Guide de la supervision des émetteurs de monnaie électronique

Guide technique

Décembre 2018

Denise Dias et Stefan Staschen

CGAP

Groupe consultatif d'assistance aux pauvres
1818 H Street NW, MSN IS7-700
Washington DC 20433
Internet : www.cgap.org
Courriel : cgap@worldbank.org
Téléphone : +1 202 473 9594

Droits et licences
L'utilisation de cet ouvrage est soumise aux conditions de la licence Creative Commons Attribution 4.0 International Public License (https://creativecommons.org/licenses/by/4.0/). Conformément aux termes de la licence Creative Commons Attribution, il est possible de copier, de distribuer, de transmettre et d'adapter le contenu de l'ouvrage, notamment à des fins commerciales, sous réserve du respect des conditions suivantes :

Mention de la source—L'ouvrage doit être cité de la manière suivante : Dias, Denise, et Stefan Staschen. 2018. « Guide de la supervision des émetteurs de monnaie électronique ». Guide technique. Washington : CGAP.

Traductions—Si une traduction de cet ouvrage est produite, veuillez ajouter à la mention de la source de l'ouvrage, le déni de responsabilité suivant : Cette traduction n'a pas été réalisée par le CGAP et ne doit pas être considérée comme une traduction officielle. Le CGAP ne saurait être tenu responsable du contenu de la traduction ni des erreurs qui peuvent y figurer.

Adaptations—Si une adaptation de cet ouvrage est produite, veuillez ajouter à la mention de la source le déni de responsabilité suivant : Cet ouvrage est une adaptation d'une œuvre originale du CGAP/de la Banque mondiale. Les idées et opinions exprimées dans cette adaptation n'engagent que l'auteur ou les auteurs de l'adaptation et ne sont pas validées par le CGAP/la Banque mondiale.

Pour tous renseignements sur les droits et licences, s'adresser à CGAP Publications, 1818 H Street, NW, MSN IS7-700, Washington, DC 20433 USA ; courriel : cgap@worldbank.org

Table des matières

Introduction

La mise en place d'un cadre réglementaire spécialisé pour les établissements non bancaires émetteurs de monnaie électronique (EME) est l'un des quatre fondements réglementaires qui favorisent le développement de services financiers numériques inclusifs dans les marchés émergents et les économies en développement (Staschen et Meagher, 2018). Pour les besoins du présent guide, les EME désignent tout établissement agréé - bancaire ou non - qui a pour vocation d'émettre de la monnaie électronique ou des comptes à valeur stockée similaires, même s'ils opèrent sous une dénomination différente, par exemple banque à objet limité ou banque de paiement[1].

Un cadre de réglementation spécial des EME ne peut être efficace que s'il s'accompagne des transformations nécessaires de la fonction de supervision. La supervision vise trois objectifs : i) s'assurer que les EME détectent les risques, les gèrent comme il convient et mettent en œuvre des mesures d'atténuation ; ii) veiller au respect de la réglementation ; et iii) préparer des procédures de gestion d'une crise des EME. Une supervision efficace permet à l'autorité de supervision de déceler et de gérer les risques avant qu'ils ne prennent de l'ampleur et de contribuer à réviser la réglementation sur la base de données factuelles. La question qui se pose est la suivante : comment superviser efficacement les EME ?

Une supervision proportionnelle permettra d'optimiser l'emploi de ressources limitées et d'éviter d'inhiber l'innovation et le développement des EME. Il n'existe pas une démarche proportionnelle universelle applicable à tous les EME, et ce qui sera proportionnel dans un pays peut être jugé disproportionnel dans un autre. Pour définir une approche, il faut comprendre les risques inhérents à un EME, à la lumière des activités que la loi autorise ces établissements à mener. À l'instar des banques, les EME collectent les fonds des clients et promettent de les rembourser, mais contrairement aux banques, ils n'accordent pas de crédits ni n'entreprennent d'opérations à risque. En réalité, les EME

[1] Ainsi, un EME peut être un établissement non bancaire (une entité qui ne mène pas d'activités d'intermédiation sur les fonds collectés auprès du public) ou une banque spécialisée dans l'émission de monnaie électronique et qui n'est pas autorisée à prêter des fonds, à l'instar des banques de paiement en Inde, des banques de niche au Mexique et des banques de paiement des services au Nigeria. Dans ce modèle d'établissement, les fonds des clients ne sont pas détenus dans des comptes de dépôt traditionnels, bien qu'ils soient accessibles par l'intermédiaire d'agents ou de supports numériques comme les téléphones mobiles (par exemple les prestataires de services bancaires à distance au Pakistan). Sauf indication contraire, le terme « banque » désigne aux fins de la présente publication les établissements bancaires classiques autorisés à mener des activités d'intermédiation et d'utilisation des fonds des clients.

sont généralement tenus d'avoir une contrepartie liquide de tout l'argent électronique qu'ils émettent (l'argent dû aux clients). En raison de cette différence fondamentale, les EME présentent un profil de risque moins important et n'ont pas besoin, par conséquent, d'une supervision réglementaire aussi rigoureuse que pour les banques.

La démarche proportionnelle détermine aussi si l'EME a une importance systémique en raison de sa taille, de la transversalité de ses activités, ou de tout autre caractéristique[2]. Le niveau de supervision variera par conséquent d'un EME à l'autre. Ainsi, une proportionnalité légère consistant en une surveillance ex situ et au contrôle de l'application des règles de protection des fonds suffira pour certains EME, notamment les plus petits dans un pays donné. Pour d'autres EME (plus grands, plus systémiques ou plus problématiques) dans le même pays, la démarche proportionnelle se traduira par des inspections couvrant tous les domaines traités dans cette publication et plus. De surcroît, la démarche adoptée par chaque pays dépendra de tout un ensemble de facteurs propres au contexte, comme les priorités en matière de supervision, l'expertise et les technologies existantes (SupTech)[3], et le niveau de mise en œuvre de la supervision axée sur les risques.

La présente publication a pour but de i) donner des orientations générales aux autorités de supervision des marchés émergents et économies en développement qui élaborent des stratégies en vue d'une supervision proportionnelle des EME et de ii) servir de référence pour la rédaction ou l'amélioration des manuels de supervision dans quelques domaines précis. Après la présentation générale du principe de la proportionnalité et de son application à la supervision des EME, le document décrit les procédures de supervision à adopter au cours des phases d'accréditation, de surveillance ex situ et d'examen des EME. Le document puise dans l'expérience des auteurs eux-mêmes, les entretiens avec un échantillon d'autorités de supervision[4], et les écrits en la matière, notamment les normes internationales et les guides de la supervision accessibles au public.

Les sujets traités concernent particulièrement la protection des fonds des clients, les risques opérationnels, les risques liés au blanchiment des capitaux et au financement

[2] Selon le Comité de Bâle sur le contrôle bancaire (BCBS) (2016a, p. 2) : « [D]ans certains pays, les institutions financières non bancaires ne seront peut-être pas systémiques sur la base de la valeur des fonds dont elles assurent l'intermédiation, mais peuvent avoir un caractère systémique en raison du nombre et du type de clients qu'elles servent ».

[3] SupTech est le terme utilisé pour désigner la technologie innovante mise au service de la supervision par les organismes concernés. Voir Broeders et Prenio (2018) et Dias (2018).

[4] Des entretiens en personne, téléphoniques ou écrits ont été organisés en 2017 avec des autorités financières chargées de superviser les établissements émetteurs de monnaie électronique dans les pays suivants : Autriche, Colombie, France, Ghana, Hong Kong, Inde, Luxembourg, Malaisie, Mexique, Myanmar, Nigéria, Ouganda, Pérou, Philippines, Royaume-Uni, Singapour et Tanzanie.

du terrorisme, ainsi que les plans de développement et la surveillance ex situ des EME. Il existe certainement d'autres domaines importants pour la supervision des EME qui ne sont pas abordés dans ce document. Par exemple, les mesures correctives et de mise en œuvre, la résolution des EME, l'examen de la compétence et de l'honorabilité des EME, les aspects transnationaux de la supervision des EME, et le rôle de l'interopérabilité, du *cloud computing* (l'informatique en nuage) et des interfaces de programmation d'applications (API) dans la supervision des EME. Le présent document ne couvre pas non plus tous les risques importants, en partie parce que certains de ces domaines sont traités dans d'autres publications. (Voir au Tableau 1 les définitions des risques les plus pertinents pour les EME, dont certains sont examinés dans le présent document).[5]

Alors que certaines autorités de supervision trouveront la combinaison de toutes les procédures décrites dans le présent document excessive ou complexe, d'autres la jugeront insuffisante et superficielle. Notre intention n'est nullement de proposer une liste exhaustive de sujets et de procédures, mais de montrer comment les analyses peuvent être menées dans les domaines couverts. À la lumière de leur ligne de supervision générale, les autorités de supervision peuvent incorporer tout ou partie des procédures dans leurs manuels et les déployer lors d'examens généraux ou spécialisés, de la surveillance ex situ ou d'évaluations thématiques.

Enfin, les procédures décrites sont manuelles, exigeant une nombreuse main-d'œuvre, la seule option possible dans de nombreux marchés émergents et économies en développement où la SupTech est à peine naissante. Des exemples sont donnés de cas où la SupTech pourrait réduire la charge de travail des autorités de supervision. Le niveau d'utilisation des technologies influera sur l'efficacité et la proportionnalité de la supervision des EME.

Ce document est destiné principalement aux autorités de supervision des marchés émergents et économies en développement chargées de la surveillance des EME. Les autorités de régulation, les décideurs et les organisations internationales qui encouragent une supervision efficace des EME pour une plus grande inclusion financière dans les marchés émergents et les économies en développement pourront aussi y trouver quelque intérêt.

[5] La protection des clients, la collecte des données dans le cadre de la supervision des EME et les conséquences du recours des EME à des agents sont traitées dans Dias (2013) ; Dias et Staschen (2017) ; et Dias, Noor et Staschen (2015) respectivement.

2. *La proportionnalité dans la supervision des EME*

2.1 Supervision proportionnelle des EME

Dans une démarche de supervision proportionnelle, les anticipations du superviseur doivent être à la mesure du profil de risque de l'EME (les risques liés aux activités de l'EME) et de son importance systémique. Ces anticipations déterminent le degré de supervision appliqué et la quantité des ressources employées. D'une manière générale, les EME demandent un examen moins rigoureux que les banques classiques. Le niveau d'intensité de la supervision variera d'un EME à l'autre : les EME de grande taille, systémiques ou problématiques peuvent exiger la supervision de tous les domaines traités dans cette publication, voire davantage, alors qu'une approche plus légère (limitée par exemple à la surveillance ex situ et/ou à l'évaluation des mesures de protection des fonds) peut suffire pour les petits EME ne présentant pas de problèmes particuliers.

Il n'existe pas une méthode universelle en la matière. Ce qu'une autorité de supervision juge proportionnel sera perçu comme disproportionnel par une autre. Les autorités de supervision ont des points de vue différents quant aux outils de supervision (suivi du marché, examens ex situ et in situ et évaluations thématiques), à la portée de la supervision (les domaines couverts) et à la profondeur de la supervision (le niveau de détail des examens, les techniques utilisées - procédures analytiques et audits - et leur fréquence).

2.2 Les banques et les EME : Des champs d'activités différents et des profils de risque différents

Jadis, les banques collectaient l'argent et d'autres avoirs (notamment l'or) auprès des clients pour les protéger (*fonction fiduciaire*). Après avoir noté que tous les clients (déposants) ne réclamaient pas la totalité de leurs avoirs au même moment, les banques ont entrepris de prêter une partie de ces avoirs à d'autres clients (*fonction d'intermédiation*). Ce fut l'avènement des services bancaires modernes, qui comportent des risques inhérents (liés au crédit, à l'asymétrie des échéances, aux liquidités et aux fonds propres). En acceptant ces risques, les banques jouent un rôle crucial dans la distribution des fonds dans l'économie. Les fonctions d'intermédiation et de levier de financement créent des risques fondamentaux, mais les banques entreprennent aussi de nombreuses autres opérations risquées, localement et au niveau transnational. Elles offrent en outre des services de paiement. À cause de leur complexité et des risques qu'elles assument (que les

Encadré 1. Méthodes de supervision des EME

Toutes les autorités de supervision interrogées pour les besoins de la présente étude assurent quelque supervision des EME, même dans les pays qui dispensent les petits EME d'agrément ou de supervision (notamment la France, le Luxembourg et le Royaume-Uni). Toutes assurent au moins le recueil de statistiques périodiques pour le suivi du marché, et certains (comme au Luxembourg) y ajoutent des examens de la sûreté et de la robustesse - vérification de la santé financière d'un EME - ainsi que des examens institutionnels. La plupart des autorités de supervision interrogées suivent des procédures établies qui couvrent quelques risques au niveau institutionnel et du marché et dont la portée et l'intensité sont très variables. Ainsi, certaines procédures ne couvriront qu'un petit nombre de problèmes systémiques, comme l'efficacité et la concurrence à l'aide de statistiques semestrielles (Banque centrale du Brésil), d'autres recueilleront fréquemment une foison de données et feront des inspections périodiques in situ sur les principaux risques, notamment la protection des clients et des fonds (c'est le cas de la majeure partie des autorités de supervision en Afrique subsaharienne), d'autres encore appliqueront une méthode basée sur les risques qui englobe tous les types de risque (à l'instar de la Commission de surveillance du secteur financier du Luxembourg).

petits déposants sont incapables d'évaluer à un coût raisonnable) et de leur importance pour l'économie, les banques sont depuis très longtemps fortement réglementées.

Les EME sont moins complexes, ils n'assurent aucune fonction d'intermédiation ou de levier pour les fonds des clients. Toutefois, ce qu'ils ont en commun avec les banques c'est la fonction fiduciaire : ils collectent les fonds auprès des clients qu'ils promettent de rembourser à une future date indéterminée[6]. Tout comme les banques, les EME doivent gérer les risques pour tenir cette promesse. Il existe pourtant une différence fondamentale : les banques gèrent tout un ensemble complexe de risques interreliés et elles attirent d'autres capitaux (elles ne disposent pas de fonds suffisants pour rembourser tous les déposants en même temps), alors que les EME sont tenus par la loi de toujours disposer de fonds suffisants pour rembourser intégralement tous leurs clients. Les règles de protection des fonds visent à protéger les clients et elles allègent la fonction de supervision. Les EME sont tenus de constituer un capital distinct équivalent à la somme totale des fonds collectés

[6] Cette fonction fiduciaire existe quelque que soit la définition qu'un pays donne aux dépôts de monnaie électronique par opposition aux dépôts bancaires.

auprès des clients et il leur est interdit de les placer. De surcroît, les pays plafonnent les transactions réalisées pour les comptes de monnaie électronique afin de limiter les risques pour les clients et les opérations, ainsi que les risques de blanchiment des capitaux[7]. Les EME ne connaissent pas la plupart des risques financiers auxquels s'exposent les banques.

Il n'en demeure pas moins que les EME comportent des risques. Plus important encore, les EME proposent des services de paiement (retraits, transferts et achats) au moyen d'une large gamme de supports faisant appel aux systèmes informatiques, aux télécommunications, aux partenariats d'entreprises, aux dispositifs d'externalisation, à un vaste réseau de personnel et d'agents, aux liens avec les commerçants et aux infrastructures de paiement, comme les transferts et d'autres systèmes de paiement. Ces éléments créent des risques opérationnels, des risques de blanchiment des capitaux/de financement du terrorisme, et des risques pour les clients, entre autres. Le Tableau 1 énumère les risques institutionnels les plus importants en ce qui concerne les EME, dont certains sont traités dans le présent document.

2.3 Les EME posent-ils un risque systémique ?

Les banques sont soumises à une surveillance rigoureuse en raison de leur importance systémique. Les facteurs fondamentaux pris en compte sont, entre autres, i) l'importance des financements bancaires dans l'économie, ii) la taille de la banque ou du groupe bancaire, iii) le risque d'un retrait massif des dépôts bancaires (notamment par un effet de contagion d'une banque en difficulté à une banque saine), et iv) les maillages entre les banques. Par exemple, une banque peut compter dans sa clientèle de grandes entreprises qui jouent un rôle de premier plan dans l'économie ; s'il advenait qu'elle cesse subitement de financer ces clients, le pays pourrait en souffrir. Ou encore, une banque peut avoir des millions de clients qui se ruent pour retirer leurs fonds parce qu'ils ont appris que l'établissement est en difficulté. Cette ruée peut s'étendre à d'autres banques. Enfin, parce que les banques prêtent et empruntent entre elles dans un circuit dynamique de transactions interbancaires, plus elles dépendent d'une certaine banque (par exemple pour les liquidités intrajournalières), plus la banque en question sera systémique. Et si cette banque fait faillite, d'autres sont susceptibles de la suivre.

