou de véhicules similaires	
B.2. Autres	
C. Autres activités ne générant pas de risque de crédit ou de contrepartie	
Total (A+B+C)	

  - préciser les indicateurs utilisés pour mesurer le couple rendement-risques des différentes activités ;
  - indiquer à quelle granularité et à quelle fréquence les indicateurs sont calculés et suivis ;
  - préciser les éventuels objectifs quantitatifs ou limites assortis aux indicateurs;

– description des dispositifs de maîtrise des risques précités et contrôles afférents ;

– préciser parmi les lignes d'activité internes présentées dans la description générale des activités, lesquelles sont encadrées par une politique de collatéralisation ;

– pour chaque ligne d'activité encadrée par une politique de collatéralisation :
  - résumer ses principes ;
  - présenter les critères d'éligibilité, de disponibilité et de quantité des sûretés permettant de s'assurer que ces sûretés protègent les expositions générées par ces opérations, conformément aux dispositions de l'article 7 de l'arrêté portant application de la loi SRAB ;
  - préciser comment les critères de quantité et de disponibilité des sûretés sont adaptés à leur qualité et au niveau des risques induits par les opérations garanties par ces sûretés ;
  - lorsque les critères de qualité et de disponibilité ne sont pas respectés, indiquer si la mise en place d'une exigence de quantité plus importante est prévue et si oui dans quelle mesure ;
  - indiquer si la politique prévoit des dérogations éventuelles à son application. Le cas échéant, décrire comment elles sont encadrées ;
  - préciser si des indicateurs sont utilisés pour mesurer le degré de collatéralisation des opérations. Si oui, les définir et commenter leur utilisation opérationnelle ;

– résumer les principes retenus pour encadrer les degrés de concentration (i) des expositions individuelles sur un OPC ou un autre véhicule similaire ayant recours à l'effet de levier de manière substantielle, et (ii) des sûretés obtenues de la part de cette contrepartie.

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

***Rappel** : Pour l'exercice 2024, les activités informatiques externalisées ne devront pas être traitées dans cette partie. Les éléments les concernant seront à décrire dans une annexe spécifique qui sera disponible ultérieurement et qui reprendra les dispositions du règlement européen 2022/2554 sur la résilience opérationnelle numérique du secteur financier, dit règlement DORA, dont l'entrée en vigueur est fixée au 17 janvier 2025.*

– 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 *(analyse préalable menée sur la criticité de l'activité à externaliser et l'évaluation des risques associés…)* avant que celle-ci ne soit effective ~~(notamment quand cela peut affecter les TIC de l'établissement)~~ ;

~~– adaptations prises pour se conformer à l'exigence de tenue d'un registre comprenant les informations visées à la section 11 des Orientations de l'ABE sur l'ensemble des dispositifs d'externalisation (cf. article 238 de l'arrêté du 3 novembre 2014 modifié);~~

– description des activités externalisées[16] (au sens des paragraphes q) et r) de l'article 10 de l'arrêté du 3 novembre 2014 modifié) et proportion par rapport à l'activité globale de l'établissement *(dans son ensemble et domaine par domaine)* ;

~~– communication de l'extraction annuelle du registre mentionnant les dispositifs d'externalisation portant sur les activités essentielles ou importantes (au sens de l'article 10 de l'arrêté du 3 novembre 2014 modifié) ;~~

– 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 modifié, 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 ;

– descriptif de la méthodologie d'évaluation de la qualité de la prestation et sa fréquence de revue ;

– 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 ;

– description des procédures d'identification, d'évaluation et de gestion des conflits d'intérêts liés au dispositif d'externalisation de l'établissement, y compris entre entités du même groupe ;

– description des plans de poursuite d'activité et de la stratégie de sortie définis pour les activités critiques ou importantes externalisées : formalisation des scénarii et objectifs retenus ainsi que des

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

mesures alternatives envisagées, présentation des tests réalisés (fréquence, résultats…), reporting à la direction (sur les tests, les mises à jour apportées aux plans ou à la stratégie de sortie) ;

- 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 modifié) ;
- 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 modifié) ;
- 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 de 2ème niveau 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 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 de 2ème niveau 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 et de l'accès aux comptes de paiement et à leurs informations

SOMMAIRE

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, ainsi qu'à **la sécurité de l'accès aux comptes de paiement et à leurs informations** dans le cadre de la fourniture des services d'initiation de paiement et d'information sur les comptes. 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 ses missions définies au I de l'article L. 141-4 et à l'article L. 521-8 du Code monétaire et financier et, pour les annexes établies par les établissements ayant leur siège social dans les collectivités françaises du Pacifique, à l'Institut d'émission d'Outre-Mer (IEOM) pour l'exercice de ses missions définies à l'article L. 721-20 du même Code[17].

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 modifié. Par ailleurs, dans la mesure où la compétence de la Banque de France porte sur le territoire français, seuls les moyens de paiement offerts en France (ou les comptes de paiement ouverts en France) sont concernés par la présente annexe, excluant donc les services des établissements fournis via leurs succursales installées à l'étranger.

Les établissements gestionnaires de moyens de paiement sans être pour autant leurs émetteurs doivent renseigner cette annexe. Les établissements qui n'émettent ni ne gèrent aucun moyen de paiement portent la mention : « L'établissement n'émet ni 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, ainsi que celui de l'accès aux comptes de paiement tenus par l'établissement.

Cette annexe comporte 5 parties :

- une partie portant sur la présentation de chaque moyen et service 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 et de l'accès aux comptes (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 et de sécurité de l'accès aux comptes (III) ;

[17] Pour les prestataires de services de paiement ayant leur siège social dans une Collectivité française du Pacifique (Nouvelle-Calédonie, Polynésie française, îles Wallis-et-Futuna), la mention « Banque de France » doit être remplacée par celle de « IEOM » dans la présente annexe et les références au « territoire français » par « Collectivités françaises du Pacifique ».

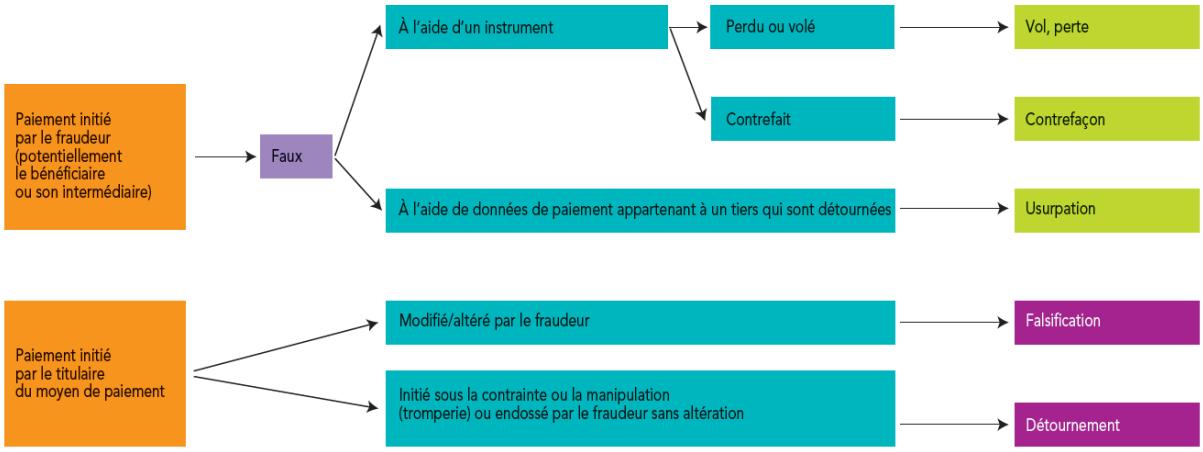
- une partie relative au rapport d'audit sur la mise en œuvre des mesures de sécurité inscrites dans les RTS (*Regulatory Technical Standards*)[18] (IV) ;
- une annexe comprenant la matrice de cotation des risques de fraude et un glossaire pour la définition des termes techniques/acronymes utilisés par l'établissement dans l'annexe (V).

