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

Juillet ~~2022~~2023

Rapport sur le contrôle interne
Établissements de paiement, prestataires de services d'information sur les comptes et établissements de monnaie électronique

(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 2

1. Présentation générale des activités exercées et des risques encourus par l'établissement 3
2. Modifications significatives apportées à l'organisation du dispositif de contrôle interne 3
3. Gouvernance 5
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) 6
5. Recensement des opérations avec les dirigeants effectifs, les membres de l'organe de surveillance et les actionnaires principaux (cf. articles 113 et 259 g) de l'arrêté du 3 novembre 2014 modifié 6
6. Risque de non conformité (hors risque de blanchiment des capitaux et de financement du terrorisme) 7
7. Risque de crédit et de contrepartie (cf. articles 106 à 121 de l'arrêté du 3 novembre 2014 modifié) 8
8. Risque opérationnel 12
9. Risque comptable 14
10. Gestion de la trésorerie 15
11. Dispositif de contrôle interne des dispositions relatives à la protection des fonds de la clientèle 15
12. Politique en matière d'externalisation 16
13. Informations spécifiques aux établissements agréés pour fournir les services d'initiation de paiement et/ou d'informations sur les comptes 17
14. 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 18

Annexe 1 70

Annexe 2 72

Préambule

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

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

Le présent document s'appuie sur une version « fusionnée » des rapports établis en application des articles 258 à 266 de l'arrêté du 3 novembre 2014 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 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.

Le rapport de contrôle interne doit être remis au SGACPR au plus tard **le 30 avril** suivant la fin de chaque exercice.

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

1.1. Description des activités :

– description synthétique des activités exercées, y compris des activités de nature hybride conformément à l'article L. 522-3 du Code monétaire et financier ;

– 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…),
  - pour les activités de paiement, préciser les services de paiement fournis conformément à l'article L. 314-1 du Code monétaire et financier,
  - présentation des procédures définies pour ces nouvelles activités,
  - description du contrôle interne des nouvelles activités ;

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

– identité de l'organisme professionnel affilié à l'Association française des établissements de crédit et des entreprises d'investissement auquel l'établissement a adhéré.

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

– description, dispositif de formalisation et de mise à jour de la cartographie des risques, mise en exergue des principales évolutions au cours de l'exercice écoulé ;

– 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 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) ;

– 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 processus d'agrégation des données sur les risques (cf. article 104 de l'arrêté du 3 novembre 2014 modifié).

1.3. Incident majeur

– dispositif mis en place pour identifier les incidents majeurs en application de l'article 96 de la directive (UE) 2015/2366 du 25 novembre 2015 concernant les services de paiement (directive dite « DSP 2 ») et des Orientations ABE n°2021/03 ;

– process retenu pour procéder aux déclarations initiales et complémentaires auprès des autorités de tutelle.

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 ou en communiquant la charte de contrôle interne en vigueur.

2.1. Au dispositif de contrôle permanent « 1er et 2ème niveau 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. article 259 f) 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 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 de la fonction d'audit interne ;
- principales actions projetées dans le domaine du contrôle périodique (plan d'audit… cf. article 259 f) de l'arrêté du 3 novembre 2014 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 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).

3.2. Implication des organes dirigeants dans le contrôle interne

3.2.1. Modalités d'information de l'organe de surveillance :

– modalités d'approbation des limites par l'organe de surveillance (cf. article 224 de l'arrêté du 3 novembre 2014 modifié) ;

– modalités d'information de l'organe de surveillance en cas de survenance d'incidents significatifs 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 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 par les responsables 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 et en particulier éventuelles défaillances relevées, et mesures décidées pour y remédier (cf. article 243 de l'arrêté du 3 novembre 2014 modifié).

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 :

- dans le cadre de l'examen par l'organe de surveillance des incidents significatifs et majeurs révélés par les procédures de contrôle interne, principales insuffisances constatées, coûts engendrés, 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 (cf. article 224 de l'arrêté du 3 novembre 2014 modifié).

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 ;
- 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) de l'arrêté du 3 novembre 2014 modifié)

Joindre une annexe comprenant~~ :~~

les **caractéristiques des engagements** ~~**ayant fait l'objet d'une déduction**~~**envers** **des** ~~**fonds propres prudentiels**~~ **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~~ ;~~.

