DONNER
VIE AUX
POLITIQUS
INTELLIGE
NTES

CYBER-SÉCURITÉ POUR L'INCLUSION FINANCIÈRE : CADRE ET GUIDE DES RISQUES

Note sur la directive no. 37
Octobre 2019

NOTE SUR LA DIRECTIVE

SOMMAIRE

REMERCIEMENTS

L'AIF remercie le président du sous-groupe sur la cyber-sécurité, Komitas Stepanyan, de la Banque centrale d'Arménie, pour son excellent leadership. Nous tenons également à remercier les pays membres suivants qui ont contribué à ce travail : Bank of Ghana ; Bank Al-Maghrib ; Central Bank of Nigeria ; Bank of Namibia ; Central Bank of Sudan, et Reserve Bank Fiji. L'AIF remercie également Paul Makin pour avoir aidé le sous-groupe à effectuer les recherches nécessaires et à rédiger le document.

L'AIF remercie également les partenaires privés, les experts et les parties prenantes qui ont contribué à l'élaboration de ce document. Parmi eux figurent la Banque centrale européenne, GSMA, Mastercard, Visa, le FMI, l'UIT, le CGAP et le Forum économique mondial.

Ali Ghiyazuddin Mohammad et Kennedy Komba, de l'unité de gestion de l'AIF, ont également apporté des contributions et des commentaires précieux concernant les cadre.

Le secteur des services financiers numériques est soutenu par les partenaires financiers de l'AIF.

1 INTRODUCTION

1.1 CONTEXTE

Ces dernières années, les régulateurs et les superviseurs du secteur financier sont devenus de plus en plus conscients du fait que les services financiers destinés à favoriser l'inclusion financière (IF) dans le monde entier deviennent vulnérables aux cyber-menaces, principalement en raison du rôle croissant des services numériques (y compris les technologies mobiles et autres) dans la prestation de services financiers.

Avec la numérisation croissante des services financiers, le volume de données numériques sensibles augmente de façon exponentielle, avec comme impact, des violations croissantes de données concernant les personnes et les systèmes. Ainsi, la nécessité de mettre en place des mesures
de protection contre l'accès illicite à ces données devient de plus en plus important.

Dans le cadre de mise en œuvre de leur rôle de facilitateur et de coordinateur pour l'amélioration de l'inclusion financière à l'aide des services financiers numériques ciblant les consommateurs sous-bancarisés et non avertis, les membres de l'AIF ont compris qu'ils avaient besoin d'orientations spécifiques pour faire face aux risques de cyber-sécurité du côté de la demande. Des solutions du côté de l'offre sont également nécessaires, qui mettent l'accent sur les particularités des services financiers ayant comme cible le segment inférieur de la pyramide. À cet égard, le groupe de travail de l'AIF sur les services financiers numériques (SFN) a mis en place un sous-groupe sur la cybersécurité afin d'évaluer les risques liés à la cyber-sécurité à la lumière des technologies numériques et des innovations de la FinTech. En outre, le sous-groupe fournira également des recommandations stratégiques pour surveiller, identifier, gérer et atténuer les risques liés à la cyber-sécurité, y compris l'élaboration d'un guide des risques liés à la cyber-sécurité, c'est-à-dire le présent document.

1.2 GUIDE DES RISQUES LIÉS A LA CYBER-SÉCURITÉ

1.2.1 OBJECTIF

L'objectif principal de ce document est de fournir des principes clés et des bonnes pratiques qui aideront les autorités de surveillance à concevoir des outils permettant au secteur financier de faire face aux risques liés à la cyber-sécurité. Le guide est également utile pour les prestataires de services financiers. Il leur permet de renforcer leur gestion des cyber-risques pour la prestation de services financiers qui ciblent les consommateurs mal desservis du dernier kilomètre, au bas de la pyramide.

1.2.2 MÉTHODOLOGIE

L'élaboration du présent guide des risques s'est inspirée des éléments suivants :

- Entretiens avec des parties prenantes, notamment des membres de l'AIF actifs dans le domaine de la cyber-sécurité, des systèmes de paiement internationaux, des autorités de régulation supranationales, des concepteurs d'autres cadres de cyber-sécurité et des experts indépendants du secteur.
- Méta-analyse des cadres existants, avec un accent particulier sur ceux mis en avant par les parties prenantes.
- Développement d'un modèle générique de paiements numériques et de services financiers avec une composante importante d'inclusion financière.
- Élaboration d'un ensemble de recommandations à l'usage des régulateurs pour l'élaboration d'une politique de cyber-sécurité.

2 MODÈLE DE PAIEMENTS NUMÉRIQUES ET DE SERVICES FINANCIERS

Les services financiers comportant un élément important d'inclusion financière diffèrent des services financiers traditionnels dans un certain nombre de domaines clés, notamment :

- **Segment clients :** les services sont offerts à des segments de la population jusqu'ici non desservis ou mal desservis, qui effectuaient auparavant la majorité de leurs transactions par des moyens informels.
- **Moyen de transaction :** il s'agit généralement d'une technologie lourde impliquant des transactions en libre-service ou assistées par un agent, effectuées par le biais d'un dispositif numérique.
- **Canal** : les transactions sont effectuées soit par l'intermédiaire d'agents, soit directement par un canal électronique tel qu'un téléphone portable.
- **Caractéristiques des segments d'utilisateurs :** nombre d'entre eux sont des clients à faible revenu dont les connaissances numériques ou financières sont limitées (bien qu'il soit admis qu'il serait très simplificateur de caractériser tous les clients de cette manière, il est important de comprendre que cela s'applique à une proportion significative).
- **Transactions :** elles sont généralement de faible valeur et de faible volume par client - les services clients cherchent généralement à compenser cela en essayant d'atteindre un volume global élevé pour l'ensemble du service.

Par conséquent, les risques de cyber-sécurité auxquels ces services sont confrontés sont quelque peu différents, reflétant les différentes possibilités d'attaque et les possibilités limitées de défense disponibles. Outre les risques directement pris en compte par les principaux cadres de cyber-sécurité élaborés et appliqués avec succès dans le monde industrialisé, il existe des catégories de risques très spécifiques que ces cadres ne prennent pas en compte, compte tenu du contexte dans lequel ils ont été élaborés. Ces cadres n'intègrent généralement pas les considérations relatives à l'inclusion financière.
Les risques mentionnés ici sont examinés en détail à la section 3, ainsi que les stratégies d'atténuation.

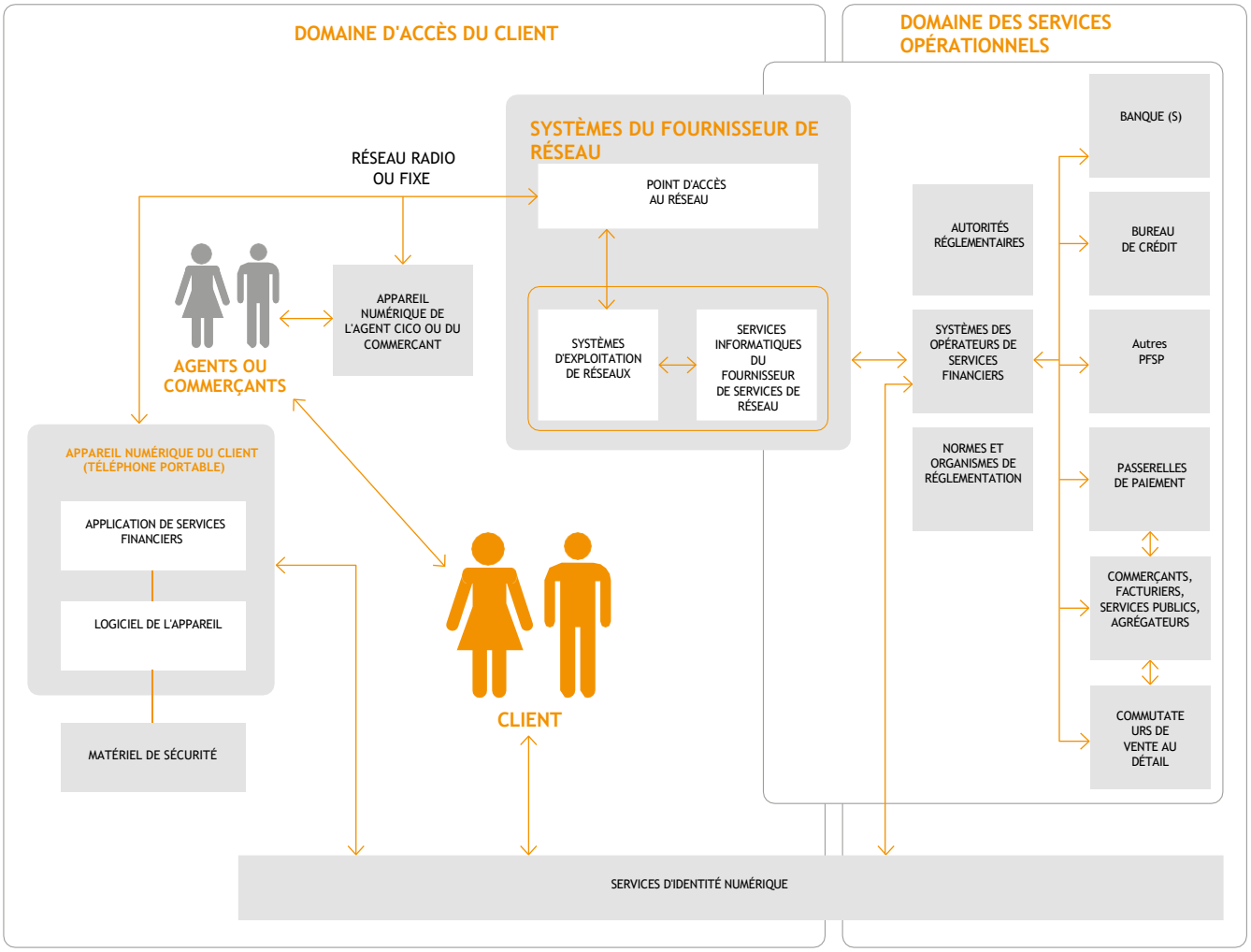
Pour comprendre ces risques supplémentaires, il est important de disposer d'un modèle ou d'un cadre qui serve à la fois de référence et de moyen de classification. Cette section présente donc un modèle de service abstrait pour un service financier destiné partiellement ou totalement aux personnes mal desservies. Ce modèle est destiné à servir deux objectifs principaux :

- Promouvoir une compréhension commune de ce qu'est un service - y compris l' " écosystème de services " dans lequel il opère ;
- Servir de point de référence pour les recommandations elles-mêmes, en donnant un contexte à chaque élément.

