G. Aspects de la réglementation et du contrôle prudentiels applicables à l'ensemble des secteurs

En sa qualité d'autorité de contrôle prudentiel, la Banque a compétence sur une série de domaines qui recouvrent plusieurs secteurs et ne sont donc pas abordés dans les parties du présent Rapport consacrées aux banques, aux entreprises d'assurance et aux infrastructures de marchés financiers.

L'année 2018 a notamment été marquée par des évolutions marquantes du cadre légal européen en matière de prévention du blanchiment de capitaux et du financement du terrorisme ainsi qu'au niveau national, par l'entrée en vigueur de la nouvelle loi anti-blanchiment.

L'entité d'assurance qualité, qui vise à assurer que les activités de surveillance prudentielle et de résolution de la Banque répondent à un certain nombre d'exigences de qualité, a poursuivi ces travaux.

En matière de FinTech et de numérisation, la Banque a adressé un questionnaire à une sélection représentative d'établissements des secteurs des établissements de crédit, des infrastructures de marché, des établissements de paiement, des établissements de monnaie électronique et des entreprises d'assurance afin d'obtenir un aperçu sectoriel des tendances et évolutions importantes. Un point d'attention spécifique a concerné la transposition de la deuxième directive européenne sur les services de paiement (PSD2).

Dans un contexte de poursuite de hausse des cybermenaces, la Banque a activement contribué à la poursuite du développement, au niveau européen, d'un cadre réglementaire pour la gestion des cyber-risques et de recommandations en la matière. Au cours de l'année sous revue, elle a également mené plusieurs missions d'inspection portant sur les cyber-risques et a mis en place un cadre pour le piratage éthique. Enfin, en collaboration avec Febelfin, la Banque a poursuivi ses travaux visant à cartographier la fraude en e-banking.

En matière de gouvernance et de collaboration des réviseurs au contrôle prudentiel, l'année sous revue s'est caractérisée par l'élaboration d'une approche commune par la Banque et la FSMA en matière d'expertise des responsables de la fonction de compliance, par la publication d'une communication concernant le renouvellement de l'agrément des réviseurs et d'une nouvelle circulaire « fit and proper ». Par ailleurs, la Banque a collaboré au suivi apporté aux recommandations des commissions Optima et Panama Papers.

Enfin, en 2018, la Banque a sensibilisé les établissements financiers aux risques qui résulteraient d'un scénario de « hard brexit », notamment par la voie de contrats conclus avec des contreparties britanniques.

1. Prévention du blanchiment de capitaux et du financement du terrorisme

En matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) à l'échelon européen, l'année 2018 a vu des évolutions marquantes du cadre légal, ainsi que l'émergence de nouveaux projets résultant d'incidents significatifs pouvant être considérés comme les révélateurs de faiblesses du cadre légal existant ou de sa mise en pratique.

Ces évolutions se couplent en Belgique à celles qui résultent de l'entrée en vigueur de la nouvelle loi anti-blanchiment du 18 septembre 2017[1]. La Banque a dès lors attaché une attention particulière pendant l'année écoulée à la mise en application effective de cette nouvelle loi.

1.1 Évolution et mise en œuvre du cadre légal européen et nouveaux projets pour l'avenir

La 5e directive européenne en matière de LBC/FT[2] est entrée en vigueur le 9 juillet 2018. Engagée en réponse aux attentats terroristes qui ont frappé l'Europe en 2015, cette directive vise essentiellement à renforcer le cadre légal européen et des États membres en ce qui concerne entre autres les mesures de vigilance applicables en matière de monnaie électronique ou à l'égard des pays à haut risque, et la transparence des sociétés et constructions juridiques, en clarifiant notamment la portée de la notion de « bénéficiaires effectifs » des trusts et des fiducies. Elle instaure une obligation pour les États membres d'établir la liste des fonctions publiques importantes dont l'exercice en leur sein confère la qualité de « personne politiquement exposée » requérant l'exercice d'une vigilance accrue[3]. Elle impose également aux États membres de soumettre les opérateurs en monnaies virtuelles aux obligations préventives du blanchiment de capitaux et du financement du terrorisme (BC/FT) et à un contrôle du respect de ces obligations. La nouvelle directive vise par ailleurs à améliorer le fonctionnement des cellules nationales de renseignements financiers et la coopération entre elles, ainsi que le fonctionnement et l'interconnexion des registres nationaux des bénéficiaires effectifs des sociétés et constructions juridiques. Elle instaure également une nouvelle obligation pour les États membres de mettre en place un registre ou un mécanisme central permettant d'identifier les titulaires de comptes bancaires ou de comptes de paiement et de coffres-forts. Enfin, la 5e directive comprend en outre diverses dispositions visant à faciliter et à intensifier la coopération entre les autorités nationales de contrôle compétentes en matière de LBC/FT, ainsi qu'avec les autorités de contrôle prudentiel, en ce compris la BCE agissant dans le cadre du SSM.

Cette 5e directive anti-blanchiment devant être transposée dans les droits nationaux des États membres pour le 10 janvier 2020, la Banque participe au groupe

1 Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces.

2 Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE (JO de l'UE du 19 juin 2018).

3 Si certaines catégories de personnes politiquement exposées, tels que les chefs d'État, les chefs de gouvernement, les ministres, et ainsi de suite, sont univoques, d'autres catégories, tels les officiers supérieurs des forces armées, les membres des organes d'administration, de direction ou de surveillance des entreprises publiques, etc., peuvent donner lieu à des interprétations divergentes et être clarifiées par l'établissement d'une telle liste.

de travail coordonné par le SPF Finances – Trésorerie – qui est chargé d'élaborer, sur le plan technique, un avant-projet de loi de transposition. La Banque veillera notamment à proposer dans ce cadre des dispositions législatives qui clarifient et renforcent de manière adéquate les obligations de coopération des autorités nationales de contrôle en matière de LBC/FT, dans une perspective d'efficacité accrue de ce contrôle.

Sur un plan factuel, plusieurs incidents sont récemment survenus en Europe, qui semblent mettre au jour des faiblesses dans la mise en application du cadre légal européen de LBC/FT et de son contrôle dans certains États membres de l'Union européenne. Face à ces événements, la Commission européenne a publié le 12 septembre 2018 une communication[1] dans laquelle elle énumère les mesures législatives et non législatives qu'elle prône pour renforcer à court terme tant le contrôle prudentiel des banques que leur contrôle en matière de LBC/FT, ainsi que ses pistes de réflexion à plus long terme.

Au nombre des mesures législatives à court terme, la Commission annonce sa volonté d'achever de lever les entraves juridiques à l'échange d'informations entre les autorités de contrôle prudentiel et de contrôle de LBC/FT des banques par des modifications à apporter à la directive sur les exigences de fonds propres[2]. Elle annonce par ailleurs sa volonté de compléter la revue en cours des règlements fondateurs des trois autorités européennes de supervision[3] par des dispositions modificatives additionnelles relatives à leurs rôles en matière de LBC/FT. Ces modifications additionnelles visent en premier lieu à centraliser les compétences en matière de LBC/FT au sein de l'EBA, en ce compris dans les secteurs d'activité qui relèvent des compétences de l'EIOPA ou de l'ESMA. Elles entendent ensuite clarifier le contenu des tâches de cette dernière en la matière et renforcer les outils juridiques mis à sa disposition à cet effet. La Commission envisage entre autres de prévoir une obligation pour l'EBA d'informer le Parlement européen, le Conseil et la Commission des lacunes graves non résolues qu'elle identifierait dans le cadre, notamment, de ses « peer reviews », ainsi qu'un pouvoir d'injonction tant aux autorités nationales de contrôle qu'aux établissements financiers. Enfin, la Commission souhaite attribuer à court terme à l'EBA un rôle central dans la coopération avec les autorités des pays tiers.

Sur le front des mesures non législatives à court terme, la Commission encourage les autorités européennes de supervision, en particulier l'EBA, à faire usage des pouvoirs dont elles sont d'ores et déjà dotées. Cela inclut, notamment, l'élaboration d'« orientations communes » ainsi que la mise en œuvre de « peer reviews » et de procédures pour infraction à la législation européenne, afin de veiller, d'une part, à une prise en compte adéquate des risques de BC/FT par les autorités en charge du contrôle prudentiel des banques, même lorsque ces autorités ne sont pas simultanément chargées des responsabilités spécifiques de contrôle en matière de LBC/FT et, d'autre part, à un renforcement de l'efficacité et de la convergence au travers de l'Europe du contrôle qui est exercé par les autorités nationales en matière de LBC/FT. La Commission encourage également la BCE à conclure dans le délai imparti le protocole d'accord avec les autorités de contrôle de LBC/FT qui est requis par la 5e directive en vue d'organiser leur coopération, et à clarifier les modalités de prise en compte des risques de BC/FT dans l'exercice de ses compétences de contrôle.

La Commission européenne a publié une série de mesures visant à renforcer le contrôle en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme

À plus long terme, la Commission annonce qu'elle examinera la possibilité de procéder à des réformes plus approfondies qui pourraient inclure, d'une part, le remplacement de la directive actuelle d'harmonisation minimale en matière de LBC/FT par un

1 « Communication de la Commission au Parlement européen, au Conseil européen, à la Banque centrale européenne, au Comité économique et social et au Comité des régions – Renforcer le cadre de l'Union en matière de surveillance prudentielle et de surveillance anti-blanchiment applicable aux établissements financiers », 12 septembre 2018, COM (2018) 645 final.

2 Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE.

3 Règlement (UE) n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission; règlement (UE) n° 1094/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/79/CE de la Commission; et règlement (UE) n° 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/77/CE de la Commission.

règlement européen directement applicable dans l'ordre juridique des États membres et qui procéderait à une harmonisation complète des législations nationales en la matière, ainsi que, d'autre part, la création ou la désignation d'une autorité européenne auprès de laquelle serait centralisée la responsabilité d'exercer la supervision en matière de LBC/FT.

Depuis la publication de cette communication particulièrement importante de la Commission européenne, la Banque s'est impliquée activement et de manière constructive dans les discussions techniques relatives aux initiatives législatives à court terme susvisées. Convaincue de la nécessité d'apporter une réponse européenne forte et efficace aux incidents récemment constatés, la Banque attache une attention particulière à s'assurer, dans ce contexte, d'une haute qualité technique des modifications qu'il est envisagé d'apporter à la législation européenne et à veiller à maintenir un équilibre adéquat entre les dispositions spécifiquement relatives au contrôle en matière de LBC/FT, d'une part, et au contrôle prudentiel, d'autre part.