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 »[19].

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 typologies de fraude aux moyens de paiement retenue pour la déclaration statistique auprès de la Banque de France.

Présentation schématique des différentes typologies de fraude



Note : Cette présentation schématique est à considérer en complément des guides officiels de la Banque de France relatifs aux collectes statistiques sur la fraude aux moyens de paiement.

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. **~~À partir du~~Depuis le rapport annuel 2023 sur l'exercice 2022, il est également attendu que les établissements remplissent la partie consacrée au chèque.** En ce qui concerne le chèque, le rapport annuel de contrôle interne permet de remonter à la Banque de France une information sur l'offre de produits et de services liés au chèque, sur l'organisation opérationnelle de l'activité ou sur l'évolution de la fraude au cours de l'année et les dispositifs de maîtrise des risques mis en place, ce que ne permet pas l'exercice annuel d'autoévaluation au Référentiel de Sécurité du Chèque de la Banque de France (RSC).

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.

[18] Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication

[19] Cf. Guide de remplissage de la fraude : https://www.banque-france.fr/stabilite-financiere/securite-des-moyens-de-paiement-scripturaux/collectes-statistiques-reglementaires-espace-declarants

S'agissant de la partie IV, elle est destinée à recueillir les résultats du rapport d'audit devant être établi par l'établissement en application de l'article 3 du règlement délégué (UE) 2018/389 de la Commission européenne du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication ou RTS (*Regulatory Technical Standards*). Ces normes techniques constituent des exigences essentielles pour la sécurité des moyens de paiement scripturaux et pour la sécurité des accès aux comptes de paiement et à leurs informations. Ce rapport a pour objet d'évaluer la conformité de l'établissement au regard des exigences de sécurité inscrites dans les RTS. Il se présente sous la forme d'un questionnaire reprenant les mesures de sécurité prévues dans les RTS et pour lesquelles l'établissement doit fournir des réponses argumentées sur leur mise en œuvre ou le cas échéant, sur le plan d'action envisagé pour s'y conformer. Les éléments de preuve correspondants doivent être mis à la disposition de la Banque de France sur sa demande. Conformément à l'article 3 des RTS, il est rappelé que ce rapport d'audit doit être établi annuellement par les équipes du contrôle périodique de l'établissement. Toutefois, concernant l'évaluation de la conformité de l'établissement à l'article 18 des RTS en cas d'usage à la dérogation qui y est visée, celle-ci doit être réalisée par un auditeur externe indépendant et qualifié la première année de sa mise en œuvre puis ensuite tous les 3 ans. Cette évaluation a pour objet de vérifier la conformité des conditions de mise en œuvre de l'exemption au titre de l'analyse des risques et en particulier du taux de fraude mesuré par l'établissement pour le type d'opération de paiement concerné (c'est-à-dire au regard de l'instrument de paiement utilisé et du montant de l'opération de paiement) ; cette évaluation réalisée par un auditeur externe doit être annexée à la partie IV sur les conclusions du rapport d'audit.

Remarque importante concernant les établissements bancaires affiliés à un groupe, réseau ou organe central, ce dernier étant responsable au niveau central du dispositif de contrôle interne et de maîtrise des risques sur la sécurité des moyens de paiement et de l'accès aux comptes.

- 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'établissement en charge du dispositif de contrôle et de maîtrise des risques 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 du groupe, réseau ou organe central et décrit par celui-ci dans sa propre annexe, 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'établissement en charge du dispositif de contrôle interne et de maîtrise des risques dans sa propre annexe »*.

- S'agissant du rapport d'audit sur la mise en œuvre des mesures de sécurité inscrites dans les RTS (IV), l'établissement affilié en est dispensé et doit mentionner *« qu'il se réfère à ce qui a été décrit par l'établissement en charge du dispositif de contrôle interne et de maîtrise des risques dans sa propre annexe* ».

Quand l'établissement renvoie le lecteur à l'annexe produite par l'établissement en charge du dispositif de contrôle interne et de maîtrise des risques pour la sécurité des moyens des paiements et de l'accès aux comptes, il spécifie l'identité exacte et le code interbancaire de l'établissement en question.

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 ET SERVICES 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
Carte perdue ou volée	Le fraudeur utilise une carte de paiement à la suite d'une perte ou d'un vol, à l'insu du titulaire légitime.
Carte non parvenue	La carte a été interceptée lors de son envoi entre l'émetteur et le titulaire légitime. Ce type de fraude se rapproche de la perte ou du vol. Cependant, il s'en distingue dans la mesure où le porteur peut difficilement constater qu'un fraudeur est en possession d'une carte lui étant

	destinée. Dans ce cas de figure, le fraudeur s'attache à exploiter des vulnérabilités dans les procédures d'envoi des cartes.
Carte contrefaite	Le fraudeur utilise (i) une carte contrefaite, qui suppose la création d'un support donnant l'illusion d'être une carte de paiement authentique et/ou susceptible de tromper un automate ou un terminal de paiement de commerçant ou (ii) d'une carte falsifiée qui consiste à modifier les données magnétiques, d'embossage ou de programmation d'une carte authentique. Dans les deux cas, le fraudeur s'attache à ce qu'une telle carte supporte les données nécessaires pour tromper le système d'acceptation.
Numéro de carte usurpé	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.
Autre	Tout autre motif de fraude comme l'utilisation d'un numéro de carte cohérent mais non attribué à un porteur puis utilisé en vente à distance, la modification par le fraudeur d'un ordre de paiement légitime (falsification), la manipulation du payeur ou la contrainte à l'égard de celui-ci ayant pour effet d'obtenir un paiement par carte (détournement) etc.

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
Carte perdue ou volée	*Ex : au point de vente*	
Carte non parvenue		
Carte contrefaite		
Numéro de carte usurpé		
Autre		

En tant qu'établissement acquéreur :

Typologie de fraude	Canal d'initiation	Mesures de couverture
Carte perdue ou volée		
Carte non parvenue		
Carte contrefaite		
Numéro de carte usurpé		
Autre		

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 contrefait un ordre de virement ou usurpe les identifiants de la banque en ligne du donneur d'ordre légitime afin d'initier un ordre de paiement. Dans ce cas de figure, les identifiants peuvent notamment être obtenus via des procédés de piratage informatique (*phishing*, *malware*, etc.) ou sous la contrainte.
Falsification de l'ordre de virement	Le fraudeur intercepte et modifie un ordre de virement ou un fichier de remise de virement légitime.
Détournement	Le fraudeur amène, par la tromperie (notamment de type ingénierie sociale, c'est-à-dire en usurpant l'identité d'un interlocuteur du payeur : responsable hiérarchique, fournisseur, technicien bancaire, etc.), le titulaire légitime du compte à émettre régulièrement un virement à destination d'un numéro de compte qui n'est pas celui du

	bénéficiaire légitime du paiement ou qui ne correspond à aucune réalité économique. Par exemple, sont considérées comme répondant à cette définition les cas de « fraude au Président » ou de fraude au changement de coordonnées bancaires.