Le diagramme de la figure 1 présente le modèle de service utilisé dans l'analyse du risques de cyber-sécurité liés à l'inclusion financière.

Le modèle, qui est présenté du point de vue du consommateur, illustre la gamme d'acteurs impliqués dans la fourniture de services et les divers moyens d'interconnexion et d'interaction entre eux. Il a été légèrement résumé afin de mettre en évidence les éléments et les relations qui inter opèrent pour fournir un service financier comportant un élément important d'inclusion financière. En particulier, l'utilisation par un consommateur
d'un appareil numérique (tel qu'un téléphone mobile) ou d'un service OTC est supposé être une caractéristique d'un service qui soutient l'inclusion financière.

FIGURE 1 : MODÈLE DE PAIEMENTS ET DE SERVICES FINANCIERS NUMÉRIQUES



3 PRINCIPES DE LA CYBER-SÉCURITÉ

3.1 INTRODUCTION

Le présent guide présente sept principes clés de cyber-sécurité visant spécifiquement les initiatives d'inclusion financière.

- Deux principes sont destinés aux autorités de réglementation et de surveillance, pour leur permettre d'améliorer leurs cadres réglementaires, leurs approches réglementaires et leur collaboration en matière de questions liées à la cyber-sécurité des services financiers, avec une composante importante qui vise à relever les défis de l'inclusion financière.
- Les cinq autres principes définissent les exigences à imposer aux prestataires de services et visent à permettre aux autorités de régulation de bien mener leurs activités de supervision des prestataires de services.

3.2 PRINCIPES DESTINÉ S AUX RÉGULATEURS, DÉCIDEURS POLITIQUES ET AUTORITÉS DE SURVEILLANCE

La cyber-sécurité ne constitue pas un problème uniquement pour les fournisseurs de services. Les autorités de surveillance et de contrôle ont pour mission de garantir la sécurité des services et la protection des clients en respectant deux principes essentiels.

PRINCIPE I : RÉGLEMENTS ET CONFORMITÉ

Établir et maintenir les exigences réglementaires que les fournisseurs de services doivent respecter ; informer et aider les fournisseurs de services à se conformer à l'environnement réglementaire ; adapter les réglements à l'évolution de l'environnement ; appliquer des approches fondées sur des principes, et contrôler la sécurité des infrastructures publiques essentielles.

PRINCIPE II : COOPÉRATION

Veiller à ce que les mesures soient prises de concert avec les homologues internationaux, coopérer avec les multiples agences nationales actives dans le domaine de la cyber-sécurité, partager les informations sur les menaces et les incidents, et veiller à ce que les PSF disposent de ressources humaines suffisamment qualifiées pour faire face aux menaces liées à la cyber-sécurité.

3. 3 PRINCIPES DESTINÉS AUX PRESTATAIRES DE SERVICES

Ces principes imposent des exigences aux prestations de services financiers comportant un élément important d'inclusion financière, et visent à soutenir les régulateurs dans la supervision du respect de ces exigences par les prestataires de services :

PRINCIPE III : PROTECTION DES CLIENTS

Comprendre les capacités des clients de services financiers, les identifier, préserver la confidentialité de leurs données et veiller à leur identification effective en les accueillant et lors des transactions.

PRINCIPE IV : SÉCURISER LA FOURNITURE DES SERVICES

Comprendre les canaux de prestation de services et l'infrastructure qui sert d'interface entre les clients des PSF, et veiller à ce que les informations restent confidentielles et que l'intégrité des transactions soit maintenue.

PRINCIPE V : GESTION DES RISQUES INTERNES

Veiller à ce que l'intégrité des services des PSF soit préservée par des contrôles et des processus internes qui permettent une gestion efficace des risques à l'échelle de l'entreprise pour la fourniture de services sécurisés.

PRINCIPE VI : COMPRENDRE SES PARTENAIRES

Veiller à ce que les partenaires soient impliqués via un processus approprié sans augmenter de manière significative les risques pour les clients ou votre service.

PRINCIPE VII : LE LONG TERME

Veiller à ce que votre service maintienne sa sécurité face à l'émergence de nouvelles menaces ; que les autorités de régulation soient informées à la fois des risques existants et de vos plans pour y faire face ; effectuer régulièrement des audits, et veiller à ce que toutes les exigences en matière de rapports soient respectées, etc.

3.4 RÉGULATEURS

3.4.1 PRINCIPE 1 : RÉGLEMENTS ET CONFORMITÉ

Établir et maintenir les exigences réglementaires que les fournisseurs de services doivent respecter ; informer et aider les fournisseurs de services à se conformer à l'environnement réglementaire ; adapter les réglementations à l'évolution de l'environnement ; appliquer des approches fondées sur des principes et contrôler la sécurité des infrastructures publiques essentielles.

RÉFÉRENCE	RECOMMANDATIONS
R-1	Élaborer ou adopter un cadre de cyber-sécurité pour indiquer aux PSF ce que l'on attend d'eux. Ce cadre doit tenir compte de l'adéquation à la taille de l'établissement régulé et aux risques qu'il présente pour les clients.
R-2	Examiner les questions de responsabilité qui peuvent se poser si les normes de sécurité ne sont pas respectées par les PSF, en particulier si le non-respect de ces normes entraîne des pertes financières. Les questions à prendre en compte comprennent : > Communication obligatoire à l'autorité et aux clients concernés > Exigences de remboursement des pertes sur les comptes des clients > Responsabilités potentielles pour les pertes subies par les clients
R-3	Envisager d'autoriser des normes techniques de sécurité moins strictes (y compris, par exemple, l'USSD) en équilibrant le risque plus élevé avec une responsabilité plus stricte - voir également la recommandation C-10.
R-4	Élaborer une politique concernant les aspects pratiques de la mise en œuvre des procédures de contrôle, y compris l'élaboration ou l'adoption d'un cadre d'évaluation de la cyber-sécurité.
R-5	Mettre particulièrement l'accent sur l'évaluation de la qualité, de la disponibilité et des mécanismes de surveillance continue des transactions par les PSF. Ceci particulièrement dans le contexte du risque supplémentaire encouru par l'utilisation de l'USSD et du SMS pour les services financiers mobiles.
R-6	Si possible, nommer un responsable de la sécurité des systèmes d'information (CISO). Cette personne sera chargée d'élaborer et de mettre en œuvre un programme de sécurité de l'information visant à protéger les systèmes et les données internes, ainsi que les données sensibles fournies par les PSF dans le cadre de leurs obligations en matière de rapports. Les prérogatives du CISO doivent se distinguer du cahier de charge des services informatiques ou MIS. L'avantage d'un tel poste sera uniquement dans une fonction de rapport direct aux directeurs, évitant ainsi le risque que les questions relatives à la cyber-sécurité passent par d'autres départements spécifiques. Ces meilleures pratiques du secteur s'appliquent aussi bien aux autorités de régulation qu'aux PSF.
R-7	Les données sensibles fournies par les PSF aux autorités de surveillance, y compris les données concernant leurs clients, doivent répondre pratiquement aux mêmes mesures internes de cyber-sécurité que celles des PSF. À cette fin, les autorités de régulation/surveillance doivent envisager d'adopter les meilleures pratiques internationales en matière de contrôles techniques de cyber-sécurité à usage interne, à la fois lorsqu'elles offrent des services numériques et lorsqu'elles sont destinataires ou dépositaires de données confidentielles provenant d'entités réglementées.
R-8	Établir une base de référence nationale pour une évaluation commune des rapports sur la préparation à la cybercriminalité dans l'ensemble du secteur financier. Les PSF sont tenus de procéder à des évaluations annuelles de leur niveau de préparation à la cybercriminalité et de fournir les rapports correspondants à l'autorité de surveillance.
R-9	Élaborer une approche permettant de fournir une évaluation correcte et normalisée de l'approche proposée par chaque PSF pour remédier aux lacunes identifiées. Les lacunes identifiées dans l'évaluation de la préparation cybernétique d'un PSF sont généralement traitées dans un addenda au rapport d'évaluation annuel.
R-10	Examiner les rapports relatifs aux transactions suspectes (RTS) reçus des différents PSF, en les comparant à ceux du reste du secteur financier, et agir s'ils diffèrent de manière significative, au niveau de nombre de rapports escomptés ou alors au niveau de détails fournis.
R-11	Visiter régulièrement les centres opérationnels des PSF pour vérifier que les processus documentés et les points de contrôle sont respectés. Vérifier également qu'un contrôle actif des transactions (y compris celui de la lutte contre le blanchiment d'argent) est en place, le cas échéant.
R-12	Renforcer les capacités internes afin de satisfaire aux exigences prudentielles énoncées dans le présent document.
R-13	Élaborer des programmes de sensibilisation à la cyber-sécurité à l'intention du personnel des PSF et des autorités de régulation/supervision.
R-14	Intégrer des clauses d'application dans toutes les lignes directrices et les cadres nationaux relatifs à la cyber-sécurité, de sorte que la non-conformité d'un PSF entraîne des sanctions conformément aux réglements nationaux.
R-15	Prendre des mesures pour contrôler la sécurité des infrastructures numériques stratégiques, y compris les systèmes d'identité numérique, les systèmes de paiement, les commutateurs financiers, etc. et agir pour alerter les PSF en cas de problème.