Il convient de noter que, lorsqu'elles seront adoptées et en vigueur, ces nouvelles dispositions seront susceptibles d'avoir une incidence directe importante sur les responsabilités de la Banque, en ses qualités tant d'autorité nationale de contrôle en matière de LBC/FT que d'autorité de contrôle prudentiel.

Par ailleurs, réagissant au même contexte que la Commission européenne, le Conseil européen a également rendu publiques le 4 décembre 2018[1] ses conclusions relatives à un plan d'action anti-blanchiment, qui balise les actions qu'il entend voir mises en œuvre dans de brefs délais tant par la Commission européenne et les autorités européennes que par les États membres et leurs autorités nationales compétentes, en vue de remédier aux insuffisances constatées.

1.2 Mise en application de la loi anti-blanchiment du 18 septembre 2017

Communication aux établissements financiers concernant leurs obligations en matière de LBC/FT

À la suite de l'entrée en vigueur de la loi anti-blanchiment du 18 septembre 2017, la Banque a estimé nécessaire, en vue d'une application effective de celle-ci, de se doter d'un instrument efficace de communication lui permettant de fournir aux établissements financiers une information complète, aisée et régulièrement mise à jour leur permettant de connaître et de comprendre de manière détaillée l'ensemble des obligations légales et réglementaires auxquelles elles sont tenues en la matière. À cet effet, la Banque a créé une nouvelle rubrique sur son site internet dans laquelle elle a rassemblé l'ensemble des textes pertinents en matière de LBC/FT (loi, règlements, travaux préparatoires, lignes directrices européennes et internationales, etc.), en les structurant par thème de manière à faciliter les recherches. Cette rubrique permet en outre d'adresser aux établissements financiers les recommandations et commentaires que la Banque estime nécessaires aux fins d'une application correcte et effective des dispositions de la loi et du règlement anti-blanchiment.

Après avoir mis en ligne, dès le début de l'année 2018, la structure de la nouvelle rubrique du site et l'ensemble des documents de référence, la Banque l'a progressivement enrichie en y ajoutant, en plusieurs étapes, thème par thème, ses commentaires et recommandations, après avoir soumis ses projets à la consultation des associations professionnelles du secteur financier. À la fin de 2018, cette rubrique du site contenait ainsi l'ensemble des recommandations que la Banque a jugé utile de formuler pour tous les aspects pertinents de la matière. Des mécanismes d'avertissement sont prévus afin d'informer les établissements financiers chaque fois que des modifications significatives sont apportées au site. Celui-ci offre en outre la possibilité de consulter ses versions antérieures. Dans une prochaine étape, la Banque envisage également la mise en ligne de cette rubrique de son site en langue anglaise.

À l'avenir, la Banque mettra ce site régulièrement à jour, chaque fois qu'elle l'estimera nécessaire, notamment pour tenir compte de l'évolution des normes et des recommandations des instances internationales compétentes en matière de LBC/FT, du cadre légal et réglementaire européen et national, de l'interprétation des règles applicables, etc.

Méthodologie du contrôle fondé sur les risques

La Banque étant légalement tenue d'exercer ses compétences de contrôle en recourant à une approche fondée sur les risques, il lui appartient de mettre en

1 *Anti-Money Laundering Action Plan – Council Conclusions*, 4 décembre 2018.

œuvre une méthodologie de contrôle conforme aux orientations communes relatives à la surveillance fondée sur les risques adoptées le 7 avril 2017 par les autorités européennes de supervision[1] et auxquelles la Banque a déclaré vouloir se conformer.

À cet effet, et en se basant sur l'expérience acquise au cours des années précédentes, la Banque collecte les informations initiales synthétiques qui lui sont nécessaires concernant les risques inhérents de BC/FT auxquels chaque établissement financier est exposé, le degré apparent de conformité de ses mécanismes de LBC/FT avec les obligations légales et réglementaires, et le degré apparent d'efficacité de ces mécanismes grâce au questionnaire périodique dont la version 2018 a été établie sur une base sectorielle[2]. De plus, la Banque s'est dotée en 2018 d'outils informatiques complémentaires lui permettant de bénéficier d'une préanalyse automatisée des réponses au questionnaire périodique introduites en ligne par chaque établissement financier, et de tenir compte en outre de l'ensemble des informations disponibles, en ce compris, notamment, le résultat des contrôles hors site antérieurs et des inspections effectuées sur place, les informations de nature prudentielle, ou les informations pouvant être obtenues auprès des réviseurs agréés ou de sources externes fiables, pour allouer à chaque établissement financier le profil de risque qui lui convient.

Ce profil de risque détermine le degré de priorité, la fréquence et l'intensité des contrôles à exercer hors site. Ceux-ci peuvent inclure entre autres, selon les cas, l'examen détaillé des organigrammes, des politiques et des procédures internes de l'établissement financier concerné, la collecte et l'analyse d'informations plus précises auprès de lui, l'examen de rapports d'audit interne et du suivi qui y a été donné, la tenue de réunions avec le responsable de la LBC/FT et avec le haut dirigeant responsable. Le cas échéant, des visites sur place peuvent être organisées afin de permettre à l'équipe de contrôle de percevoir plus concrètement l'état de la situation, sans que ces visites ne se déroulent selon la méthodologie d'audit appliquée lors des inspections sur place. Le contrôle hors site inclut également le suivi des plans d'action établis par les établissements financiers à l'issue des inspections antérieurement effectuées sur place. Ces actions de contrôle hors site visent à déterminer les mesures que l'établissement financier concerné doit adopter et mettre en application dans un délai raisonnable pour remédier aux faiblesses épinglées. Elles peuvent déboucher, lorsque cela s'avère nécessaire, sur le recours aux pouvoirs de contrainte que la loi anti-blanchiment du 18 septembre 2017 attribue à la Banque, telles que la fixation de délais de remédiation, l'imposition d'astreintes, l'injonction de remplacer les dirigeants, la suspension d'activités, etc.

La Banque continue de renforcer ses outils de contrôle fondé sur les risques

Le profil de risque attribué aux établissements financiers en tenant compte des résultats des actions antérieures de contrôle sert également de base pour déterminer les priorités des inspections à effectuer sur place en matière de LBC/FT, ainsi que les sujets sur lesquels ces inspections porteront.

Action de contrôle de la mise en œuvre effective des nouvelles dispositions légales et réglementaires

À la suite de l'entrée en vigueur de la loi anti-blanchiment du 18 septembre 2017, il incombe à la Banque de s'assurer que les établissements financiers qui relèvent de ses compétences légales de contrôle prennent dans un délai raisonnable les mesures nécessaires pour se conformer pleinement et efficacement à leurs nouvelles obligations légales et réglementaires. La plus cruciale d'entre elles concerne l'obligation de procéder à une évaluation globale des risques de BC/FT sur laquelle doivent se fonder leurs politiques et procédures internes de LBC/FT. La Banque a dès lors entrepris une action de contrôle dans le cadre de laquelle elle a invité l'ensemble des établissements financiers qui relèvent de ses compétences à procéder sans retard à une telle évaluation globale des risques, complétée d'une analyse systématique des faiblesses de leurs mécanismes internes de LBC/FT au regard tant de leurs nouvelles obligations légales et réglementaires que des risques qu'elles ont relevés, et d'un plan d'action en vue de remédier à ces faiblesses dans un délai raisonnable[3].

1 « Orientations communes concernant les caractéristiques d'une approche fondée sur les risques pour la surveillance en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, et la marche à suivre dans le cadre de la surveillance fondée sur les risques – Les orientations relatives à la surveillance fondée sur les risques », ESAs 2016 72, 7 avril 2017.

2 Circulaire NBB_2018_01 du 15 janvier 2018/Questionnaire périodique relatif à la prévention du blanchiment de capitaux et du financement du terrorisme.

3 Circulaire NBB_2018_02 du 24 janvier 2018/Évaluation globale des risques en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

La Banque leur a demandé de lui adresser pour la fin du mois de mars 2018 un rapport intermédiaire relatif à ces travaux afin de s'assurer qu'ils avaient effectivement été entrepris, suivi, à la mi-juillet 2018, d'un rapport final synthétisant les conclusions de leur analyse des risques, de leur analyse des faiblesses et de leur plan d'action pour y remédier.

La Banque intègre ces informations dans son processus de contrôle fondé sur les risques tel que décrit ci-dessus, en accordant la priorité à l'examen des informations fournies par les établissements financiers auxquels elle a attribué un profil de risque élevé. Outre qu'elle poursuivra son action de contrôle en 2019, la Banque a attiré l'attention des établissements financiers sur le fait qu'il est requis de renouveler ces travaux lorsque cela s'avère nécessaire afin d'adapter leurs mécanismes internes de LBC/FT à l'évolution des risques auxquels ils sont exposés.

Action de contrôle spécifique en matière de transmission de fonds

Compte tenu des risques élevés spécifiquement liés aux activités de transmission de fonds dans le cadre desquelles des espèces sont largement utilisées, la Banque a achevé en 2018 une action horizontale de contrôle lancée en 2017 et consistant en l'examen d'un échantillon de transactions effectuées par des agents des principaux établissements de paiement de droit belge ou étrangers (*Money remitters*) opérant sur le territoire belge. Dans un premier temps, cette action de contrôle a conduit la Banque à adresser à chacun des établissements de paiement concernés des recommandations individualisées pour remédier aux faiblesses identifiées.

Sur la base de l'ensemble des analyses réalisées et des renseignements complémentaires reçus, la Banque a cependant aussi constaté que certaines lacunes sont fréquentes dans les procédures et systèmes de contrôle de ces établissements. Les points d'attention relevés concernent essentiellement la supervision des agents, les erreurs d'encodage, la vigilance concernant les transactions entre contreparties belges, les situations pouvant révéler une fragmentation de transactions et enfin la nécessité d'une gestion exclusive par la fonction de compliance des demandes de renseignements et des alertes.