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

6. 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 (BC-FT) sont à remettre dans le rapport sur l'organisation des dispositifs de contrôle interne de LCB-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.*

6.1. 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)

6.2. Évaluation et maîtrise du risque de réputation

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

6.4. Procédures permettant le signalement des manquements, infractions et dysfonctionnements

Indiquer :

- les procédures mises en place pour permettre à tout dirigeant ou préposé de faire part, au responsable de la 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).

6.5 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).

6.6. 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).

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

6.8. 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).

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

***Nota bene** : Seuls les établissements de paiement et les établissements de monnaie électronique qui effectuent des opérations de crédit sont concernés par l'intégralité de cette partie.*

Les autres établissements sont tenus de compléter la dernière sous-partie relative au risque de contrepartie.

7.1. 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.

7.2. Dispositif de mesure et de surveillance des risques :

– détail sur les 10 principales expositions (après grappage des contreparties) ;

– *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 ;

- ~~adaptations prises par l'établissement pour se mettre en conformité avec les orientations de l'ABE sur l'application de la définition du défaut qui sont entrées en vigueur depuis le 1er janvier 2021 ;~~

- 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) ;

- 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, 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) et de l'organe de surveillance sur le niveau des risques de crédit (cf. article 230 de l'arrêté du 3 novembre 2014 modifié) ;

- rôles des dirigeants effectifs et de l'organe de surveillance dans la définition, le contrôle et la révision de la stratégie globale en matière de risques de crédit 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) 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 d'approbation par l'organe de surveillance des limites proposées par les dirigeants effectifs (cf. article 253 de l'arrêté du 3 novembre 2014 modifié) ;

- 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.

7.3. Risque de concentration

7.3.1. Risque de concentration par contrepartie :

- outil de suivi du risque de concentration par contrepartie : 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, précisions sur les procédures d'identification des bénéficiaires liés (définition d'un seuil quantitatif au-delà duquel cette recherche est systématique ...), 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.

7.3.2. Risque de concentration sectorielle :

- outil de suivi du risque de concentration sectorielle : 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.

7.3.3. 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.

7.4. Résultats des contrôles permanents de 2ème niveau menés sur les activités de crédit :

- principales insuffisances relevées ;
- mesures correctives engagées pour remédier aux insuffisances relevées, date de réalisation prévisionnelle de ces mesures et état d'avancement de leur mise en œuvre à la date de rédaction du présent rapport *;*
- modalités de suivi des recommandations résultant des contrôles permanents *(outils, personnes en charge)* ;
- modalités de vérification de l'exécution dans des délais raisonnables des mesures correctrices décidées au sein des entreprises, par les personnes compétentes (cf. articles 11 f) et 26 a) de l'arrêté du 3 novembre 2014 modifié).

7.5. 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.).

7.6. 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.

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

7.8. Gestion du risque de contrepartie et de concentration pour les établissements non autorisés à exercer une activité de crédit

- présentation de la part des 20 premières contreparties contribuant au chiffre d'affaires et au PNB ;
- mesures prises pour limiter le risque de concentration d'activité ;
- contrôles mis en place pour suivre le risque de concentration d'activité ;
- présentation des principales contreparties (banques, prestataires tels que agents…) à qui sont confiés les fonds de l'établissement ; modalités de suivi des notations de ces contreparties ;
- contrôles mis en place pour suivre le risque de contrepartie.

8. Risque opérationnel

8.1. 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 ;
- définition d'un incident significatif retenu par l'organe de surveillance dans le cadre de l'article 98 de l'arrêté du 3 novembre 2014 modifié (*joindre en annexe le procès-verbal de séance au cours de laquelle le seuil a été validé*).

8.2. 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 synthétique des techniques d'assurance éventuellement utilisées.

8.3. 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 dans le dispositif de contrôle permanent ;
- description des principaux risques opérationnels avérés au cours de l'exercice et des coûts engendrés (incidents de règlement, erreurs, fraudes, cybersécurité, …) et des enseignements qui en ont été tirés.

8.4. 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).

8.5. Risque informatique :

8.5.1. Gouvernance

– 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 dans la définition, le contrôle et la révision de la stratégie informatique globale).

8.5.2. 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 des risques informatiques (définition des rôles et responsabilités des acteurs[1], 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 aux risques informatiques[2]…) ;

– description du dispositif de contrôle permanent et périodique des systèmes d'information et synthèse des constatations des contrôles effectués (voir 8.6) ;

- présentation de la cartographie des risques informatiques incluant notamment les risques 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)[3].