3.4.2 PRINCIPE II : COOPÉRATION

Veiller à ce que les mesures soient prises de concert avec les homologues internationaux, coopérer avec les multiples agences nationales qui s'occupent de la cyber-sécurité, partager les informations sur les menaces et les incidents, et veiller à ce que les PSF disposent de ressources humaines adéquates pour faire face aux menaces liées à la cyber-sécurité.

RÉFÉRENCE	RECOMMANDATIONS
O-1	Lorsqu'un PSF rencontre un problème de cyber-sécurité avec violation de ses données, ou dans le cas d'une fraude signalée aux autorités de surveillance, ces dernières doivent examiner la menace cybernétique y associée et, le cas échéant, avertir les autres entités régulées de l'attaque.
O-2	La création d'un organisme national de sensibilisation et d'alerte en matière de cyber-sécurité doit être envisagée ; si l'organe de surveillance estime qu'il n'a pas de capacités suffisantes, il doit envisager de trouver des partenaires régionaux ou internationaux pour mettre en place un tel service.
O-3	Mettre en place un centre d'opérations de cyber-sécurité (CSOC) et une équipe d'intervention d'urgence informatique (CERT) à l'échelle du secteur.
O-4	Faciliter la coopération entre le CSOC/CERT national et le CSOC/CERT régional/international en place.

3.5 SERVICES FINANCIERS FOURNISSEURS

Les exigences énoncées dans la présente section s'appliquent spécifiquement aux activités attendues des PSF comportant un élément spécifique d'inclusion financière. Elles visent également à aider les autorités de régulation à superviser les activités des prestataires de services dans le respect de leurs obligations.

3.5.1 PRINCIPE III : LE CLIENT

Comprendre les compétences des clients en matière de services financiers, les identifier, préserver la confidentialité de leurs données et s'assurer que vous savez qui ils sont à leur retour.

RÉFÉRENCE	RECOMMANDATIONS
C-1	**Capacité des services financiers** Les PSF doivent mettre en place un programme de soutien et de formation en faveur des clients dont les connaissances numériques et/ou financières sont limitées. Le programme doit inclure des aspects pertinents des risques liés à la cyber-sécurité et les mesures d'atténuation de ces risques par les clients.
C-2	**KYC et diligence raisonnable proportionnés et fondés sur le risque** Il est particulièrement important que chaque client d'un PSF soit soumis à un processus d'identification et de vérification rigoureux lors de son enregistrement, en utilisant de manière appropriée les innovations technologiques telles que l'analyse de l'empreinte numérique d'un client et les services KYC partagés ou basés sur les services publics. Cela ne signifie pas que chaque client doit présenter des preuves tangibles de son identité. Il convient plutôt d'adopter une approche proportionnée de KYC : chaque client doit présenter tous les documents d'identité dont il dispose. Ces informations doivent ensuite être vérifiées et leur accès aux services financiers doit être en fonction des résultats de ce processus, selon un modèle conforme aux recommandations du GAFI. Ainsi, un client potentiel disposant d'une identité numérique, délivrée par un gouvernement et passée par une authentification biométrique fiable, qui peut également fournir un passeport et un justificatif de son adresse de résidence, se verrait généralement proposer la gamme complète des services financiers (sous réserve de vérifications supplémentaires au cas par cas, telles que la solvabilité). En revanche, un client qui n'est en mesure de fournir qu'un seul document d'identité sur papier, comme une carte d'électeur, et qui ne peut pas fournir d'autres documents, ne se verra offrir qu'un accès de base à un compte transactionnel, assorti de limites strictes en matière de solde et d'opérations. On suppose qu'il y aurait une gradation de l'accès entre ces deux extrêmes, éventuellement composée de trois à cinq niveaux. Dans tous les cas, ils doivent être définis conformément aux exigences de la réglementation nationale, ou en accord avec les autorités de régulation (s'il n'y a pas d'autre définition).
C-3	Les clients doivent pouvoir améliorer le niveau de service auquel ils ont accès en fournissant des documents d'identité supplémentaires au prestataire de services financiers.
C-4	Il convient également d'envisager de fournir des services aux clients qui ne peuvent présenter aucune pièce d'identité, à condition qu'un client déjà connu du fournisseur de services financiers produise une attestation de leur identité. Bien entendu, cela doit obéir à des règles strictes : > Cela ne peut être possible qu'en accord avec les autorités compétentes et sous leur contrôle ; > Si le client qui a fourni l'attestation fait l'objet d'une enquête pour une raison quelconque (identité mise en doute, liens avec la fraude, le blanchiment d'argent ou le financement du terrorisme), son compte doit être immédiatement fermé.

RÉFÉRENCE	RECOMMANDATIONS
C-5	Une fois qu'il a été décidé d'accorder un service à un client, un " compte d'enregistrement " du client doit être créé. Il s'agira en fait d'une identité numérique utilisée pour accéder aux services. Il se distingue des comptes de services financiers et est utilisé pour faciliter la gestion de la relation avec le client plutôt que la gestion des services fournis au client. Cette mesure vise principalement à s'assurer que toutes les relations d'un client avec un PSF sont correctement gérées. Cela permet d'adopter une approche axée sur le client, plutôt que sur le produit, pour soutenir les activités de lutte contre le blanchiment d'argent et de suivi des transactions du PSF. Ce compte d'enregistrement doit être identifié par une identité de client, délivrée à un client sous la forme d'un numéro de client ou d'un autre jeton d'identification. Le numéro de téléphone mobile d'un client peut être utilisé, mais cela doit s'accompagner de procédures permettant de gérer les changements de numéros de téléphone au fil du temps. Des contrôles doivent également être effectués, étant donné qu'un numéro de téléphone mobile peut faire l'objet d'attaques, telles que le SIM Swap.
C-6	**Authentification** Lorsqu'ils initient une transaction ou accèdent à des données privées (telles que les détails de leur compte ou de leur transaction), les clients doivent être tenus de se faire identifier à l'aide des outils fournis par le PSF. L'authentification à un seul facteur peut suffire pour les transactions de faible valeur ou la simple consultation d'un compte, mais il convient d'envisager l'utilisation de plusieurs facteurs (y compris la biométrie) pour les changements de compte, l'initiation de transactions plus importantes ou lorsque le volume global sur une période prolongée a atteint un seuil défini.
C-7	**Confidentialité et protection des données** Les données des clients, comme celles qui sont présentées lors de leur première prise en charge et celles générées pendant la durée de la relation avec le PSF (y compris les données relatives aux transactions), doivent être bien protégées. Elles doivent être stockées uniquement sous forme cryptée et ne doivent jamais être divulguées qu'au client ou aux membres dûment autorisés du personnel du PSF. Le choix des algorithmes cryptographiques, de la longueur des clés, des outils de gestion des clés, etc. ne doit se faire que sur les conseils d'experts en cyber-sécurité.
C-8	Les transactions de gré à gré (OTC) doivent être autorisées si le contexte spécifique d'un pays l'exige. Toutefois, cela doit être fait d'une manière soigneusement planifiée, de manière à ce que chaque partie à une transaction soit correctement identifiée. Cela comprend le client initiateur, l'agent initiateur, l'agent destinataire et le client destinataire. Une situation dans laquelle seuls les agents sont liés à une transaction et où les clients restent anonymes n'est pas acceptable.
C-9	Si les limitations sur les connaissances financières essentielles signifient qu'un client n'est pas encore prêt à effectuer ses transactions lui-même et qu'il aurait besoin d'assistance (ce qui est parfois - mais pas toujours - la raison du recours aux services de gré à gré), il convient de lui proposer de tels services, mais de manière conforme à la recommandation précédente.
C-10	**Responsabilité des clients** Les responsabilités des clients doivent être définies à la fois en fonction de leurs capacités et de leur possibilité d'influer sur la fiabilité et la sécurité du service. Au cours des entretiens menés, certains intervenants ont fait remarquer que certain nombre de PSF ont un accord avec les clients qui les rend responsables des perte dans le domaine de l'accès des clients (voir figure 1). Malheureusement il n'y a eu que peu ou pas d'investissement dans l'amélioration de la cyber-sécurité dans ce domaine, même si les clients n'ont aucune influence, par exemple, sur la sécurité d'un réseau mobile. Cette approche n'est ni acceptable ni durable, car elle porte un préjudice à la confiance des clients dans le PSF et, plus largement, à l'ensemble du secteur financier. Les clients peuvent ignorer cette responsabilité, ce qui renforce la nécessité de mettre en place des mécanismes efficaces de protection du consommateur. Pour y remédier on pourrait recourir à un transfert de responsabilité, de manière similaire à l'initiative PSD2 de l'Union européenne. Cela signifie que les pertes sont automatiquement considérées comme relevant de la responsabilité du PSF jusqu'à preuve du contraire et qu'elles doivent être remboursées au client immédiatement. Toutefois, si une enquête ultérieure révèle que la responsabilité du client est en fait engagée, le remboursement doit être annulé. Dans certains cas, cela peut nécessiter une réserve de fonds dédiés aux remboursements - mais en contrepartie, les cas doivent être résolus rapidement, idéalement dans un délai de trois jours ouvrables.
C-11	**Littératie numérique** Il incombe aux clients d'être vigilants et de veiller à ce que personne n'accède à leurs comptes pour effectuer des transactions non autorisées. Ils ne doivent en aucun cas communiquer leur code PIN ou leur mot de passe à quiconque, peu importe le degré de confiance envers la personne. S'ils utilisent un smartphone, ils ont l'obligation d'installer les mises à jour de sécurité dès qu'elles sont disponibles. Ce message doit être communiqué de manière claire- et souligné - au client lors de l'enregistrement.