La Banque a dès lors jugé nécessaire de faire connaître à l'ensemble du secteur, par la publication d'une communication[1], les leçons générales qu'elle tire de cette action horizontale de contrôle, tout en mettant explicitement l'accent sur l'importance que revêt le respect rigoureux des obligations découlant du cadre légal et réglementaire de LBC/FT, ainsi que le respect des politiques et procédures internes mises en place au sein des établissements de paiement.

Contrôle de LBC/FT à l'occasion des nouvelles demandes d'agrément ou d'enregistrement d'entités assujetties à la loi anti-blanchiment du 18 septembre 2017

Dans le cadre du traitement des demandes d'agrément de nouveaux établissements financiers et d'enregistrement de nouvelles succursales ou d'autres formes d'établissements sur le territoire belge qui sont assujettis à la loi anti-blanchiment du 18 septembre 2017 et qui relèvent des compétences de contrôle de la Banque, celle-ci s'assure que ces entités se conformeront pleinement à leurs obligations en la matière, notamment en ce qui concerne leur gouvernance et leurs modalités d'organisation, leurs politiques, leurs procédures et leurs contrôles internes, en se fondant sur une analyse globale des risques appropriée.

L'année 2018 a été marquée par l'introduction d'un nombre particulièrement important de dossiers de cette nature en raison, notamment, de l'imminence de la sortie du Royaume-Uni de l'Union européenne et de la décision de nombreux établissements financiers qui y étaient établis de se relocaliser sur le territoire de l'Union. Le secteur des établissements de paiement et de monnaie électronique, mais également celui des établissements de crédit sont particulièrement concernés. Dans le cadre de ces dossiers, la Banque attache une attention particulière à obtenir l'assurance que le centre de décision relatif à l'exercice de la fonction de LBC/FT est effectivement localisé au sein de l'entité belge et que les mesures organisationnelles mises en œuvre permettent un exercice effectif de cette fonction.

Le traitement de ces dossiers a eu une incidence très significative sur l'affectation des ressources humaines allouées par la Banque à l'exercice de ses compétences de contrôle en matière de LBC/FT.

1 Communication NBB_2018_21 du 20 juin 2018/Analyse horizontale de contrôle consistant en l'examen d'un échantillon de transactions passées par des agents liés de différents établissements de paiement.

2. Assurance qualité (Quality assurance)

L'entité d'assurance qualité a poursuivi ses travaux, entamés en 2016, qui ont pour objectif d'assurer que les activités de surveillance prudentielle et de résolution de la Banque (dans un contexte tant national qu'international) répondent aux exigences de qualité en la matière.

Plus de la moitié des travaux réalisés l'ont été dans le domaine de la surveillance bancaire et se sont articulés autour de trois axes principaux : la finalisation d'une mission d'assurance qualité dont l'objectif était d'évaluer dans quelle mesure la gouvernance, l'organisation et le fonctionnement mis en place par la Banque dans le contexte du SSM lui permettent de jouer adéquatement son rôle d'autorité compétente nationale vis-à-vis de la BCE ; un rôle d'interlocuteur unique auprès de la BCE et de contributeur à ses travaux d'assurance qualité dans le cadre du SSM ; et la poursuite des travaux visant à améliorer la qualité des processus, procédures et contrôles appliqués au sein des services opérationnels chargés de la surveillance des établissements moins importants (LSI).

L'entité d'assurance qualité a également été amenée à intervenir de manière ponctuelle, en tant que facilitateur, coordinateur ou pourvoyeur d'avis, dans toute une série de dossiers transversaux, c'est-à-dire traitant de thèmes qui concernent plusieurs services de surveillance prudentielle à la fois. Ces actions ont été menées à l'initiative de l'entité d'assurance qualité ou en réponse à une demande du management de la Banque. À titre d'exemple, l'entité d'assurance qualité a joué un rôle important en 2018 afin d'assurer que les recommandations transversales de l'Audit interne adressées à des services de surveillance prudentielle soient adéquatement appliquées.

Le réseau de correspondants d'assurance qualité issus des services opérationnels de surveillance et de résolution de la Banque a, pour sa part, poursuivi ses travaux. Ceux-ci ont porté, d'une part, sur l'échange régulier et structuré d'informations dans le domaine de la qualité et, d'autre part, sur la concertation pour la définition d'initiatives permettant d'améliorer la qualité de leurs activités. Cela a permis d'assurer la poursuite de la mise en œuvre, au sein de ces services, des objectifs définis sur le plan de la qualité pour assurer l'exercice d'une surveillance efficace, efficiente et rigoureuse.

3. FinTech

Ces dernières années, sous l'impulsion d'innovations technologiques et de l'évolution des préférences des consommateurs, le secteur financier s'est caractérisé par un degré croissant de numérisation ainsi que par l'introduction de nombreuses nouvelles applications, de nouveaux processus ou de nouveaux produits. La transformation numérique et FinTech[1] sont des concepts étroitement liés qui sont définis, d'une part, par l'arrivée sur le marché de nouveaux prestataires de services innovants et, d'autre part, par des initiatives d'établissements existants visant à améliorer l'organisation, la fourniture de services et l'offre de produits à l'aide d'innovations technologiques.

La Banque reconnaît l'importance de ces évolutions et a donc pris différentes mesures pour engager un dialogue sur ces questions avec les acteurs du marché, tant nouveaux qu'établis. Dans ce contexte, la Banque a, entre autres, mis en place, en collaboration avec la FSMA, un point de contact central (« *FinTech single point of contact* ») pour traiter les questions relatives aux FinTech[2].

Compte tenu de l'influence possible des nouvelles technologies sur le marché financier, la Banque a également souhaité disposer d'un aperçu sectoriel des tendances et évolutions importantes en matière de Fintech et de numérisation dans le paysage financier belge. Ainsi, au second semestre de 2017, la Banque a adressé un questionnaire structuré à une sélection représentative d'établissements des secteurs des établissements de crédit, des infrastructures de marché, des établissements de paiement, des établissements de monnaie électronique et des compagnies d'assurance.

La Banque a sensibilisé le secteur financier aux défis concernant les FinTech et la numérisation

1 Le Conseil de stabilité financière (*Financial Stability Board*, FSB) définit la notion de FinTech comme l'innovation financière fondée sur la technologie, susceptible de donner lieu à des nouveautés en matière de modèles stratégiques, d'applications, de processus ou de produits, avec une incidence importante sur les marchés et établissements financiers ainsi que sur la prestation de services financiers.

2 Le point central de contact pour FinTech se trouve sur la page Internet https://www.nbb.be/fr/supervision-financiere/generalites/point-de-contact-fintech.

Le questionnaire vise à examiner les perspectives et observations générales en matière de FinTech, les perspectives relatives à certains modèles d'entreprise et technologies spécifiques, la stratégie concrète suivie par les établissements à l'égard des Fintech, et d'éventuelles observations ou remarques concernant la réglementation et le contrôle. L'enquête horizontale visait également à dégager un aperçu de l'attitude des différents acteurs vis-à-vis des FinTech, de l'incidence que ces évolutions peuvent avoir sur leur modèle d'entreprise actuel et des mesures qu'ils envisagent de prendre pour y faire face.

3.1 Questionnaire aux établissements de crédit

Les réponses des établissements de crédit ont montré notamment qu'ils prévoient, en premier lieu, de se moderniser afin de rester pertinents à l'avenir. Il est également relativement plausible, pour les banques, que les services financiers deviennent de plus en plus modulaires et que les banques puissent maintenir une activité suffisante tandis qu'un grand nombre de nouvelles sociétés spécialisées reprendront certaines activités spécifiques, notamment en les proposant directement sur les plateformes des banques et des grandes entreprises technologiques.

Les banques estiment asseoir leur force principalement en raison de leurs portefeuilles de clients établis, de leur connaissance de ces clients et de la confiance qu'ils leur accordent. Mais elles sont d'avis qu'elles ont également un avantage sur les nouveaux établissements financiers sur le plan des connaissances et de l'expérience des réglementations souvent complexes, d'une part, et de la gestion des risques, d'autre part.

En revanche, le secteur bancaire belge est préoccupé par son infrastructure informatique souvent vieillissante, qui peut entraîner une augmentation des coûts d'exploitation, une inefficacité des processus ou une augmentation des risques qui y sont liés, et des difficultés à mettre en œuvre des modèles d'entreprise innovants. En outre, un certain nombre de banques se sont avérées ne pas avoir de stratégie claire en matière de FinTech et de numérisation, ce qui signifie qu'elles n'ont pas une image claire de la situation et procèdent souvent avec retenue. Dans chaque segment de marché, des exemples clairs de ces banques sans stratégie d'innovation ont été trouvés, alors que certains de leurs concurrents directs qui étaient plus avancés développaient clairement des avantages concurrentiels concrets. Il est apparu que les banques de taille plus modeste se positionnaient souvent comme des « suiveuses », soulignant qu'elles

étaient moins à même, sur le plan de la capacité opérationnelle et financière, d'expérimenter, mais aussi que les grandes banques présentaient pour les entreprises FinTech une attractivité accrue sur le plan des opportunités de coopération.

En ce qui concerne l'incidence des FinTech, les banques soulignent en particulier les cyber-risques, ainsi que les risques pour leur rentabilité et leur stratégie, et le risque que leur rôle perde de son importance si les clients concluent des transactions directement avec des investisseurs, supprimant ainsi leur rôle d'intermédiation.

À la fin de 2018, la Banque a publié les résultats de cette analyse sur son site internet[1], soulignant un certain nombre de bonnes pratiques dans ce contexte. L'élaboration, la mise en œuvre et la gestion d'une stratégie claire, dans laquelle le rôle et la participation du conseil d'administration s'avèrent être un facteur de succès important, sont au cœur de ces recommandations. Les banques doivent par ailleurs être suffisamment conscientes du fait que, dans certains cas, les projets de FinTech et de numérisation sont nécessaires pour maintenir la position actuelle sur le marché et le modèle d'entreprise existant et pour continuer à répondre aux besoins évolutifs des clients.