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		

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	Le fraudeur créancier émet des prélèvements vers des numéros de compte qu'il a obtenus illégalement et sans aucune autorisation ou réalité économique sous-jacente (« opération de paiement non autorisée » dans la terminologie de l'ABE). 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). Exemple 3 : Le créancier émet sciemment des prélèvements déjà émis (qui ont soit déjà été réglé, soit fait l'objet de rejets pour opposition du débiteur).
Détournement	Le fraudeur débiteur usurpe l'identité et l'IBAN d'un tiers pour la signature d'un mandat de prélèvement sur un compte qui n'est pas le sien (« manipulation du payeur par le fraudeur » dans la terminologie de l'ABE).

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		

En tant qu'établissement du créancier :

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

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	Émission illégitime d'un effet de commerce par un fraudeur en utilisant une formule vierge.
Contrefaçon	Faux effet de commerce créé de toutes pièces par le fraudeur, émis sur une banque existante ou une fausse banque.
Falsification	Effet de commerce régulier intercepté par un fraudeur qui l'altère volontairement par grattage, gommage ou effacement.
Détournement, rejeu	Effet de commerce perdu ou volé après compensation dans les systèmes de paiement et présenté à nouveau à l'encaissement.

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		
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 de délivrance / de remise	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. Grille d'analyse des risques et principaux incidents de fraude

a. Rappel de la typologie de fraude applicable

Typologie de fraude	Description
Vol, perte	- Utilisation par le fraudeur d'un chèque perdu ou volé à son titulaire légitime revêtu d'une fausse signature qui n'est ni celle du titulaire du compte, ni celle de son mandataire. - Émission illégitime d'un chèque par un fraudeur utilisant une formule vierge.
Contrefaçon	Faux chèque créé de toutes pièces par le fraudeur, émis sur une banque existante ou une fausse banque.
Falsification	Chèque régulier intercepté par un fraudeur qui le modifie volontairement par des procédés mécaniques et/ou chimiques (par ex. grattage, gommage ou effacement) dans son montant ou dans son ordre.
Détournement, rejeu	- Chèque régulièrement émis, perdu ou volé, intercepté dans le circuit d'acheminement vers le bénéficiaire et encaissé sur un compte

	différent de celui du bénéficiaire légitime. La formule est correcte, le nom du bénéficiaire est inchangé et la ligne magnétique située en bas du chèque est valide, tout comme la signature du client. - Chèque perdu ou volé après compensation dans les systèmes de paiement et présenté à nouveau à l'encaissement. - Chèque émis par le titulaire légitime sous la contrainte ou la manipulation.

b. Cotation globale du risque de fraude sur les chèques

En référence à la matrice de cotation utilisée par l'établissement pour évaluer le risque de fraude qui est à communiquer dans la partie V 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 tiré :

Typologie de fraude	Canal de délivrance des formules	Mesures de couverture
Vol, perte		
Contrefaçon		
Falsification		
Détournement, rejeu		

En tant qu'établissement du remettant (y compris la lutte contre les remises frauduleuses réalisées par l'intermédiaire du client remettant) :

Typologie de fraude	Canal de remise	Mesures de couverture
Vol, perte		
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 de délivrance des formules	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 de remise	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.

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 ET DE L'ACCÈS AUX COMPTES

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 ET DE SÉCURITÉ DE L'ACCÈS AUX COMPTES

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		
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			
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		
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		
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 – RAPPORT D'AUDIT SUR LA MISE EN ŒUVRE DES MESURES DE SÉCURITÉ INSCRITES DANS LES RTS (*REGULATORY TECHNICAL STANDARDS*)

Concernant la partie relative aux normes communes et sécurisées de communication, l'établissement renseigne le questionnaire en fonction de la solution d'interface d'accès mise en place pour les PSP tiers.

Réf. Articles Règlement (UE) 2018/389	Questions posées au PSP	Évaluation de la conformité	
		oui / partiellement / non/NC)	Pour chacune des mesures de sécurité, préciser les modalités de mise en œuvre. En cas de non-conformité ou conformité partielle, présenter le plan d'action prévu avec les échéances de mise en œuvre. Si le PSP n'est pas concerné (NC) par la mesure de sécurité, le justifier
Mesures de sécurité pour l'application de la procédure d'authentification forte du client			
Code d'authentification			
4	Lorsque le PSP applique la procédure d'authentification forte du client, celle-ci est-elle bien fondée sur deux ou plusieurs éléments appartenant aux catégories « connaissance», «possession» et «inhérence», et donne-t-elle lieu à la génération d'un code d'authentification ?		
	Le code d'authentification est bien accepté qu'une seule fois par le PSP lorsque le payeur utilise ce code dans les situations listées ci-après ? - pour accéder à son compte de paiement en ligne ; - pour initier une opération de paiement électronique ; - pour exécuter une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation abusive.		
	Le PSP prévoit-t-il des mesures de sécurité garantissant le respect de chacune des exigences listées ci-après ? - aucune information sur l'un des éléments appartenant aux catégories « connaissance », « possession » et « inhérence » ne peut être déduite de la divulgation du code d'authentification ;		

	- il n'est pas possible de générer un nouveau code d'authentification en se basant sur un autre code d'authentification généré au préalable ; - le code d'authentification ne peut pas être falsifié.		
	Le PSP veille-t-il à ce que l'authentification au moyen de la génération d'un code d'authentification intègre chacune des mesures listées ci-après ? - lorsque l'authentification pour accès à distance, paiements électroniques à distance et toute autre action grâce à un moyen de communication à distance susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation abusive n'a pas généré de code d'authentification, il n'est pas possible de déterminer lequel des éléments (connaissance, possession et inhérence) était incorrect ; - le nombre de tentatives d'authentification infructueuses consécutives au bout duquel les actions prévues à l'article 97, paragraphe 1, de la directive (UE) 2015/2366 sont bloquées à titre temporaire ou permanent ne dépasse pas cinq au cours d'une période donnée ; - les sessions de communication sont protégées contre l'interception des données d'authentification communiquées durant l'authentification et contre la manipulation par des tiers non autorisés ; - le délai maximal d'inactivité du payeur, une fois que celui-ci s'est authentifié pour accéder à son compte de paiement en ligne, ne dépasse pas cinq minutes.		
	En cas de blocage temporaire suite à des tentatives d'authentification infructueuses, la durée de celui-ci et le nombre de nouveaux essais sont-ils fixés sur la base des caractéristiques du service fourni au payeur		