3.5.2 PRINCIPE IV : FOURNIR LE SERVICE

Comprendre les canaux et l'infrastructure de prestation de services qui relient les PSF et leurs clients, et veiller à ce que les informations restent confidentielles et l'intégrité des transactions préservée

RÉFÉRENCE	RECOMMANDATIONS
S-1	Les PSF doivent s'efforcer de garantir une sécurité de bout en bout entre le client et leurs propres systèmes internes. Les FSP doivent se référer aux cadres et normes de cyber-sécurité nationaux et internationaux. Il ne faut pas se fier à la sécurité des systèmes et réseaux externes. Ceux-ci sont rarement conçus et développés dans l'optique d'une sécurité qui répond au niveau des services financiers. Par exemple, la sécurité des réseaux de téléphonie mobile a été conçue pour : > Veiller à ce que les revenus des opérateurs de téléphonie mobile soient protégés contre tout accès non autorisé ; > Préserver la confidentialité des conversations et des données des téléphones portables. Les exigences en matière de cyber-sécurité d'un service financier sont nettement plus élevées. Il incombe donc au PSF de garantir lui-même la sécurité, la confidentialité et l'intégrité de son service.
S-2	Comme cela a été souligné dans la section 2, l'utilisation de l'USSD pour la fourniture de services financiers présente d'importantes vulnérabilités en matière de sécurité : > Il n'y a pas de sécurité qui part du combiné du client jusqu'aux systèmes de back-office de l'opérateur mobile, ce qui permet aux pirates d'espionner les détails du compte et les codes PIN, et conduire ainsi à la perte des fonds du client ; > Un cyber-attaquant peut envoyer une session USSD au client de manière à ce qu'il ait l'impression d'être contacté par le PSF. Ils peuvent s'en servir pour demander au client de modifier son code PIN, qui peut alors être saisi, ce qui permet de pirater le compte et entraîner la perte de fonds. Les mêmes préoccupations s'appliquent à l'utilisation des SMS, qui ne doivent pas être utilisés pour les codes PIN à usage unique (OTP), car ils peuvent être interceptés par des cyber-attaquants. La seule exception est l'utilisation d'applications SIM Toolkit qui procèdent à leur propre cryptage des SMS, mais uniquement lorsque ce cryptage a fait l'objet d'un examen indépendant. La recommandation n'est pas d'abandonner l'USSD et les SMS, même si cela serait préférable. Cependant, à la lumière des vulnérabilités mises en évidence, il est tout d'abord recommandé que, lorsque les USSD/SMS sont utilisés, un contrôle actif et détaillé des transactions soit mis en place dans les systèmes centraux du PSF afin d'identifier et d'arrêter les transactions frauduleuses. Deuxièmement, une stratégie doit être adoptée pour gérer la migration à partir de ces services exposés. Pour les autorités de régulation, il est recommandé que lorsqu'un service repose sur l'USSD ou les SMS non cryptés pour la livraison, les conditions de service imposées aux clients ne soient pas telles qu'ils soient responsables de la fraude qui se produit dans le service client.
S-3	Avec l'augmentation du taux de pénétration des smartphones, les prestataires de services financiers doivent envisager de fournir aux clients une application suffisamment sécurisée pour leur permettre d'accéder à leurs services. L'accès à l'application doit être sécurisé à l'aide d'un code PIN ou d'un code biométrique (le cas échéant), et les développeurs de l'application doivent prévoir des moyens de défense techniques contre les cyber-attaques. Par exemple : > L'application doit être cryptée, afin d'empêcher les pirates de procéder à une rétro-ingénierie de l'application pour en extraire les données et les clés. > Toute clé cryptographique (par exemple, pour le chiffrement de bout en bout) doit être fragmentée et distribuée (cachée) dans l'application, et n'être reconstituée qu'en cas de besoin. > La finalité de toutes les données utilisées dans l'application doit être dissimulée à l'aide d'outils de développement appropriés. > L'application doit être développée pour fonctionner dans le bac à sable d'un smartphone lorsqu'il est disponible. Il s'agit d'un bac à sable technologique pour la protection cryptographique des services en direct, différent d'un bac à sable réglementaire. > Lorsqu'un tel bac à sable est disponible, l'application doit utiliser l'environnement d'exécution sécurisé (EES) du téléphone portable. Il peut s'agir de la carte SIM du téléphone ou d'une carte SEE dédiée dans un smartphone. > Le prestataire de services financiers doit exiger du client qu'il s'assure que le logiciel du système d'exploitation de son smartphone est toujours à jour ; l'application ne doit pas être lancée si le système d'exploitation n'offre pas le niveau de sécurité requis. En outre, l'application ne doit jamais être lancée si le téléphone portable a été " jailbreaké ". Les contrôles CIS-20 constituent une ressource utile dans ce domaine.
S-4	Lorsqu'un PSF n'est pas en même temps un opérateur de réseau mobile (ORM), il doit entretenir de bonnes relations avec tous les ORM de son pays, afin de limiter et de contrôler les échanges de cartes SIM. Les swaps doivent être désactivés pour les SIM qui appartiennent à des personnalités ou qui font partie du service du PSF (SIM des agents et des employés). En effet, les numéros de téléphone portable de ces personnes sont souvent mis à disposition dans le cadre de leurs activités normales et sont donc vulnérables aux cyber-attaques basées sur les échanges de cartes SIM. Les swaps SIM multiples contre un seul compte sur une courte période doivent être désactivés.
S-5	Lorsqu'un centre national d'opérations de cyber-sécurité (CSOC) et une équipe d'intervention d'urgence informatique (CERT) sont en place, le PSF est censé contribuer et participer à leurs activités. Cela s'ajoute à l'exigence de base qui est la conformité avec les normes de cyber-sécurité nationales et internationales émises par les autorités de régulation respectives.

3.5.3 PRINCIPE V : GESTION DES RISQUES INTERNES

Veiller à ce que l'intégrité du service d'un PSF soit préservée par des contrôles et des processus internes, et que le personnel soit géré de manière appropriée, etc.

RÉFÉRENCE	RECOMMANDATIONS
I-1	La cyber-sécurité d'un service financier peut être compromise par des employés malveillants. Les PSF doivent donc procéder à des vérifications d'antécédents appropriées et spécifiques à chaque pays lorsqu'ils recrutent du personnel à des postes sensibles : > Identifier correctement le personnel au moyen des mêmes processus d'identification et de vérification que ceux utilisés lors de l'accueil des clients ; > Demander et consulter les casiers judiciaires ou de police appropriés afin d'éviter d'engager des fraudeurs ou des cybercriminels connus ; > Les membres du personnel doivent faire l'objet d'une vérification des références de crédit lorsqu'elles sont disponibles, afin d'identifier ceux qui sont surendettés et donc susceptibles d'être vulnérables à la corruption. Ces vérifications d'antécédents doivent s'appliquer à tous les membres du personnel occupant des postes de responsabilité, y compris les cadres supérieurs, tout membre du personnel, quel que soit son grade, impliqué dans l'accès ou la configuration de la plate-forme DFS, ou dans des activités financières avec des partenaires bancaires ou des comptes de clients, et les personnes en contact avec les clients qui peuvent identifier des comptes susceptibles d'être ciblés par des cyber-attaquants. En outre, ces vérifications des antécédents doivent être répétées périodiquement.
I-2	Les employeurs doivent appliquer des mesures rigoureuses d'atténuation des risques en ce qui concerne l'accès aux systèmes informatiques de leurs employés importants occupant des postes sensibles (définis au point I-1). Cet accès comprend les règles d'autorisation, les procédures d'accès, l'utilisation restreinte d'appareils électroniques non autorisés dans certains locaux professionnels, y compris les ordinateurs portables personnels, les téléphones mobiles, les tablettes, etc.
I-3	Il est essentiel que toutes les interactions du personnel avec la plate-forme du PSF soient enregistrées et que ces enregistrements fassent autorité. Cela implique que tout accès du personnel aux systèmes informatiques doit être soumis à une authentification de qualité, telle que l'authentification à deux facteurs ; par exemple, un nom d'utilisateur et un mot de passe, ainsi qu'un code QR scanné à l'aide d'un téléphone portable. L'envoi de SMS pour les OTP n'est pas recommandé. Le personnel occupant des postes sensibles (qui, de préférence, ne devrait pas avoir leur téléphone portable sur eux : voir I-2) doit recevoir un porte-clés qui génère des codes d'accès temporaires, et son utilisation doit être imposée pour toutes les connexions. Pour des raisons de contrôle, toutes les activités menées par l'ensemble du personnel doivent être enregistrées, qu'elles soient ou non couronnées de succès. La piste d'audit qui en résulte ne doit pas être modifiable et l'accès à ces journaux doit être limité. Ces journaux doivent faire l'objet d'un audit périodique.
I-4	Toutes les fonctions opérationnelles et de gestion fournies par la plateforme de services du PSF devraient être soumises à un accès basé sur le rôle, de sorte que, par exemple, si leur rôle n'implique pas le mouvement de fonds ou l'examen des comptes des clients, ils ne doivent pas avoir accès à ces fonctionnalités.
I-5	L'accès basé sur les rôles décrit au point I-4 doit être utilisé pour mettre en œuvre les contrôles du préparateur/contrôleur (parfois appelés contrôles " à quatre yeux "), en particulier en ce qui concerne les transferts de fonds et d'autres transactions sensibles. Ce type d'accès permet à un membre du personnel de " faire ", ou de créer les détails d'une transaction de transfert de fonds, et à un autre de " vérifier/approuve " la transaction. Aucune personne ne devrait jamais se voir attribuer les deux rôles. Ces contrôles doivent être renforcés par l'enregistrement des connexions et par la mise à disposition des cadres supérieurs et des autorités externes d'outils d'investigation et d'audit.
I-6	Un élément important du plan de continuité des activités est la définition et la mise en œuvre de processus opérationnels détaillés. Il est recommandé d'entreprendre cette démarche car elle améliore les opérations d'une entreprise et atténue les problèmes d'erreur de la part du personnel, de dépendance excessive à l'égard du personnel clé et de manque de partage des connaissances entre les membres du personnel. Il convient d'adopter un système de gestion des processus d'entreprise (BPMS) qui, lorsqu'il est correctement mis en œuvre, permet de gérer les opérations quotidiennes d'un prestataire de services financiers et de réduire la dépendance à l'égard du personnel essentiel.
I-7	La PSF doit identifier un ensemble de points de contrôle qui peuvent être incorporés dans les processus opérationnels afin de renforcer la cyber-sécurité de base du service. Il peut s'agir de : > La spécification d'une valeur de transaction au-delà de laquelle une autorisation supplémentaire est requise ; > Une personne particulière dont la présence authentifiée est nécessaire à l'exécution d'une fonction ; > Restrictions quant au moment où une fonction spécifique peut être exercée (par exemple, pendant les heures de bureau).
I-8	Le rapprochement régulier des transactions entre les comptes des clients et les comptes bancaires du PSF est une activité essentielle, indispensable au maintien de l'intégrité d'un service financier. Dans ce contexte, la réconciliation a deux fonctions principales : > Veiller à ce que tous les soldes des clients soient sécurisés. > Fournir un indicateur précoce des fraudes potentielles perpétrées par la violation des contrôles de cyber-sécurité et des contrôles de création de valeur internes et externes.