Toutes les autorités de supervision interrogées—y compris dans les pays où les EME ont atteint une envergure certaine—s'accordent à dire que les EME dans leurs pays posent peu ou pas de risque systémique.

[7] Voir Staschen et Meagher (2018) et CPMI (2016, p. 26 et 27).

Tableau 1. Les risques liés aux EME

Risque	Description
Risque de perte ou d'emploi impropre des fonds des clients (traité dans le présent document)	C'est le risque que i) les employés de l'EME ou ses agents ou des parties tierces aient accès aux fonds des clients et les utilisent, notamment pour les prêter ou les investir, que ii) les EME ne gèrent pas les soldes des comptes des clients, et que iii) les clients ne puissent disposer de leurs fonds parce que l'EME est en faillite ou que la banque retient ces fonds. Bien que ce risque puisse sembler faire partie d'autres risques décrits dans le tableau, il est singularisé parce qu'il est au centre de l'activité de supervision.
Risques opérationnels et informatiques (Couvert en partie dans ce document)	Gouvernance et contrôles internes - l'absence d'une bonne gouvernance des risques, de supervision du conseil d'administration et d'un cadre efficace de contrôle institutionnel peut conduire à la matérialisation des risques.
	Risques liés aux données et à la cybersécurité - c'est le risque que les avoirs physiques et numériques, comme les données sur les clients, le matériel informatique et les réseaux soient exposés. Ce risque est étroitement lié aux risques de fraude et de violation des données confidentielles[a].
	Risque lié au règlement - c'est le risque que le remboursement attendu n'aie pas lieu. Il couvre le risque d'illiquidité et de crédit des contreparties. Les faillites opérationnelles de l'EME ou de ses contreparties peuvent créer un risque lié au règlement.
	Risque de fraude - fraudes internes (par les employés par exemple) et externes (notamment par les clients et les cybercriminels). Le nombre de cas de fraude signalé dans les EME à travers le monde ne cesse de croître, particulièrement les fraudes internes par le personnel, parfois en collusion avec les agents.
	Risques pour la continuité des activités - faiblesses dans la gestion, l'entretien ou la robustesse des équipements, des réseaux, des connexions et des installations physiques ; incapacité à se préparer aux catastrophes ou à les affronter (inondations, incendies par exemple) ; et le manque de compétences fondamentales. Ce risque peut entraîner une interruption des opérations.
	Risques liés aux agents - un élément central du risque opérationnel qui peut amplifier le risque de blanchiment d'argent/de financement du terrorisme, les risques pour les clients, et d'autres risques. Tous les risques opérationnels ne sont pas imputables aux technologies. Bon nombre découlent des comportements des individus, comme le non-respect des politiques en raison du manque de formation ou de la non application de la réglementation. En ce qui concerne les EME, il existe un risque de manque de liquidité (ce qu'on appelle généralement « illiquidité de l'agent ») au niveau des agences et un risque lié à la non vérification des antécédents des clients.
	Risques liés aux parties tierces - outre les risques liés aux agents, les EME font face à des risques liés à leurs relations d'affaires (par exemple les opérateurs des systèmes de paiement, des cartes, des télécommunications, les prestataires des services d'informatique en nuage et les entités reliées par des interfaces de programmation d'applications).
Risque d'illiquidité (non traité dans ce document)	Le risque que l'EME ne dispose pas de fonds suffisants pour faire face à ses obligations (fournisseurs, sous-traitants, employés) en temps voulu. Ce scénario est différent de celui où les agents de l'EME n'ont pas de liquidités pour servir les clients.
Risque lié au blanchiment d'argent/ au financement du terrorisme (traité dans ce document)	Le risque que les comptes et transactions impliquant la monnaie électronique ne soient utilisés pour financer des activités terroristes et blanchir le produit d'activités criminelles. Pour limiter ce risque, les transactions en monnaie électronique et les soldes des comptes des clients sont généralement soumis à des plafonds réglementaires.
Risques pour les clients (non traité dans ce document)	Communication peu efficace ou non communication d'informations essentielles, clauses contractuelles iniques, produits inadaptés, pratiques commerciales injustes, absence de mécanismes de règlement des différends à l'amiable (notamment des voies de recours internes). Les risques liés à la confidentialité des données, les risques de perte des fonds et les retards dans la conclusion des transactions sont autant de sujets de préoccupation.
Risques stratégiques (partiellement traités dans ce document)[b]	Le risque de pertes graves à cause de mauvaises décisions stratégiques (expansion dans de nouveaux marchés par exemple) qui pourraient couler l'EME.
Risques juridiques (non traités dans ce document)	Situations où les droits et obligations des parties à un contrat (par exemple la responsabilité vis-à-vis des clients en cas d'échec d'une transaction) sont incertains. Il peut s'agir par exemple de l'absence de protection légale des fonds des clients regroupés dans des comptes de fiducie et des coûts potentiels des exigences légales envers un EME en cas de non-respect de la réglementation (par exemple le droit du travail).

Source : CPMI (2016, 2014, 2000).

[a] Voir CGAP (2018).

[b] Une partie de l'analyse stratégique des risques est réalisée lors de l'examen des plans de développement, sujet qui est traité à la section 3.

Bien qu'ils n'offrent pas de financement, les EME peuvent assurer les services de stockage des fonds et de paiement à leurs clients. Les autorités de supervision des marchés émergents et économies en développement doivent déterminer si un EME pose un risque systémique et comprendre que certains de ces établissements peuvent devenir des géants en très peu de temps. Pour déterminer l'importance systémique d'un EME, les autorités de supervision doivent poser les questions suivantes :

- Un EME peut-il devenir si important (en termes de nombre et de types de clients) que la survie de nombreuses personnes serait gravement compromise si cet EME faisait faillite et se trouvait donc dans l'incapacité de fournir un service vital ou très apprécié ?
- L'échec d'un EME pourrait-il entamer la confiance du public dans ce secteur et donc, déclencher un effet de contagion ?
- L'échec d'un EME pourrait-il entamer la confiance du public dans les banques ou d'autres institutions financières réglementées ?
- Quels types d'entreprises (services publics, sociétés privées) s'appuient largement sur les EME ? Dans quelle mesure une perturbation des opérations des EME nuirait-elle à ces entreprises ? Des pertes considérables sont-elles envisageables ?
- Un EME est-il devenu un système de paiement d'importance systémique ?[8]
- Un EME peut-il introduire des risques dans le système de paiement national ?[9]
- Un EME peut-il influer sur les banques en les mettant plus en contact avec de grands déposants (soldes importants dans les comptes de monnaie électronique) ?[10]
- Un EME peut-il compromettre la rentabilité des banques en leur faisant concurrence pour la clientèle, en limitant l'accès aux réseaux d'agents, etc. ?
- Un EME peut-il servir d'intermédiaire pour le blanchiment d'importants montants d'argent illégal ?

2.4 Accroître l'efficacité des visites in situ par une meilleure préparation ex situ

Le principe de la proportionnalité exige de rechercher l'efficacité de la surveillance ex situ et des procédures in situ et ex situ pendant un examen[11]. Par exemple, anticiper le

[8] CPMI (2001, p. 14) donne des orientations sur la manière de déterminer qu'un système de paiement a une importance systémique. Ces orientations concernent exclusivement la stabilité du secteur financier et ne couvrent pas la protection des consommateurs, la concurrence et la prévention des délits, qui peuvent être des considérations importantes pour les EME.

[9] Les EME peuvent participer au système de paiement national—plus précisément en étant reliés au système de règlement brut en temps réel—dans un petit nombre de pays uniquement (par exemple au Royaume-Uni).

[10] Voir Kerse et Staschen (2018) pour en savoir plus sur le risque de concentration.

[11] Le mot « examen » est utilisé dans le présent document pour désigner une évaluation visant un seul EME. Un examen comporte souvent à la fois des procédures ex situ et in situ et sa portée peut considérablement varier. Les pays emploient différents termes pour désigner l'évaluation d'une institution.

travail de préparation ex situ (c'est-à-dire assurer une surveillance ex situ continue et de qualité et, pendant les examens, demander et analyser les documents et les données avant de descendre sur le terrain) peut optimiser la visite in situ. Pour préparer une visite sur le terrain, il peut s'avérer nécessaire de demander des informations à l'EME (politiques/procédures et un ensemble de données granulaires), et puis d'assurer le suivi par des requêtes spéciales (par exemple, un échantillon de transactions).

Certaines autorités de supervision dans les marchés émergents et économies en développement n'adressent qu'une seule demande de documents avant la visite sur le terrain.

La souplesse dans la préparation d'un examen qui comporte des visites in situ permet aux autorités de supervision de faire plusieurs demandes à l'EME et d'organiser les premières conclusions en vue du suivi une fois sur le terrain. Cette démarche s'avère plus efficace et fait gagner du temps aussi bien à l'autorité de supervision qu'à l'EME.

De surcroît, les outils de SupTech pourraient rendre l'analyse des données, les audits des systèmes, les tests de pénétration, etc. plus efficace et efficients. Les applications d'apprentissage automatique, qui sont largement accessibles, peuvent identifier des tendances et des corrélations qui indiqueraient, par exemple, des changements non autorisés dans les dossiers des clients, des tentatives d'intrusion et des transactions suspectes[12]. Cependant, la qualité du produit des outils de SupTech en aval dépendra de celle des données utilisées en amont, de sorte que l'autorité de supervision peut devoir elle-même améliorer d'abord ses propres données.[13]

Les données s'entendent des informations classiques régulièrement communiquées par les EME et des données non normalisées (non structurées), telles que les anciens rapports de supervision, les demandes d'agrément, les rapports de gestion, les évaluations thématiques, les accords d'agence, les contrats des clients, etc. La supervision est plus efficace lorsque ce type de données est utilisé, mais elles ne s'obtiennent pas toujours facilement.

Les autorités de supervision des marchés émergents et économies en développement ont beaucoup de mal à utiliser les données non structurées, non normalisées. Elles passent de longues heures à parcourir des documents dans lesquels l'information est présentée sous une forme narrative ou en données numériques non structurées, en format PDF ou sur du papier imprimé.

[12] Voir Dias (2018) et FSI (2018) pour plus d'exemples.
[13] Voir Dias et Staschen (2017) pour en savoir plus sur les données de supervision et les mécanismes de collecte des données sur les services financiers numériques.

Les solutions SupTech permettent, entre autres, d'utiliser des logiciels d'analyse pour intégrer un nombre varié de formats de données et les rendre utilisables[14]. Ainsi, grâce aux logiciels d'analyse, les utilisateurs peuvent rechercher et analyser automatiquement des documents numérisés, et faire une analyse croisée des données structurées et non structurées à partir de sources variées afin d'éclairer les investigations menées dans le cadre des activités de supervision. Les outils de SupTech peuvent considérablement faciliter le tri et l'analyse de gros documents-textes comme les politiques et les manuels de procédure.

2.5 Une supervision des EME axée sur les risques

Les autorités de supervision peuvent appliquer une méthodologie basée sur les risques pour préparer une démarche de supervision proportionnée des EME. Cette méthodologie offre une vue systématisée des risques et de leur importance relative dans un EME et d'un EME à l'autre et peut aider à normaliser les procédures en matière de supervision. Elle aide aussi les autorités de supervision à augmenter ou à réduire le niveau de supervision des différents EME dans le temps, dans une démarche structurée, qui tient compte des évaluations antérieures des EME. Dans une approche axée sur les risques, les procédures de supervision, comme celles décrites dans la présente publication, sont appliquées à la lumière d'une première évaluation des risques reposant sur une analyse complète des données. La matrice des risques sert généralement à résumer le profil de risque d'une institution réglementée.

Il n'existe pas un modèle universel de méthodologie axée sur les risques ou de matrice des risques que toutes les autorités de supervision des EME pourraient utiliser. En général, chaque autorité de supervision a sa définition du risque, des catégories de risque et des facteurs de risque, et les pondérations relatives que l'une ou l'autre choisit d'attribuer à chaque matrice des risques sont elles aussi différentes. Ces autorités créent en outre une notation des risques et des méthodes d'évaluation des tendances différentes. Une matrice des risques conçue pour une banque ne cadrera pas avec le profil de risque d'un EME et devra être adaptée.

Certes, toutes les autorités de supervision interrogées ont indiqué qu'elles utilisaient une approche axée sur les risques pour superviser les banques, mais seules quelques-unes ont adapté leur méthodologie aux EME.

[14] Voir Bauguess (2018) pour en savoir plus sur les données de supervision lisibles en machine (données sous une forme utilisable par les logiciels d'analyse).

Encadré 2. Supervision axée sur les risques

Dans une approche axée sur les risques, l'activité de supervision se concentre sur les risques les plus importants que présentent les marchés réglementés[a]. Des orientations sont ainsi formellement données sur ce que doivent être les priorités de l'activité de supervision, comment cette dernière doit être menée, et comment les décisions doivent être prises.

Les méthodologies axées sur les risques sont généralement synthétisées dans des matrices des risques. Une matrice des risques décrit tous les risques inhérents à un type d'activité - notamment les fonctions autorisées pour le type d'institution concerné - et tous les facteurs de risque correspondant à chaque catégorie de risque. Elle pondère les facteurs et les catégories de risque par rapport à leur importance relative pour le type d'activité concerné. En se fondant sur l'évaluation effective des risques concernant une institution, les autorités de supervision indiquent dans quelle mesure l'institution en question réussit ou non à atténuer les risques inhérents à ses activités au moyen de la gouvernance, de la gestion des risques et des contrôles internes. La dernière phase de la méthodologie consiste à attribuer une cote de risque à chaque institution qui sera comparable d'une institution à l'autre. La matrice permet de mieux planifier l'activité de supervision et de mieux employer les ressources. Plus il existe des domaines de risque dans un type d'institution réglementé, plus la matrice aidera à définir les priorités de l'activité de supervision et à synthétiser les résultats des examens.

[a] Pour en savoir plus sur la supervision axée sur les risques, voir Wright (2018).

2.6 Modalités organisationnelles de la supervision des EME

Il n'existe certes pas une manière unique d'envisager l'hébergement de la fonction de supervision des EME, mais la monnaie électronique est un service financier et la supervision devrait donc ressortir aux autorités du secteur financier (par exemple la Banque centrale) et non aux autorités des télécommunications, même lorsque les EME sont des filiales des opérateurs de téléphonie mobile[15]. Les modalités internes concernant la supervision des EME varieront d'une autorité du secteur financier à l'autre.

[15] Dans au moins un pays, le Kenya, la banque centrale peut autoriser les opérateurs de téléphonie mobile à devenir des EME, auquel cas les activités liées à la monnaie électronique sont régulées par la banque centrale qui en assure la supervision. Dans la plupart des pays pourtant, l'EME doit être une entité juridique distincte spécialisée dans l'émission de monnaie électronique.

Dans tous les pays étudiés, les autorités du secteur financier confient la supervision des EME à une entité de supervision financière - généralement la banque centrale - plutôt qu'à d'autres entités du secteur financier comme le ministère des finances. Dans un petit nombre de pays, une entité de supervision indépendante (par exemple, une haute autorité bancaire) assume cette fonction. Dans la plupart de ces cas, la banque centrale continue d'assurer la régulation des paiements et le contrôle des systèmes de paiement (en mettant l'accent sur l'infrastructure, la sécurité et l'efficacité).

Au Royaume-Uni, un régulateur indépendant - le Payment Services Regulator (PSR) - fut créé en 2015. Le PSR assure la régulation des prestataires des services de paiement et des opérateurs des systèmes de paiement, tandis que le Financial Conduct Authority supervise les prestataires des services de paiement, dont les EME. La Bank of England se charge de la supervision du système de paiement national pour en garantir la stabilité et de la gestion des principaux systèmes de paiement.