	et de l'ensemble des risques correspondants qui y sont associés, en tenant compte, au minimum, des facteurs énoncés à l'article 2 § 2 des RTS ? Le payeur est-il bien averti avant que le blocage ne devienne permanent ?		
	En cas de blocage permanent, une procédure sécurisée est-elle mise en place pour permettre au payeur d'utiliser à nouveau les instruments de paiement électronique bloqués ?		
Établissement d'un lien dynamique			
5	Lorsque le PSP applique la procédure d'authentification forte du client (conformément à l'article 97 § 2 de la directive (UE) 2015/2366) respecte-t-il les exigences listées ci-après ? - le payeur est informé du montant de l'opération de paiement et du bénéficiaire ; - le code d'authentification généré est spécifique au montant de l'opération de paiement et au bénéficiaire approuvé par le payeur lors de l'initiation de l'opération ; - le code d'authentification accepté par le prestataire de services de paiement correspond au montant spécifique initial de l'opération de paiement et à l'identité du bénéficiaire approuvé par le payeur ; - toute modification du montant ou du bénéficiaire entraîne l'invalidation du code d'authentification généré.		
	Le PSP applique-t-il des mesures de sécurité garantissant la confidentialité, l'authenticité et l'intégrité de chacun des éléments listés ci-après ? - le montant de l'opération et le bénéficiaire durant l'ensemble des phases de l'authentification ; - les informations qui s'affichent pour le payeur durant l'ensemble des phases de		

	l'authentification, y compris la génération, la transmission et l'utilisation du code d'authentification.		
	Lorsque le PSP applique l'authentification forte du client (conformément à l'article 97 § 2 de la directive (UE) 2015/2366) respecte-t-il les exigences listées ci-après ? - en ce qui concerne les opérations de paiement liées à une carte pour lesquelles le payeur a donné son consentement quant au montant exact des fonds à bloquer en vertu de l'article 75 § 1 de ladite directive, le code d'authentification est spécifique au montant au blocage duquel le payeur a donné son consentement et que le payeur a approuvé lors de l'initiation de l'opération ; - en ce qui concerne les opérations de paiement pour lesquelles le payeur a donné son consentement à l'exécution d'une série d'opérations de paiement électronique à distance en faveur d'un ou de plusieurs bénéficiaires, le code d'authentification est spécifique au montant total de la série d'opérations de paiement et aux bénéficiaires désignés.		
Exigences relatives aux éléments appartenant à la catégorie « connaissance »			
6	Le PSP a-t-il mis en place des mesures pour atténuer le risque que les éléments d'authentification forte du client appartenant à la catégorie « connaissance » ne soient mis au jour par des tiers non autorisés ou divulgués à ceux-ci ?		
	L'utilisation par le payeur des éléments d'authentification forte appartenant à la catégorie « connaissance » fait-elle l'objet de mesures d'atténuation des risques visant à éviter leur divulgation à des tiers non autorisés ?		
Exigences relatives aux éléments appartenant à la catégorie «possession»			

7	Le PSP a-t-il mis en place des mesures pour atténuer le risque que les éléments d'authentification forte du client appartenant à la catégorie « possession » ne soient utilisés par des tiers non autorisés ?		
	L'utilisation par le payeur des éléments d'authentification forte appartenant à la catégorie « possession » fait-elle l'objet de mesures visant à éviter leur copie ?		
Exigences relatives aux dispositifs et logiciels associés à des éléments appartenant à la catégorie «inhérence»			
8	Le PSP a-t-il mis en place des mesures pour atténuer le risque que des éléments d'authentification appartenant à la catégorie « inhérence » qui sont lus par des dispositifs et des logiciels d'accès fournis au payeur ne soient mis au jour par des tiers non autorisés ? Au minimum, le PSP veille-t-il à ce qu'il soit très peu probable, avec ces dispositifs et logiciels d'accès, qu'un tiers non autorisé soit authentifié comme étant le payeur ?		
	L'utilisation par le payeur des éléments d'authentification appartenant à la catégorie « inhérence » fait-il l'objet de mesures garantissant que ces dispositifs et logiciels empêchent toute utilisation non autorisée desdits éléments qui passerait par un accès auxdits dispositifs et logiciels ?		
Indépendance des éléments			
9	Le PSP veille-t-il à ce que l'utilisation des éléments d'authentification forte du client des catégories « possession », « connaissance » et « inhérence », fasse l'objet de mesures garantissant que, sur le plan de la technologie, des algorithmes et des paramètres, la compromission d'un des éléments ne remet pas en question la fiabilité des autres ?		
	Lorsque l'un des éléments d'authentification forte du client ou le code d'authentification proprement dit		

	est utilisé au travers d'un dispositif multifonctionnel, le PSP a-t-il mis en place des mesures de sécurité pour réduire le risque qui découlerait de l'altération de ce dispositif multifonctionnel et ces mesures d'atténuation prévoient-elles bien chacun des éléments listés ci-après ? - l'utilisation d'environnements d'exécution sécurisés distincts grâce au logiciel installé sur le dispositif multifonctionnel ; - des mécanismes permettant de garantir que le logiciel ou le dispositif n'a pas été altéré par le payeur ou par un tiers ; - en cas d'altérations, des mécanismes permettant de réduire les conséquences de celles-ci.		
DÉROGATIONS À L'OBLIGATION D'AUTHENTIFICATION FORTE DU CLIENT			
Analyse des risques liés à l'opération			
18	*Pour la mise en œuvre des articles 18 à 20, l'établissement pourra se référer à la note de l'Observatoire de la sécurité des moyens de paiement publiée dans son rapport annuel 2020 sur l'exemption liée à l'analyse des risques liés à l'opération, qui ~~sera prochainement~~est accessible sur son site internet.* En cas d'usage de l'exemption au titre de l'analyse des risques, le PSP respecte-t-il bien les exigences listées ci-après ? - le taux de fraude pour ce type d'opération est équivalent ou inférieur aux taux de référence en matière de fraude mentionnés en annexe du règlement délégué 2018/389 pour les «paiements électroniques à distance liés à une carte» et les «virements électroniques à distance» respectivement ; - le montant de l'opération ne dépasse pas la valeur-seuil de dérogation correspondante		

	mentionnée en annexe du règlement délégué 2018/389 ; - le PSP n'a décelé aucun des éléments suivants à l'issue d'une analyse en temps réel des risques : i) des dépenses anormales ou un type de comportement anormal du payeur ; ii) des informations inhabituelles concernant l'utilisation du dispositif ou logiciel du payeur à des fins d'accès ; iii) des signes d'infection par un logiciel malveillant lors d'une session de la procédure d'authentification ; iv) un scénario connu de fraude dans le cadre de la prestation de services de paiement ; v) une localisation anormale du payeur ; vi) une localisation du bénéficiaire présentant des risques élevés. - A minima les facteurs liés aux risques listés ci-après sont pris en compte : i) les habitudes de dépenses antérieures de l'utilisateur individuel de services de paiement ; ii) l'historique des opérations de paiement de chacun des utilisateurs de services de paiement du prestataire de services de paiement ; iii) la localisation du payeur et du bénéficiaire au moment de l'opération de paiement dans les cas où le dispositif d'accès ou le logiciel est fourni par le prestataire de services de paiement ; iv) l'identification de comportements de paiement anormaux de l'utilisateur de services de paiement par rapport à l'historique de ses opérations de paiement.		