RÉFÉRENCE	RECOMMANDATIONS
I-9	La cryptographie est essentielle au fonctionnement du DFS et à la protection des données et de la confidentialité. Il permet de garantir la confidentialité et l'intégrité des communications entre : > Un PSF et ses clients, fournisseurs et autres parties externes ; > Le personnel du PSF et les systèmes inter processus ; > Les systèmes inter-processus d'un PSF (pour éviter les attaques par rejeu). Toutes les données doivent être cryptées en transit et au repos. En ce qui concerne les données au repos, toutes les données des clients, qu'elles soient personnelles ou relatives à des transactions, doivent être cryptées avant d'être stockées, pour que les personnes ayant accès au système ne puissent pas voir les données. Cela permet un accès basé sur les rôles, pour que seule une personne qui s'est authentifiée comme ayant les bonnes informations d'identification puisse voir les données en clair. Toutes les transactions et activités du personnel doivent être enregistrées pour les audits ou enquêtes ultérieurs.
I-10	La sécurité physique est la première étape pour assurer la cyber-sécurité et permettre de limiter les possibilités de subversion des cyber-contrôles. Les PSF bien gérés se concentrent à parts égales sur la sécurité physique et la cyber-sécurité. Au minimum, la sécurité physique comprend les éléments suivants : > Une seule entrée, strictement contrôlée, dans les locaux du PSF. > S'assurer que les autres entrées sont sécurisées et que les sorties de secours sont équipées d'alarmes. > Veiller à ce que toutes les pièces soient sécurisées avec des serrures biométriques et qu'elles exigent à la fois une « entrée » et une « sortie » afin d'éviter les files d'attente. Cela signifie également garantir que l'accès à toutes les pièces soit restreint en fonction du (rôle) de l'employé. > Permettre une surveillance vidéo et un enregistrement 24 heures sur 24 de toutes les zones. Cela est primordial dans la dissuasion et la détection des crimes. Il convient d'insister sur le fait que les caméras ne doivent pas être orientées vers des écrans susceptibles d'afficher des informations sensibles. - Ces enregistrements doivent être disponibles au minimum pendant un mois, mais de préférable pour une durée d'un an. - Il doit être permis aux enquêteurs agréés de télécharger et archiver les enregistrements à des fins d'enquête sur les fraudes.
I-11	Il est recommandé que les PSF mettent en œuvre des fonctions actives et automatisées de suivi des transactions et d'alerte. Outre la détection et la prévention de la fraude, le suivi actif et automatisé des transactions peut contribuer aux obligations de conformité d'un PSF en matière de lutte contre le blanchiment d'argent/ lutte contre le financement du terrorisme (LBC/FT).
I-12	Un responsable de la lutte contre la fraude doit être nommé. Le rôle consiste à surveiller les transactions, à soumettre des déclarations de transactions suspectes aux autorités réglementaires et à participer aux enquêtes complémentaires en coopération avec ces autorités.
I-13	Le PSF doit mettre en œuvre des outils modernes d'investigation des transactions dotés de la fonctionnalité " suivre l'argent ", qui peuvent être utilisés pour enquêter rapidement et efficacement sur des délits potentiels.
I-14	Les grandes entreprises dont la part de marché est supérieure à 10 % doivent nommer un responsable de la sécurité de l'information (CISO), chargé d'élaborer et de mettre en œuvre un programme de sécurité de l'information.
I-15	Les PSF doivent fournir à l'ensemble du personnel opérationnel et de développement des compétences en matière de cyber-sécurité et une formation au développement.

3.5.4 PRINCIPE VI : COMPRENDRE SES PARTENAIRES

Garantir l'implication des partenaires par le biais de processus appropriés sans augmenter de manière significative les risques pour les clients ou le service.

RÉFÉRENCE	RECOMMANDATIONS
P-1	Il existe des mesures de sécurité physique supplémentaires qui s'appliquent uniquement aux visiteurs des locaux d'un PSF, différentes de celles du personnel : > Tous les visiteurs doivent être identifiés (à l'aide d'une carte d'identité ou d'un document similaire) et enregistrés. > Les visiteurs ne doivent pas être autorisés à emporter des équipements électroniques dans les zones opérationnelles ou sensibles. > Les visiteurs peuvent être autorisés à emporter des téléphones mobiles et des ordinateurs portables uniquement dans les zones non opérationnelles. Toutefois, les numéros de série des ordinateurs portables doivent être enregistrés et le personnel du PSF doit utiliser ces informations pour vérifier que les visiteurs repartent avec le même équipement que celui qu'ils ont apporté, afin d'éviter de changer les ordinateurs portables. > Les visiteurs doivent être accompagnés à tout moment par un membre du personnel qui est responsable de leur conduite. > Les membres du personnel désignés doivent surveiller l'activité des visiteurs en permanence. En particulier, les visiteurs ne doivent pas être autorisés à : - Se promener dans le bâtiment sans être accompagnés ; - Insérer des clés USB ou des dispositifs similaires dans les ordinateurs portables, les imprimantes, etc. de l'entreprise.
P-2	Un processus doit être développé et intégré dans le fonctionnement d'un PSF pour l'accueil des fournisseurs et la gestion ultérieure de la relation. Les objectifs de ce processus doivent être les suivants : > Permettre à l'équipe de direction du PSF d'acquérir une compréhension des risques susceptibles de découler des activités internes du fournisseur ; > Comprendre les relations du fournisseur avec des tiers qui peuvent, par exemple, les contraindre à fournir un accès inapproprié aux informations opérationnelles ou sur les clients du PSF ; > Identifier les relations avec le personnel clé du PSF, qui sont susceptibles de conduire à la collusion et à la fraude. En plus d'être un élément essentiel de sélection des fournisseurs, ce processus de vérification doit également faire partie intégrante de la diligence raisonnable annuelle, appliquée à toutes les relations avec les fournisseurs.
P-3	Lorsqu'il établit une relation avec un fournisseur, le PSF doit prendre des mesures pour s'assurer qu'il existe une compréhension commune de la répartition des responsabilités et des obligations en cas de fraude.

3.5.5 PRINCIPE VII : LE LONG TERME

Veiller au maintien de sécurité du service d'un PSF lorsque de nouvelles menaces émergent ; garantir que les autorités réglementaires sont informées à la fois des risques existants et des mesures pour y remédier ; garantir que des audits sont effectués régulièrement et que toutes les exigences en matière de rapports sont respectées, etc.

RÉFÉRENCE	RECOMMANDATIONS
L-1	La direction et le conseil d'administration d'un PSF doivent adopter et mettre en œuvre les meilleures pratiques internationales en matière de cyber-sécurité. Utilisées de manière appropriée, cela facilitera le respect des nouvelles exigences nationales en matière de réglementation et de surveillance.
L-2	Afin de contribuer au développement continu de la préparation à la cyber-sécurité, chaque PSF doit adopter un outil d'évaluation des meilleures pratiques internationales en matière de cyber-sécurité et intégrer l'utilisation de cet outil dans ses processus opérationnels de base, dans le but d'améliorer le niveau de préparation à la cyber-sécurité au fil du temps.
L-3	Le directeur informatique de chaque PSF doit adopter et mettre en œuvre des contrôles techniques de cyber-sécurité conformes aux meilleures pratiques internationales afin de renforcer la cyber-sécurité technique et ses systèmes et services.
L-4	Dans le prolongement des points L-1 à L-3, le prestataire de services financiers doit se doter d'une capacité à identifier les nouvelles menaces pour la cyber-sécurité et à y faire face à mesure qu'elles apparaissent.
L-5	Les PSF doivent évaluer leur niveau de préparation à la cybercriminalité en utilisant l'outil d'évaluation de la cyber-sécurité de la FFIEC. Cette évaluation doit être menée au moins une fois par an et les autorités de régulation et de surveillance doivent être informées des résultats.
L-6	Lorsque le niveau de cyber-préparation d'un PSF n'est pas conforme aux normes attendues, le PSF doit informer les autorités de régulation et de surveillance des mesures qu'il compte prendre pour combler cette lacune, en se référant en particulier à la FSSCC CSP.
L-7	Toute défaillance en matière de cyber-sécurité entraînant une violation de données ou une fraude doit être immédiatement signalée aux autorités compétentes.

3.6 RÉSUMÉ DE RISQUES

Le tableau suivant énumère les principaux acteurs, décrit leur rôle dans la fourniture de services financiers, met en évidence les principaux risques auxquels ils sont exposés et présente les impacts ou implications de haut niveau de la réalisation de ces risques.