Les démarches divergent aussi à l'intérieur des autorités de supervision. Dans la majorité des pays africains étudiés (Ghana, Kenya, Rwanda, Tanzanie), le service des paiements de la banque centrale - qui s'occupe principalement de contrôler les systèmes de paiement - est devenu le superviseur des EME. Dans la plupart des cas, les fonctions de contrôle et de supervision sont séparées des opérations bancaires centrales (notamment les systèmes de règlement brut en temps réel, la compensation des chèques, les opérations des marchés). À Hong Kong et Singapour où la banque centrale fait aussi office d'autorité de supervision des EME, c'est le service de la supervision de la banque qui joue ce rôle de superviseur. Dans les pays où il existe une entité indépendante de supervision financière distincte de la banque centrale (Autriche, France, Luxembourg, Mexique, Royaume-Uni), cette entité comprend très souvent une équipe dédiée aux prestataires des services de paiement.

D'après l'expérience des autorités de supervision interrogées, il est très utile d'avoir une équipe spécialisée dans les risques opérationnels et informatiques qui couvre toutes les entités réglementées, notamment les EME. C'est le cas par exemple dans les pays suivants : Autriche, Brésil, France, Hong Kong, Luxembourg, Malaisie, Mexique, Pérou, Philippines et Singapour. Dans certains de ces pays, on trouve aussi des équipes dédiées au blanchiment des capitaux/financement du terrorisme et aux pratiques sur le marché, et certains autres ont des équipes spécialisées dans la cybersécurité (à l'instar du Financial Conduct Authority au Royaume-Uni).

Toutes les modalités organisationnelles exigent un minimum de coordination. La coordination interinstitutionnelle est importante sur le plan de la régulation (par exemple, la régulation des opérateurs de téléphonie mobile sur l'accès à des canaux comme l'USSD) et de la supervision (notamment le suivi par les autorités chargées de la protection des données, l'évaluation de l'impact des activités liées à la monnaie électronique sur les

activités des opérateurs de téléphonie mobile et vice-versa, le suivi de l'assurance mobile par l'autorité de supervision des assurances, etc.). La coordination entre les services est nécessaire, par exemple, entre les services de contrôle des paiements et de supervision des EME, entre la supervision des EME et la supervision des banques (pour puiser dans l'expérience en matière d'examen des banques, vérifier le respect des limites imposées aux transactions liées à la monnaie électronique dans les banques et coordonner les actions en cas de résolution de l'EME), et entre les équipes de supervision des EME et les équipes spécialisées (risques opérationnels).

3. Octroi d'agréments aux EME : Examen du plan d'affaires

Dans bon nombre de pays, les EME ont besoin d'obtenir un agrément pour mener leurs activités[16]. Les autorités de supervision effectuent toute une série d'analyses des demandes d'agrément pour s'assurer que l'EME, son propriétaire et sa direction satisfont à un certain nombre de critères, notamment aux exigences de fonds propres, d'honorabilité et de compétence. Certaines autorités de supervision procèdent à une inspection des EME avant qu'ils n'entrent en activité et vérifient ainsi les antécédents des actionnaires importants, des membres du conseil d'administration, des hauts cadres et d'autres fonctions essentielles dans l'établissement.

Nous n'abordons pas dans cette section toutes les questions concernant la procédure d'agrément. L'accent est davantage mis sur des indications fondamentales concernant l'analyse des plans d'affaires des EME.

Dans les juridictions où les EME sont soumis à une procédure d'agrément, toutes les autorités de supervision interrogées exigent un plan d'affaires (et des prévisions financières), et certaines (comme le CSSF de Luxembourg et la Bank Indonesia) exigent en outre une mise à jour périodique de ce plan après l'octroi de l'agrément.

Les plans d'entreprise peuvent être examinés du double point de vue de leur qualité en tant qu'outil de planification, et de leur robustesse intrinsèque.

Un mauvais plan d'entreprise peut indiquer soit une incapacité dans la planification, soit une volonté de soustraire des informations à l'attention de l'autorité de supervision. Un plan qui est mauvais dans son contenu peut laisser entrevoir un risque stratégique découlant d'un mauvais sens des affaires. Ces considérations valent autant pour les plans d'affaires des nouveaux EME que pour ceux des institutions déjà établies. Les EME peuvent mettre à jour leurs plans périodiquement pour adapter les stratégies et les prévisions aux évolutions du marché et à leurs résultats antérieurs.

[16] Le terme « agrément » est utilisé ici au sens large pour désigner toute procédure d'autorisation statutaire à laquelle doit se soumettre l'EME avant de commencer toute activité ou de poursuivre ses activités si une nouvelle réglementation est adoptée. Dans d'autres pays, on parle aussi « d'enregistrement » et « d'autorisation ».

Lorsqu'elles évaluent la qualité d'un plan d'entreprise, les autorités de supervision doivent garder à l'esprit les points suivants :

- Le plan doit être complet et exhaustif.
- La somme des parties du plan doit se tenir, sans trop d'incohérences.

Certes, l'organisation d'un plan d'entreprise et les intitulés de ses différentes parties ne répondent pas à un canon particulier, mais d'une manière générale un plan complet (quel que soit le type d'organisation) décrit la stratégie globale, les opérations et les prévisions financières. Le Tableau 2 donne un exemple de structure du plan d'affaires d'un EME

Dans un mauvais plan d'entreprise, des éléments importants peuvent ne pas être abordés ou être mal traités. Et même lorsque ces éléments sont abordés et traités en détail, il peut survenir des incohérences. À titre d'exemple, un EME peut prévoir une croissance irréaliste du nombre de clients et de transactions sans préparer une stratégie de gestion de la concurrence ni un plan ambitieux d'élargissement du réseau d'agences, ou encore sans prévoir des ressources suffisantes pour couvrir les dépenses de commercialisation. Les autre incohérences peuvent concerner, entre autres, l'asymétrie entre les recettes prévues et l'étroitesse du segment de marché ciblé (par exemple, uniquement des agriculteurs en

Tableau 2. Possible structure d'un plan d'affaires d'un EME

Risque	Description
Le plan stratégique	i. Mission, vision, objectif ii. Étude de marché a. Panorama du marché, taille totale et potentiel de croissance b. Tendances du marché, aperçu de la concurrence c. Segments de marché et segments cibles d. Positionnement (les besoins des segments cibles auxquels on répond) e. Produits/services offerts f. Parts de marché prévues g. Facteurs de succès (par exemple, réseau d'agents, conception du produit, engagement des actionnaires, réglementation, partenariats, technologies, infrastructure) iii. Analyse des forces, faiblesses, opportunités et menaces iv. Récapitulatif de la stratégie de l'entreprise
Le plan opérationnel	i. Produits et services ii. Modèle économique et partenariats iii. Croissance et stratégie d'investissement iv. Stratégie de commercialisation v. Gouvernance, structure organisationnelle et effectifs vi. Systèmes, contrôles et gestion des risques vii. Feuille de route de la mise en œuvre (calendrier)
Plan financier (aussi prévisions financières ou plan de viabilité)	i. Hypothèses de base (taux d'inflation, coût des fonds, croissance du PIB) ii. Capital de départ, plan d'investissement et d'apport de capitaux, source des fonds iii. Recettes prévues, dépenses d'investissement, dépenses de fonctionnement, pertes/profits iv. Principaux indicateurs de performance financière v. États financiers prévisionnels

milieu rural), des dépenses d'investissement élevées (mobilier, infrastructure informatique, logiciels de gestion des risques) par rapport à un faible budget, et des disparités dans l'exposé du plan et les prévisions financières.

L'autorité de supervision doit avoir des connaissances sur les activités de l'EME en général, et sur les conditions du marché local en particulier, pour déterminer si les hypothèses sous-tendant les prévisions financières sont raisonnables; Ainsi, l'étude de marché qu'aura faite l'EME (description des concurrents et de leur stratégie, taille du marché, accès à des infrastructures comme les services de mobilité bancaire et des compétences spécialisées) peut être inexacte, et d'autres hypothèses (croissance du PIB, coût du financement, indicateurs socioéconomiques et démographiques, taille du segment de marché cible, taux d'adoption par les clients, accroissement des recettes, etc.) peuvent être par trop optimistes. L'objectif est de juger de la rationalité des prévisions ; aucun plan n'est infaillible.

Des experts de la planification et de l'analyse financière, s'il y en a, peuvent vérifier les calculs des prévisions financières. Pour ce faire, ces dernières doivent être numérisées (en format Excel ou autre) pour permettre un examen minutieux des formules. La prochaine section donne des orientations de base pour l'analyse des principaux indicateurs de performance en vue de l'octroi de l'agrément.

Pour évaluer les plans d'entreprise des EME (particulièrement les prestataires d'argent mobile), les autorités de supervision doivent considérer la trajectoire de développement type d'un EME, selon les schémas vus avec les transactions liées à l'argent mobile qui reposent sur de nombreux réseaux d'agences. (Cette trajectoire peut ne pas s'appliquer à d'autres modèles d'entreprise). Trois phases de croissance sont présentées ci-dessous :[17]

- Démarrage—dépenses d'investissement importantes, accroissement des dépenses de fonctionnement, probabilité de pertes
- Expansion importante—accroissement des dépenses de fonctionnement, accroissement des recettes, bénéfices modiques, investissement dans la conquête des clients grâce au personnel de vente et la commercialisation
- Maturité—potentielles sources de revenus supplémentaires grâce à la diversification des produits et aux partenariats, bénéfices solides

[17] Almazán et Vonthron (2014) notent que la part la plus importante des dépenses de fonctionnement en ce qui concerne les EME dans les premières années d'activité est celle consacrée aux investissements dans la plateforme de monnaie électronique et la mise en place d'un réseau d'agents qui comporte des charges de commission et des efforts sur le plan commercial. Un petit bénéfice peut être tiré dans la deuxième ou la troisième année, alors que les charges liées à l'acquisition d'agents et aux commissions continuent d'être élevées par rapport aux recettes.

4. Surveillance ex situ des EME

Le suivi permanent - ou la surveillance - ex situ est un facteur clé de la supervision des EME axée sur les risques. La surveillance continue permet aux autorités de supervision de noter (et comparer dans le temps) les variations dans les profils de risque des différents EME. Elle leur permet aussi de détecter les signaux de risques pouvant faire anticiper les activités de supervision (notamment les mesures correctives) (comme une inspection sur la protection des fonds, la fraude ou les risques stratégiques). Surveiller signifie étudier le marché de l'EME (par exemple le développement du marché) et chaque EME, parce que la surveillance est une partie intégrante de la planification de la supervision, de l'examen des EME et du processus réglementaire.

Seul un petit nombre des autorités de supervision des marchés émergents et économies en développement interrogées réalisent une étude complète du marché (surveillance ou contrôle) de façon continue, alors que cette pratique est courante chez les autorités de supervision des pays développés.

La surveillance ex situ peut comporter l'analyse de données internes standardisées et non structurées émanant de l'autorité de supervision (notamment les rapports soumis par les EME) et de données externes (statistiques publiques et données des opérateurs de téléphonie mobile). Elle peut aussi intégrer des données financières (principaux indicateurs, par exemple) et des données non financières (plaintes des clients, volume des transactions)[18]. En règle générale, l'analyse suit une méthodologie normalisée et des critères uniformisés définis par l'autorité de supervision en fonction de ses objectifs (voir quelques exemples au Tableau 3). Au regard des objectifs fixés, la profondeur et la fréquence des analyses dépendront des données, de la technologie disponible, des compétences de l'autorité de supervision et des priorités définies dans la méthodologie axée sur les risques.

L'évaluation des résultats financiers des EME peut ne pas être la priorité première de l'autorité de supervision, mais le suivi efficace et continu des principaux indicateurs financiers et d'autres mesures des activités peut aider à fixer les priorités de l'activité de supervision.

[18] Voir Dias et Staschen (2017) pour un aperçu des données recueillies par les autorités de supervision des EME.

Tableau 3. Exemples d'objectifs de la surveillance ex situ et données s'y rapportant

Objectifs	Exemples de données utilisées
Mesurer le risque systémique et l'importance relative des EME	Volume et valeur de l'ensemble des transactions des EME par rapport aux transactions bancaires ou aux transactions du système de règlement brut en temps réel ou d'autres systèmes de paiement, taille du flottant et nombre de clients par rapport au total des dépôts bancaires et des clients des banques. Nombre et type de flux financiers importants (par exemple, les salaires des fonctionnaires et les transferts sociaux), valeur totale des transactions par rapport au PIB ou à la valeur totale des paiements effectués par les banques par le système de règlement en temps réel, les perturbations opérationnelles des EME considérées comme systémiques, etc.
Surveiller le développement du marché et l'inclusion financière[a]	Nombre et localisation des agents ; chevauchement des agences avec le champ des opérateurs de téléphonie mobile (tours) et autres indicateurs démographiques et socioéconomiques officiels (par exemple, les écoles, les établissements de santé, la population totale) ; le nombre d'agents par adulte ou la population totale par segment de la population (rural/urbain) ; nombre et valeur des transactions totales des EME par type de transaction (par exemple, vérifier si les moyens de paiement numériques gagnent en importance, par rapport au numéraire) ; nombre de transactions entre EME et entre EME et banques (interopérabilité) ; nombre d'agents partagés/exclusifs, etc. Pourcentage d'adultes se trouvant dans un certain périmètre d'un agent ou d'autres points d'accès ; taux de pénétration des comptes en milieu urbain et rural ; par population adulte totale et par certaines ventilations comme par sexe, âge ou niveau de revenu ; nombre de clients d'EME ayant un compte bancaire, une assurance ou un crédit, pourcentage de comptes EME actifs, etc.
Évaluer la performance individuelle et relative des EME, et fixer des indicateurs de référence	Indicateurs de performance clés (voir le Tableau 4)
Vérifier la conformité aux exigences réglementaires	Ratio de fonds propres minimum par rapport aux émissions totales de monnaie électronique, ratio de liquidité minimum, limites réglementaires aux soldes ou dépôts, flottant total par rapport au solde dans le compte de monnaie électronique, solde du compte de monnaie électronique par rapport au total des dépôts dans les banques hébergeant les comptes de monnaie électronique, etc.
Blanchiment des capitaux/financement du terrorisme	Profils des volumes et valeurs des transactions par type, agent, localisation (notamment les lieux considérés comme risqués comme les villes frontalières), statistiques des transactions suspectes signalées, etc.
Protection des clients et concurrence	Nombre de plaintes par type de plainte et statut, commissions par type de transaction ; localisation et durée des interruptions des services des opérateurs de téléphonie mobile et des EME ; nombre de transactions ratées (non achevées) ; durée, localisation et fréquence des pannes du système ; volume des fraudes, types et localisation ; etc. Commissions interbancaires sur les transactions d'interopérabilité, part de marché des EME, recettes par rapport au volume des transactions, commissions pour un type précis de transaction (transfert entre particuliers, dépôts, retraits), nombre et localisation des agents exclusifs, commissions d'agents, etc.

[a] Voir CPMI (2017) pour les normes en matière de statistiques des paiements de détail afin de mesurer le développement du marché, et CPMI (2016, p. 59–62) pour les indicateurs du suivi de l'inclusion financière.

Toutes les autorités de supervision interrogées ont indiqué que les états financiers (bilan, compte de résultat), les indicateurs prudentiels (les ratios de fonds propres et de liquidité, par exemple) et les indicateurs de performance clés (notamment le rendement des actifs, le rendement des capitaux propres, les dépenses d'investissement, etc.) sont exigés à des degrés divers et des fréquences variables.

Le Tableau 4 présente quelques indicateurs financiers et commerciaux. Le type et le nombre d'indicateurs utilisés dépendront des préférences et des capacités d'analyse de l'autorité de supervision ainsi que de la disponibilité d'outils de SupTech et de données saisies. De nombreux indicateurs peuvent être extraits des états financiers communiqués périodiquement par les EME, alors que pour d'autres, des données supplémentaires (par exemple, les émissions totales de monnaie électronique ; le nombre de comptes/de clients ; les commissions versées aux agents ; les commissions des partenariats avec des parties tierces, comme les établissements de crédit ; et les commissions par type de produit) doivent être recueillies.

Toutes les autorités de supervision interrogées rencontrent les EME en dehors du cadre précis des examens, mais peu nombreuses sont celles qui intègrent cette possibilité de recueillir des informations dans leur méthodologie officielle de supervision axée sur les risques. Par exemple, certaines organisent des réunions d'information annuelles ou prévoient des rencontres avec telle ou telle institution, tandis que d'autres rencontrent les EME de façon ponctuelle, au gré des besoins ou des demandes des EME

Les autorités de supervision recueillent aussi des informations sur le marché dans le cadre de la surveillance continue du marché. Elles rencontrent les EME, les associations professionnelles et les parties tierces averties[19]. Les autorités de supervision peuvent évoquer leurs attentes en matière de conformité, leurs préoccupations du moment et les grandes conclusions de leur activité de supervision lors de leurs rencontres avec les EME.