3.2 Questionnaire aux établissements de paiement, aux établissements de monnaie électronique et aux infrastructures de marchés financiers

Il est ressorti en premier lieu du questionnaire soumis aux établissements de paiement, aux établissements de monnaie électronique et aux infrastructures de marchés financiers, qu'en dépit de l'introduction de nouvelles technologies et de l'innovation dans le secteur, la plupart des processus de compensation et de liquidation se déroulent toujours sur les infrastructures de paiement et de marchés existantes. Les infrastructures de marchés et établissements de paiement interrogés ont constaté que les nouveautés dans le domaine visent principalement à optimiser la relation avec le consommateur (*front-end*). Ensuite, l'enquête montre que les répondants constatent une intensification de la concurrence sur le marché des paiements, ce qui met sous pression les marges des acteurs existants. Ce constat s'explique pour le secteur d'une part par la nécessité d'améliorer l'expérience client, et d'autre part par l'apparition sur le marché du concept d'« *Open Banking* » (cf. section G.4), permettent l'apparition de nouveaux fournisseurs tiers. Enfin, la majorité des répondants ont également indiqué qu'ils suivaient de près l'évolution de la numérisation du secteur financier.

3.3 Questionnaire aux entreprises d'assurance

Le questionnaire envoyé par la Banque aux entreprises d'assurance avait pour but de lui permettre de se forger une idée des réflexions menées par les différents acteurs existants et de connaître leur vision de l'incidence des InsurTech[2] sur les marchés européen et belge de l'assurance et des principaux obstacles légaux qui pourraient empêcher les entreprises d'assurance belges de pouvoir mettre en œuvre leur stratégie en la matière.

Il ressort des réponses reçues qu'à court terme le phénomène InsurTech est plutôt perçu comme une opportunité d'amélioration des services pour les entreprises d'assurance que comme un risque immédiat. Les entreprises d'assurance se préparent à l'arrivée de ces nouvelles technologies et l'impact de celles-ci sur leur modèle d'entreprise ou sur leur organisation interne est généralement discuté au sein des Conseils d'administration et des Comités de direction. Les fonctions de contrôle indépendantes sont également consultées lors du processus de décision et des groupes spécifiques sont constitués en interne. Les principales inquiétudes du secteur portent davantage sur les modifications à apporter à leur modèle d'entreprise que sur l'apparition de nouveaux entrants sur le marché. Les entreprises d'assurance estiment également que la législation actuelle limite dans certains cas, à des fins de protection des consommateurs, l'application de nouvelles technologies.

À moyen terme, les processus internes des entreprises d'assurance pourront être améliorés par le biais, notamment, d'une meilleure organisation informatique, par la création de nouveaux départements (par exemple, *data management*) ou par la robotisation accrue des tâches récurrentes. Les processus

1 Analyse de l'impact de fintech et de la numérisation sur le secteur et le contrôle bancaires belges, BNB, 22 novembre 2018 (https://www.nbb.be/fr/articles/analyse-de-limpact-de-fintech-et-de-la-numerisation-sur-le-secteur-et-le-controle-bancaires).

2 InsurTech fait référence à l'utilisation d'innovations technologiques pour réaliser des économies et accroître l'efficacité du modèle actuel du secteur de l'assurance. InsurTech explore les opportunités, telles que l'offre de polices ultra-personnalisées et l'utilisation de nouveaux flux de données à partir de dispositifs Internet pour évaluer de manière dynamique les primes en fonction du comportement observé.

d'estimation du montant des sinistres et de lutte contre la fraude seront également améliorés, ce qui aura des répercussions sur les primes des contrats. Les entreprises d'assurance s'attendent à une plus forte personnalisation de la couverture des risques et, en conséquence, à un repli de la mutualisation des risques.

À plus long terme, les entreprises d'assurance considèrent en général que, au cours des dix prochaines années, la numérisation et les InsurTech joueront un rôle essentiel sur le marché sur le plan de la distribution de produits, du service aux clients, voire dans le *design* de produits ou dans le cadre de l'évaluation des risques et de la tarification. Les modifications apportées à la manière dont les produits seront développés, tarifés ou distribués limiteront dans certains cas la fonction des entreprises d'assurance à un rôle de « porteur de risque ».

4. Open Banking

L'important développement de la numérisation du secteur financier est alimentée par la transposition de la deuxième directive européenne sur les services de paiement (PSD2)[1]. Cette directive, qui a été transposée en droit belge par la loi du 11 mars 2018, porte sur de récentes innovations dans le secteur des paiements et impose aux prestataires de services de paiement de procéder à l'ouverture de leur infrastructure de comptes de paiement (*Open Banking*). Cela doit permettre à de nouveaux acteurs d'entrer sur le marché des services de paiement et d'offrir des services d'initiation de paiement et d'information sur les comptes. L'ouverture de l'infrastructure des comptes de paiement s'accompagne d'exigences de sécurité strictes qui doivent pouvoir être respectées par les prestataires de services de paiement (banques, établissements de paiement et établissements de monnaie électronique).

L'entrée en vigueur de la directive PSD2 permet à de nouveaux acteurs d'entrer sur le marché des services de paiement

À cette fin, la directive PSD2 introduit deux nouvelles catégories de prestataires de services de paiement dans le cadre réglementaire, à savoir les prestataires de services d'initiation de paiement et d'information sur les comptes. Ces deux types de prestataires de services disposeront, tout comme les autres établissements agréés à cette fin, du droit d'accéder aux comptes de paiement d'un utilisateur de services de paiement pour autant que ce dernier y ait explicitement consenti. L'une des applications envisageables de cette modification du cadre légal est la possibilité pour un prestataire de services d'information sur les comptes de consolider dans une application unique le solde des différents comptes détenus par un particulier auprès d'une série d'établissements financiers. Pour ce qui est des prestataires de services d'initiation de paiement, le nouveau régime leur permet d'initier des paiements directement au départ du compte de paiement d'un utilisateur vers un bénéficiaire. Le schéma ci-dessous présente ces nouveaux modèles d'entreprise, rendus possibles dans le nouveau cadre législatif.

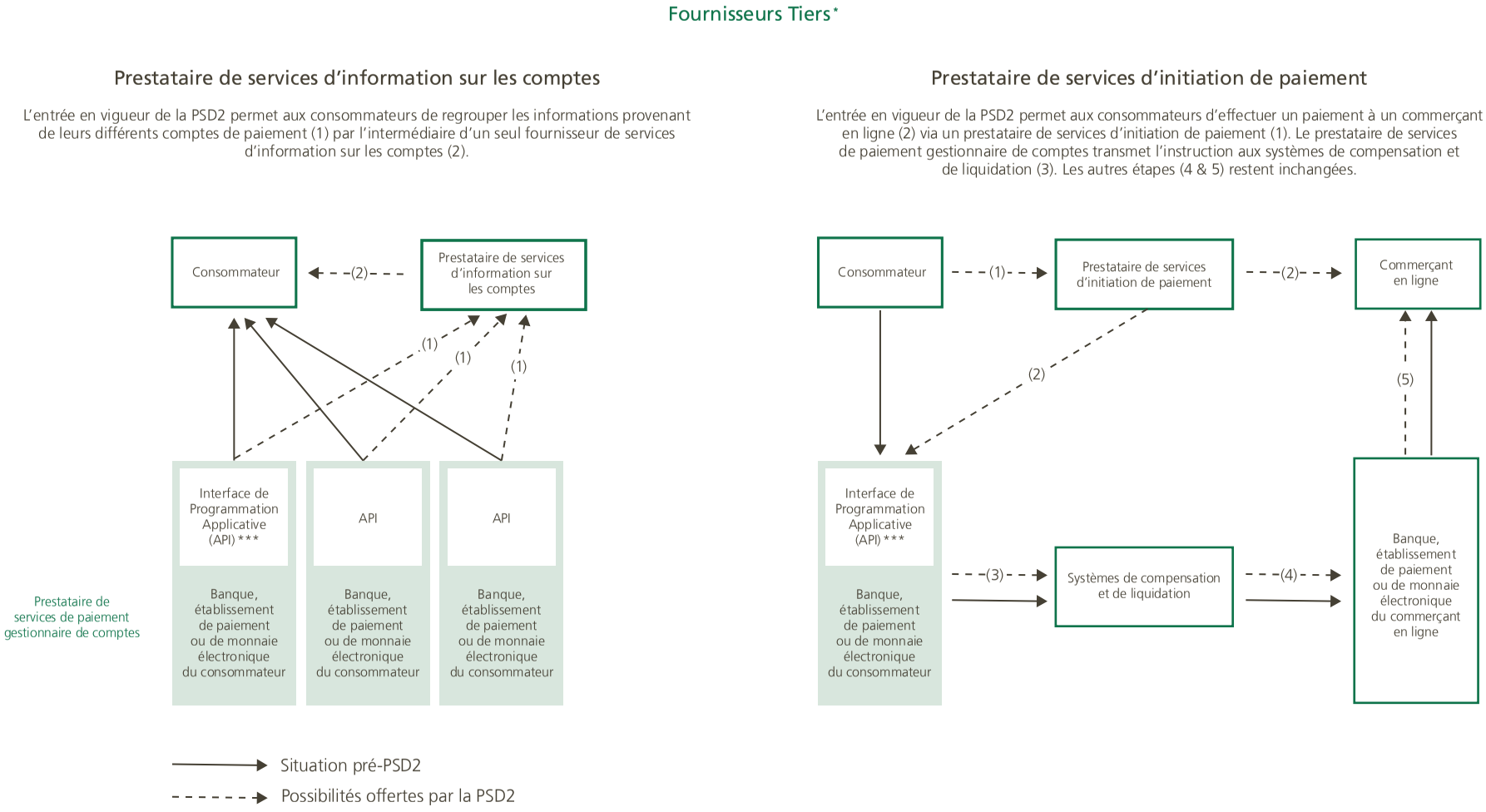
Les établissements de crédit, de paiement et de monnaie électronique existants pourront également offrir ces nouveaux services. Grâce à ce nouveau cadre législatif, chacun de ces acteurs pourra, à la demande de son client, consulter les comptes de paiement ou initier des paiements à partir des comptes détenus par ce client auprès d'un autre établissement financier. Pour l'utilisateur de services de paiement, qu'il s'agisse d'une personne physique ou morale, il deviendra ainsi possible de gérer tous ses comptes de paiement via une seule application d'un seul prestataire de services. Cette évolution devrait encore intensifier la concurrence entre les prestataires de services financiers pour conserver leurs clients et en acquérir de nouveaux.