TABLEAU 1 : PAIEMENTS ET SERVICES FINANCIERS NUMÉRIQUES : ACTEURS, RÔLES, RISQUES ET IMPACTS

ACTEUR	DESCRIPTION	PRINCIPAUX RISQUES	IMPACTS
Client	Le client peut ou non utiliser un appareil numérique tel qu'un téléphone portable pour accéder aux services.	> Faible culture financière, numérique et/ou cybernétique > Ingénierie sociale, permettant la fraude à l'encontre du client > Erreurs	> Perte de fonds > Perte de données personnelles
Appareil numérique du client	Le client peut utiliser un appareil pour accéder au service ou utiliser un service OTC.	> Piratage > Écoutes téléphoniques	Perte des fonds du client
Application de services financiers	> Une application que le client peut utiliser dans ses interactions avec le service, y compris les transactions. > Peut être fourni par le PSF ou par une FinTech.	> Piratage > Interception/écoute	> Perte de fonds > Perte de données personnelles
Marchand	Veut vendre au client et est prêt à accepter le paiement par le numérique.	> Faible culture numérique > Formation inadéquate	Disponibilité des services limitée ; confiance limitée.
Dispositif numérique du commerçant	L'appareil numérique du commerçant peut être un téléphone portable.	> Piratage > Écoutes téléphoniques	Perte des fonds du client ou du commerçant
Agent	> Fournit des services au client. Ces services peuvent comprendre l'enregistrement des clients, les services d'encaissement et de décaissement (CICO) ou une gamme complète de services financiers via un modèle de gré à gré (OTC). > Dans certaines circonstances, un commerçant peut également jouer le rôle d'agent.	> Faible culture numérique > Formation inadéquate > Personnel peu fiable	> Disponibilité des services et fiabilité réduites > Fraude contre le client > Fraude contre l'agent (par le personnel)
Appareil numérique de l'agent	Utilisé pour fournir des services aux clients et pour gérer la prestation de services. Il peut s'agir d'un téléphone portable.	> Piratage > Écoutes téléphoniques	Disponibilité des services réduite; confiance réduite
Service d'identité numérique	Utilisé pour établir l'identité du client lors de l'accueil. Dans certains pays, ce service offre également des services d'authentification à utiliser lors des transactions financières, mais en général, la fonction d'authentification est assurée par le PSF.	> Faible enregistrement > Authentification faible lors de l'accueil des nouveaux arrivants > Lien avec des dossiers de crédit incorrects, permettant la fraude	> Identification peu fiable des clients > Fraude intraçable (ou autres délits) > Prêts inappropriés par le PSF
Réglementation autorités	Définir le cadre réglementaire et prudentiel environnement dans lequel les services peuvent être offerts et identifier le personnel qui doit veiller à ce que ces attentes sont respectées.	Manque de familiarité avec risques techniques (fintech, services financiers numériques, réseaux mobiles)	> Distribution inappropriée de responsabilité > Diminution des clients protection > Perte de confiance dans les services
Normes & définition des normes corps	Définir comment les différents partenaires du service prestation peut interopérer, et définir les attentes en matière de qualité de ce service.	Normes inappropriées entraînant une insécurité, inapproprié ou peu fiable services	> Diminution de la fiabilité > Perte de confiance dans les services

Réseau de communication	Il peut s'agir d'un téléphone portable ou d'un réseau Wi-Fi, ou d'une configuration similaire.	> Écoutes téléphoniques > Interception > Redirection > Spoofing > Hameçonnage	> Perte des fonds du client, de l'agent ou du commerçant > Piratage de compte client > Perte de données des clients ou des commerçants
Les systèmes d'un opérateur de réseau	Ceux-ci sont constitués de > Les stations de base du réseau opérationnel, situées dans tout le pays, qui fournissent un accès local à une dorsale qui interconnecte l'ensemble du réseau ; > Un centre d'exploitation du réseau central, lui-même composé de systèmes d'exploitation du réseau (qui fournissent le service de communication) et de systèmes internes de l'opérateur du réseau. les systèmes IT, qui gèrent les systèmes opérationnels et fournissent un soutien administratif.	> Hameçonnage > Spoofing > Écoutes téléphoniques > Interception	> Perte des fonds du client, de l'agent ou du commerçant > Détournement de compte d'un client, d'un agent ou d'un commerçant > Perte de données des clients, des agents ou des commerçants
Les systèmes du PSF	Utilisé pour fournir des services financiers aux clients, y compris potentiellement aux personnes mal desservies.	> Contrôles internes inadéquats > Acteurs malveillants internes > Absence de plan de continuité des activités > Mauvais outils d'investigation de la fraude	> Violation de données ; perte de données de service, à la fois financières et non financières > Service peu fiable > Perte de réputation > Incapacité à lutter contre la criminalité financière
Banques	> Détient les fonds des clients. > Il est à noter que la banque et le PSF peuvent être la même organisation, bien que il n'est pas rare qu'ils soient différents.	> Absence de réconciliation adéquate, d'où un risque de fraude supplémentaire > Concentration des fonds ; faillite potentielle de la banque entraînant la perte des fonds des clients > Acteurs malveillants internes	Défaillance systémique
Autres prestataires de services externes	Soutenir le PSF dans la prestation de ses services. Il peut s'agir, par exemple, de partenaires techniques, tels que des services de serveur ou d'hébergement, ou de partenaires logistiques chargés de gérer des réseaux d'agents.	> Perturbation des services > Piratage > Spoofing	Perte de réputation et donc de confiance
BUREAU DE CRÉDIT	Soutenir le PSF dans la prestation de ses services	Erreurs dans les dossiers de crédit	Risque financier pour le PSF dû à des prêts inappropriés

3.7 À NOTER : L'USSD, LES SMS ET LE RISQUE CYBERNÉTIQUE

L'USSD est largement utilisé pour la prestation de services financiers aux personnes mal desservies, et il est reconnu que cela est souvent nécessaire pour toute une série de raisons qui dépassent le cadre du présent document. Cependant, l'USSD présente d'importantes faiblesses en matière de sécurité :

- Il n'y a pas de sécurité qui part du combiné du client jusqu'aux systèmes de back-office de l'opérateur mobile, ce qui permet aux pirates d'espionner les détails du compte et les codes PIN, et conduire ainsi à la perte des fonds du client ;
- Un cyber-attaquant peut envoyer une session USSD au client de manière à ce qu'il ait l'impression d'être contacté par le PSF. Ils peuvent s'en servir pour demander au client de modifier son code PIN, qui peut alors être saisi, ce qui permet de pirater le compte et entraîner la perte de fonds.

Les mêmes préoccupations s'appliquent à l'utilisation des SMS, qui ne doivent pas servir pour les codes PIN à usage unique (OTP) car ils peuvent être interceptés par des cyber-attaquants ; la seule exception étant l'utilisation d'applications SIM Toolkit qui procèdent à leur propre cryptage des SMS.

Tant que les clients et les PSF ne disposeront pas de la technologie nécessaire pour sécuriser totalement les données privées et que les transactions ne seront pas plus abordables, les PSF devront surveiller attentivement et durablement les transactions. Ainsi, les PSF doivent prioriser l'identification des anomalies et l'intervention appropriée. Les approches visant à atténuer ces risques sont présentées à la section 3.5.2 du présent document.

4 CONTEXTE : CADRES EXISTANTS

4.1 INTRODUCTION

Les régulateurs et les autorités de surveillance du secteur financier savent qu'il existe déjà un large éventail de cadres de cyber-sécurité : certains généralisés, d'autres visant à protéger une infrastructure essentielle d'un pays, certains officialisés dans des normes nationales ou internationales, tandis que d'autres sont spécialisés dans un secteur particulier de l'économie, notamment le secteur financier.

Le présent document n'a pas pour objet de proposer une alternative à ces cadres. Au contraire, comme cela a été souligné à la section 1.2.1, ce guide est destiné à compléter les cadres, en mettant en évidence et en soulignant les risques liés à l'adoption de pratiques et de technologies devenues courantes lorsqu'un service est axé sur les priorités de l'inclusion financière.

Dans la poursuite de cet objectif, il est important de mettre en lumière le paysage des cadres de cyber-sécurité dans lequel le présent document doit s'inscrire. Sur la base d'entretiens avec un large éventail de parties prenantes, cette section présente une vision consensuelle du large éventail de cadres de cyber-sécurité supranationaux pertinents pour les autorités de régulation et les PSF.

En outre, les autorités de régulation d'un certain nombre de pays ont pris l'initiative d'élaborer des cadres nationaux en matière de cyber-sécurité qui portent sur l'ensemble du secteur financier de leur pays, sans mettre l'accent sur l'inclusion financière. Certains de ces cadres sont également résumés dans cette section.

4.2 CADRES SUPRANATIONAUX

En ce qui concerne les cadres supranationaux de cyber-sécurité, les parties prenantes ont souligné à plusieurs reprises l'importance et la pertinence des cadres dans les sous-sections suivantes.

4.2.1 NIST

Le National Institute of Standards and Technology (NIST) des États-Unis a publié son premier cadre de cyber-sécurité en 2014. Il s'agit d'un cadre influent, qui sous-tend de nombreux autres cadres de cyber-sécurité publiés par d'autres organismes à travers le monde. Le NIST a publié[1] la version actualisée (1.1) de son Framework for Improving Critical Infrastructure Cybersecurity le 16 avril 2018.

Depuis la publication de la version 1.0 en février 2014, le cadre NIST est devenu le point de départ par défaut pour de nombreuses organisations souhaitant aborder les questions de cyber-sécurité. Malgré son caractère fondateur et son influence, le cadre du NIST est très général ; il vise à améliorer la cyber-sécurité des infrastructures essentielles dans tous les secteurs de l'économie et ne peut pas être utilisé directement par les PSF sans être rendu plus spécifique. Les sections suivantes décrivent certaines approches à cet égard.

4.2.2 FFIEC

Le Federal Financial Institutions Examination Council (FFIEC) s'est inspiré du cadre de cyber-sécurité du NIST et a développé un outil d'évaluation de la cyber-sécurité, spécifiquement destiné au secteur financier, permettant aux institutions de d'évaluer leur propre état de préparation en matière de cyber-sécurité. L'outil a été publié[2] en mai 2017, en réponse au volume et à la sophistication sans cesse croissante des cyber-menaces. Le développement de cet outil s'est inspiré du cadre de cyber-sécurité du NIST.

L'objectif de cet outil est d'aider les institutions financières à identifier leurs risques et à déterminer leur niveau de préparation en matière de cyber-sécurité. En outre, il est structuré de manière à fournir à ces institutions un processus reproductible et normalisé pour mesurer l'évolution de leur préparation à la cyber-sécurité au fil du temps.