Calcul du taux de fraude			
19	Pour chaque type d'opération («paiements électroniques à distance liés à une carte» et « virements électroniques à distance»), le PSP veille-t-il à ce que les taux de fraude globaux soient équivalents ou inférieurs aux taux maximaux de référence tel que fixés dans l'annexe des RTS ?		
	Pour chaque type d'opération («paiements électroniques à distance liés à une carte» et « virements électroniques à distance»), les taux de fraude sont bien calculés par le PSP : - par le montant initial des opérations de paiement frauduleuses (approche « fraude brute ») divisé par la valeur totale de l'ensemble des opérations de paiement avec ou sans authentification forte ; - et, sur une base trimestrielle glissante (90 jours).		
Suspension des dérogations sur la base de l'analyse des risques liés à l'opération			
20	En cas de recours à l'exemption au titre de l'analyse des risques (art. 18), le PSP dispose-t-il d'une procédure permettant de notifier immédiatement auprès de la Banque de France tout dépassement du taux de fraude maximal autorisé (tel que fixé par l'annexe des RTS) et pour fournir une description des mesures envisagées pour rétablir la conformité du taux de fraude ?		
	Le PSP a-t-il bien prévu de suspendre immédiatement la mise en œuvre de la dérogation au titre de l'analyse des risques (art. 18) en cas de dépassement du taux maximal autorisé pendant deux trimestres consécutifs ?		
	Après la suspension, le PSP a-t-il bien prévu de faire usage à nouveau de la dérogation au titre de l'analyse des risques (art. 18) que lorsque le taux de fraude calculé est resté égal ou inférieur au taux maximal autorisé pendant un trimestre et, dispose-t-il d'une		

	procédure prévoyant d'en informer dans ce cas la Banque de France en communiquant les éléments attestant que le taux de fraude est redevenu conforme au taux maximal autorisé ?		
Contrôle			
21	En cas d'usage des dérogations à l'authentification forte (art. 10 à 18), le PSP a-t-il mis en place un dispositif pour enregistrer et contrôler, pour chaque type d'opérations de paiement et sur une base au moins trimestrielle, les données listées ci-après ? - la valeur totale des opérations de paiement non autorisées ou frauduleuses, la valeur totale de l'ensemble des opérations de paiement et le taux de fraude qui en découle, comprenant une ventilation par opérations de paiement initiées grâce à l'authentification forte du client et au titre de chacune des dérogations ; - la valeur moyenne des opérations, comprenant une ventilation par opérations de paiement initiées grâce à l'authentification forte du client et au titre de chacune des dérogations ; - le nombre d'opérations de paiement pour lesquelles chacune des dérogations a été appliquée et le pourcentage qu'elles représentent par rapport au nombre total d'opérations de paiement.		
CONFIDENTIALITÉ ET INTÉGRITÉ DES DONNÉES DE SÉCURITÉ PERSONNALISÉES DES UTILISATEURS DE SERVICES DE PAIEMENT			
Exigences générales			
22	Le PSP veille-t-il à la confidentialité et à l'intégrité des données de sécurité personnalisées de l'utilisateur de services de paiement, notamment des codes d'authentification, durant l'ensemble des phases de l'authentification en respectant les exigences listées ci-après ?		

	- les données de sécurité personnalisées sont masquées lorsqu'elles sont affichées et ne sont pas lisibles dans leur intégralité lorsqu'elles sont entrées par l'utilisateur de services de paiement durant l'authentification ; - les données de sécurité personnalisées en format de données ainsi que le matériel cryptographique lié au cryptage des données de sécurité personnalisées ne sont pas conservés en texte clair ; - le matériel cryptographique secret est protégé de toute divulgation non autorisée.		
	Le PSP consigne-t-il intégralement par écrit le processus de gestion du matériel cryptographique utilisé pour crypter ou rendre illisibles d'une autre manière les données de sécurité personnalisées ?		
	Le PSP veille-t-il à ce que le traitement et le routage des données de sécurité personnalisées et des codes d'authentification aient lieu dans des environnements sécurisés suivant des normes sectorielles rigoureuses et largement reconnues ?		
Création et transmission des données			
23	Le PSP veille-t-il à ce que la création des données de sécurité personnalisées ait lieu dans un environnement sécurisé ?		
	Les risques d'utilisation non autorisée des données de sécurité personnalisées ainsi que des dispositifs et du logiciel d'authentification à la suite de leur perte, vol ou copie avant leur livraison au payeur sont-ils bien maitrisés ?		
Association avec l'utilisateur de services de paiement			
24	Le PSP veille-t-il à ce que seul l'utilisateur de services de paiement soit associé, de manière sécurisée, aux données de sécurité personnalisées, aux dispositifs		

	d'authentification et au logiciel en respectant les exigences listées ci-après ? - l'association de l'identité de l'utilisateur de services de paiement avec les données de sécurité personnalisées et les dispositifs et le logiciel d'authentification a lieu dans des environnements sécurisés relevant de la responsabilité du prestataire de services de paiement, comprenant au moins les locaux du prestataire de services de paiement et l'environnement internet fourni par le prestataire de services de paiement, ou d'autres sites internet sécurisés similaires utilisés par ce dernier et par ses services de retrait à des distributeurs automatiques de billets, et tenant compte des risques liés aux dispositifs et composants sous-jacents utilisés au cours du processus d'association qui ne sont pas sous la responsabilité du prestataire de services de paiement ; - l'association, grâce à un moyen de communication à distance, de l'identité de l'utilisateur de services de paiement avec les données de sécurité personnalisées et les dispositifs ou le logiciel d'authentification est effectuée à l'aide d'une authentification forte du client.		
Livraison des données ainsi que des dispositifs et du logiciel d'authentification			
25	Le PSP veille-t-il à ce que la livraison des données de sécurité personnalisées ainsi que des dispositifs et du logiciel d'authentification à l'utilisateur de services de paiement soit effectuée d'une manière sécurisée qui permette de prévenir les risques liés à leur utilisation non autorisée à la suite de leur perte, vol ou copie en appliquant au moins chacune des mesures listées ci-après ? - des mécanismes de livraison efficaces et sécurisés garantissent que les données de sécurité		

	personnalisées ainsi que les dispositifs et le logiciel d'authentification sont livrés à l'utilisateur de services de paiement légitime ; - des mécanismes permettent au prestataire de services de paiement de vérifier l'authenticité du logiciel d'authentification livré à l'utilisateur de services de paiement grâce à l'internet ; - des dispositions garantissent que, lorsque la livraison des données de sécurité personnalisées a lieu en dehors des locaux du prestataire de services de paiement ou grâce à un moyen de communication à distance : i) aucun tiers non autorisé ne peut obtenir plus d'un élément des données de sécurité personnalisées ou des dispositifs ou du logiciel d'authentification lorsque la livraison est effectuée grâce au même moyen de communication ; ii) les données de sécurité personnalisées ou les dispositifs ou le logiciel d'authentification doivent être activés avant de pouvoir être utilisés ; - des dispositions garantissent que, si les données de sécurité personnalisées ou les dispositifs ou le logiciel d'authentification doivent être activés avant leur première utilisation, cette activation est effectuée dans un environnement sécurisé conformément aux procédures d'association visées à l'article 24.		
Renouvellement des données de sécurité personnalisées			
26	Le PSP veille-t-il à ce que le renouvellement ou la réactivation des données de sécurité personnalisées respecte les procédures applicables à la création, à l'association et à la livraison de ces données et des		