[19] Voir BCBS (2016b) pour les indications sur la connaissance du marché.

Tableau 4. Exemples d'indicateurs financiers et commerciaux pour la supervision des EME

Indicateurs commerciaux
Émissions totales de monnaie électronique (flottant)
Nombre de comptes détenus par l'EME
Nombre de clients de l'EME
Nombre et valeur des transactions
Indicateurs financiers
BAIIDA : Bénéfices avant intérêts, impôts, dépréciation et amortissement
Marge de BAIIDA (marge nette) : BAIIDA en % des recettes brutes
Ratio des OPEX : Dépenses d'exploitation (OPEX) en % des recettes brutes
Ratio des CAPEX : Dépenses d'investissement (CAPEX) en % des recettes brutes
ROE : Le rendement des capitaux propres (ROE) est égal au résultat net en % des capitaux propres
ROA : Le rendement des actifs (ROA) est égal au résultat net en % des actifs
Recettes brutes : Revenu total des activités commerciales (notamment la fourniture aux clients des services de paiement, de retrait ou de transfert contre une commission)
Sources des recettes
• Commissions des transactions par type de produit/service
• Commissions récoltées auprès des partenaires (assureurs, prêteurs)
• Autres sources de revenu (produit des intérêts et investissements)
Revenu des commissions en % des recettes brutes
Revenu des commissions en % du nombre de transactions
Revenu des commissions en % du nombre de clients de monnaie électronique
OPEX : Dépenses d'exploitation, par types de dépense (commissions d'agents, par exemple)
OPEX par nombre de salariés
Total des commissions d'agents et des frais des gestionnaires du réseau d'agents
Total des commissions d'agents en % du nombre d'agents
Total des commissions d'agents en % du nombre de transactions
CAPEX : Dépenses d'investissement (mise à jour de la plateforme de monnaie électronique, par exemple)
Capital : Fonds réservés sous forme de capital (par exemple, fonds propres)
Ratio de fonds propres (solvabilité) : Que la réglementation exige ou non des EME qu'ils constituent un capital ou niveau de fonds propres minimum correspondant aux actifs ou au flottant, il est utile de contrôler leur solvabilité.
Ratio de liquidité : Les actifs à court terme (numéraires et autres actifs hautement liquides, tels que les obligations d'État) en % des exigibilités à court terme (par exemple, les salaires, les frais locatifs, les sommes à payer)

5. Contrôles des EME (procédures ex situ et in situ)

5.1 Introduction

Outre la surveillance continue ex situ, il arrive souvent que les autorités de supervision examinent un EME en s'attardant particulièrement sur un domaine de risque, quelques domaines de risque ou tous les domaines de risque. Les démarches en la matière varient en fonction des EME et d'un pays à l'autre. Par exemple, une autorité de supervision peut procéder à l'examen de tous les EME à un moment donné uniquement pour vérifier leur conformité aux exigences de protection des fonds, alors que les examens ultérieurs sur ce sujet ou d'autres (comme la protection des clients) peuvent être déclenchés par les résultats de la surveillance ex situ. D'une manière générale, lorsque les fonds sont bien protégés, l'amplitude et le degré de détail de la supervision peuvent être plus limités, du moins en ce qui concerne les EME non systémiques. Pour ce qui est des grands EME, les autorités de supervision peuvent approfondir les analyses sur la protection des fonds et élargir le champ des examens en y ajoutant d'autres domaines de risque, comme les risques opérationnels et les contrôles du blanchiment des capitaux/financement du terrorisme.

Bien que les pratiques divergent en matière de supervision, toutes les autorités de supervision interrogées s'accordent à dire que le domaine le plus important dans la supervision des EME est celui de la protection des fonds des clients. Les autres domaines prioritaires sont, entre autres, les risques opérationnels, les contrôles du blanchiment des capitaux et/ou du financement du terrorisme, ainsi que la protection des consommateurs. Toutes les autorités de supervision ne couvrent pas tous ces domaines (quelques-uns ne vérifient même pas la protection des fonds), tandis que d'autres (aucun dans les marchés émergents et économies en développement) couvrent les domaines mentionnées et bon nombre d'autres, comme le risque stratégique.

La présente section ne propose pas de directives pour l'examen de tous les domaines de risque qu'une autorité de supervision peut couvrir en ce qui concerne les EME, grandes ou petites (voir le Tableau 1). Elle se borne à décrire les procédures applicables lors de l'évaluation de trois domaines importants dans la supervision des EME : la protection des fonds (Section 5.2), les risques opérationnels (Section 5.3), et les contrôles du blanchiment des capitaux/financement du terrorisme (Section 5.4). Dans chaque cas, nous rappelons brièvement les exigences réglementaires courantes, suggérons l'amplitude de l'examen et,

Encadré 3. Revue des politiques et des manuels de procédure — une technique d'examen clé

Les pratiques en matière de gestion des risques et les opérations de l'EME sont censées être consignées par écrit dans des politiques et des manuels de procédure adoptées par les administrateurs de l'EME et appliquées par la direction de l'établissement, sous la supervision du conseil d'administration. Ces documents sont généralement étudiés par les autorités de supervision pour a) évaluer s'ils sont complets, raisonnables et en cohérence avec la réglementation et les normes internationales, et b) orienter en partie les questions de suivi que pourraient poser les autorités de supervision lors des examens ex situ et in situ. Les autorités de supervision peuvent demander et analyser les politiques et manuels de procédure se rapportant à tous les domaines traités dans la présente section. Un EME qui n'a pas de politiques ni de manuels de procédure ou qui, s'il en a, ne les met pas à jour, devrait susciter des questions chez l'autorité de supervision.

enfin, donnons des exemples de procédures ex situ et in situ. Ces procédures peuvent être adoptées totalement ou en partie, collectivement ou séparément, dans le cadre d'examens généraux de l'EME ou d'évaluations thématiques[20].

Bon nombre d'examens comportent une étude des politiques et des manuels de procédure. Une démarche en trois étapes pour le faire est décrite ci-après : I) étudier les manuels et les politiques ex situ, ii) recueillir des données factuelles sur leur mise en œuvre (ex situ et in situ), et iii) vérifier l'information par l'observation, des entretiens et des audits du système (in situ).

5.2 Protection des fonds

5.2.1 Principales exigences réglementaires

Dans la plupart des cas, la réglementation sur les EME comporte des exigences de protection des fonds reposant sur deux éléments :

- La séparation des fonds. Les EME sont tenus de réserver une somme minimale pour garantir leurs émissions totales ou leur passif de monnaie électronique *(flottant en*

[20] Outre la surveillance ex situ et les examens portant sur des EME spécifiques, les évaluations thématiques peuvent s'avérer utiles, particulièrement au cours des premières années de supervision d'un EME. Les évaluations thématiques aident l'autorité de supervision à mieux comprendre des questions précises, ce qui lui permet de comparer les bonnes et les mauvaises pratiques et de faire part de ses attentes à l'EME. Les évaluations peuvent aussi aider l'autorité de régulation à améliorer la réglementation. Les évaluations thématiques portent sur un sujet ou un petit nombre de sujets (par exemple, la protection des fonds) mais ils couvrent plusieurs EME. Ils peuvent comporter des procédures ex situ et in situ telles que celles décrites dans la présente section. Seules quelques-unes des autorités de supervision interrogées font des évaluations thématiques des EME.

monnaie électronique). Généralement, ils doivent garantir la totalité du flottant, en déposant un montant équivalent dans un compte désigné (*compte de monnaie électronique*) distinct des comptes utilisés pour les transactions courantes (règlement des factures, paiement/perception des commissions, etc.). Il peut exister plus d'un compte de monnaie électronique[21].

- ***Exigence de liquidité.*** La réglementation exige d'investir le flottant (si les investissements sont permis) uniquement en liquides et en actifs à faible risque, tels que les obligations d'État, ou le déposer simplement dans un compte auprès d'une banque commerciale (qui peut ou non verser des intérêts).
- ***Exigence de diversification.*** Certaines réglementations exigent de déposer le flottant dans plus d'une banque pour contrer le risque de faillite d'une banque[22].

- **L'isolation des fonds.** Les dispositifs d'isolation des fonds protègent le flottant des créanciers de l'EME (par exemple, les établissements de crédit, les investisseurs, les fournisseurs, les salariés, l'État). Pour ce faire, la réglementation peut exiger l'ouverture d'un compte spécial, comme un compte de fiducie ou un compte séquestre[23].
  - ***Flottant non grevé.*** La réglementation peut interdire aux EME d'engager le flottant (par exemple, en nantissement d'un prêt) et/ou peut fixer que les fonds constituant le flottant ne font pas partie des actifs de l'EME[24].

La protection efficace des fonds par les EME ne tient pas uniquement à la sûreté du flottant; elle dépend aussi de la capacité à identifier clairement les plaintes des clients et à déterminer si l'information que contient la plainte n'a pas été déformée. Ainsi, la protection des fonds se ressent de la gestion des risques opérationnels (notamment les risques de fraude et ceux liés aux erreurs et aux fautes, à la continuité des activités, au système informatique et à la cybersécurité). La présente section traite de quelques problèmes opérationnels en ce qui concerne la protection des fonds, les autres questions s'y rapportant étant abordées dans la Section 5.3. Les autorités de supervision doivent par ailleurs évaluer si la multiplication des comptes de monnaie électronique dans plusieurs banques rend la protection des fonds moins efficace. Enfin, la protection vise essentiellement à garantir les liquidités pour répondre aux demandes des clients dans les

[21] La présente section examine la stratégie la plus couramment utilisée par les EME pour protéger leur flottant : le déposer dans un compte auprès d'une banque commerciale et/ou le préserver dans des investissements sans risque. D'autres stratégies, qui pourraient avoir une incidence sur les questions juridiques, opérationnelles et de supervision abordées dans cette publication, sont décrites dans Mehmet et Staschen (2018).
[22] Du point de vue de la supervision bancaire, cette exigence réduit le risque encouru par les grands déposants dans une seule banque. Voir Kerse et Staschen (2018).
[23] Voir Staschen et Meagher (2018), puis Greenacre et Buckley (2014).
[24] Les engagements sur le flottant seront invalides en fonction de la réglementation d'un pays sur les comptes de fiducie ou séquestres.

deux cas de figure suivants : i) pendant la période d'activité de l'EME (dont il est question dans cette section) et ii) en cas de faillite de l'EME.

5.2.2 Portée des examens

Vérifier le solde des comptes de monnaie électronique est le moyen le plus simple de s'assurer qu'un EME satisfait à l'exigence de protection des fonds. Toutefois, les autorités de supervision devront utiliser d'autres procédures d'examen si elles veulent évaluer la qualité des politiques, des procédures et des systèmes au-delà des soldes indiqués par les EME (par exemple, pour confirmer l'exactitude des montants et évaluer la gestion des risques par l'EME et les contrôles internes qui influent sur la protection des fonds). Un examen complet de la fonction de protection des fonds couvrira les éléments suivants :[25]

- Existence et suffisance des fonds dans le compte de monnaie électronique
- Modalités et statut juridique du compte
- Procédures garantissant le solde requis (rapprochement, par exemple)
- Gouvernance et gestion du compte de monnaie électronique
- Liquidité du flottant (types d'investissement et pas d'engagements)
- Contrôles et déclarations exacts du flottant et des soldes des clients

5.2.3 Procédures d'examen

5.2.3.1 EXISTENCE ET SUFFISANCE DES FONDS DANS LE COMPTE DE MONNAIE ÉLECTRONIQUE

Les autorités de supervision peuvent comparer les informations sur le flottant et celles sur les soldes des comptes. Pour confirmer la véracité de ces informations, les autorités de supervision peuvent analyser les relevés des comptes de monnaie électronique afin de :

- Vérifier les données d'identification du compte de monnaie électronique (notamment le numéro du compte, l'agence, le titulaire du compte) par rapport à ce qui est indiqué dans l'accord/le contrat du compte et dans les rapports périodiques transmis.
- Vérifier les soldes des comptes de monnaie électronique à plusieurs dates butoir et les comparer à l'encours total du flottant déclaré aux mêmes dates pour confirmer la concordance[26].

[25] Plusieurs des autorités de supervision des marchés émergents et économies en développement interrogées vérifient seulement que les comptes de monnaie électronique ont des fonds suffisants.
[26] Des disparités pourraient signifier que les contrôles ne sont pas efficaces, que ces disparités sont intentionnelles, ou même que des fraudes existent.

- Si les intérêts et les produits des investissements sont versés dans le compte de monnaie électronique et utilisés par l'EME (notamment pour être distribués aux clients), il convient de vérifier que le solde total déclaré n'intègre pas ces montants car ils peuvent faire l'objet d'une exigence distincte, outre celle concernant le flottant[27].
- Vérifier que les opérations de crédit et de débit ne sont pas concentrées autour des dates de déclaration, ce qui pourrait faire soupçonner des insuffisances dans les rapprochements ou des disparités intentionnelles qui seraient camouflées.

Ces procédures reposent sur l'hypothèse que le flottant déclaré est exact. Les autorités de supervision peuvent vérifier l'exactitude du flottant déclaré en suivant les procédures décrites à la section 5.2.3.6.

5.2.3.2 MODALITÉS ET STATUT JURIDIQUE DU COMPTE DE MONNAIE ÉLECTRONIQUE

Les comptes de monnaie électronique sont généralement ouverts auprès des banques. Si un compte de fiducie ou de garantie bloqué, ou tout autre type de compte spécial est exigé, l'autorité de supervision peut en examiner la formalité (c'est-à-dire s'il est conforme à la réglementation applicable aux comptes de fiducie /séquestres) et les clauses (qui varieront en fonction de la banque dépositaire). Pour ce faire, l'autorité de supervision étudie l'accord d'ouverture d'un compte de cantonnement (fiduciaire, séquestre ou autre) entre l'EME/l'administrateur et la banque pour vérifier qu'il se conforme à des exigences précises, qui seraient stipulées dans la législation du pays concerné sur les comptes de fiducie ou dans toute autre loi applicable. Dans le cas des comptes de fiducie, certains pays exigent qu'un administrateur (qui peut être la banque dépositaire dans certains pays) soit désigné pour gérer les fonds pour le compte des clients de l'émetteur de monnaie électronique, tandis que d'autres pays laissent la gestion du compte de monnaie électronique à l'EME. Les accords varieront en conséquence.

L'accord d'ouverture du compte de fiducie peut indiquer le degré et les modes d'accessibilité du compte et les modalités de retrait des fonds, notamment pour être investis dans d'autres actifs, etc. L'accord peut décrire en détail les pouvoirs et les obligations de l'administrateur par rapport aux obligations de l'EME, ainsi que le rôle de l'autorité de supervision, notamment sa prérogative statutaire de soumettre l'administrateur à des

[27] Si les produits des investissements et des intérêts ne sont pas distribués ou utilisés de quelque autre manière, il n'y a aucune raison évidente de ne pas en tenir compte dans le contrôle de la conformité à l'exigence du solde minimum, sauf dans les cas où la loi l'interdit.

inspections. Les mêmes limites quant à l'utilisation des fonds et leur accessibilité peuvent être imposées dans le cas des comptes séquestres[28].

5.2.3.3 PROCÉDURES EFFICACES DE RAPPROCHEMENT

Il est essentiel de comprendre comment l'EME assure le rapprochement du compte de monnaie électronique avec le flottant pour confirmer l'efficacité de la protection des fonds. L'EME doit veiller à ce que le solde du compte de monnaie électronique soit toujours suffisant et de nombreuses réglementations exigent un rapprochement quotidien.

Les autorités de supervision des marchés émergents et économies en développement interrogées en savent peu sur la manière dont les EME rapprochent les comptes de monnaie électronique du flottant. Les procédures de rapprochement varient considérablement d'un EME à l'autre et peuvent donc être très manuelles (un employé de l'EME appelle la banque à la fin de chaque journée pour augmenter/réduire le solde du compte de monnaie électronique) ou entièrement automatisées (le compte s'ajuste automatiquement une fois [traitement par lots] ou plusieurs fois [traitement en temps réel] grâce aux systèmes intégrés de l'EME et de la banque).