L'approche du FFIEC est largement admirée et adoptée, et a eu un impact sur de nombreuses initiatives, y compris le CROE de la Banque centrale européenne, qui est résumé plus loin dans la présente section.

4.2.3 CPMI-OICV

Le Comité sur les paiements et les infrastructures de marché (CPMI) de la Banque des règlements internationaux (BRI), en collaboration avec le Conseil de l'Organisation internationale des commissions de valeurs (OICV), a élaboré en juin 2016 le document[3] intitulé "Guidance on cyber resilience for financial market infrastructures" (Cyber Guidance). Les orientations s'appliquent à une infrastructure nationale complète des marchés financiers (IMF), définie comme "les institutions d'importance critique chargées de la compensation, du règlement et de l'enregistrement des transactions monétaires et autres transactions financières".

Les orientations se fondent sur des principes plutôt que sur des normes spécifiques, compte tenu de la nature dynamique de la cyber-sécurité et des menaces qui pèsent sur les systèmes et les services. Un aspect important à souligner est qu'il vise à compléter - et non à remplacer - les orientations en matière de cyber-sécurité axées sur les technologies de l'information. A l'inverse, il souligne que la cyber-sécurité ne se limite pas aux technologies de l'information.

1 https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11
2 https://www.ffiec.gov/cyberassessmenttool.htm
3 https://www.bis.org/cpmi/publ/d146.htm

Ainsi, il suggère qu'une organisation a besoin à la fois d'un cadre fondé sur des principes et d'un cadre de cyber-sécurité informatique, fonctionnant de concert pour garantir la sécurité d'une institution financière contre les cyber-menaces.

4.2.4 BCE CROE

La Banque centrale européenne (BCE) a publié4ses "Cyber resilience oversight expectations for financial market infrastructures" (CROE) en décembre 2018. Lors de l'élaboration du CROE, la BCE s'est inspirée d' une série de documents d'orientation et de cadres internationaux, notamment le CPMI-IOSCO, le NIST et le FFIEC. L'objectif du CROE est d'aider les autorités de contrôle et de surveillance dans leur tâche d'examen de la conformité aux orientations du CPMI et de l'OICV; en substance, il s'apparente à un cadre d'évaluation.

Le CROE de la BCE est un document important qui fournit une passerelle extrêmement utile entre les exigences
énoncées dans le CPMI-IOSOC, le NIST et dans d'autres documents, et les processus dont les institutions financières doivent disposer pour se mettre en conformité. Il le fait d'une manière adaptée à l' évolution de l'institution et à l'environnement dans lequel elle opère.

Toutefois, il n'est pas conçu comme un cadre formel de cyber-sécurité et n'a pas vocation à l'être. Ceci reflète son rôle principal d'outil à l'usage des autorités de contrôle et de surveillance. Le CROE aide les autorités à évaluer les cadres de cyber-sécurité utilisés par les organismes qu' elles supervisent. Essentiellement, il contribue à développer la capacité des autorités à évaluer la cyber-sécurité des institutions qu'elles supervisent, un élément important du puzzle de la cyber-sécurité.

4.2.5 PROFIL DE CYBER-SÉCURITÉ DU FSSCC

Le Conseil de coordination du secteur des services financiers (FSSCC) des États-Unis a été créé en 2002 par des représentants
du secteur financier aux États-Unis. Il travaille en collaboration avec les agences gouvernementales américaines pour protéger les infrastructures vitales du secteur financier américain contre les incidents cybernétiques et physiques. Le FSSCC a publié la version 1[5] de son profil de cyber-sécurité (CSP) le 25 octobre 2018. Le cadre s'inspire fortement du cadre NIST et des orientations CPMI-IOSCO. Les questions d'évaluation sont basées sur les orientations et les cadres de surveillance pertinents ainsi que sur les correspondances avec les contrôles ISO/IEC 27001/2.

L'élaboration du FSSCC DSP est intervenue, du moins en partie, en réponse à l'approche fragmentaire des réglementations et cadres existants. Une majeure partie de ces cadres découlent des fonctions, catégories et sous-catégories du cadre NIST, mais ne fournissent qu'une couverture partielle ou adoptent une approche tellement arbitraire que leur utilité est compromise.

Le FSSCC a décidé d'éviter cela en adoptant une approche globale et pansectorielle. Malgré cela, il convient de rappeler que ce systéme est né dans le secteur financier des États-Unis, dont on peut s'attendre à ce qu'il ait une capacité différente de celles des institutions financières (en particulier les plus petites) et des organismes de surveillance des économies émergentes.

4.2.6 CENTER FOR INTERNET SECURITY - THE CIS 20 CONTROLS

Conformément à la recommandation CPMI-IOSCO selon laquelle une organisation doit disposer à la fois d'un cadre fondé sur des principes et d'un cadre de cyber-sécurité informatique, un certain nombre de parties prenantes ont souligné la valeur du "CIS 20" en tant qu'exemple majeur de ce dernier.

Le Center for Internet Security (CIS) est une entité à but non lucratif basée aux États-Unis. Selon leurs propres termes, ils "exploitent le pouvoir d'une communauté informatique mondiale pour protéger les organisations privées et publiques contre les cyber-menaces". Cette initiative est particulièrement intéressante en raison de son approche "ascendante" de la cyber-sécurité. Plutôt qu'un ensemble
de principes imposés par les régulateurs, les autorités de surveillance ou les consortiums de grandes banques, l'approche CIS repose sur l'expertise de ceux qui s'occupent de la cyber-sécurité de manière continue. Il s'agit donc d'un complément utile à d'autres approches.

Ce qui revêt une importance particulière pour le présent guide est ce qu'il est convenu d'appeler les "contrôles CIS 20". Il s'agit d'un ensemble de 20 contrôles et lignes directrices en matière de cyber-sécurité
qui, ensemble, répondent aux besoins de la majorité des institutions, notamment celles du secteur financier, en matière de cyber-sécurité. La version actuelle au moment de la rédaction est la 7.[16], publiée le 1er avril 2019. Une publication distincte illustrant la conformité avec le cadre de cyber-sécurité du NIST est disponible auprès du CIS, bien qu'elle n'ait pas été revue dans le cadre de la préparation du présent guide.

4 https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

5 https://www.ffiec.gov/cyberassessmenttool.htm

6 https://www.cisecurity.org/controls/

4.3 CADRES NATIONAUX

4.3.1 INTRODUCTION

Lors de l'examen des cadres de cyber-sécurité mis en place par les autorités de régulation, les entretiens avec les parties prenantes ont permis d'en identifier trois en particulier qui reflètent la complexité accrue des réponses des agences nationales aux préoccupations croissantes des acteurs du secteur financier en matière de cyber-sécurité:

- **"Outil d'évaluation de la maturité de la cyber-sécurité" de l'Arménie ;**
- **"Directives sur la cyber-sécurité et la sécurité de l'information "du Ghana ;**
- **Le "cadre de cyber-sécurité basé sur les risques" du Nigeria.**

Par coïncidence, ces trois documents ont été publiés en 2018, reflétant à la fois l'urgence croissante ressentie par les autorités de régulation dans les économies émergentes et leur volonté de s'engager activement avec le secteur financier pour résoudre les problèmes.

La nature de ces cadres varie considérablement, comme on l'a déjà vu avec les cadres supranationaux. Cela est en partie lié aux priorités de chaque autorité nationale. Les cadres nigérian et ghanéen fournissent une spécification claire de
ce que l'on attend des institutions financières (et en cela, elles s'apparentent au FSSCC CSP), tandis que le cadre arménien se concentre sur la manière dont- par le biais d'activités individuelles détaillées-, une institution financière peut atteindre le niveau de cyber-sécurité nécessaire (semblable au cadre du FFIEC).

4.3.2 ARMÉNIE

Au cours de la période 2007-2010, afin d'améliorer la gouvernance, les processus et les procédures en matière d'informatique et de sécurité de l'information, la Banque centrale d'Arménie (CBA)
a adopté la norme ISO 27001 pour les systèmes de gestion de la sécurité de l'information, ce qui lui a permis d'obtenir la certification en 2012. Au cours de cette période, l'ABC a défini des règles de cyber-sécurité concernant les institutions financières réglementées, en utilisant un ensemble simplifié d'exigences basées sur la norme ISO 27001. En 2013, l'ABC a étendu cette mesure en incluant l'obligation pour toutes les institutions financières d'être certifiées ISO 27001
d'ici à 2015, la certification devant être effectuée par un organisme de certification international reconnu.

Plus récemment, le service d'audit interne de l'ABC a mis au point un outil d'auto-évaluation de la cyber-sécurité, d'abord à usage interne, puis à l'intention
des institutions financières réglementées. Cet outil est destiné à les aider (ainsi que les autorités de surveillance) à comprendre leur profil de risque inhérent et leur maturité en matière de cyber-sécurité.

Il s'agit d'un instrument précieux qui, grâce à l'automatisation du cadre FFIEC, offre une avancée significative dans l'utilisabilité de ce cadre. Son utilisation par les institutions financières doit donc être encouragée. Toutefois, la manière dont il pourra être utilisé par les autorités de contrôle et de surveillance n'a pas été déterminée.

4.3.3 GHANA

En octobre 2018, la Banque du Ghana a publié[7] "Cyber & Information Security Directive", à l'intention du secteur des services financiers au Ghana, et qui :

> "...fournit un cadre pour l'établissement de protocoles et de procédures de cyber-sécurité et de sécurité de l'information pour les scénarios de routine et d'urgence, la délégation des responsabilités, la communication et la coopération inter- et intra-entreprise, la coordination avec les autorités gouvernementales, la mise en place de mécanismes de rapports, les mesures de sécurité physique pour les centres de données informatiques et les salles de contrôle, et la garantie de la sécurité des données et des réseaux".

En ce qui concerne les réglementations et normes internationales, le document fait notamment référence aux normes ISO27001[8] (sécurité de l'information), ISO27032 [9] lignes directrices pour la cyber-sécurité), PCI-DSS (sécurité des transactions par carte) et au cadre et aux lignes directrices sur la cyber-sécurité [10] publiés par le NIST, basé aux États-Unis, dont l'expertise dans ce domaine est largement reconnue.