[1] Notamment ceux de la fonction informatique

[2] Joindre le dernier tableau de bord destiné à les informer

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

8.5.3. 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 tels que définis par l'orientation de l'ABE émise en application de l'article 96 de la directive DSP2.
- 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).

8.5.4. 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).

8.5.5 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).

8.6. 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).

8.7. Conclusion synthétique sur l'exposition au risque opérationnel

9. Risque comptable

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

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

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

9.2. 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…).

10. Gestion de la trésorerie

– descriptif des mesures de suivi de la trésorerie mis en place ;

– détailler la politique de gestion de trésorerie validée par la Direction générale / le Comité de surveillance ;

– détailler la nature des placements de trésorerie, en précisant leur degré de disponibilité et leur évolution au cours de l'exercice.

11. Dispositif de contrôle interne des dispositions relatives à la protection des fonds de la clientèle

– schémas complets et description de l'ensemble des flux financiers par type d'opération de paiements/d'émission de monnaie électronique permettant de retracer, de manière chronologique (dont délais), les flux de collecte de fonds en contrepartie d'un ordre de paiement/de l'émission de monnaie électronique ainsi que l'alimentation des différents comptes concernés, de l'origination des ordres à leur réalisation effective ;

– présentation de la méthode mise en œuvre pour assurer la protection des fonds reçus de la clientèle et description de l'outil de calcul du montant des fonds reçus des clients et à cantonner ;

– pour les établissements assurant la protection des fonds reçus en les plaçant dans un ou plusieurs comptes ouverts spécialement à cet effet auprès d'un établissement de crédit :communication de toute modification apportée à la convention de compte de cantonnement (joindre en annexe la nouvelle convention le cas échéant), 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 (joindre en annexe le nouveau contrat de garantie et de cautionnement le cas échéant) ;

– présentation des procédures mises en place pour veiller au respect des dispositions relatives à la protection des fonds de la clientèle des établissements, des vérifications associées et présentation des éventuels incidents ou insuffisances mis en évidence par ces vérifications.

12. Politique en matière d'externalisation

- présentation de la stratégie de l'établissement ou du groupe en matière d'externalisation ;
- 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 (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 activités essentielles ou importantes (au sens de l'article 10 de l'arrêté du 3 novembre 2014 modifié) pour lesquelles l'établissement a prévu de les externaliser en ayant recours à un prestataire de services et proportion par rapport à l'activité globale de l'établissement ;
- description des conditions dans lesquelles a lieu le recours à l'externalisation : 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, de se rendre sur place au sein du prestataire extérieur, etc. ;
- description du dispositif de contrôle permanent et périodique des activités externalisées ;
- description du dispositif d'identification, de gestion et de suivi des risques associés à l'externalisation ;
- description des dispositifs mis en œuvre par l'établissement pour conserver l'expertise nécessaire afin de contrôler effectivement les activités externalisées et gérer les risques associés à l'externalisation ;
- 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 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 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.

13. Informations spécifiques aux établissements agréés pour fournir les services d'initiation de paiement et/ou d'informations sur les comptes

- fournir une attestation d'assurance responsabilité civile professionnelle ou une garantie comparable valable pour l'exercice en cours. L'attestation fournie doit obligatoirement préciser que le contrat d'assurance responsabilité civile professionnelle ou la garantie comparable en cours n'est complété par aucun acte séparé instituant une franchise de quelque nature que ce soit ;
- dans l'hypothèse où le contrat initialement souscrit a été modifié, fournir le nouveau contrat ;
- pour les établissements de paiement agréés pour fournir le service d'initiation de paiement :
    - compléter le tableau ci-dessous :

	Données en EUR pour l'année civile précédente
Valeur des demandes de remboursement et d'indemnisation effectuées par les utilisateurs et par les prestataires de services de paiement gestionnaires de comptes	
Nombre des transactions de paiement initiées	
Valeur globale des transactions de paiement initiées	

    - fournir le détail, le cas échéant, des activités non réglementées exercées au sein de l'établissement, et l'attestation d'assurance responsabilité civile professionnelle ou une garantie comparable couvrant ces activités si une telle couverture a été souscrite ;
- pour les établissements autorisés à fournir le service d'information sur les comptes :
    - compléter le tableau ci-dessous :