La première étape consiste à étudier les politiques et procédures pertinentes, qui doivent décrire le processus de rapprochement et désigner le personnel responsable. L'absence de politiques et de procédures officielles peut limiter la protection des fonds. De surcroît, il est important de comprendre comment l'argent se crée (c'est-à-dire les situations qui augmentent le flottant) ou est détruit (les situations qui réduisent le flottant). Les modes de création/de destruction de la monnaie électronique peuvent varier d'un EME à l'autre. Par exemple, pour les EME qui travaillent avec des intermédiaires qui achètent de grosses quantités de monnaie électronique (ceux qu'on appelle souvent les super agents ou distributeurs) qu'ils distribuent (vendent) à des agents (qui vendent à leur tour la monnaie électronique aux consommateurs de détail), le flottant n'est touché que lorsque ces intermédiaires achètent de la monnaie électronique, et non lorsque les agents et les clients font des transactions (achètent/vendent la monnaie électronique).

Il est aussi important de savoir si le rapprochement se fait en une ou plusieurs fois par jour, ou si les transferts sont faits immédiatement lorsque la monnaie électronique est créée/détruite (temps réel) ou de toute autre manière. Ainsi, certains EME permettent à certains intermédiaires, agents et négociants de payer la monnaie électronique en virant

[28] Certaines autorités de supervision interrogées en Afrique vérifient les modalités de paiement des intérêts et des commissions imposées par les banques, en partie parce que les banques ferment la voie aux EME en leur proposant des conditions inacceptables ou en leur refusant ce service.

directement les fonds dans le compte de monnaie électronique. Dans d'autres cas, l'on a une opération unique de rapprochement chaque jour, avant la fermeture de la banque pour rendre compte de la création/destruction nette de monnaie électronique enregistrée pendant la journée. Enfin, les transferts à destination ou à partir du compte de monnaie électronique peuvent être automatisés ou déclenchés manuellement.

Les autorités de supervision doivent déterminer si l'EME utilise différents modes de rapprochement et en évaluer les risques.

Du point de vue de la supervision, l'automatisation efficace des opérations de rapprochement (en temps réel ou en différé) doit pouvoir réduire les erreurs et les retards. S'il existe des contrôles de la sécurité et de l'intégrité des données, ils devraient pouvoir minimiser les risques de fraude et d'accès non autorisé au compte de monnaie électronique. Même lorsque les procédures sont automatisées, il importe d'étudier l'organisation du système i) en posant des questions sur les codes qui y sont intégrés pour déclencher les transferts entre le ou les compte(s) bancaire(s) de l'EME[29] et le compte de monnaie électronique, et ii) en identifiant les étapes qui exigent une intervention manuelle, afin d'en évaluer les risques. Les autorités de supervision doivent par ailleurs évaluer comment se passe le rapprochement lorsqu'un administrateur intervient dans la gestion du compte de monnaie électronique[30].

Grâce à une connaissance détaillée de l'ensemble du processus, les autorités de supervision peuvent évaluer le risque d'illiquidité du compte de monnaie électronique en raison des insuffisances des contrôles internes ou des malversations des employés au niveau de l'EME, de la banque ou de l'administrateur. Dans le cas des rapprochements automatiques, les autorités de supervision peuvent tester le système en simulant des variations du flottant, un accès non autorisé aux informations sur le flottant et la modification de ces informations, l'achat ou la vente par des agents ou des super agents. Parmi les autres techniques envisageables, on a l'observation intégrale d'un processus de rapprochement (lorsqu'il est manuel) et l'examen des pistes d'audit des rapprochements (si le processus est automatisé). Si l'examen décrit à la Section 5.2.3.1 fait apparaître des disparités, l'autorité de supervision peut étudier les fiches sur les rapprochements aux dates où sont notées les incohérences et demander des explications[31].

---

[29] Il s'agit du ou des compte(s) bancaire(s) qu'utilise l'EME pour ses activités, notamment pour recevoir les commissions et les dépôts des clients et pour acquitter les charges salariales par exemple. Les fonds déposés dans le compte de monnaie électronique proviennent de ces comptes (à moins que les acheteurs de monnaie électronique puissent payer en déposant directement l'argent dans le compte de monnaie électronique).

[30] En fonction des accords, les procédures d'examen peuvent devoir s'étendre à l'administrateur.

[31] Les autorités de supervision peuvent chercher à en savoir davantage sur les incohérences en vérifiant si elles sont signalées dans un quelconque rapport de gestion ou d'audit interne, et dans quelle mesure et de quelle manière ces incohérences sont ordinairement rapportées au conseil d'administration, au comité des risques ou au comité d'audit, si tant est qu'il en existe.

Si l'EME garde le flottant en dépôts dans plusieurs banques, l'autorité de supervision peut demander à savoir comment l'EME divise le flottant (par exemple, si cela dépendra des banques dans lesquelles les super agents disposent de comptes). L'EME doit pouvoir s'assurer que le rapprochement se fait avec la même efficacité pour toutes les banques. L'autorité de supervision doit déterminer si les procédures de rapprochement diffèrent d'une banque à l'autre et mesurer leur efficacité[32].

5.2.3.4 GOUVERNANCE ET GESTION DU COMPTE DE MONNAIE ÉLECTRONIQUE

La gouvernance et la gestion des comptes de monnaie électronique tiennent une place importante dans le rapprochement et la sécurité des fonds. Les EME doivent avoir des politiques et procédures opérationnelles écrites qui régissent l'accès au compte de monnaie électronique et le fonctionnement de celui-ci. Dans la plupart des cas, seuls quelques employés désignés sont habilités à accéder au compte de monnaie électronique et à y réaliser des transactions. De surcroît, l'EME doit prévoir un dispositif d'intervention qui garantisse la continuité des opérations de rapprochement même en l'absence du principal opérateur.

Les règles d'accès et de transmission à l'échelon supérieur doivent être proportionnées à la structure, la taille et la complexité de l'EME (par exemple, dans un grand EME, le personnel subalterne peut avoir accès au compte de monnaie électronique) et à son dispositif de rapprochement (entièrement automatisé ou manuel). Les règles doivent être consignées, et elles doivent définir les transactions autorisées pour chaque profil d'utilisateur. L'autorité de supervision peut examiner la liste des employés et les profils d'utilisateur de chacun pour identifier ceux qu'elle doit interroger pour en savoir davantage sur le respect des politiques de l'EME et sur les cas de violation de ces politiques. Des contrôles similaires doivent être institués si le compte de monnaie électronique est géré par un administrateur.

Outre les règles d'accès et les profils d'utilisateur, il devrait exister des règles officielles de gestion des fonds (notamment les transferts à destination ou à partir du compte de monnaie électronique). Ceci s'applique aux opérations de rapprochement, mais aussi à d'autres situations, en ce qui concerne par exemple les responsabilités et les procédures pour la vérification périodique des intérêts ou autres revenus qui arrivent dans le compte de monnaie électronique, ainsi que leur retrait ou leur distribution et le

[32] En fonction de la réglementation, les EME peuvent être tenus de répartir le flottant entre plusieurs banques suivant certains critères (par exemple, la portion maximale des émissions totales de monnaie électronique par banque). Dans un tel scénario, l'autorité de supervision peut appliquer des procédures supplémentaires pour vérifier la conformité à ces exigences et critères spécifiques.

traitement des erreurs, telles que des transferts résultant de petits problèmes dans les codes informatiques. L'autorité de supervision peut tester les politiques de l'EME au moyen d'audits du système.

5.2.3.5 LIQUIDITÉ DU FLOTTANT

L'autorité de supervision peut aussi procéder à des vérifications pour s'assurer que l'EME satisfait aux exigences de liquidité (c'est-à-dire vérifier les investissements autorisés sur le flottant). La plupart des réglementations nationales sont strictes. Soit elles interdisent les investissements (en exigeant par exemple que les fonds soient déposés dans des comptes à vue), soit elles autorisent les investissements uniquement dans les actifs prescrits/autorisés par l'autorité de supervision. Certaines permettent (et quelques-unes peuvent exiger) qu'un pourcentage du flottant soit investi dans des obligations d'État à faible risque. Seul un petit nombre (notamment la Banque centrale des États d'Afrique de l'Ouest) autorise des investissements risqués dans les titres[33].

L'autorité de supervision peut commencer par s'enquérir de la politique/stratégie d'investissement (profil de risque, rendement cible, actifs), de toute modification récente de la politique (et des motifs de cette révision), et du processus de prise de décision. D'une manière générale, le conseil d'administration doit approuver la stratégie d'investissement et les fonctions de gestion des risques, et le comité des risques, s'il en existe un, doit contrôler les résultats. L'autorité de supervision peut aussi demander si la stratégie d'investissement varie en fonction des comptes de monnaie électronique, demander et examiner les données factuelles sur les investissements réalisés (par exemple, les relevés des comptes d'investissement, les relevés des comptes de monnaie électronique montrant les transferts vers les comptes d'investissement), évaluer les résultats de ces investissements et le niveau de risque qu'ils présentent, confirmer les informations auprès des gestionnaires des investissements.

Un autre aspect digne d'intérêt est l'interdiction réglementaire d'engager le flottant en garantie d'un prêt ou en tout autre type de nantissement. L'autorité de supervision peut interroger les hauts cadres sur les sujets préoccupants relevés lors des différents entretiens avec le personnel de l'EME chargé des emprunts. Pour mieux comprendre la situation, l'autorité de supervision peut examiner les emprunts de l'EME (contrats de prêt)[34].

[33] Voir Kerse et Staschen (2018).

[34] Dans les pays où la loi sur les comptes de fiducie (ou toute autre loi) reconnaît les droits de propriété des clients sur le solde du compte de monnaie électronique, cette forme de garantie est généralement nulle et de nul effet (ce qui veut dire qu'un créancier de l'EME ne peut prétendre au flottant même s'il est engagé en nantissement dans le contrat de prêt entre lui et l'EME).

5.2.3.6 FIABILITÉ DES CONTRÔLES ET DES DÉCLARATIONS DU FLOTTANT ET DES SOLDES DES CLIENTS

L'une des responsabilités fondamentales de l'EME est d'assurer un contrôle fiable des soldes de ses clients. L'EME doit communiquer à l'autorité de supervision le montant exact du flottant (somme de tous les soldes des clients), qui est un élément clé de l'activité de supervision. Pour évaluer cette fonction, l'autorité de supervision peut procéder de la manière suivante :

- **Déterminer si les soldes des clients sont soumis à des contrôles fiables :**[35]
  - Étudier les données sur les plaintes pour recenser celles qui porteraient sur des soldes insuffisants ou inexacts.
  - Examiner le compte dormant de l'EME et ses pratiques de gestion.
  - Examiner les procédures de règlement des transactions non électronique de l'EME[36].
  - Vérifier les règles qui autorisent l'accès à la plateforme de monnaie électronique et si certains profils sont habilités à modifier les soldes des clients et dans quelles circonstances. Tester les règles en éprouvant le système (en modifiant par exemple sans une autorisation les soldes des clients).
  - Si la faiblesse des contrôles est un sujet préoccupant, simuler des transactions pour vérifier si le système actualise correctement les soldes clients après chaque type de transaction effectué.
  - S'enquérir des règles sur les montants déposés provisoirement dans des comptes de règlement ou d'attente et de l'incidence sur les soldes des clients, aussi bien l'expéditeur que le bénéficiaire[37].
- Déterminer si les informations communiquées sur le flottant sont exactes :
  - Comparer les rapports antérieurs sur le flottant à des dates butoir avec les rapports générés à la demande de l'autorité de supervision et en sa présence (in situ) directement de la plateforme de monnaie électronique de l'EME (système des comptes).
  - Demander comment sont produits les rapports statutaires périodiques sur le flottant, quel est le personnel responsable et si les procédures utilisées pour produire le

[35] Les contrôles doivent être les mêmes pour tous les types de clients, notamment les agents.
[36] La plupart des législations dans les marchés émergents et économies en développement exigent que les transactions en monnaie électronique soient réalisées en temps réel (c'est-à-dire que le solde du client doit immédiatement être touché), mais il existe des exceptions. Dans les cas où les transactions hors ligne sont autorisées, le solde du client sera temporairement décalé jusqu'à la finalisation de la transaction. Ces problèmes et d'autres qui sont liés aux risques opérationnels (par exemple, la sécurité des données et leur récupération après un sinistre) sont importants pour assurer un accès continu aux informations actualisées sur le solde du client.
[37] Ces comptes sont destinés à recevoir les fonds à titre provisoire, le temps de régler les transactions ou les fonds non classés et litigieux (par exemple, lorsqu'un client envoie de l'argent au mauvais numéro et le signale à l'EME avant le règlement de la transaction).

rapport sont manuelles. Interroger le personnel responsable sur les insuffisances du système (par exemple, si le système n'est pas capable de renseigner automatiquement le champ sur les émissions totales de monnaie électronique ou tout autre champ dans le rapport statutaire). Si des problèmes sont relevés, demander au personnel de simuler la production d'un rapport en présence de l'autorité de supervision et s'enquérir des mesures prises lorsque des erreurs sont décelées dans les rapports.

- Demander si les transactions en attente (c'est-à-dire les sommes provisoirement enregistrées dans les comptes d'attente ou de règlement) sont intégrées dans les émissions totales déclarées à l'autorité de supervision et si elles sont prises en compte pour la reconstitution du compte de monnaie électronique. Tester les règles en éprouvant le système.

5.3 Risque opérationnel

5.3.1 Principales exigences réglementaires

Les risques opérationnels s'entendent des risques de perte résultant i) de l'échec des procédures internes, des ressources humaines et des systèmes ou ii) d'événements externes (BCBS, 2011, p. 3). La réglementation sur les EME peut leur imposer d'une manière générale de gérer leurs risques opérationnels, notamment les risques liés aux agents, aux fraudes, aux cybermenaces, aux systèmes informatiques et à la continuité des activités. Cette réglementation exige généralement une structure minimale de gouvernance et de gestion des risques, sous la forme par exemple d'une fonction de supervision du conseil d'administration et d'un auditeur interne, la définition des responsabilités de la haute direction, qui couvriraient la rédaction des politiques et procédures et la définition des fonctions de contrôles internes et de gestion des risques, et enfin, des fonctions de contrôle de la conformité aux dispositions réglementaires. Certains pays peuvent appliquer aux EME une réglementation distincte sur l'externalisation des services et imposer ainsi des règles au stockage des données par exemple (*cloud computing* externalisé) et à l'accès de l'autorité de supervision aux parties sous-traitantes (BCBS, 2016a, p. 28 [EC 8]. Il peut aussi exister une réglementation sur la sécurité des données et la continuité des affaires.

5.3.2 Portée des examens

Le risque opérationnel est complexe et a notamment des liens avec d'autres domaines, que sont la protection des fonds, le blanchiment des capitaux/financement du terrorisme et la protection des consommateurs. Procéder à un examen complet du risque opérationnel peut s'avérer pénible, surtout qu'il ne se justifie pas forcément pour tous les EME. En se fondant sur sa stratégie axée sur les risques, l'autorité de supervision doit déterminer dans

quelle mesure et à quelle fréquence elle examinera les risques opérationnels dans chaque EME et ajuster le calendrier au fil du temps.

La présente section ne traite pas de tous les aspects du risque opérationnel ni ne propose une structure pour une évaluation complète. Elle propose plutôt des orientations de haut niveau sur les aspects suivants :[38]

- Gouvernance des risques
- Cadre global de gestion des risques opérationnels
- Prévention et gestion de la fraude
- Sécurité des données (cybersécurité incluse)
- Continuité des activités et récupération des données après sinistre

Si le gros des procédures peut être appliqué par des généralistes, certaines peuvent demander des inspections spécialisées (par exemple, pour évaluer la robustesse de l'infrastructure informatique, tester les défenses en cybersécurité, etc.). L'autorité de supervision peut engager des auditeurs externes si la loi l'y autorise, quand elle ne dispose pas d'une expertise interne. De surcroît, les outils de SupTech peuvent aider l'autorité de supervision à pallier en partie le manque de capacités, en ce qui concerne, par exemple, l'analyse de grands fichiers de données sur les transactions.

5.3.3 Procédures d'examen

5.3.3.1 GOUVERNANCE DES RISQUES

Chaque EME doit disposer d'un cadre formel de gestion des risques opérationnels, y compris des risques informatiques. Le cadre de gestion des risques doit être conçu en fonction des activités de l'EME. De plus, la chaîne de gouvernance et des responsabilités doit être clairement définie—dans des accords formels—entre l'EME et la société mère[39].

Bon nombre des EME étudiés appartiennent à des opérateurs de réseaux mobiles et « utilisent » le cadre de gestion des risques (et l'infrastructure de base) de leur société mère, même si chez un opérateur de réseau mobile, la gestion des risques concerne davantage les risques liés à l'activité des télécommunications, et non à la monnaie électronique.