La directive est divisée en plusieurs parties, qui établissent des exigences par rapport aux systèmes et services, et définissent les responsabilités des principaux acteurs.
Ces exigences couvrent un large éventail et contiennent de nombreux conseils très pertinents et utiles.

La directive représente une avancée significative pour garantir la cyber-sécurité des PSF au Ghana à la fois en ce qui concerne les approches recommandées et l'ampleur de sa vision.

4.3.4 NIGERIA

Reconnaissant à la fois la croissance rapide dans les transactions dans le secteur financier nigérian (notamment le secteur émergent de la fintech), et la prévalence croissante des cyberattaques contre les institutions financières, la Banque centrale du Nigéria (CBN) a publié son Cadre de cyber-sécurité basé sur le risque[11], applicable à toutes les banques de dépôt et prestataires de services de paiement, le 10 octobre 2018, et la date de mise en conformité intégrale a été fixée au 1er janvier,
2019. Ce projet fait suite à une première version publiée en juin 2018, qui a été révisée après consultation avec les différents intervenants du secteur.

---

7 https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

8 Spécification d'un système de gestion de la sécurité de l'information (SGSI). Un SGSI est un cadre de politiques et de procédures qui comprend tous les contrôles juridiques, physiques et techniques impliqués dans les processus de gestion des risques liés à l'information d'une organisation.

9 Contexte : L'ISO 27032 n'est pas une norme que l'on peut certifier ; c'est l'une des différences les plus importantes par rapport à l'ISO 27001, qui vise la certification d'un SMSI. L'objectif principal de la norme ISO 27032 est de fournir un guide pour la cyber-sécurité par le biais de recommandations spécifiques. Ainsi, la norme ISO 27001 se concentre sur une organisation et son SMSI, tandis que la norme ISO 27032 est axée sur le cyberespace et constitue un cadre de collaboration.

10 https://www.nist.gov/cyberframework

11 https://www.cbn.gov.ng/out/2018/bsd/risk%20based%20cybersecurity%20framework%20final.pdf

Le cadre de la CBN adopte une approche différente de celle instituée par le Ghana : qui est celle d'établir des lignes directrices générales, en se référant à des experts/autorités internationaux tels que le NIST et le PCI-DSS, pour recueillir des conseils détaillés.

Voici quelques aspects importants du cadre de la CBN :

- Le responsable de la sécurité de l'information (CISO) d'une institution financière doit rendre compte directement au directeur général. Le RSSI ne doit en aucun cas rendre compte au responsable des TI. Bien qu'il s'agisse d'une meilleure pratique reconnue par l'industrie, on ne saurait trop insister sur l'importance de cet aspect.
- Dans le cadre d'une auto-évaluation de la résilience en matière de cyber-sécurité, le Cadre exige que les institutions déterminent à la fois leur profil actuel de cyber-sécurité et le niveau souhaité/cible, ainsi qu'une feuille de route détaillée pour atteindre l'objectif dans un délai imparti.
- Des exigences minimales sont fixées pour établir et développer la résilience opérationnelle en matière de cyber-sécurité, y compris des exigences pour comprendre l'environnement opérationnel, technologique et commercial d'un établissement; pour renforcer durablement la résilience en matière de cyber-sécurité et développer une capacité de renseignement sur les cyber-menaces.
- Les institutions sont toutes tenues de signaler à la CBN toutes les cyber-attaques, qu'elles se soldent ou non par un succès, dans les 24 heures qui suivent le forfait. La portée de cette mesure n'est pas claire. On peut supposer qu'elle n'inclut pas les attaques de "sondage" générales qui se produisent en permanence sur l'internet, car les attaquants sondent les systèmes pour détecter les portes électroniques évidentes qui ont été laissées ouvertes [12]. Il serait utile de clarifier le seuil avant qu'un rapport ne soit requis ou produit.

Le Cadre de la CBN, comme on pouvait s'y attendre, est une ressource importante et précieuse, qui établit des principes clairs et fournit de nombreuses orientations aux PSF sur la manière de s'y conformer.

12 Tout appareil connecté à l'internet peut s'attendre à voir sa connexion internet sondée plusieurs fois par jour, en comptant sur un pare-feu pour le protéger.

GLOSSAIRE

TERME	DESCRIPTION
AIF	Alliance pour l'inclusion financière
AML	Lutte contre le blanchiment d'argent
API	Interface de programmation d'applications
BIS	Banque des règlements internationaux
BoG	Banque du Ghana
BPMS	Système de gestion des processus d'entreprise
CA	Autorité compétente
CAF	Cadre d'évaluation cybernétique
CBA	Banque centrale d'Arménie
CBN	Banque centrale du Nigéria
CERT	Équipe d'intervention en cas d'urgence informatique
CFT	Lutte contre le financement du terrorisme
CICO	Encaissement, décaissement
CII	Infrastructure d'information critique
CIS	Centre pour la sécurité de l'Internet
RSSI	Responsable des risques liés à la sécurité de l'information
CNI	Infrastructures nationales critiques
CPMI	Commission des paiements et des infrastructures de marché
CROE	Attentes en matière de supervision de la cyber-résilience
CSA	Agence de cyber-sécurité
CSIRT	Équipe d'intervention en cas d'incident de sécurité informatique
CSOC	Centre d'opérations de cyber-sécurité
CSP	Profil de cyber-sécurité
SFN	Services financiers numériques
DFS WG	Groupe de travail sur les services financiers numériques (SFN)
DGSSI	Direction générale des systèmes de sécurité de l'information
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
L'UE	Union européenne
GAFI	Groupe d'action financière
FFIEC	Conseil fédéral d'examen des institutions financières
FI	Inclusion financière ou institution financière, selon le contexte
Fintech	Produits de technologie financière
Fintech	Entreprise de technologie financière ou prestataire de services financiers
FMI	Infrastructure des marchés financiers
s.o.	Prestataire de services financiers

TERME	DESCRIPTION
FSSCC	Conseil de coordination du secteur des services financiers
IGP	Indicateur de bonne pratique
OICV	Organisation internationale des commissions de valeurs
ISMS	Système de gestion de la sécurité de l'information
MAS	Autorité monétaire de Singapour
MFI	Institution de microfinance
MNO	Opérateur de réseau mobile
NCSC	Centre national de cyber-sécurité
NCSS	Stratégie nationale de cyber-sécurité
NIS	Réseaux et systèmes d'information
OES	Opérateurs de services essentiels
OTC	En vente libre
OTP	PIN à usage unique
PEP	Personne politiquement exposée
NIP	Numéro d'identification personnel
PFMI	Principes pour les infrastructures des marchés financiers
RegTech	Technologie réglementaire
DP	Demande de proposition
SACCO	Organisation coopérative d'épargne et de crédit
SEE	Environnement d'exécution sécurisé
PME	Petites et moyennes entreprises
SMS	Service de messages courts
SOC	Centre des opérations de sécurité
STR	Déclaration de transaction suspecte
SupTech	Technologie de supervision
TRM	Gestion des risques technologiques
USSD	Données de service supplémentaires non structurées

ANNEXE A
ENTRETIENS AVEC LES PARTIES PRENANTES

Les parties prenantes suivantes ont été interrogées au cours de la préparation de ce document.

NOM	TITRE	ORGANISME	RÔLE
Komitas Stepanyan	Chef adjoint de l'audit interne	Banque centrale d'Arménie	Autorité de régulation
Daniel Klu, RSSI	Responsable de la sécurité de l'information	Banque du Ghana	Autorité de régulation
Hakima El Alami	Directeur adjoint chargé de la supervision des systèmes et des moyens de paiement, et de l'inclusion financière	Banque Al-Maghrib, Maroc	Autorité de régulation
Fadwa Jouali	Responsable du développement des Fintech et des paiements	Banque Al-Maghrib, Maroc	Autorité de régulation
Mustapha Hadadi	Département de l'organisation et des systèmes d'information	Banque Al-Maghrib, Maroc	Autorité de régulation
Stephen Mathew Ambore	Chef, Services financiers numériques	Banque centrale du Nigéria	Autorité de régulation
Candy Ngula	Directeur adjoint	Banque de Namibie	Autorité de régulation
Thomas Lammer	Expert principal en infrastructures de marché, division de la surveillance	Banque centrale européenne	Autorité de régulation
Klaus Löber	Chef de division, Infrastructures de marché et paiements	Banque centrale européenne	Autorité de régulation
Killian Clifford	Directeur des politiques et du plaidoyer	GSMA	Organe de l'industrie
Munir Bello	Responsable technique de la certification de l'argent mobile	GSMA	Organe de l'industrie
Brian Muthiora	Directeur de la réglementation, Mobile Money	GSMA	Organe de l'industrie
Juliet Maina	Responsable du plaidoyer et de la réglementation, Mobile Money	GSMA	Organe de l'industrie
Daniel Schwartz	Directeur, Affaires politiques mondiales	Carte Mastercard	Organe de l'industrie
Amina Tirana	Responsable des politiques, de la recherche et de la mesure de l'impact social	Visa	Organe de l'industrie
Michael Nunes	Conseiller du Chef du gouvernement	Visa	Organe de l'industrie
Frank Adelmann	Expert du secteur financier (cyber-sécurité)	FMI	Organisme international
Vijay Mauree	Coordinateur de programme, département des groupes d'étude, TSB	ITU	Organisme international de normalisation
David Medine	Conseiller principal	CGAP	Organisme international
Seán Doyle	Chef de projet, gouvernance et politique en matière de cyber-sécurité	Forum économique mondial	Organisme international
Leon Perlman	-	Indépendant	Expert du secteur
David Cracknell	-	Premiers principes	Expert du secteur
Abbie Barbir	-	Alliance FIDO	Expert du secteur
Dave Birch	-	Consulter Hyperion	Expert du secteur

Alliance pour l'inclusion financière
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaisie
t +60 3 2776 9000 **e** info@afi-global.org www.afi-global.org
Alliance pour l'inclusion financière AFI.History @NewsAFI @afinetwork