Étant donné qu'un nouveau type d'acteurs peut accéder aux comptes de paiement, les dispositions supplémentaires à respecter par le secteur en matière d'informatique et de sécurité constituent un pilier important de ce nouveau paysage d'« Open Banking ». Il s'agit plus précisément de l'application d'une authentification forte des clients, pour l'initiation et l'exécution sécurisées des paiements, et de la mise en œuvre de normes de communication ouvertes communes et sécurisées, pour l'interaction qui aura lieu entre les prestataires de services de paiement gestionnaires de comptes (c'est-à-dire

1 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE.

Graphique 101

Aperçu schématique des processus opérationnels liés aux nouveaux services de paiement



Source : NBB.

(*) Fournisseurs tiers : un fournisseur tiers peut-être (1) un prestataire de services d'initiation de paiement, agréé par la Banque et soumis à un statut réglementaire plus limité (du fait qu'il n'entre pas en possession defonds des clients), ou un prestataire de services d'information sur les comptes, enregistré auprès de la Banque (et qui n'entre pas davantage en possession de fonds des clients). Les prestataires tiers peuvent également être des banques, des établissements de paiement ou des établissements de monnaie électronique.

(**) Prestataires de services de paiement gestionnaires de comptes : banques, établissements de paiement ou établissements de monnaie électronique agréés par la Banque et soumis à son contrôle.

(***) API : *Application Programming Interface* ou Interface de Programmation Applicative.

les banques, les établissements de paiement et les établissements de monnaie électronique), les prestataires de services d'information sur les comptes et les prestataires de services d'initiation de paiement. Afin d'assurer une application uniforme de la nouvelle réglementation dans l'EEE, l'EBA est chargée de l'élaboration de normes techniques en la matière.

L'authentification forte des clients requiert l'utilisation d'au moins deux des trois éléments suivants qui doivent être indépendants et confidentiels : un élément que seul l'utilisateur connaît (par exemple, un code PIN), un élément que seul l'utilisateur possède (par exemple, une carte de paiement) et un élément propre à l'utilisateur (par exemple, des données biométriques, comme une empreinte digitale). Comme les normes techniques réglementaires sont établies selon un point de vue neutre par rapport aux modèles technologiques et aux modèles d'entreprise, les acteurs du marché peuvent mettre à profit l'innovation pour élaborer de nouveaux produits qui tiennent compte de cette exigence. Ainsi, il existe déjà des cartes de paiement qui utilisent une empreinte digitale plutôt qu'un code PIN pour appliquer une authentification client forte.

En ce qui concerne les normes de communication, la directive PSD2 introduit l'obligation pour les prestataires de services de paiement gestionnaires de comptes de fournir au minimum une interface permettant aux prestataires de services d'information sur les comptes et aux prestataires de services d'initiation de paiement d'accéder aux informations relatives aux comptes de paiement qu'ils gèrent. La pratique actuelle d'accès de tiers sans identification (qualifié dans le jargon sectoriel de « *screen scraping* ») ne sera donc plus autorisée pour la communication entre ces acteurs lorsque les normes techniques réglementaires entreront en vigueur, le 14 septembre 2019. Il est important de noter que ces normes techniques ne s'appliquent qu'aux comptes de paiement, conformément au champ d'application de la directive PSD2. Les normes ne s'appliquent donc pas à l'accès aux comptes qui ne sont pas considérés comme des comptes de paiement.

L'évolution du marché des paiements et de l'« *Open Banking* » montrera si les différents objectifs de la directive PSD2, tels que la promotion de la concurrence et de l'innovation, la contribution à l'intégration des paiements au sein de l'UE et la facilité accrue d'utilisation pour les clients, seront atteints.

5. Cyber-risques et risques informatiques

5.1 Poursuite de l'augmentation des cybermenaces et des menaces liées à l'informatique

La numérisation des processus opérationnels du secteur financier, déjà fortement informatisé, s'est encore intensifiée au cours de l'année sous revue. Le degré d'interconnectivité entre les processus opérationnels des différents acteurs financiers est également resté très élevé. Par ailleurs, les établissements financiers optent de plus en plus pour des modèles d'entreprise dans lesquels les services informatiques sont sous-traités, selon une spécialisation soit opérationnelle soit fonctionnelle. La numérisation accrue et plus diversifiée des canaux d'accès pour les clients des établissements financiers et des IMF contribue également à la complexité du paysage financier et à l'augmentation du risque opérationnel.

Dans le monde entier, les cyberattaques se font de plus en plus sophistiquées et puissantes, et le secteur financier en constitue l'une des cibles potentielles (cf. encadré 17). Le nombre de cyberattaques ciblées et de longue durée devrait encore augmenter à l'avenir. Les cyberattaques peuvent être internes ou externes à l'établissement et les motivations des attaquants peuvent être diverses, allant du vol financier à l'espionnage géostratégique et au sabotage en passant par le terrorisme et le militantisme. La capacité des cybercriminels à dissimuler l'attaque dans certains cas permet le détournement sur de longues périodes, la divulgation intentionnelle, la modification ou la destruction de données financières sensibles ou critiques.

Dans ces circonstances, il est difficile pour les établissements financiers et les IMF de protéger adéquatement leurs systèmes et services informatiques et leurs données électroniques contre les différentes attaques. Les cybermenaces évoluant très rapidement, il est plus important que jamais de veiller à ce que les capacités de défense des établissements et des IMF leur permettent de réagir avec souplesse à l'évolution des modes d'attaque. Des solutions pour recueillir des informations sur les menaces, les attaquants et les types d'attaques potentiels sont dans ce contexte essentielles. En outre, il est également utile pour les établissements financiers de connaître le profil de risque du client et/ou de la contrepartie pour déterminer le risque de fraude lié à certaines transactions.

Dans le cadre de la banque de détail, par exemple, cela se fait au moyen de mécanismes de sécurité intégrés dans l'application de services bancaires par internet ou sur dispositifs mobiles. Dans le cadre des activités des banques correspondantes, un exemple est le *Customer Security Programme* (CSP), mis en place par SWIFT pour faciliter l'évaluation du risque de contrepartie.

ENCADRÉ 17

Quelques exemples d'incidents et menaces de cyber-sécurité connus en 2018

Meltdown/Spectre: En janvier, des vulnérabilités spécifiques à la technique d'exécution spéculative ont été exposées, cette technique consistant en une optimisation du processeur qui est invariablement appliquée dans (tous) les processeurs modernes. Bien que les fabricants de puces aient, dans la mesure du possible, entre-temps mis à jour le microcode afin de limiter les possibilités d'exploitation de ces vulnérabilités, il est probable que seule une adaptation matérielle des futurs processeurs pourra à terme assurer une protection totale. Pour l'instant, aucun incident concret n'a été recensé dans le secteur financier qui soit basé sur l'exploitation de ces vulnérabilités.

Coincheck Inc: En janvier, il a été signalé que des fraudeurs avaient volé plus de 500 millions de cryptomonnaies XEM, la monnaie spécifique à la plate-forme blockchain NEM (*New Economy Movement*). Au moment des faits, les cryptomonnaies XEM volées représentaient environ 400 millions de dollars. Une plateforme d'échange pour ces cryptomonnaies, Coincheck, a été piratée.

Mexique: En mai, l'on a appris que plusieurs banques mexicaines avaient été victimes d'une cyberattaque. Les fraudeurs auraient crédité de faux comptes, après quoi des sommes importantes auraient été retirées en espèces. Les comptes des clients n'auraient pas été touchés par l'attaque. Selon les rapports, les fraudeurs ont réussi à abuser de modules de logiciels mis au point par les banques ou des tiers qui permettent d'effectuer des transactions via un système de paiement interbancaire mexicain local. Le système de paiement interbancaire local lui-même n'a pas été compromis: seuls les points d'accès à ce réseau dans les établissements individuels ont été touchés.

Supermicro: En octobre, les médias se sont largement fait l'écho de la manipulation possible des cartes mères Supermicro pendant le processus de production, ce qui rendrait ces composants matériels vulnérables à l'espionnage. Comme ces cartes-mères sont utilisées dans le monde entier dans des infrastructures de serveurs, l'impact était potentiellement énorme. Toutefois, après enquête, Supermicro a déclaré qu'aucune preuve n'avait été trouvée par rapport aux allégations précédemment dévoilées par les médias de par le monde. Ces divulgations ont néanmoins attiré l'attention sur le danger de cyberattaques via les fournisseurs de matériel, de logiciels et de services informatiques. Plus tôt en 2018, les autorités américaines et britanniques avaient explicitement mis en garde contre le danger que représente ce type d'attaque.

Outre le cyber-risque, la forte dépendance à l'égard des solutions informatiques dans le secteur financier présente également d'autres défis. Les établissements traditionnels sont incités, sous la pression d'acteurs innovants, des nouvelles technologies, des attentes des clients ou des risques de sécurité croissants, à renouveler leurs architectures informatiques parfois fort vieillissantes, mais la complexité de leur environnement informatique rend cet objectif difficile à réaliser à court terme de manière responsable, c'est-à-dire sans prendre de risques disproportionnés. Il existe également un risque important de dépendance croissante à l'égard de tiers pour les services informatiques et de composants de systèmes informatiques standardisés. En particulier, les solutions de *cloud* sont de plus en plus utilisées pour des processus de plus en plus importants. La nécessité de soumettre les solutions de récupération après incident, qui doivent garantir la continuité, à des tests suffisamment représentatifs reste également un point d'attention important.

Il est crucial de veiller à ce que le secteur financier puisse réagir avec souplesse à l'évolution des cybermenaces

Il importe donc que les organes d'administration des acteurs financiers disposent de l'expertise et des informations nécessaires pour être en mesure de surveiller les risques de manière appropriée et de les maintenir dans des limites acceptables. En outre, tous les collaborateurs de ces entreprises doivent être conscients des cyber-risques et des risques informatiques, afin de comprendre comment ces risques peuvent survenir et de quelle manière il leur est demandé de réagir.

L'évaluation et la promotion de la maîtrise des cyber-risques et des risques informatiques constituent également des priorités absolues pour le contrôle prudentiel et *l'oversight* des établissements financiers et des IMF, la coopération européenne et internationale y prenant une importance croissante. Au niveau des établissements individuels, il est vivement recommandé de renforcer encore les mesures et les efforts de protection contre les risques informatiques et cybernétiques. L'attention nécessaire est accordée par ailleurs aux stratégies de maîtrise intersectorielles en cours d'élaboration en Belgique et à l'étranger. Ces deux aspects sont exposés plus en détail dans les paragraphes qui suivent.