	Données en EUR pour l'année civile précédente
Valeur des demandes de remboursement et d'indemnisation résultant de l'engagement de leur responsabilité vis-à-vis du prestataire de services de paiement gestionnaire du compte ou de l'utilisateur de services de paiement à la suite d'un accès non autorisé ou frauduleux aux données des comptes de paiement ou d'une utilisation non autorisée ou frauduleuse de ces données	
Nombre de comptes de paiement auxquels l'établissement a accédé	
Nombre de clients	

    - fournir le détail, le cas échéant, des activités non réglementées exercées au sein de l'établissement, et l'attestation d'assurance responsabilité civile professionnelle ou une garantie comparable couvrant ces activités si une telle couverture a été souscrite.

14. 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

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
   1.2. Organisation opérationnelle de l'activité
   1.3. Grille d'analyse des risques et principaux incidents de fraude

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

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

4. Chèque
   4.1. Présentation de l'offre
   4.2. Organisation opérationnelle de l'activité chèque
   4.3. Grille d'analyse des risques et principaux incidents de fraude

5. Monnaie électronique
   5.1. Présentation de l'offre
   5.2. Organisation opérationnelle de l'activité monnaie électronique
   5.3. Description des principaux incidents de fraude

6. Services d'information sur les comptes et d'initiation de paiement
   6.1. Présentation de l'offre
   6.2. Organisation opérationnelle de l'offre
   6.3. Présentation des mesures de protection des données de paiement sensibles

II. Présentation des résultats du contrôle périodique sur le périmètre des moyens de paiement scripturaux et de l'accès aux comptes

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

IV. Rapport d'audit sur la mise en œuvre des mesures de sécurité inscrites dans les RTS (Regulatory technical standard)

V. Annexes

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

INTRODUCTION

Rappel du cadre règlementaire

Cette annexe est consacrée à la sécurité des **moyens de paiement scripturaux**, définis à l'article L. 311-3 du Code monétaire et financier, émis ou gérés par l'établissement, 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[4].

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) ;

[4] 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*) (IV)[5];

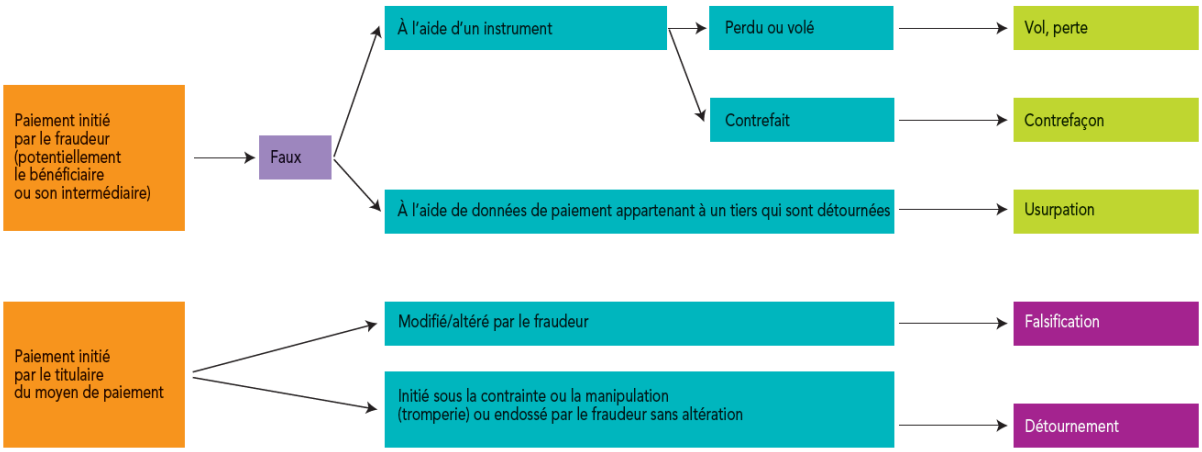
- une annexe comprenant la matrice de cotation des risques de fraude et un glossaire pour la définition des termes techniques/acronymes utilisés par l'établissement dans l'annexe (V).