[38] Voir l'annexe 4 pour plus d'indications. Des aspects importants liés à la fiabilité des services de paiement, notamment la finalisation des paiements et l'achèvement des transactions en cas de coupure de la communication ou de tout autre problème, ne sont pas spécifiquement traités dans cette publication.
[39] Il est bon que l'EME recrute un personnel expert en services financiers pour assurer la gestion des risques. Dans un au moins des pays étudiés, les opérateurs des réseaux mobiles peuvent être autorisés à remplir l'office des EME (au lieu d'être tenus de créer une filiale). Cette pratique peut exposer l'EME aux risques concernant les opérateurs de réseaux mobiles et vice-versa, retarder l'adoption de bonnes pratiques de gestion des risques et compliquer les examens de supervision.

À l'instar des banques, les grands EME doivent formellement établir trois lignes de défense : i) contrôles des secteurs opérationnels ou de gestion, ii) fonctions de gestion des risques et de conformité aux dispositions réglementaires, et iii) auditeurs internes et externes indépendants. Les EME de plus petite envergure peuvent appliquer le même concept sur une structure moins formelle, mais les auditeurs internes doivent toujours être indépendants des unités opérationnelles, de la gestion des risques et de la conformité aux dispositions réglementaires, et ils doivent rendre compte directement au conseil d'administration. La plupart des lois sur les EME leur impose, quelle que soit leur taille, d'engager des auditeurs externes. Le conseil d'administration des grands EME devrait comporter un comité des risques (à défaut, le contrôle des risques pourrait être assuré par un comité d'audit), alors que le conseil d'administration des EME plus petits doit compter au moins un membre qui s'y connaît en gestion des risques.

5.3.3.2 CADRE GLOBAL DE GESTION DES RISQUES OPÉRATIONNELS

L'autorité de supervision peut évaluer l'existence, la qualité et la mise en œuvre d'un cadre pour les risques opérationnels. Le cadre doit recenser toutes les sources de risque opérationnel, comme les pannes du système informatique, les fraudes, les violations de la sécurité des données, les interruptions du service, les vols, etc. Il doit être approuvé par le conseil d'administration et être à la mesure de la taille et de la complexité de l'EME. En règle générale, un bon cadre remplit les fonctions suivantes :

- Il définit la structure de gouvernance des risques.
- Il organise un cycle répétitif d'activités de gestion des risques (c'est-à-dire des processus et systèmes routiniers pour identifier, mesurer, suivre, signaler et atténuer les risques).
- Il couvre trois aspects : i) éviter les risques, ii) gérer la matérialisation des risques, et iii) éviter les répétitions en améliorant les processus de gestion des risques et des contrôles.
- Il met en place des procédures et des système pour estimer et contrôler les pertes.
- Il mesure la propension de l'EME au risque et prévoit des contre-mesures en cas de dépassement du seuil de tolérance au risque (sous la forme d'une réserve de capital ou d'une assurance, par exemple)[40].
- Il établit une fonction d'audit interne indépendant qui rend compte directement au conseil d'administration.
- Il définit des cadres pour le recrutement de parties tierces, leur suivi et la dénonciation des accords avec ces tiers, comme les accords de sous-traitance et de partenariat,

[40] Important lorsqu'un EME est dans une phase de croissance rapide car, pendant cette période, la qualité des contrôles opérationnels et de la gestion de risques peut baisser.

ainsi que pour la vérification initiale des antécédents et les contrôles ponctuels des parties tierces.
- Il est régulièrement examiné.

L'examen commence par l'étude ex situ des documents pertinents, qui peuvent être les politiques et manuels de procédure, les rapports sur les risques, les rapports d'audit interne et externe et les rapports sur les incidents (par exemple, les fraudes, les perturbations)[41]. La vérification in situ, notamment l'observation, les entretiens et les tests sur le système, s'inspirent de ces analyses ex situ. Le travail in situ consiste principalement à tester si le cadre de gestion des risques est effectivement appliqué et à assurer le suivi des résultats de la préparation ex situ. Par exemple, l'autorité de supervision peut vérifier si les contrôles internes sont intégrés dans les activités quotidiennes de l'EME et si les systèmes informatiques permettent effectivement d'identifier, de suivre et de signaler les risques, y compris les données sur les pertes estimées et subies (par exemple, les remboursements aux clients pour des transactions non autorisées, le paiement des franchises d'assurance en cas de réclamation, la perte de matériel à cause des pannes de courant, etc.)[42].

L'autorité de supervision peut examiner le processus de production des rapports sur les risques opérationnels qu'elle reçoit et vérifier si les données qui y figurent correspondent aux informations contenues dans le système informatique de gestion des risques de l'EME (c'est-à-dire, si les données sont exactes et complètes). Si des disparités apparaissent, l'autorité de supervision peut demander les rapports de gestion interne des risques opérationnels au lieu du rapport standard.

5.3.3.3 PRÉVENTION ET GESTION DE LA FRAUDE

Les EME peuvent être confrontés à plusieurs types de fraude[43]. Ils ont donc besoin de répertorier ces fraudes et de les intégrer au cadre de gestion des risques opérationnels et dans leur logiciel de détection des fraudes. Une gestion informelle, incomplète ou laxiste de la fraude dans l'EME (par exemple, aucune enquête sur les cas de fraude) doit soulever des questions chez l'autorité de supervision.

---

[41] L'autorité de supervision doit essayer d'évaluer le niveau d'indépendance de l'auditeur interne. Si l'auditeur n'est pas indépendant, ses rapports ont peu de valeur. Les rapports de l'auditeur externe peuvent aussi fournir des informations pertinentes.

[42] Bien qu'ils visent principalement les banques grandes et complexes, les principes du BCBS (2013) « *Principles for Effective Risk Data Aggregation and Risk Reporting* » donnent des lignes directrices qui peuvent être personnalisées pour des institutions moins complexes comme les EME.

[43] Voir la typologie des fraudes dans Buku et Mazer (2017).

Le risque de fraude, sous la forme d'un accès non autorisé du personnel de l'EME aux fonds des clients, est l'une des inquiétudes majeures des autorités de supervision des marchés émergents et économies en développement interrogées. Les fraudes internes méritent particulièrement l'attention - la plupart des cas de fraude ayant fait la une des journaux dans les marchés émergents et économies en développement étudiés ont été commis par des employés, quelquefois avec la complicité des agents.

L'autorité de supervision peut procéder ainsi qu'il suit :[44]

- Vérifier (ex situ) qu'il existe des politiques et procédures appropriées pour éviter les fraudes, les identifier et y répondre ; que les types de fraude sont identifiés ; et que les responsabilités sont clairement définies.
- Évaluer dans quelle mesure l'EME vulgarise efficacement en interne sa politique d'identification et de sanction des fraudeurs, qu'il s'agisse d'employés ou d'agents.
- Étudier (ex situ) les cas de fraude sur une longue période pour déceler les types de fraude, les taux de croissance de la fraude, les domaines touchés et les pertes subies. Cet examen devra évaluer le niveau de respect des politiques de l'EME, l'efficacité de la gestion du risque de fraude et l'incidence des pertes subies sur la santé financière de l'EME. Comparer les résultats obtenus avec ceux d'autres EME.
- S'enquérir des raisons de la fraude et des mesures prises pour éviter que cela se reproduise. Porter une attention particulière aux récidives.
- Si les capacités analytiques le permettent ou si les logiciels pertinents sont disponibles, demander et faire l'audit (ex situ) des fichiers de données granulaires pour vérifier les informations fournies par l'EME au sujet des fraudes, afin de détecter des écarts inhabituels dans le déroulement des transactions (par exemple, la concentration de retraits importants sur une courte période et dans un espace géographique)[45].
- Examiner les informations fournies par l'EME sur les cas de fraude signalés par son système de détection des fraudes et sur les paramètres utilisés pour générer des drapeaux rouges.
- Vérifier les droits d'accès au système des comptes de monnaie électronique et demander quels employés peuvent effacer et modifier les données, transférer des fonds, etc. S'enquérir des contrôles destinés à limiter l'accès à la plateforme et à protéger les

[44] Au regard de la forte incidence des fraudes en ce qui concerne un certain type de transactions de monnaie électronique (l'argent mobile en Afrique subsaharienne), l'autorité de supervision peut devoir faire une évaluation thématique de la prévention et de la gestion de la fraude.

[45] En dépit des avantages qu'il y aurait à réaliser l'audit de grands fichiers de données granulaires pour évaluer comment un EME gère et signale ses risques opérationnels, notamment le risque de fraude, la plupart des autorités de supervision des marchés émergents et économies en développement interrogées n'avaient ni l'expertise ni les logiciels analytiques requis.

données de connexion des clients, et des exceptions à la règle. Déterminer au moyen d'enquêtes et de tests sur le système si les employés sont capables de créer/détruire manuellement la monnaie électronique.

- Analyser les pistes d'audit pour rechercher, par exemple, des connexions inhabituelles ou des tentatives de connexion non autorisées par des employés et des agents (lors du service de nuit par les employés, par exemple) et simuler des actions non autorisées.
- S'enquérir de la fréquence des mises à jour du système de détection des fraudes et de la gestion des correctifs de sécurité (acquisition, test, installation et suivi des changements de code).
- Évaluer la gestion des comptes de règlement (comptes provisoires ou d'attente). De mauvaises pratiques de rapprochement peuvent ouvrir une brèche aux fraudeurs[46].

5.3.3.4 SÉCURITÉ DES DONNÉES (CYBERSÉCURITÉ INCLUSE)

La sécurité des données est un aspect important de la gestion des risques dans les EME, du fait de leurs activités qui dépendent des données numériques, de leurs larges réseaux d'agents et de leur connectivité croissante à des parties tierces. Les EME, quelle que soit leur taille, ont besoin de formaliser des stratégies efficaces de sécurisation des données dans un programme de sécurisation des données. Un bon programme de sécurisation des données se caractérise par ce qui suit :[47]

- Il est approuvé par le conseil d'administration de l'EME qui en est responsable.
- Il désigne un responsable (la personne en charge de la sécurité de l'information, par exemple) du programme.
- Il se fonde sur l'évaluation ou les évaluations des risques faites par l'EME ou des experts externes. Il recense et classe les données en fonction de leur sensibilité.
- Il couvre toutes les installations et tous les systèmes utilisés pour accéder aux données, les collecter, les stocker, les utiliser, les transférer, les sécuriser et les éliminer.
- Il classe les risques liés à la sécurité des données en deux catégories, les risques internes et les risques externes, et il identifie leurs sources, la probabilité de leur matérialisation et leurs conséquences.
- Il couvre les mesures de protection administratives, techniques et physiques afin de garantir la sécurité, la confidentialité et l'intégrité des données, dans le but i) d'éviter les risques (**prévention**), ii) d'identifier les risques (**détection**), et iii) de réponde à la

[46] On en veut pour exemple ce cas de fraude très médiatisé en Ouganda de transferts non autorisés de fonds à destination/à partir de comptes de monnaie électronique. Voir Morawczynski (2015).
[47] La sécurité des données et la confidentialité des données sont liées, même si elles relèvent de domaines de supervision différents. Cette section ne traite pas de la confidentialité des données (par exemple, l'EME demande-t-il le consentement du client avant de partager des informations à des fins commerciales).

matérialisation des risques (**traitement**). Voir l'encadré 4 pour des exemples de mesures de protection.
- Il encadre l'évaluation continue et périodique de l'efficacité du programme et des améliorations qui en découlent.

En fonction de l'EME et de l'expertise disponible, l'examen peut combiner l'analyse documentaire, les entretiens, l'observation et les tests sur le système. Il peut permettre les actions suivantes :[48]

- Recueillir des données factuelles qui montrent que le programme de sécurité protège effectivement l'EME contre les risques et continuera de le faire au regard des activités de l'EME et de sa stratégie de développement.
- Analyser et interroger davantage les résultats des évaluations des risques.
- Examiner les rapports d'audit et la mise en œuvre des recommandations y figurant.
- Étudier la sécurité des données dans les accords de sous-traitance, concernant notamment le *cloud computing*, le traitement des transactions, le développement d'interfaces de programmation d'applications (API), et d'autres domaines[49].
- Analyser les données sur les risques (par exemple, les violations signalées de la sécurité des données, les actes de piratage des données, la contamination par des virus, etc.).
- Évaluer la sécurité physique des dispositifs sensibles (stockage/traitement des données).
- Tester les principales fonctions de contrôle, en procédant notamment à l'analyse des vulnérabilités, à des tests d'intrusion, à l'analyse des pistes d'audit, etc.

Le programme de sécurité d'un EME n'est pas plus solide que son maillon le plus faible. Par exemple, de nombreux EME en Afrique et en Asie utilisent les données de services supplémentaires non structurées, (plus connues sous l'acronyme anglais USSD), considérées comme un canal faiblement sécurisé de transport des données des clients. De même, les EME utilisent généralement les numéros d'identification personnelle (PIN) pour authentifier les clients, mais bon nombre de ces clients communiquent leurs PIN aux agents de l'EME. Bien que de nombreux pays utilisent les codes USSD et les agents pour faciliter l'inclusion financière, l'autorité de supervision doit évaluer comment les EME atténuent les risques liés à la sécurité des données (notamment par l'authentification

[48] Voir l'annexe 4 pour des sources supplémentaires.
[49] Toutes les autorités de supervision des marchés émergents et économies en développement interrogées se sont dites préoccupées de l'impartition du *cloud computing* par les EME, particulièrement lorsqu'elle est transnationale, parce que l'accès aux données et aux dispositifs de stockage des données pour les besoins de la supervision s'en trouve compliqué. L'Inde par exemple a rendu public récemment une directive qui impose aux prestataires des services de paiement de stocker toutes les données relatives à leurs opérations exclusivement en Inde, leur interdisant ainsi formellement d'avoir recours au cloud computing transnational (voir Baur-Yazbeck [2018]).

Encadré 4. Exemples de mesures de sécurité appliquées par les EME

Un EME peut mener les actions suivantes dans le cadre de son programme de sécurisation des données :

- Appliquer un système de double contrôle et séparer les tâches.
- Vérifier les antécédents du personnel essentiel et lui dispenser une formation spécialisée.
- Annuler sans délai les droits d'accès des employés sur le départ.
- Dresser l'inventaire des ressources technologiques (appareils physiques, connexions à des réseaux).
- Faire des mises à jour périodiques des systèmes et gérer les changements de codes (gestion des correctifs).
- Employer des outils modernes de contrôle pour détecter les fraudes et les intrusions.
- Mettre en place un programme de cybersécurité qui offre un cadre pour l'identification des risques, les protections, la détection, la réaction et la récupération, les tests et les rapports. Les mesures de sécurité doivent englober i) l'encodage des données en transit et des donnée stockées (CGAP 2018), ii) les pare-feu et les protections antivirus, et iii) les analyses de vulnérabilité et les tests d'intrusion.
- Faire partie de groupes de partage de l'information et prendre des dispositions en faveur de la formation continue.
- Contrôler l'accès aux systèmes et aux dispositifs essentiels, tester la résilience sur les contrôles manuels et assurer la sécurité physique.
- Prendre des mesures pour protéger les données de la destruction, de la perte ou des effets néfastes d'un incident tel un incendie ou une inondation, et pour réagir à ces incidents.
- Prévoir un cadre pour la sécurité des données dans les accords de sous-traitance et de partenariat.

biométrique, les mots de passe à usage unique, la détection des anomalies ou l'abandon progressif de l'USSD).

5.3.3.5 CONTINUITÉ DES ACTIVITÉS

La gestion de la continuité des activités est un pan important de la gestion des risques opérationnels qui doit être bien mis en place dans les grands EME[50]. Les dispositifs en la

[50] Voir l'annexe 4 pour plus d'indications.

matière devraient permettre à l'EME de reprendre rapidement les opérations essentielles et de restaurer l'infrastructure informatique de base en cas de perturbations tant mineures que graves (interruption des télécommunications, pannes de courant, catastrophes naturelles, par exemple). La gestion de la continuité des activités permet aux entreprises de répondre aux crises et d'en minimiser les effets.