5.2 Lignes directrices en matière de résilience aux cyber-risques

Au cours des dernières années, la Banque a contribué dans une large mesure à l'élaboration d'un cadre réglementaire visant à améliorer la maîtrise des cyber-risques et des risques informatiques. Le 1er janvier 2016, la circulaire prudentielle[1] relative aux attentes de la Banque en matière de continuité et de sécurité opérationnelles des établissements financiers d'importance systémique est entrée en vigueur. En outre, la Banque a activement contribué à la mise en place d'un cadre réglementaire européen pour la gestion des cyber-risques et des risques informatiques sous les auspices de l'EBA. Cela a conduit d'une part à la publication des orientations de l'EBA à l'intention des autorités de contrôle sur l'évaluation du risque lié aux TIC dans le cadre du processus de contrôle et d'évaluation prudentiels (*Supervisory Review and Evaluation process*, SREP) pour les établissements de crédit et les entreprises d'investissement[2], qui sont entrées en vigueur le 1e janvier 2018. D'autre part, cela s'est traduit par des recommandations de l'EBA pour l'externalisation (*outsourcing*) par les établissements financiers aux fournisseurs de services de *cloud*[3]. Plusieurs normes, orientations et recommandations techniques ont également été publiées par l'EBA dans le cadre de la deuxième directive européenne sur les services de paiement (PSD2), couvrant les aspects cyber et informatiques. L'EBA prépare par ailleurs des orientations sur l'externalisation en général et sur la gestion des risques liés aux TIC et des risques en matière de sécurité.

Plusieurs initiatives ont été prises à cet égard pour les IMF également. En juin 2016, le Comité sur les paiements et les infrastructures de marché (*Committee on Payments and Market Infrastructures*, CPMI) et l'Organisation internationale des commissions de valeurs (*International Organization of Securities Commissions*, IOSCO) ont publié des lignes directrices sur la cyber-résilience[4], qui sont immédiatement applicables aux IMF. Sur la base de ces lignes directrices, l'Eurosystème a élaboré au cours de l'année sous revue les *Cyber Resilience Oversight Expectations* (CROE), qui ont été finalisées en décembre 2018 après un cycle de consultation publique. En mai 2018, le CPMI a publié une stratégie[5] visant à réduire le risque de fraude dans les paiements de gros. Cette stratégie propose des mesures de prévention, de détection et de remédiation de la fraude et souligne la nécessité d'une communication adéquate en la matière de la part de l'ensemble des acteurs concernés des secteurs public et privé. En sa qualité de coprésidente du groupe de travail au sein du CPMI, la Banque a apporté une contribution significative à cette stratégie. La Banque, à l'instar des autres banques centrales membres, travaille également à la mise en œuvre de cette stratégie.

5.3 Activités opérationnelles

Les cyber-risques et les risques informatiques constituent pour la Banque un point d'attention dans le cadre de son contrôle prudentiel et de son *oversight*. Dans ce domaine, elle s'intéresse, d'une part, à la sécurisation des établissements financiers et des IMF individuels et à la confiance qu'ils inspirent, et, d'autre part, au secteur dans son ensemble. L'approche pour les établissements individuels est double. D'une part, les établissements doivent détenir des fonds propres pour couvrir leurs risques opérationnels, qui comprennent les cyber-risques et les risques informatiques. D'autre part, la sécurité opérationnelle et la robustesse des processus critiques des établissements financiers et des IMF font l'objet d'un suivi soutenu. La disponibilité, l'intégrité et la confidentialité des systèmes informatiques et des données sont à cet égard essentielles. La Banque a effectué plusieurs missions d'inspection en 2018 (pour les banques relevant du SSM) afin de vérifier le respect du cadre réglementaire et la gestion adéquate des systèmes informatiques en matière de cyber-risques et de risques informatiques. Par ailleurs, la Banque surveille ces risques auprès des établissements financiers et des IMF dans le cadre de ses activités de contrôle permanentes et récurrentes.

La Banque accorde également une attention croissante aux initiatives sectorielles. Ainsi, le SSM effectue régulièrement des analyses transversales sur des sujets liés à l'informatique et aux aspects cybernétiques. Il a par exemple été demandé en 2018 à toutes les banques importantes ainsi qu'aux plus grandes

1 Circulaire NBB_2015_32 du 18 décembre 2015 relative aux attentes prudentielles complémentaires en matière de continuité et de sécurité opérationnelles des établissements financiers d'importance systémique.

2 Orientations de l'EBA sur l'évaluation du risque lié aux TIC dans le cadre du processus de contrôle et d'évaluation prudentiels (SREP), mai 2017.

3 Recommandations de l'EBA sur l'externalisation vers des fournisseurs de services en nuage (cloud services), décembre 2017.

4 CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures, juin 2016.

5 Reducing the risk of wholesale payments fraud related to endpoint security (https//www.bis.org/cpmi/publ/d178.htm).

banques moins importantes de répondre à un questionnaire qui doit fournir, pour les aspects informatiques, des renseignements importants pour le SREP annuel, et qui permettra par ailleurs de procéder à des analyses transversales.

Dans son rôle d'autorité sectorielle pour l'application de la loi sur la sécurité et la protection des infrastructures critiques (principalement les banques et les IMF), la Banque évalue également l'efficacité des systèmes de contrôle de ces infrastructures, organise des exercices sectoriels et coordonne les incidents opérationnels ayant un caractère systémique pour le secteur financier belge.

Afin de mettre en œuvre la recommandation du *High Level Expert Group* (HLEG) sur l'avenir du secteur financier belge d'accorder suffisamment d'attention à la cybersécurité, le *Financial Sector Cyber advisory Council* (FSCC) a été constitué, sous la présidence de la Banque. Il est composé de représentants du Centre pour la Cybersécurité Belgique, de Febelfin, d'Assuralia et du secteur financier. Le FSCC s'efforce d'accroître la cyber-résistance du secteur financier belge en procédant à une série d'initiatives.

La Banque a mis en place un cadre pour le piratage éthique

Une réalisation concrète à cet égard est la mise en place d'un cadre pour le piratage éthique par la Banque, à savoir TIBER-BE (*Threat Intelligence-Based Ethical Red Teaming Belgium*). Ce programme constitue la partie belge d'une méthodologie qui a été élaborée par l'Eurosystème et vise à accroître la cyber-résistance des établissements financiers et des IMF individuels au moyen de tests sophistiqués, et à fournir des observations importantes sur la cybersécurité du secteur financier belge dans son ensemble. La Banque encourage ces exercices en sa qualité de gardienne de la stabilité financière, et ces tests s'opèrent dès lors indépendamment de ses compétences en matière de contrôle prudentiel et *d'oversight*.

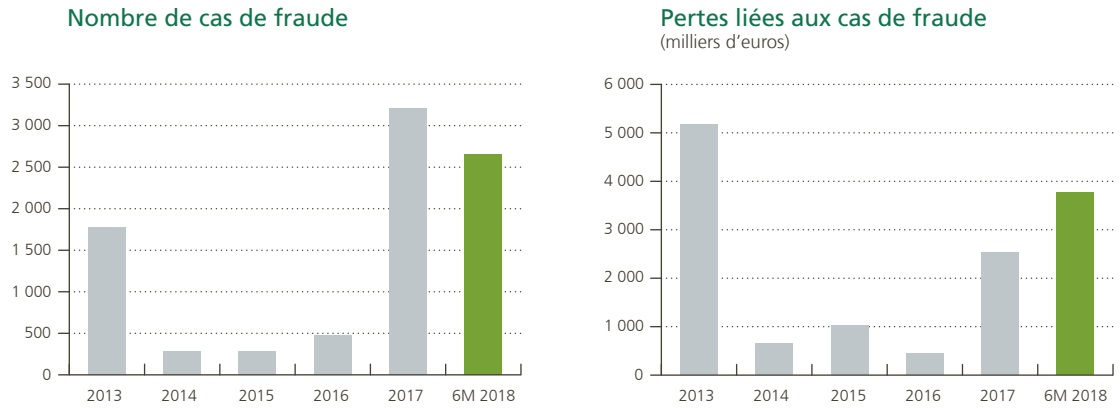
5.4 Fraude dans les services bancaires par internet

En 2018, l'étroite collaboration avec Febelfin, entre autres, s'est poursuivie afin de recenser les fraudes en *e-banking* et de sensibiliser les consommateurs. La nette tendance à la hausse du nombre de cas de fraudes en *e-banking* observée en 2017, et des pertes financières qui en résultent, s'est confirmée au premier semestre de 2018.

Tout comme les années précédentes, les cas de fraude en *e-banking* signalés en 2018 par les particuliers étaient presque exclusivement le résultat de

Graphique 102

Fraude en *e-banking*



Source : Febelfin.

techniques frauduleuses par lesquelles des cybercriminels trompent les utilisateurs d'*e-banking* afin d'obtenir leurs codes de sécurité personnels (généralement après un contact téléphonique ou via un site Internet factice). L'augmentation des cas de fraude en 2017 et 2018 est donc due à une augmentation du nombre d'attaques plutôt qu'à l'utilisation de techniques de fraude innovantes. Dans ce contexte, la Banque suit également de près l'évolution des risques liés à l'entrée en vigueur de la directive PSD2.

6. Évolutions en matière de gouvernance et mission de collaboration des réviseurs au contrôle prudentiel

Expertise des responsables de la fonction de *compliance*

Le rapport de 2016 du *High Level Expert Group* (HLEG) sur l'avenir du secteur financier belge contenait une série de recommandations relatives au renforcement de la gouvernance dans les établissements financiers. Elles avaient déjà débouché en 2017 sur des modifications apportées aux différentes lois sectorielles, notamment pour permettre à la Banque d'imposer aux responsables de la fonction de *compliance* les mêmes exigences d'expertise que celles déjà appliquées par la FSMA. Par conséquent, en 2018, la Banque et la FSMA ont élaboré une approche commune afin de mieux harmoniser les exigences des deux autorités de contrôle en ce qui concerne l'évaluation de l'expertise des responsables de la fonction de *compliance*. Ces exigences ont été fixées dans un règlement de la Banque[1].