	dispositifs d'authentification conformément aux articles 23, 24 et 25 des RTS ?		
Destruction, désactivation et révocation			
27	Le PSP a-t-il mis en place des procédures efficaces en vue d'appliquer chacune des mesures de sécurité listées ci-après ? - la destruction, la désactivation ou la révocation sécurisée des données de sécurité personnalisées et des dispositifs et du logiciel d'authentification ; - lorsque le prestataire de services de paiement distribue des dispositifs et logiciels d'authentification réutilisables, la réutilisation sécurisée d'un dispositif ou logiciel est établie, décrite par écrit et mise en œuvre avant sa mise à disposition d'un autre utilisateur de services de paiement ; - la désactivation ou la révocation des informations liées aux données de sécurité personnalisées conservées dans les systèmes et bases de données du prestataire de services de paiement et, le cas échéant, dans des registres publics.		
Normes ouvertes communes et sécurisées de communication			
Applicables par le PSP gestionnaire de comptes en cas de non mise en œuvre d'une interface d'accès dédiée : accès via le site de banque en ligne avec authentification du tiers			
29	Le PSP veille-t-il à ce que l'ensemble des opérations (authentification, consultation et initiation de paiement) avec l'utilisateur du service de paiement, y compris des commerçants, d'autres PSP et d'autres entités soient bien tracées avec des identifiants uniques, non prédictibles et horodatées ?		
30-1	Le PSP a-t-il mis à disposition des PSP tiers une interface d'accès qui respecte les exigences listées ci-après ? - les PSP tiers sont en mesure de s'identifier auprès du PSP ;		

	- les PSP tiers sont en mesure de communiquer de manière sécurisée avec le PSP pour exécuter leurs services de paiement.		
30-2	Le PSP rend-t-il l'ensemble des procédures d'authentification proposées aux utilisateurs de services de paiement utilisables par les PSP tiers aux fins de l'authentification des utilisateurs de services de paiement ?		
30-2-a-b	L'interface d'accès du PSP respecte-t-elle les exigences listées ci-après ? - le PSP est en capacité de commencer l'authentification forte sur la requête d'un PSP tiers qui a préalablement recueilli le consentement de l'utilisateur ; - les sessions de communication entre le PSP et les PSP tiers sont établies et maintenues tout au long de l'authentification.		
34-1	L'accès des PSP tiers au site de banque en ligne du PSP se fait au moyen de certificats qualifiés de cachet électronique ou de certificats qualifiés d'authentification de site internet ?		
35-1	L'intégrité et la confidentialité des données de sécurité personnalisées et les codes d'authentification qui transitent par les flux de communication ou qui sont stockés dans les systèmes d'information du PSP sont-elles assurées ?		
35-5	Le PSP veille-t-il à ce que les données de sécurité personnalisées et les codes d'authentification qu'ils communiquent ne soient aucun moment lisibles directement ou indirectement par un membre du personnel ?		
36-1	Le PSP respecte-t-il les exigences listées ci-après ? - il fournit aux PSP tiers les mêmes informations provenant des comptes de paiement désignés et des opérations de paiement associées que celles		

	qui sont mises à la disposition de l'utilisateur de services de paiement en cas de demande directe d'accès aux informations sur le compte, pour autant que ces informations ne comportent pas de données de paiement sensibles - immédiatement après avoir reçu l'ordre de paiement, ils fournissent aux PSP tiers les mêmes informations sur l'initiation et l'exécution de l'opération de paiement que celles qui sont fournies ou mises à la disposition de l'utilisateur de services de paiement lorsque ce dernier initie directement l'opération ; - sur demande, il fournit immédiatement aux PSP tiers, sous la forme d'un simple «oui» ou «non», que le montant nécessaire à l'exécution d'une opération de paiement est disponible ou non sur le compte de paiement du payeur.		
36-2	En cas d'erreur ou d'événement imprévu au cours de la procédure d'identification ou d'authentification ou lors de l'échange d'éléments d'information, les procédures du PSP prévoient-elles l'envoi d'un message de notification aux PSP tiers, en indiquant les raisons de l'erreur ou de l'événement imprévu ?		
Applicables par le PSP gestionnaire de comptes en cas de mise en œuvre d'une interface d'accès dédiée et dotée d'un mécanisme de secours (accès banque en ligne avec authentification du tiers)			
29	Le PSP veille-t-il à ce que l'ensemble des opérations (authentification, consultation et initiation de paiement) avec l'utilisateur du service de paiement, y compris des commerçants, d'autres PSP et d'autres entités soient bien tracées avec des identifiants uniques, non prédictibles et horodatées ?		
30-1	Le PSP a-t-il mis à disposition des PSP tiers une interface d'accès qui respecte les exigences listées ci-après :		

	- les PSP tiers sont en mesure de s'identifier auprès du PSP ; - les PSP tiers sont en mesure de communiquer de manière sécurisée avec le PSP pour exécuter leurs services de paiement.		
30-2	Le PSP rend-t-il l'ensemble des procédures d'authentification proposées aux utilisateurs de services de paiement utilisables par les PSP tiers aux fins de l'authentification des utilisateurs de services de paiement ?		
30-2-a-b	L'interface d'accès du PSP respecte-t-elle les exigences listées ci-après ? - le PSP est en capacité de commencer l'authentification forte sur la requête d'un PSP tiers qui a préalablement recueilli le consentement de l'utilisateur ; - les sessions de communication entre le PSP et les PSP tiers sont établies et maintenues tout au long de l'authentification.		
30-3	Le PSP veille-t-il à ce que son interface d'accès suive les normes de communication publiées par des organisations européennes ou internationales de normalisation ? Les spécifications techniques de l'interface d'accès font-elles l'objet d'une documentation mentionnant une série de routines, de protocoles et d'outils dont les PSP tiers ont besoin pour permettre l'interopérabilité de leurs logiciels et applications avec les systèmes du PSP ?		
30-4	En cas de modifications des spécifications techniques de l'interface d'accès, sauf en cas d'urgence, le PSP a-t-il bien prévu une mise à disposition après des PSP tiers au moins trois mois avant leur mise en œuvre ? Les procédures du PSP prévoient-elles de décrire par écrit les situations d'urgence dans lesquelles les		