L'autorité de supervision doit évaluer le plan de continuité des activités de l'EME pour s'assurer des éléments suivants :

- Le plan décrit des scénarios de crise et analyse leurs effets potentiels[51].
- Des stratégies de gestion des imprévus et de reprise des activités existent, qui recensent les dispositifs, individus, processus, systèmes informatiques, données essentiels, ainsi que des capacités alternatives de traitement des données.
- Le personnel est bien préparé (grâce notamment à des simulations) à exécuter le plan.
- Le plan est soumis à des tests et des examens périodiques (l'autorité de supervision peut analyser les résultats de ces tests).
- Les systèmes de base de l'EME subissent des tests de résistance.
- Les politiques, les contrôles manuels et automatiques ainsi que les modalités de mutualisation des risques avec des parties tierces existent bel et bien et garantissent la conduite à bonne fin des transactions, même en cas d'interruption de la communication avant la fin ou d'une défaillance de la partie tierce (par exemple, les services d'engagement des paiements)[52].

D'après ce qu'il ressort des marchés émergents et économies en développement objet de la présente étude, les défaillances de l'infrastructure des télécommunications et d'électricité, qui se traduisent par l'interruption des services des EME, sont courantes. Ce type de dépendance vis-à-vis de parties tierces crée des risques. Il semble que l'on investisse peu dans les dispositifs de gestion des imprévus et que l'autorité de supervision n'insiste pas beaucoup sur les améliorations. Les autres formes de perturbation signalées ont trait à des interruptions imprévues ou programmées des systèmes des EME. Dans les pays africains étudiés, des interruptions importantes ont été enregistrées en raison de mises à jour de la plateforme de monnaie électronique. C'est fut le cas en 2017 au Kenya avec une interruption de près de 12 heures de M-PESA à cause d'une mise à jour du système (Capital Business 2017).

[51] Il est recommandé de réaliser une analyse d'impact sur l'entreprise et une évaluation des risques pour éclairer la conception de la stratégie de gestion des imprévus.

[52] De nombreuses lois et réglementations sur les systèmes de paiement comportent des dispositions couvrant ces situations, mais elles sont peu appliquées dans les marchés émergents et économies en développement concernés par la présente étude, ce qui renforce la vulnérabilité des clients.

L'autorité de supervision peut coordonner avec l'autorité de régulation des télécommunications pour accéder à des données ou des analyses susceptibles de mieux l'éclairer sur les perturbations des services des télécommunications. Ces perturbations pourraient être comparées avec celles des EME pour trouver comment améliorer les dispositifs de gestion des imprévus. Bon nombre d'EME des marchés émergents et économies en développement sont rattachés à un seul opérateur de réseau mobile et ne cherchent généralement pas à s'affilier à d'autres, ce qui les rend plus vulnérables aux perturbations opérationnelles.

L'examen ex situ serait l'occasion pour l'autorité de supervision d'étudier les données sur la fréquence, la localisation et la durée des perturbations ; les transactions avortées ou incomplètes ; et les pannes du système ainsi que les raisons de ces pannes (et les solutions apportées), et de faire le suivi des promesses antérieures d'amélioration. L'autorité de supervision disposant de l'expertise requise peut demander et faire l'audit des fichiers de données granulaires sur les transactions et les connexions aux systèmes pour déceler des tendances inhabituelles qui pourraient indiquer un échec des dispositifs de gestion des imprévus et détecter des perturbations non signalées à l'autorité de supervision.

5.4 Blanchiment des capitaux/financement du terrorisme

5.4.1 Principales exigences réglementaires

Les EME sont souvent concernés par les lois sur le blanchiment des capitaux et le financement du terrorisme et ils sont, par conséquent, tenus de signaler les transactions suspectes au service de renseignements financiers et de mettre en place des systèmes et des contrôles destinés à réduire le risque de telles opérations. Les lois propres aux EME imposent davantage des limites aux soldes et aux transactions dans les comptes de monnaie électronique des clients et des agents, notamment des limites aux soldes mensuels, à la valeur de chaque transaction ou au volume total des transactions mensuelles et, parfois, au nombre de comptes que peut détenir un client. Si les EME respectaient ces lois, les risques liés au blanchiment des capitaux et/ou au financement du terrorisme seraient considérablement réduits. De surcroît, la réglementation oblige les EME à vérifier les antécédents des clients, notamment leur identité et celle des agents (y compris par la collecte et le stockage des informations requises à l'ouverture d'un compte), et à surveiller les transactions pour déceler tout écart du comportement attendu du profil d'un client ou d'un agent.

La plupart des autorités de supervision des marchés émergents et économies en développement interrogées pour les besoins de la présente étude n'appliquent pas de procédure de supervision spéciale (ex situ ou in situ) pour évaluer la gestion des risques de blanchiment des capitaux et/ou de financement du terrorisme par les EME. Quelques-unes ont cependant créé des équipes spéciales chargées des évaluations en la matière. Les pratiques dans ce secteur d'activités donnent à penser que la surveillance des transactions liées au blanchiment des capitaux et/ou au financement du terrorisme et la vérification des antécédents des clients ne sont pas toujours suffisantes. En Afrique par exemple, il arrive que les clients s'enregistrent eux-mêmes pour plusieurs comptes de monnaie électronique auprès du même EME et de plusieurs EME, passant ainsi outre les limites imposées aux transactions. Cette pratique met à nu les faiblesses des contrôles et des systèmes de gestion des risques.

5.4.2 Portée des examens

L'imposition de limites aux transactions et aux soldes n'est efficace que si les procédures d'ouverture des comptes sont conformes à la loi et si la surveillance des transactions est efficace. Autrement, des clients peuvent avoir plusieurs comptes, s'associer à des agents et à d'autres clients et outrepasser les limites imposées à des fins criminelles. Les contrôles doivent être intégrés (encodés) dans les systèmes de l'EME, et une surveillance efficace demande des logiciels spécialisés. L'examen du blanchiment des capitaux et/ou du financement du terrorisme doit couvrir au moins les aspects suivants :

1. Le respect des limites statutaires
2. Les procédures d'ouverture des comptes (clients et agents)
3. L'établissement des profils des produits, des clients et des agents
4. La surveillance des transactions

5.4.3 Procédures d'examen

Comme dans d'autres domaines, l'autorité de supervision peut analyser (ex situ) les politiques écrites et les manuels de procédure de l'EME décrivant les fonctions de contrôle interne, la politique de gestion des risques, le personnel responsable et les systèmes informatiques en ce qui concerne le blanchiment des capitaux et/ou le financement du

terrorisme[53]. Les politiques et les manuels de procédure doivent tout au moins cadrer avec la loi applicable ; il est toutefois préférable qu'ils soient plus détaillés. L'examen peut porter particulièrement sur les questions suivantes :

- Les règles écrites sont-elles respectées dans la pratique et existe-t-il des brèches importantes qui favorisent la violation de ces règles.
- Dans quelle mesure les dispositions sur les obligations et les contrôles concernant le blanchiment des capitaux et/ou le financement du terrorisme et les modifications qui y sont apportées sont efficacement communiqués dans l'ensemble de l'institution.
- Des typologies de blanchiment des capitaux raisonnables sont-elles intégrées dans le programme de gestion des risques.
- Comment se fait la détection, la confirmation et le signalement des transactions suspectes, et comment l'EME y remédie-t-il.
- Si (et pour quelle raison) un grand nombre de transactions suspectes ont été détectées par le système ou au niveau du personnel opérationnel/de l'agent, mais n'ont pas été signalées au service de renseignements financiers.
- L'étude ex situ des rapports d'audit interne et externe et le suivi in situ.

Comme dans le cas des risques opérationnels, l'autorité de supervision peut procéder à des analyses automatiques ou manuelles des données de transaction granulaires et des événements signalés, tels que les dossiers d'ouverture de compte, pour déceler les situations suspectes et les écarts par rapport à la règle et aux politiques de l'EME. Ces données peuvent être étudiées sur place ou recueillies avant les procédures in situ[54].

5.4.3.1 RESPECT DES LIMITES STATUTAIRES

L'autorité de supervision peut procéder ainsi qu'il suit :

- Analyser (ex situ) les politique et procédures relatives aux limites statutaires, mesurer le niveau d'application (ex situ et in situ) et évaluer les exceptions.
- Évaluer l'efficacité des contrôles automatiques incorporés dans les systèmes pour déceler, traiter et signaler les transactions suspectes.

[53] Malheureusement, plusieurs des EME des marchés émergents et économies en développement étudiés ne disposent pas de services, de personnel, de logiciels spécialisés. Ils s'appuient plutôt sur le programme de lutte contre le blanchiment des capitaux et/ou du financement du terrorisme de leur société mère. Au regard des différences entre les services d'émission de monnaie électronique et de téléphonie mobile, les fonctions de contrôle du blanchiment des capitaux et/ou du financement du terrorisme gagneraient à être personnalisés pour les EME.
[54] Quelques-unes des autorités de supervision des marchés émergents et économies en développement interrogées ont accès à des données de transaction hautement granulaires, mais elles ne font pas des analyses sophistiquées (à l'aide par exemple de logiciels analytiques modernes) pour relever les risques opérationnels et ceux liés au blanchiment des capitaux et/ou au financement du terrorisme.

- Tester les systèmes en simulant des transactions interdites.
- S'enquérir des contrôles automatiques et des critères d'alerte ou de signalement et en demander une démonstration.
- Examiner le fichier des violations ou des tentatives de violation des limites, et s'enquérir de leurs causes et des solutions qui y ont été apportées.
- Faire une analyse chronologique des fichiers de données granulaires pour vérifier les informations fournies par l'EME et confirmer le respect constant ou non des limites statutaires.
- Vérifier s'il existe des contrôles qui essaient d'identifier les clients disposant de plusieurs comptes auprès de l'EME et dans d'autres EME.
- Enquêter davantage sur les types de compte qui suscitent des interrogations (par exemple, les comptes ouverts par les clients eux-mêmes, les comptes qui ont été signalés à plusieurs reprises).
- Demander des informations sur les employés habilités à modifier les règles sur les limites ou d'autres systèmes et demander si de telles révisions ont été faites par le passé, comment elles sont proposées et approuvées.

5.4.3.2 PROCÉDURES D'OUVERTURE DES COMPTES

Pour vérifier que les procédures d'ouverture des comptes sont conformes aux politiques et règles sur les EME, l'autorité de supervision peut procéder ainsi qu'il suit :

- Interroger le personnel opérationnel et les agents sur les procédures (notamment à distance) d'ouverture des compte (en décrivant chaque étape et chaque règle par exemple), leur demander s'il existe des exceptions, s'ils trouvent difficile de respecter les procédures (examiner les cartes d'identité par exemple), et si des clients ont pu ouvrir plusieurs comptes.
- S'il existe des données granulaires sur les transactions, vérifier s'il apparaît une concentration des volumes d'ouverture des comptes à certaines périodes/dans certains lieux ou agences, demander puis analyser la documentation sur un échantillon de comptes qui paraitraient suspects.
- Observer des agents et/ou des employés en train d'ouvrir des comptes pour des clients.
- Faire des évaluations mystères[55].
- Évaluer la gestion des risques pour ce qui concerne le recours à la biométrie ou à d'autres procédures de connaissance du client et/ou de vérification des antécédents des clients par voie électronique.

[55] Pour en savoir plus sur les évaluations mystères, voir Mazer et coll. (2015).

- Revoir les procédures pour dénombrer et surveiller les personnes politiquement exposées et l'utilisation des listes de sanctions.
- S'enquérir et établir au moyen des documents et des entretiens avec les agents que plusieurs formations visant tous les salariés de l'agent qui réalisent les transactions en monnaie électronique ont été organisées.

5.4.3.3 ÉTABLISSEMENT DES PROFILS DES PRODUITS, DES CLIENTS ET DES AGENTS

L'autorité de supervision peut vérifier et évaluer la manière dont les EME définissent les profils des clients et des agents (par exemple, client de détail, petit agent, grand agent, super agent, etc.), la localisation (grand centre urbain, zone frontalière, village rural, etc.) et d'autres caractéristiques (revenus, date de création du compte), autant d'éléments qui, mis ensemble, peuvent aider à définir différents niveaux de risque lié au blanchiment des capitaux et/ou au financement du terrorisme et les schémas de transaction respectifs attendus. Dans la plupart des marchés émergents et économies en développement objet de la présente étude, la réglementation impose des limites aux comptes et aux transactions pour tous les clients et produits des EME, mais ces derniers peuvent renforcer les limites pour des clients (par exemple les clients vivant dans les zones frontalières) ou des produits (les envois de fonds) présentant des risques plus importants. Les agents peuvent se montrer plus flexibles en ce qui concerne les limites parce qu'ils ont besoin de grosses transactions pour servir la clientèle finale. Il est important de comprendre comment les EME définissent les profils des clients et des agents, car c'est le point de départ de la détection des comportements potentiellement à risque grâce à la surveillance des transactions.

5.4.3.4 SURVEILLANCE DES TRANSACTIONS

Les EME peuvent utiliser des logiciels spécialisés pour surveiller les transactions et comparer les comportements suspects avec les comportements attendus. Tous les EME doivent disposer de systèmes entièrement automatisés dont le niveau de sophistication dépendra cependant de la taille et de la complexité de l'EME concerné. Le système doit être capable de déceler les tentatives de transaction au-delà des limites autorisées, les transactions qui s'écartent des profils prédéfinis et d'autres situations suspectes, comme un volume important de transactions à destination/à partir de quelques comptes, un afflux de transactions, une concentration géographique, plusieurs transactions réalisées par le même client, etc.

Les systèmes d'identification des fraudes et des risques liés au blanchiment des capitaux et/ou au financement du terrorisme sont de plus en plus sophistiqués et innovants. Certains procèdent par une analyse automatique complexe en temps réel de nombreux

facteurs et données afin de détecter tout comportement suspect, ce qui rend le système capable, par exemple, de déceler l'existence de plusieurs comptes qui seraient utilisés par un même individu au moyen de fausses déclarations d'identité ou en se servant de parents ou d'amis. Ces systèmes peuvent bloquer automatiquement certains comptes et déclencher une alerte à l'intention des employés.

La qualité de la surveillance des transactions dépendra de la qualité et de la variété des données utilisées pour le logiciel d'analyse. Un système coûteux et sophistiqué utilisant l'apprentissage automatique sera aussi peu efficace qu'un autre système si les données ne sont pas de qualité. L'autorité de supervision peut s'enquérir des sources des données et de leur qualité pour évaluer dans quelle mesure le système de surveillance détecte les risques et à quelle vitesse il les signale, pour évaluer la manière dont les employés signalent et traitent les situations détectées par le système, et pour déterminer si les situations de risque confirmées sont signalées à l'autorité de supervision.

Certaines autorités de supervision des marchés émergents et économies en développement désirent collecter des données de transaction hautement granulaires pour surveiller en temps réel les risques liés au blanchiment des capitaux et/ou au financement du terrorisme, à l'image de ce que certaines institutions financières d'aujourd'hui font à l'aide de systèmes de surveillance sophistiqués. Bien qu'il soit possible de procéder de la sorte, la rentabilité d'une telle démarche n'est pas évidente dans tous les cas. L'autorité de supervision peut recueillir des données granulaires pendant un examen et réaliser les analyses voulues. Par ailleurs, la surveillance en temps réel par l'autorité de supervision ne doit jamais se substituer à l'obligation qu'a l'EME d'assurer lui-même une surveillance en temps réel. FSI (2018) et Dias (2018) donnent quelques exemples d'utilisation de données hautement granulaires et de logiciels d'analyse sophistiqués pour la surveillance du blanchiment des capitaux et/ou le financement du terrorisme par l'autorité de supervision.

6. *Conclusion*

Les émetteurs de monnaie électronique contribuent largement à l'inclusion financière dans bon nombre de marchés émergents et économies en développement. Et les autorités de supervision veillent à la sûreté des marchés de monnaie électronique en appliquant une supervision proportionnelle qui tient compte des priorités et s'attarde sur les risques les plus importants. Certes, une démarche axée sur les risques est un facteur fondamental d'efficacité de la supervision des EME, mais les outils de SupTech peuvent aider à réduire le nombre de personnes utilisées dans certaines tâches de supervision et à approfondir les analyses.

La supervision des EME est plus simple que celle des banques, car la loi impose aux EME un champ d'activités plus restreint. Par conséquent, ils présentent en principe moins de risques que les banques. La réglementation oblige en outre les EME à protéger les fonds de leurs clients en les garantissant par des actifs liquides sans risque. La protection efficace des fonds réduit considérablement les risques de perte des fonds des clients. Cela étant, cette fonction est au cœur de l'activité de supervision des EME.