La principale nouveauté concerne la réussite, par le candidat responsable de la fonction de *compliance*, d'un examen passé dans un centre de formation reconnu par la Banque et la FSMA. À cet égard, ces deux autorités ont publié, le 18 mai 2018, une communication conjointe[2] fixant les modalités selon lesquelles les établissements qui souhaitent organiser des examens doivent adresser la demande de reconnaissance aux deux autorités de contrôle. La demande de reconnaissance doit comporter les éléments permettant de vérifier que les épreuves remplissent toutes les conditions de reconnaissance (contenu des questions, composition et méthodologie travail du jury, organisation pratique, etc.).

Désormais, les responsables de la fonction de *compliance* et les autres personnes chargées de la fonction de *compliance* doivent également prendre part à un programme de formation permanente dans un

1 Règlement de la Banque du 6 février 2018 relatif à l'expertise des responsables de la fonction de *compliance*, approuvé par l'arrêté royal du 15 avril 2018 et entré en vigueur le 1er juin 2018.

2 Communication NBB_2018_19 du 18 mai 2018 concernant la demande d'agrément des examens en vue de l'exercice de la fonction de *compliance*.

établissement de formation reconnu par la FSMA sur l'avis de la Banque. À cet égard, la FSMA a publié le 8 mai 2018 une communication[1] précisant la portée de cette obligation de formation permanente, notamment en ce qui concerne la fréquence et le contenu des cours.

Renouvellement de l'agrément des réviseurs

Compte tenu de l'importance sociétale des établissements financiers et des entreprises d'assurance, la fonction de commissaire ne peut être confiée qu'à des réviseurs agréés à cet effet par la Banque. L'agrément d'un réviseur par la Banque est accordé pour une période de six ans sur la base du règlement d'agrément de la Banque du 21 décembre 2012[2]. Au plus tôt six mois et au plus tard trois mois avant l'expiration de l'agrément précédent, le réviseur agréé doit présenter d'initiative une demande de renouvellement de l'agrément pour une nouvelle période de six ans. Les premières demandes de renouvellement devraient parvenir à la Banque au cours du premier trimestre de 2019.

Dans ce contexte, la Banque a publié le 21 septembre 2018 une communication[3] expliquant la forme et le contenu de la demande de renouvellement de l'agrément. Cette communication recense les informations qu'un tel dossier doit contenir, notamment en ce qui concerne l'expérience acquise au cours des mandats auprès d'établissements soumis au contrôle (description des mandats, évaluation de la collaboration avec la Banque, plan d'approche pour l'avenir). L'objectif est d'obtenir des informations spécifiques en complément du dossier d'agrément, informations qui doivent permettre à la Banque de vérifier si les renseignements sont conformes au dossier qu'elle a constitué au fil des ans, dans le cadre d'un système d'évaluation annuelle de la qualité du fonctionnement du réviseur par mandat exercé dans un établissement soumis au contrôle. Conformément au règlement d'agrément, la Banque doit en effet justifier toute décision de refus de renouvellement d'agrément au regard des attentes sur le plan des exigences de compétence et d'efforts consentis dans l'accomplissement de la mission.

Suivi des recommandations parlementaires

Suite à la publication des recommandations des commissions parlementaires Optima[4] et Panama Papers[5], la Banque a pleinement collaboré à différentes initiatives sur le plan réglementaire, notamment en matière de transactions entre parties liées et de mécanismes particuliers.

L'adaptation du cadre légal en matière d'opérations entre parties liées a également été recommandée par le FMI dans le cadre du FSAP de 2017 (cf. chapitre A de la partie « Réglementation et contrôle prudentiels »), afin de se conformer aux Principes fondamentaux pour un contrôle bancaire efficace du Comité de Bâle (principe 20 – *transactions with related parties*). Les lois sectorielles prévoient déjà que les prêts, crédits ou garanties doivent être conclus aux conditions applicables à leur clientèle et doivent être notifiés à l'organe légal d'administration ainsi qu'à l'autorité de contrôle[6]. Afin de mettre en œuvre les recommandations, un amendement à ce régime a été préparé, qui prévoit une extension tant du champ d'application matériel (toutes les transactions entre parties liées) que du champ d'application personnel (extension à toutes les transactions intragroupe, y compris les transactions avec les filiales et les sociétés sœurs).

Afin de mettre en œuvre les recommandations des deux commissions parlementaires sur la fraude fiscale (mécanismes particuliers), un groupe de travail composé de représentants du cabinet des Finances, du Trésor, de l'Inspection spéciale des impôts, de la FSMA et de la Banque a été créé.

Ce groupe de travail a travaillé sur trois sujets :

- adaptation du cadre légal relatif aux mécanismes particuliers, afin de les signaler plus facilement à la justice ;

1 FSMA_2018_05 communication du 8 mai 2018 sur la formation permanente des *compliance officers*.

2 Règlement de la Banque du 21 décembre 2012 concernant l'agrément des réviseurs et des sociétés de réviseurs.

3 Communication NBB_2018_26 du 21 septembre 2018 concernant le renouvellement de l'agrément des réviseurs.

4 Le 7 juillet 2016, une commission d'enquête parlementaire a été constituée et a publié, le 28 juin 2017, un rapport sur la faillite d'Optima Banque : voir à ce propos « Enquête parlementaire chargée d'examiner les causes de la faillite de la banque Optima et l'éventuelle confusion d'intérêts entre le Groupe Optima et ses composantes, d'une part, et des administrations publiques, d'autre part », Doc. parl. Chambre, 2016-2017, Doc. 54 1938/007.

5 Le 21 avril 2016, une Commission spéciale « Fraude fiscale internationale/*Panama Papers* » a été constituée qui a publié son rapport le 31 octobre 2017 : voir : « Les *Panama Papers* et la fraude fiscale internationale », Doc. parl. Chambre, 2016-2017, Doc. 54 2749/001.

6 Voir l'article 72 de la loi bancaire et l'article 93 de la loi Solvabilité II.

- mise à jour des listes des mécanismes particuliers, avec examen des mécanismes pouvant être supprimés des circulaires existantes[1], de ceux devant éventuellement être reformulés, et de ceux devant être ajoutés ; et
- conclusion d'un accord de collaboration avec l'Inspection spéciale des impôts afin de pouvoir transmettre à la Banque et à la FSMA des informations utiles dans le cadre du contrôle d'un établissement financier.

Aptitude des administrateurs et des autres personnes revêtant des fonctions clés

La législation prudentielle prescrit que les administrateurs, les membres du comité de direction, les responsables des fonctions de contrôle indépendantes et les dirigeants effectifs des établissements financiers possèdent l'expertise et l'honorabilité professionnelle requises pour leur fonction. L'évaluation de l'aptitude de ces personnes est souvent décrite comme l'évaluation de leur caractère « *fit and proper* ».

Dans le sillage de la crise financière, la question de « l'aptitude » constitue depuis plusieurs années une priorité et a donné lieu à la publication d'une série de règles, d'orientations et recommandations nouvelles aux niveaux international, européen et national.

Ainsi, le 26 septembre 2017, l'EBA et l'ESMA ont publié des orientations communes sur l'évaluation de l'aptitude des membres d'organe de direction et des titulaires de postes clés[2]. La BCE a elle aussi publié récemment son Guide SSM relatif à l'évaluation de l'honorabilité et de la compétence[3]. Dans le secteur de l'assurance, les orientations de l'EIOPA sur le système de gouvernance[4] fournissent quant à elles un cadre de référence pour l'évaluation de l'aptitude tant individuelle que collective des dirigeants et des responsables des fonctions de contrôle indépendantes au sein des entreprises d'assurance.

Compte tenu du nombre croissant de règles et d'orientations en la matière, une mise à jour et une certaine forme de codification étaient nécessaires afin de maintenir une bonne vue d'ensemble du cadre applicable. En conséquence, la Banque a publié le 18 septembre 2018 une nouvelle circulaire « *fit & proper* »[5], qui visait à créer un manuel « *fit & proper* » ainsi qu'à transposer dans le cadre prudentiel belge les orientations de l'EBA et de l'EIOPA précitées.

L'objectif du manuel « *fit & proper* » est de fournir un relevé de l'ensemble des documents de réglementation et de politique applicables en la matière, et de fournir les précisions nécessaires. En outre, le manuel contient des explications sur des thèmes qui ne font pas en tant que tels l'objet de documents de politique spécifiques. Le manuel combine une approche intersectorielle avec du texte et des références spécifiques aux différents secteurs : lorsque le manuel et ses principes de base sont applicables à tous les établissements financiers soumis au contrôle de la Banque, les textes juridiques et politiques pertinents applicables aux différents types d'établissements financiers sont précisés.

La question de l'aptitude (fit & proper) constitue depuis plusieurs années une priorité aux niveaux national et international

Sur le plan du contenu, le manuel s'appuie sur les lignes directrices énoncées dans la circulaire « *fit & proper* » de 2013, qui a été abrogée avec l'introduction du manuel. En outre, une série de sujets ont été développés ou mis en avant. Ainsi, la responsabilité primaire des établissements dans l'évaluation de l'aptitude a été davantage soulignée, et les chapitres concernant l'aptitude collective, le caractère continu de l'évaluation de l'aptitude (et, si nécessaire dès lors, la réévaluation de la personne concernée), ainsi que le temps nécessaire à consacrer à l'exercice de la fonction d'administrateur ont été développés. Le manuel met également en lumière une série de nouveautés en matière d'expertise, notamment le règlement de la Banque relatif à l'expertise des responsables de la fonction de *compliance*[6] (voir ci-dessus). En ce qui concerne l'honorabilité professionnelle,

1 Il s'agit plus particulièrement de deux circulaires du 18 décembre 1997, à savoir les circulaires D1 97/9 aux établissements de crédit et D4 97/4 aux entreprises d'investissement, et de la communication D.207 du 30 novembre 2001 aux entreprises d'assurance.

2 Orientations EBA/GL/2017/12 du 26 septembre 2017 sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés. Ces orientations remplacent à partir du 30 juin 2018 les orientations EBA GL 2012/06 du 22 novembre 2012.