	modifications ont été mises en œuvre et de mettre cette documentation à la disposition de l'ACPR et de la BDF ?		
32-1	Le PSP veille-t-il à ce que son interface d'accès dédiée offre à tout moment le même niveau de disponibilité et de performances, assistance comprise, que la ou les interfaces mises à la disposition de l'utilisateur de services de paiement pour accéder directement à son compte de paiement en ligne ?		
32-2	Le PSP a-t-il défini des indicateurs de performance clés et des valeurs cibles de niveau de service de son interface d'accès qui soient transparents et au moins aussi exigeants que ceux fixés pour l'interface utilisée par leurs utilisateurs de services de paiement, tant sur le plan de la disponibilité que des données fournies ?		
32-4	La disponibilité et les performances de l'interface d'accès sont-elles contrôlées par le PSP et les statistiques correspondantes sont-elles publiées sur son site internet selon une périodicité trimestrielle ?		
33-1	Le PSP a-t-il bien prévu la mise en œuvre du mécanisme de secours après cinq demandes consécutives d'accès à l'interface dédiée du PSP tiers sans réponse dans les 30 secondes ?		
33-2	Le PSP dispose-t-il de plans de communication visant à informer les PSP tiers qui utilisent l'interface dédiée des mesures destinées à restaurer le système ainsi qu'une description des autres options immédiatement disponibles dont ils peuvent faire usage pendant ce temps ?		
33-3	Les procédures du PSP prévoient-elles la notification sans délai auprès de l'ACPR des problèmes liés à l'interface dédiée ?		
33-5	Pour l'accès à l'interface de secours, le PSP veille-t-il à identifier les PSP tiers et les authentifier selon les		

	procédures d'authentification prévues pour ses propres clients ?		
34-1	L'accès des PSP tiers à l'interface d'accès dédiée du PSP se fait au moyen de certificats qualifiés de cachet électronique ou de certificats qualifiés d'authentification de site internet ?		
35-1	L'intégrité et la confidentialité des données de sécurité personnalisées et les codes d'authentification qui transitent par les flux de communication ou qui sont stockés dans les systèmes d'information du PSP sont-elles assurées ?		
35-5	Le PSP veille-t-il à ce que les données de sécurité personnalisées et les codes d'authentification qu'ils communiquent ne soient aucun moment lisibles directement ou indirectement par un membre du personnel ?		
36-1	Le PSP respecte-t-il les exigences listées ci-après ? - il fournit aux PSP tiers les mêmes informations provenant des comptes de paiement désignés et des opérations de paiement associées que celles qui sont mises à la disposition de l'utilisateur de services de paiement en cas de demande directe d'accès aux informations sur le compte, pour autant que ces informations ne comportent pas de données de paiement sensibles - immédiatement après avoir reçu l'ordre de paiement, ils fournissent aux PSP tiers les mêmes informations sur l'initiation et l'exécution de l'opération de paiement que celles qui sont fournies ou mises à la disposition de l'utilisateur de services de paiement lorsque ce dernier initie directement l'opération ; - sur demande, il fournit immédiatement aux PSP tiers, sous la forme d'un simple «oui» ou «non», que le montant nécessaire à l'exécution d'une		

	opération de paiement est disponible ou non sur le compte de paiement du payeur.		
36-2	En cas d'erreur ou d'événement imprévu au cours de la procédure d'identification ou d'authentification ou lors de l'échange d'éléments d'information, les procédures du PSP prévoient-elles l'envoi d'un message de notification aux PSP tiers, en indiquant les raisons de l'erreur ou de l'événement imprévu ?		
Applicables par le PSP gestionnaire de comptes en cas de mise en œuvre d'une interface d'accès dédiée sans mécanisme de secours			
29	Le PSP veille-t-il à ce que l'ensemble des opérations (authentification, consultation et initiation de paiement) avec l'utilisateur du service de paiement, y compris des commerçants, d'autres PSP et d'autres entités soient bien tracées avec des identifiants uniques, non prédictibles et horodatées ?		
30-1	Le PSP a-t-il mis à disposition des PSP tiers une interface d'accès qui respecte les exigences listées ci-après : - les PSP tiers sont en mesure de s'identifier auprès du PSP ; - les PSP tiers sont en mesure de communiquer de manière sécurisée avec le PSP pour exécuter leurs services de paiement.		
30-2	Le PSP rend-t-il l'ensemble des procédures d'authentification proposées aux utilisateurs de services de paiement utilisables par les PSP tiers aux fins de l'authentification des utilisateurs de services de paiement ?		
30-2-a-b	L'interface d'accès du PSP respecte-t-elle les exigences listées ci-après ? - le PSP est en capacité de commencer l'authentification forte sur la requête d'un PSP tiers qui a préalablement recueilli le consentement de l'utilisateur ;		

	- les sessions de communication entre le PSP et les PSP tiers sont établies et maintenues tout au long de l'authentification.		
30-3	Le PSP veille-t-il à ce que son interface d'accès suive les normes de communication publiées par des organisations européennes ou internationales de normalisation ? Les spécifications techniques de l'interface d'accès font-elles l'objet d'une documentation mentionnant une série de routines, de protocoles et d'outils dont les PSP tiers ont besoin pour permettre l'interopérabilité de leurs logiciels et applications avec les systèmes du PSP ?		
30-4	En cas de modifications des spécifications techniques de l'interface d'accès, sauf en cas d'urgence, le PSP a-t-il bien prévu une mise à disposition après des PSP tiers au moins trois mois avant leur mise en œuvre ? Les procédures du PSP prévoient-elles de décrire par écrit les situations d'urgence dans lesquelles les modifications ont été mises en œuvre et de mettre cette documentation à la disposition de l'ACPR et de la BDF ?		
32-1	Le PSP veille-t-il à ce que son interface dédiée d'accès offre à tout moment le même niveau de disponibilité et de performances, assistance comprise, que les interfaces mises à la disposition de l'utilisateur de services de paiement pour accéder directement à son compte de paiement en ligne ?		
32-2	Le PSP a-t-il défini des indicateurs de performance clés et des valeurs cibles de niveau de service de son interface d'accès qui soient transparents et au moins aussi exigeants que ceux fixés pour l'interface utilisée par leurs utilisateurs de services de paiement, tant sur le plan de la disponibilité que des données fournies ?		

32-4	La disponibilité et les performances de l'interface d'accès sont-elles contrôlées par le PSP et les statistiques correspondantes sont-elles publiées sur son site internet selon une périodicité trimestrielle ?		
33-6	Le PSP a-t-il formulé une demande d'exemption de mise en place de mécanisme d'urgence auprès de l'ACPR ?		
34-1	L'accès des PSP tiers à l'interface d'accès dédiée du PSP se fait au moyen de certificats qualifiés de cachet électronique ou de certificats qualifiés d'authentification de site internet ?		
35-1	L'intégrité et la confidentialité des données de sécurité personnalisées et les codes d'authentification qui transitent par les flux de communication ou qui sont stockés dans les systèmes d'information du PSP sont-elles assurées ?		
35-5	Le PSP veille-t-il à ce que les données de sécurité personnalisées et les codes d'authentification qu'ils communiquent ne soient aucun moment lisibles directement ou indirectement par un membre du personnel ?		
36-1	Le PSP respecte-t-il les exigences listées ci-après ? - il fournit aux PSP tiers les mêmes informations provenant des comptes de paiement désignés et des opérations de paiement associées que celles qui sont mises à la disposition de l'utilisateur de services de paiement en cas de demande directe d'accès aux informations sur le compte, pour autant que ces informations ne comportent pas de données de paiement sensibles - immédiatement après avoir reçu l'ordre de paiement, ils fournissent aux PSP tiers les mêmes informations sur l'initiation et l'exécution de l'opération de paiement que celles qui sont fournies ou mises à la disposition de l'utilisateur de		

	services de paiement lorsque ce dernier initie directement l'opération ; - sur demande, il fournit immédiatement aux PSP tiers, sous la forme d'un simple «oui» ou «non», que le montant nécessaire à l'exécution d'une opération de paiement est disponible ou non sur le compte de paiement du payeur.		
36-2	En cas d'erreur ou d'événement imprévu au cours de la procédure d'identification ou d'authentification ou lors de l'échange d'éléments d'information, les procédures du PSP prévoient-elles l'envoi d'un message de notification aux PSP tiers, en indiquant les raisons de l'erreur ou de l'événement imprévu ?		