Il n'existe pas de modèle universel pour ce qui concerne la portée et la profondeur d'un exercice de supervision. Les autorités de supervision doivent adopter une approche axée sur les risques qui cadre avec leur contexte et centre leurs évaluations sur les EME les plus importants et les risques les plus gaves qu'ils présentent. La plupart des autorités de supervision voudront analyser une large gamme de risques en présence d'un grand EME, notamment les risques opérationnels, les risques liés au blanchiment des capitaux et/ou au financement du terrorisme et les risques liés à la protection des clients, avec un peu plus de détails que s'il s'agissait d'un petit EME. Une bonne méthodologie axée sur les risques repose sur la qualité des données, dont le point de départ est la surveillance permanente du marché qui permet de comparer les EME entre eux et de préparer les autorités de supervision à l'examen de chaque EME. Les orientations données dans la présente publication, en ce qui concerne particulièrement les procédures d'examen détaillées, doivent être utilisées judicieusement en fonction de l'approche spécifique des risques adoptée par l'autorité de supervision. Toutes les procédures ne s'appliqueront pas à tous les EME et certains exigeront plus que ce qui est décrit dans cette publication. D'ailleurs,

elle ne traite pas de certains aspects importants comme les pouvoirs de rectification/les mesures correctives et la résolution des EME.

Enfin, il n'y a aucune prescription quant à l'hébergement de la fonction de supervision des EME au sein d'une entité de supervision financière, mais l'autorité de supervision doit nécessairement avoir l'expérience requise en matière d'évaluations du secteur financier ainsi qu'une une connaissance précise des activités des EME.

Annexe 1. Organismes et entités interrogés

Pays/région	Organismes
Afrique l'Ouest	Banque Centrale des États de l'Afrique de l'Ouest (BCEAO)
Autriche	Oesterreichische National Bank
	Autorité des marchés financiers
Brésil	Banco Central do Brasil (BCB)
Colombie	Autorité de supervision financière
France	Autorité de contrôle prudentiel et de résolution (ACPR)
Ghana	Bank of Ghana
	MTN Mobile Money
	Airtel Money
	Tigo Cash
	Services financiers mobiles de Vodafone Ghana
Hong Kong	Autorité monétaire de Hong Kong
Inde	Inde
Jordanie	Jordanie
Luxembourg	Luxembourg
Malaisie	Bank Negara Malaysia
Mexique	National Banking and Securities Commission (CBNV)
	National Pension System Commission (CONSAR)
Myanmar	Central Bank of Myanmar
	Wave Money
Nigéria	Central Bank of Nigeria
Pakistan	State Bank of Pakistan
Paraguay	Central Bank of Paraguay
Pérou	Superintendence of Banks, Insurance and Pension Funds (SBS)
Philippines	Bangko Sentral ng Pilipinas (BSP)
Singapour	Autorité monétaire de Singapour
Tanzanie	Bank of Tanzania
	Tanzania Communications Regulatory Authority
	Tanzania Insurance Regulatory Authority
	Vodacom Tanzania
	Jumo
	Airtel Tanzania
Ouganda	Bank of Uganda
Royaume-Uni	Financial Conduct Authority

Annexe 2. Bibliographie

Principaux documents de référence

Staschen, Stefan, et Patrick Meagher. 2018. "Basic Regulatory Enablers for Digital Financial Services." Focus 109. Washington : CGAP. http://www.cgap.org/sites/default/files/Focus-Note-Basic-Regulatory-Enablers-for-DFS-May-2018.pdf

Dias, Denise, et Stefan Staschen. 2017. "Data Collection by Supervisors of DFS." Document de travail. Washington : CGAP. http://www.cgap.org/sites/default/files/Working-Paper-Data-Collection-by-Supervisors-of-DFS-Dec-2017.pdf

———. 2015. "Supervision of Banks and Nonbanks Operating through Agents. Practice in Nine Countries and Insights for Supervisors." Document de travail. Washington : CGAP. https://www.cgap.org/sites/default/files/Working-Paper-Supervision-of-Banks-and-Nonbanks-Operating-through-Agents-August-2015.pdf

Bibliographie

Alliance for Financial Inclusion (AFI). 2014. "Supervision and Oversight of Mobile Financial Services." Guideline Note No. 12, February. http://www.afi-global.org/publications/1451/Guideline-Note-12-Mobile-Financial-Services-Supervision-and-Oversight-of-MFS

Almazán, Mireya, et Nicolas Vonthron. 2014. "Mobile Money Profitability: A Digital Ecosystem to Drive Healthy Margins." Londres : Mobile Money for the Unbanked, November. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/11/2014_Mobile-money-profitability-A-digital-ecosystem-to-drive-healthy-margins.pdf

APRA (Australian Prudential Regulatory Authority). 2015. "Outsourcing Involving Shared Computing Services (including Cloud)." Information Paper, July. https://www.apra.gov.au/sites/default/files/information-paper-outsourcing-involving-shared-computing-services.pdf

Bauguess, Scott W. 2018. "The Role of Machine Readability in an AO World." Allocution principale, conférence sur la gestion de l'information financière, Boston, Mass., 3 mai. https://www.sec.gov/news/speech/speech-bauguess-050318?utm_source=Master+List&utm_campaign=036e369e76-EMAIL_CAMPAIGN_2018_05_04&utm_medium=email&utm_term=0_da5920711b-036e369e76183267633#_edn7

Buku, Mercy, et Rafe Mazer. 2017. "Fraud in Mobile Financial Services: Protecting Consumers, Providers and the System." Brief. Washington : CGAP. http://www.cgap.org/sites/default/files/Brief-Fraud-in-Mobile-Financial-Services-April-2017.pdf

BCBS (Basel Committee on Banking Supervision). 2016a. "Guidance on the Application of the Core Principles for Effective Banking Supervision to the Regulation and Supervision of Institutions Relevant to Financial Inclusion." Bâle : Banque des règlements internationaux, septembre. https://www.bis.org/bcbs/publ/d383.htm

———. 2016b. "Market Intelligence Gathering at Central Banks." Bâle : Banque des règlements internationaux, décembre. https://www.bis.org/publ/mktc08.htm

———. 2013. "Principles for Effective Risk Data Aggregation and Risk Reporting." Bâle : Banque des règlements internationaux, janvier. http://www.bis.org/publ/bcbs239.pdf

———. 2011. "Principles for Sound Management of Operational Risk." Bâle : Banque des règlements internationaux, juin. https://www.bis.org/publ/bcbs195.htm

———. 1998. "Risk Management for Electronic Banking and Electronic Money Activities." Bâle : Banque des règlements internationaux, mars, p. 18 à 20. https://www.bis.org/publ/bcbsc215.pdf

Broeders, Dirk, et Jermy Prenio. 2018. "Innovative Technology in Financial Supervision (Suptech)—The Experience of Early Users." FSI Insights on policy implementation, No. 9. Genève : Conseil de stabilité financière. https://www.bis.org/fsi/publ/insights9.pdf

CPMI (Comité sur les paiements et les infrastructures de marché). 2016. "Payment Aspects of Financial Inclusion." Bâle : Banque des règlements internationaux, avril. https://www.bis.org/cpmi/publ/d144.htm

———. 2014a. "Non-Banks in Retail Payments." Bâle : Banque des règlements internationaux, septembre. https://www.bis.org/cpmi/publ/d118.pdf

———. 2014b. "Recovery of Financial Market Infrastructures." Bâle : Banque des règlements internationaux, octobre. https://www.bis.org/cpmi/publ/d121.pdf

———. 2012. "Principles for Financial Market Infrastructures." Bâle : Banque des règlements internationaux, avril. https://www.bis.org/cpmi/publ/d101.htm

———. 2001. “Core Principles for Systemically Important Payment Systems.” Bâle : Banque des règlements internationaux, janvier. https://www.bis.org/cpmi/publ/d43.htm

———. 2000. “Clearing and Settlement Arrangements for Retail Payments in Selected Countries.” Bâle : Banque des règlements internationaux, septembre. https://www.bis.org/cpmi/publ/d40.pdf

Dias, Denise. 2018. “SupTech: Leveraging Technology for Better Supervision.” Toronto : Centre de Toronto, juillet. http://res.torontocentre.org/guidedocs/SupTech%20-%20Leveraging%20Technology%20for%20Better%20Supervision.pdf

ENISA (Agence européenne chargée de la sécurité des réseaux et de l’information). 2009. “Cloud Computing Risk Assessment,” Novembre. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

FSB (Conseil de stabilité financière). 2018. “Stocktake of Remittance Service Providers’ Access to Banking Services.” Geneva: FSB, mars. https://www.g20.org/sites/default/files/documentos_producidos/stocktake_of_remittance_service_providers_access_to_banking_services_fsb_march_2018_2.pdf

———. 2014. “Key Attributes of Effective Resolution Regimes for Financial Institutions.” Genève : FSB, octobre. http://www.fsb.org/what-we-do/policy-development/effective-resolution-regimes-and-policies/key-attributes-of-effective-resolution-regimes-for-financial-institutions.

Greenacre, Jonathan, et Ross P. Buckley. 2014. “Using Trusts to Protect Mobile Money Customers.” *Journal of Legal Studies*, 59–78.

G7. 2016. “G7 Fundamental Elements of Cybersecurity for the Financial Sector.” https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

Izaguirre, Juan Carlos, Timothy Lyman, Claire Mcguire, et Dave Grace. 2016. “Deposit Insurance and Digital Financial Inclusion.” Brief. Washington : CGAP. https://www.cgap.org/sites/default/files/Brief_Deposit_Insurance_and_Digital_Financial_Inclusion.pdf

Kemp, Katharine, et Ross P. Buckley. 2017. “Resolution Powers over E-Money Providers.” UNSW Law Research Paper No. 49, décembre. http://classic.austlii.edu.au/au/journals/UNSWLRS/2017/49.html

Piechocki, M., et T. Dabringhausen. 2015. “Reforming Regulatory Reporting: From Templates to Cubes.” The Irving Fischer Committee on Central Bank Statistics, “Combining Micro and Macro Financial Statistical Data for Financial Stability Analysis: Experiences, Opportunities and Challenges.” Varsovie : BearingPoint, 14–15 décembre. http://www.bis.org/ifc/publ/ifcb41o.pdf

Groupe de la Banque mondiale 2018.“Financial Sector’s Cybersecurity: Regulationsand Supervision.” Washington : Groupe de la Banque mondiale http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf

Wright, Paul. 2018. “Risk-Based Supervision.” Toronto : Centre de Toronto, mars. https://res.torontocentre.org/guidedocs/Risk-Based%20Supervision.pdf

Annexe 3. Documents de référence à l'intention des autorités de supervision

Guide de la supervision, manuels et autres

Association of Banks of Singapore. "Cloud Computing Implementation Guideline 1.1 for the Financial Industry in Singapore." Singapour : Association of Banks of Singapore, août. https://abs.org.sg/docs/library/abs-cloud-computing-implementation-guide.pdf

Banque centrale de l'Irlande. 2016. "Cross Industry Guidance in Respect of Information Technology and Cybersecurity Risks." Dublin : Banque centrale de l'Irlande. https://centralbank.ie/docs/default-source/Regulation/how-we-regulate/policy/cross-industry-guidance-information-technology-cybersecurity-risks.pdf?sfvrsn=2

CPMI (Comité sur les paiements et les infrastructure de marché). 2017. "Methodology of the Statistics on Payments and Financial Market Infrastructures in the CPMI Countries." Red Book Statistics. Genève : Banque des règlements internationaux. https://www.bis.org/cpmi/publ/d168.htm

Dias, Denise. 2013. "Implementing Consumer Protection in Emerging Markets and Developing Economies. A Technical Guide for Bank Supervisors." Washington : CGAP. http://www.cgap.org/sites/default/files/Technical-Guide-Implementing-Consumer-Protection-August-2013.pdf

BCE (Banque centrale européenne). 2018. "Tiber-EU Framework. How to Implement the European Framework for Threat Intelligence-Based Ethical Red Teaming." Francfort : BCE, mai. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

HKMA (Autorité monétaire de Hong Kong). 2016. "Guideline on Supervision of Stored Value Facility Licensees." Hong Kong : HKMA. http://www.hkma.gov.hk/eng/key-functions/international-financial-centre/regulatory-regime-for-svf-and-rps/regulation-of-svf.shtml

FFIEC (Conseil fédéral d'examen des institutions financières). "Annex A. Examination Procedures" in *IT Examination Handbook, Retail Payments Systems*. https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-a-examination-procedures.aspx

FFIEC (Conseil fédéral d'examen des institutions financières). "Appendix E: Mobile Financial Services on e-mobile Services," in *IT Examination Handbook, Retail Payments Systems*. https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix- e-mobile-financial-services.aspx

——."BusinessContinuityPlanning"in*ITExaminationHandbook,RetailPaymentsSystems*. https://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management/operational-risk/business-continuity-planning.aspx

———. "Principles of the Business Continuity Testing Program" in *IT Examination Handbook, Business Continuity Planning*. https://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/risk-monitoring-and-testing/principles-of-the-business-continuity-testing-program.aspx

U.S. Federal Reserve Board System, Board of Governors. "Interagency Guidelines Establishing Information Security Standards." https://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm

———. "Interagency Guidelines Establishing Information Security Standards." https://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm

FDIC (U.S. Federal Deposit Insurance Corporation). 2016. "Information Technology Risk Examination (InTREx) Information Technology Profile." Modèle d'examen des risques informatiques, juillet. https://www.fdic.gov/news/news/financial/2016/fil16043a.pdf

———. 2015. "Internal Routine and Controls" in *Security Safety Manual RMS Manual of Examination Policies*, March. https://www.fdic.gov/regulations/safety/manual/section4-2.pdf

Autres documents d'orientation

CGAP. 2018. "Cybersecurity for Mobile Financial Services: FAQs for Regulators, Supervisory Authorities and Digital Financial Services Providers." http://www.cgap.org/events/cybersecurity-mobile-financial-services

CPMI (Comité sur les paiements et les infrastructures de marché) et IOSCO (Organisation internationale des commissions de valeurs). 2016. "CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures." Bâle : Banque des règlements internationaux. https://www.bis.org/cpmi/publ/d146.pdf

CPMI (Comité sur les paiements et les infrastructures de marché). 2014. "Principles for Financial Market Infrastructures: Assessment Methodology for Oversight Expectations Applicable to Critical Service Providers." Bâle : Banque des règlements internationaux, décembre. https://www.bis.org/cpmi/publ/d123.pdf

ABE (Autorité bancaire européenne). 2017. "Guidance for the Use of Cloud Service Providers." Francfort : ABE, décembre. https://www.eba.europa.eu/-/eba-issues-guidance-for-the-use-of-cloud-service-providers-by-financial-institutions

FCA (Financial Conduct Authority). 2006. "Mystery Shopping Guide." Londres : FCA, novembre. https://www.fca.org.uk/publication/archive/fsa-mystery-shopping-guide.pdf

IFC (Société financière internationale) et Mastercard Foundation. 2016. "Digital Financial Services and Risk Management Handbook." Washington : IFC, pp. 28–39, 48–53, 68–86, 93, 95–108. https://www.ifc.org/wps/wcm/connect/06c7896a-47e1-40af-8213-af7f2672e68b/Digital+Financial+Services+and+Risk+Management+Handbook.pdf?MOD=AJPERES

Kerse, Mehmet, et Stefan Staschen. 2018. "Safeguarding Rules for Customer Funds Held by EMIs." Note technique. Washington : CGAP.

Mazer, Rafe, Xavier Gine, et Cristina Martinez. 2015. "Mystery Shopping for Financial Services." Washington : CGAP. http://www.cgap.org/publications/mystery-shopping-financial-services

SEC (Securities and Exchange Commission). 2017. "Observations from Cybersecurity Examinations." *National Exam Program Risk Alert,* Volume VI, Issue 5, 7 August. https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf

USAID (U.S. Agency for International Development) et Kenya School of Monetary Studies. 2010. "Mobile Financial Services Risk Matrix." Washington : USAID et Kenya School of Monetary Studies, pp. 30–39. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/mobilefinancialservicesriskmatrix100723.pdf

Exemples d'évaluations thématiques

La « Financial Conduct Authority » du Royaume-Uni.

Mobile Phone Insurance: https://www.fca.org.uk/publication/thematic-reviews/mobile-phone-findings.pdf

Treatment of Consumers Who Suffer Unauthorized Transactions: https://www.fca.org.uk/publication/thematic-reviews/tr15-10.pdf

QUERY:

AQ1: Please verify TOC entries against head on actual text.