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 »[6]. En conséquence, cette analyse s'effectue :

- sur la fraude brute et couvre à la fois la fraude interne et la fraude externe ;

- et, sur la base des définitions et typologie de fraude 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 rapport annuel 2023 sur l'exercice 2022, il est également attendu que les établissements remplissent la partie consacrée au chèque dès lors qu'ils fournissent un service d'encaissement de chèques.** 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.

[5] 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

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

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 concernant les prestataires de service d'information sur les comptes

Pour la partie I, les prestataires de service d'information sur les comptes doivent répondre uniquement au point consacré au service d'information sur les comptes (I.5). Par ailleurs, ils sont tenus de renseigner les parties consacrées aux résultats du contrôle périodique (II), à l'auto-évaluation de la conformité aux recommandations d'organismes externes en matière de sécurité des moyens de paiement (III) et au rapport d'audit sur la mise en œuvre des mesures de sécurité inscrites dans les RTS (IV).

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 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 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	Canaux 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** 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 moins 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 ou numéro de carte non affecté	-Le numéro de carte d'un porteur est relevé à son insu ou créé par « moulinage » (à l'aide de générateurs aléatoires de numéros de carte) et utilisé en vente à distance. .
Autres	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. Encaissement de chèque

4.1. Présentation de l'offre

a. Description de l'offre d'encaissement de chèque

Clientèle concernée	Canal d'encaissement	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.

4.2. Organisation opérationnelle de l'activité de remise de chèque

Présenter de manière synthétique le processus de traitement du chèque depuis sa réception jusqu'à sa remise aux systèmes d'échange 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 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	- 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.

Typologie de fraude	Canal de remise	Mesures de couverture
Vol, perte (faux, apocryphe)		
Contrefaçon		
Falsification		

Détournement, rejeu		

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

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.

5. Monnaie électronique

5.1. Présentation de l'offre

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

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

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

5.2. 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.

5.3. 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)

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

6.1. 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.

6.2. Organisation opérationnelle de l'offre

Présenter de manière synthétique le processus d'exécution du service d'information sur les comptes 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.

6.3. 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.

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**
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 cartes 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 avant 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 ne renseigne le questionnaire que s'il est gestionnaire de comptes de paiement et 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 sur l'exemption liée à l'analyse des risques liés à l'opération, qui sera prochainement 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 ~~mesurés pour chacun des motifs d'exemption à l'authentification forte (visés aux art. 13 à 18)~~ soient équivalents ou inférieurs ~~au~~aux taux ~~maximal autorisé par tranche~~maximaux de ~~montant~~référence tel que ~~fixé~~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 ~~pour chacun des motifs d'exemption à l'authentification forte (visés aux art. 13 à 18)~~ 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 [7]

1.1. Dispositif général de contrôle interne :

- joindre un organigramme faisant apparaître les unités consacrées au(x) contrôle(s) permanent(s) et notamment au contrôle de la conformité, ainsi qu'au contrôle périodique et le positionnement hiérarchique de leurs responsables ;
- coordination prévue entre les différents acteurs du contrôle interne ;
- 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) ;

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

– description 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.

1.4. Dispositif de contrôle périodique :

– description de l'organisation de la fonction d'audit 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) ;

– description, formalisation et date(s) de mise à jour des procédures sur lesquelles s'appuie la fonction de contrôle 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 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[8]

2.1. Le dispositif de contrôle permanent (1er et 2ème niveau) couvre-t-il l'ensemble des mesures relatives :
  2.1.1. - au renforcement de l'accès aux services bancaires et services de paiement et à la facilitation de leur usage ? Oui / Non
  2.1.2. - à la prévention du surendettement / détection ? Oui / Non
  2.1.3. - à la prévention du surendettement / accompagnement ? Oui / Non
  2.1.4. - à la formation des personnels et plus particulièrement aux points 1.1 à 1.6 ci-dessus ? Oui / Non
2.2. L'ensemble des points 2.1.1 à 2.1.4 sont-ils couverts sur le cycle de contrôle périodique ? Oui / Non
2.3. Des anomalies significatives ont-elles été détectées à l'occasion des contrôles permanents et le cas échéant périodiques au cours de l'année sous revue ? Oui / Non.
La réponse « Non » dispense de répondre aux questions 2.4 et 2.5
2.4. Si oui, indiquez les principales (dans la limite de 3)
2.5. Les actions correctives nécessaires ont-elles été mises en œuvre ? Oui/ Non

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

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