V- 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

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 [20]

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 modifié ;
- 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 modifié) (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 ou des responsable(s) 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 et services, des modifications significatives apportées à un produit, service ou process préexistant, des opérations de croissance interne et externe et des transactions exceptionnelles (cf. article 221 de l'arrêté du 3 novembre 2014 modifié) ;
- description synthétique de l'évaluation des risques faite par la fonction de gestion des risques selon des scénarios appropriés au regard de la significativité des risques induits par ces nouveaux produits et opérations ;

20. 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 de la fonction d'audit interne et de son champ d'intervention y compris pour l'activité à l'étranger *(activités, processus et entités)* ;
- moyens humains affectés à la fonction d'audit interne (cf. article 25 de l'arrêté du 3 novembre 2014 modifié) (effectif en équivalent temps plein par rapport à l'effectif total de l'établissement) ;
- si recours à un prestataire externe : fréquence d'intervention et dimension de l'équipe ;
- description, formalisation et date(s) de mise à jour des procédures sur lesquelles s'appuie la fonction d'audit interne 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 ;
- modalités de définition de la fréquence et des priorités des cycles d'audit notamment en fonction des risques identifiés au sein de l'établissement.

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 modifié) ;
- modalités de suivi et de traitement des écarts entre le système d'information comptable et le système d'information de gestion.

Annexe 2

Mesures mises en œuvre en faveur des clients en situation de fragilité financière (arrêté du 16 septembre 2020 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[21]

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)

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

Annexe 3

Tableau récapitulatif des facteurs K

Risk to	Facteur K	Définition	Définition IFR (art 4)	Référence règlementaire
Client	**AUM**	Actifs sous gestion	Valeur des actifs qu'une entreprise d'investissement gère pour ses clients, que ce soit dans le cadre d'une **gestion discrétionnaire de portefeuille** ou dans le cadre de dispositifs non discrétionnaires relevant du **conseil en investissement de nature continue**	Art 4, § 1, point 27) d'IFR (définition) ; Art 17 d'IFR (modalités de calcul)
Client	**CMH**	Fonds de clients détenus (comptes ségrégués ou non)	Montant des **fonds de clients** qu'une entreprise d'investissement détient, compte tenu des dispositifs juridiques en ce qui concerne la ségrégation des actifs et quel que soit le régime comptable national applicable aux fonds de clients détenus par l'entreprise d'investissement	Art 4, § 1, points 28) et 49) d'IFR (définition), Art 18 d'IFR (modalités de calcul) ; Art 1 du RTS IFR sur la définition des comptes ségrégués
Client	**ASA**	Actifs administrés et conservés	Valeur des actifs qu'une entreprise d'investissement **conserve et administre pour des clients**, indépendamment de la question de savoir si les actifs figurent au bilan de l'entreprise d'investissement elle-même ou sont dans des comptes de tiers	Art 4, § 1, point 29) d'IFR(définition) ; Art 19 d'IFR (modalités de calcul)
Client	**COH**	Ordres des clients traités (opérations cash et produits dérivés)	Valeur des ordres qu'une entreprise d'investissement traite pour des clients en **réceptionnant et transmettant les ordres** de clients et en e**xécutant des ordres** pour le compte de clients	Art 4, § 1, point 30) d'IFR (définition) ; Art 20 d'IFR (modalités de calcul) ; Service d'EO défini à l'art 4 § 1, point 5) de MiFID II

Firm	**TCD**	Risque de défaut d'une contrepartie	Expositions, dans le **portefeuille de négociation** d'une entreprise d'investissement, à des **instruments et opérations** visés à **l'article 25 d'IFR** qui génèrent un risque de défaut de la contrepartie	Art 4 §1 point 35) d'IFR (définition) ; Art 25 (opérations et contrats concernés) ; Art 26 à 32 (modalités de calcul et modèles applicables)
Firm	**DTF**	Risque opérationnel[22]	Valeur quotidienne des opérations qu'une entreprise d'investissement effectue en **négociant pour compte propre** ou en **exécutant des ordres pour le compte de clients en son propre nom**, à l'exclusion de la valeur des ordres qu'une entreprise d'investissement traite pour des clients en réceptionnant et transmettant leurs ordres et en exécutant des ordres pour leur compte, qui sont déjà pris en compte dans le cadre des ordres de clients traités	Art 4 §1 point 33) d'IFR (définition) ; Art 33 d'IFR (modalités de calcul)
Firm	**CON**	Risque de concentration (dépassement des grands risques)	Expositions, dans le **portefeuille de négociation** d'une entreprise d'investissement, à un client ou à un groupe de clients liés dont la valeur dépasse les limites prévues à l'article 37, paragraphe 1 et qui concerne les instruments listés à l'art 25;	Art 4 §1 point 31) d'IFR (définition) ; Art 37 d'IFR (seuils) ; Art 36 et 37 d'IFR (modalités de calcul); Art 38 d'IFR (obligation de notification en cas de dépassement des seuils) ; Art 39 d'IFR (nouvelles exigences de FP en cas de dépassement des seuils) ; **instruments listés à l'Art 25** (opérations et contrats concernés, voir K-TCD) et tous les **instruments du portefeuille de négociation** ; Art 22 (calcul de la position nette pour chaque instrument)
Market	**NPR**	Risque de position nette (Marges nettes)	Valeur des opérations enregistrées dans le **portefeuille de négociation** d'une entreprise d'investissement	Art 4 §1 point 34) d'IFR (définition) ; Art 22, point a) d'IFR (modalités de calcul) ; 3 approches : standard TSA (3ème partie, titre IV, chap. 2, 3 et 4 de CRR), standard alternative ASA (3ème partie, titre IV, chap 1 bis de CRR) et méthodes alternatives fondées sur des modèles internes AMA (3ème partie, titre IV, chap 1 ter de CRR)

[22] Sur les flux d'échanges quotidiens (opérations cash et produits dérivés)

Market	**CMG**	Marge totale requise par un membre compensateur ou une contrepartie centrale éligible	Montant de la **marge totale** requise par un membre compensateur ou une contrepartie centrale éligible, lorsque l'exécution et le règlement des opérations d'une entreprise d'investissement qui **négocie pour compte propre** ont lieu sous la responsabilité d'un **membre compensateur** ou d'**une contrepartie centrale éligible**	Art 4 §1 point 31) d'IFR (définition) ; Art 23 d'IFR (modalités de calcul)