3 Guide SSM relatif à l'évaluation de l'honorabilité et de la compétence, mai 2018.

4 Orientations de l'EIOPA sur le système de gouvernance du 14 septembre 2015, en particulier les orientations 11 à 14.

5 Circulaire NBB_2018_25 du 18 septembre 2018 sur l'aptitude des administrateurs, membres du comité de direction, responsables de fonctions de contrôle indépendantes et dirigeants effectifs d'établissements financiers.

6 Arrêté royal du 15 avril 2018 portant approbation du règlement de la Banque nationale de Belgique du 6 février 2018 relatif à l'expertise des responsables de la fonction de *compliance*.

le manuel indique désormais explicitement que le manque de transparence vis-à-vis de l'autorité de contrôle, ainsi que les infractions à la législation préventive contre le blanchiment de capitaux, à la législation sur la protection des consommateurs et à la législation fiscale, constituent des éléments qui sont pris en compte pour évaluer l'aptitude de la personne concernée.

Spécifiquement pour le secteur bancaire, le manuel aborde certaines particularités liées aux orientations de l'EBA et à la surveillance du SSM. Ainsi, dans le manuel, les exigences relatives au nombre d'années d'expérience professionnelle pertinente pour les administrateurs d'établissements importants soumis à la surveillance de la BCE sont alignées sur les seuils définis dans le Guide SSM. Par ailleurs, les décisions en matière d'aptitude relevant de la compétence de la BCE font l'objet de délais légèrement plus longs, conformes à la pratique actuelle. Enfin, le chapitre sur l'indépendance des administrateurs et la gestion des conflits d'intérêts clarifie la manière dont les dispositions en la matière prévues par la loi bancaire s'articulent par rapport au prescrit des orientations de l'EBA.

S'agissant du secteur de l'assurance et de la réassurance, les normes en matière d'expertise et d'honorabilité de 2013 ont été globalement maintenues dans le nouveau manuel. Néanmoins, un ensemble d'éléments, notamment liés au régime Solvabilité II, ont été ajoutés : (i) l'obligation de développer une politique « *fit & proper* », (ii) l'explicitation des connaissances théoriques de base attendues dans le domaine de l'assurance et de la réassurance, (iii) l'énonciation de normes spécifiques en matière d'expertise attendue des responsables de fonctions de contrôle indépendantes, (iv) la définition de normes d'expertise à respecter pour la « personne-relais » à désigner au sein de l'entreprise en cas de sous-traitance d'une fonction de contrôle indépendante, et (v) la recommandation d'avoir, dans les conglomérats financiers au sein desquels se nouent des relations d'affaires significatives entre la banque et l'entreprise d'assurance, au sein du conseil d'administration de l'entreprise d'assurance, un administrateur indépendant au sens de l'article 526ter du Code des sociétés qui ne siège pas au conseil d'administration de la banque et de l'entité-mère. En outre, les règles suivies par la Banque dans le cadre de son évaluation d'aptitude ont également été revues (interview « *fit & proper* », modalisation des décisions de la Banque, etc.).

Ce manuel étant en principe un document évolutif, publié par ailleurs en ligne, il sera régulièrement adapté aux nouvelles évolutions en la matière, de sorte que les établissements continueront à disposer à l'avenir d'un relevé actualisé du cadre prudentiel dans ce domaine.

7. Brexit

À la suite du référendum relatif à sa sortie de l'UE, le Royaume-Uni avait amorcé le 29 mars 2017 une procédure, prévue à l'article 50 du traité de l'Union, en vue de se retirer de l'Union et de devenir par conséquent un « État tiers ». À moins qu'un accord spécifique ne précise une autre date, l'ensemble du cadre réglementaire de l'UE cessera de s'appliquer au Royaume-Uni à partir du 30 mars 2019. Les établissements financiers risquent notamment de perdre leur passeport européen qui leur a permis jusqu'ici de fournir librement leurs prestations sur chaque territoire.

Depuis mai 2017, l'UE et le Royaume-Uni négocient un accord sur leur séparation afin d'éviter les conséquences graves qu'entraînerait un brexit désordonné (« hard brexit »). Un tel scénario fait peser une grande incertitude juridique sur les relations d'affaires en cours et risque de provoquer une interruption soudaine des services, qui aura des répercussions importantes sur les activités économiques. Les deux parties se sont engagées à parvenir à un accord, mais des divergences matérielles dans les deux camps pourraient empêcher qu'un accord soit conclu. L'accord, s'il est ratifié, pourrait comprendre une période de transition jusqu'au 31 décembre 2020.

Au vu des incertitudes susvisées, la Commission européenne a rappelé à toutes les parties concernées l'importance de se préparer à un scénario de « hard Brexit » qui pourrait se matérialiser dès mars 2019. Les autorités de surveillance européennes ainsi que la BCE ont, dans ce contexte, émis des avis et clarifié leurs attentes auprès du secteur financier. La Banque a à maintes reprises sensibilisé les établissements financiers belges aux risques qui résulteraient d'un scénario de « hard brexit », par la référence aux opinions publiées par l'EBA, par des enquêtes auprès du secteur et par des actions prudentielles vis-à-vis des établissements concernés.

Afin de garantir la continuité de leurs activités, les institutions financières peuvent être amenées à demander un nouvel agrément aux autorités nationales

compétentes, à modifier certaines clauses de leurs contrats ou à transférer certaines activités.

La Banque observe que, dans l'ensemble, le niveau des expositions du secteur financier belge à des contreparties britanniques est relativement limité. À la fin de juin 2018, ces expositions s'élevaient à 39 milliards d'euros pour les banques belges, soit 4 % du total de leurs actifs, et à 6 milliards d'euros, pour les entreprises d'assurance belges, ce qui correspond à 2 % de leurs investissements.

L'impact potentiel d'un « hard brexit » ne se limite toutefois pas aux expositions directes et dépend tant de la nature des activités de l'entreprise que du niveau de préparation requis, qui varie d'un établissement à l'autre.

Même s'ils ne fournissent pas directement des services à des clients sur le sol britannique, de nombreux établissements risquent d'être affectés par la voie de contrats conclus avec des contreparties britanniques. Il existe par exemple une incertitude juridique par rapport à la possibilité d'exécuter des modifications ou d'exercer certaines options dans le cadre de contrats dérivés de gré à gré existants non traités par une chambre de compensation (*central counterparty*, CCP). Pour réduire ce risque, les établissements devraient vérifier dans quels cas des autorisations doivent être obtenues auprès d'autorités nationales compétentes (respectivement la FSMA en Belgique et la Financial Conduct Authority au Royaume-Uni). Par ailleurs, des obligations émises par des établissements bancaires belges mais régies par le droit britannique, pourraient ne plus être éligibles au renflouement interne (*bail-in*), ce qui demanderait d'apporter certaines modifications aux clauses des contrats d'émission.

Même si le niveau des expositions directes du secteur financier belge est relativement limité, les défis, liés notamment à un « hard brexit », demandent une vigilance accrue

Les CCP britanniques jouent un rôle critique pour le marché financier européen. En effet, ces organismes procèdent à la compensation de plus de 90 % des

transactions de produits dérivés de taux d'intérêt en Europe. Actuellement, les CCP britanniques sont soumises au règlement européen sur les produits dérivés de gré à gré (European Market Infrastructure Regulation, EMIR). Elles risquent de perdre leur autorisation à effectuer la compensation de ces produits en Europe. L'interruption massive et soudaine des services de compensation des CCP britanniques pourrait provoquer une instabilité importante sur les marchés financiers. Afin de réduire la dépendance des établissements financiers européens aux CCP britanniques, les autorités européennes les encouragent à établir un accès auprès de CCP établies dans l'Union européenne, hors Royaume-Uni. Pour éviter des perturbations importantes sur les activités en cours, la Commission va toutefois octroyer une extension d'autorisation temporaire aux CCP britanniques. En vue de mieux encadrer les activités des CCP d'importance systémique établies dans des pays tiers, y compris, après le brexit, au Royaume-Uni, la Commission européenne envisage de conférer, dans le cadre de l'adaptation du règlement EMIR, un pouvoir accru de supervision de ces entités à l'Autorité européenne des marchés financiers.

Une série de banques belges fournissent des services bancaires au Royaume-Uni. La Banque leur a demandé de prendre contact avec les autorités britanniques en vue d'assurer la continuité de ces activités. Elles doivent également informer à temps leurs clients, notamment en cas de modification ou de cessation des services.

De même, afin d'assurer la continuité de leurs engagements envers leurs clients britanniques, certaines entreprises d'assurance belges doivent établir une succursale ou une filiale britannique. La création d'une telle entité est soumise à l'agrément des autorités britanniques et à la non-objection de la Banque.

Dans la foulée du brexit, les entreprises d'assurance britanniques risquent d'être déchues du droit d'offrir des protections aux clients de l'Espace économique européen (EEE). Dans ce contexte, plusieurs compagnies d'assurances britanniques ont déjà commencé à établir des filiales en Belgique. En s'établissant en Belgique, elles pourront également exercer leurs activités dans d'autres pays de l'Espace économique européen, soit en libre prestation de services, soit par le biais de succursales. De plus, les compagnies d'assurances doivent veiller à être encore en mesure de dédommager les contrats d'assurance existants souscrits par des clients de l'UE. Nombre d'entre elles ont déjà entrepris des actions pour transférer leurs contrats vers une entité établie dans l'UE. Cette procédure prend du temps car elle nécessite non seulement l'approbation des autorités de contrôle prudentiel nationales dans l'UE et au Royaume-Uni, mais aussi l'approbation de la Cour de justice britannique.

Il en va de même pour les établissements de paiement, les établissements de monnaie électronique et les entreprises d'investissement britanniques, qui perdront leur passeport, nécessaire à la poursuite de leurs activités auprès de leurs clients dans l'UE. Pour garantir la continuité de leurs services en Belgique/dans l'UE, une série d'établissements ont introduit ou envisagent d'introduire des dossiers d'agrément auprès de la Banque.

Les équipes du contrôle prudentiel de la Banque ont mené de nombreux dialogues avec les établissements financiers belges. Il apparaît que ceux-ci ont bien progressé dans l'identification des risques et dans la préparation aux conséquences potentielles d'un « hard brexit ». La Banque est également en discussion avec des établissements qui envisagent de modifier leur structure ou souhaitent établir une succursale ou une filiale en Belgique pour offrir des services aux clients de l'UE.