EBA/GL/2017/17

12/01/2018

Orientations

relatives aux mesures de sécurité pour les risques opérationnels et de sécurité liés aux services de paiement dans le cadre de la directive (UE) 2015/2366 (DSP2)

1. Obligations de conformité et de déclaration

Statut de ces orientations

1. Le présent document contient des orientations émises en vertu de l'article 16 du règlement (UE) n° 1093/2010[1]. Conformément à l'article 16, paragraphe 3, du règlement (UE) n° 1093/2010, les autorités compétentes et les établissements financiers mettent tout en œuvre pour respecter ces orientations.

2. Les orientations donnent l'avis de l'ABE sur des pratiques de surveillance appropriées au sein du système européen de surveillance financière ou sur les modalités d'application du droit de l'Union dans un domaine particulier. Les autorités compétentes, telles que définies à l'article 4, paragraphe 2, du règlement (UE) n° 1093/2010, qui sont soumises aux orientations, doivent les respecter en les intégrant dans leurs pratiques, s'il y a lieu (par exemple en modifiant leur cadre juridique ou leurs processus de surveillance), y compris lorsque les orientations s'adressent principalement à des établissements.

Obligations de déclaration

3. Conformément à l'article 16, paragraphe 3, du règlement (UE) n° 1093/2010, les autorités compétentes doivent indiquer à l'ABE si elles respectent ou entendent respecter ces orientations, ou indiquer les raisons du non-respect des orientations, le cas échéant, avant le 12.03.2018. En l'absence d'une notification avant cette date, les autorités compétentes seront considérées par l'ABE comme n'ayant pas respecté les orientations. Les notifications sont à adresser à compliance@eba.europa.eu à l'aide du formulaire disponible sur le site internet de l'ABE et en indiquant en objet «EBA/GL/2017/17». Les notifications doivent être communiquées par des personnes dûment habilitées à rendre compte du respect des orientations au nom des autorités compétentes. Toute modification du statut de conformité avec les orientations doit être signalée à l'ABE.

4. Les notifications seront publiées sur le site internet de l'ABE, conformément à l'article 16, paragraphe 3.

[1] Règlement (UE) n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (l'Autorité bancaire européenne), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331, 15.12.2010, p.12).

2. Objet, champ d'application et définitions

Objet et champ d'application

5. Les présentes orientations découlent du mandat conféré à l'ABE en vertu de l'article 95, paragraphe 3, de la directive (UE) nº 2015/2366[2] (DSP2).

6. Les présentes orientations définissent les exigences en matière d'établissement, de mise en œuvre et de suivi des mesures de sécurité que doivent prendre les PSP, conformément à l'article 95, paragraphe 1, de la directive (UE) 2015/2366, en vue de gérer les risques opérationnels et de sécurité, liés aux services de paiement qu'ils fournissent.

Destinataires

7. Les présentes orientations s'adressent aux PSP au sens de l'article 4, paragraphe 11, de la directive (UE) 2015/2366 et tels que visés dans la définition des «établissements financiers» à l'article 4, paragraphe 1, du règlement (UE) 1093/2010, et aux AC au sens du point i) de l'article 4, paragraphe 2, de ce même règlement, en référence à la directive abrogée 2007/64/CE[3] (à présent la directive (UE) 2015/2366[4]).

Définitions

8. Sauf indication contraire, les termes employés et définis dans la directive (UE) 2015/2366 revêtent la même signification dans les présentes orientations. En outre, aux fins des présentes orientations, les définitions suivantes s'appliquent:

[2] Directive (UE) 2015/2366 du Parlement européen et du Conseil du jeudi 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

[3] Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE (JO L 319 du 5.12.2007, p. 1).

[4] Conformément au second alinéa de l'article 114 de la directive (UE) 2015/2366, toute référence faite à la directive abrogée 2007/64/CE s'entend comme faite à la directive (UE) 2015/2366 et est à lire selon le tableau de correspondance figurant à l'annexe II de la directive (UE) 2015/2366.

Organe de direction	– Pour les PSP qui sont des établissements de crédit, ce terme a la même signification que la définition au point 7) de l'article 3, paragraphe 1, de la directive 2013/36/UE[5]; – Pour les PSP qui sont des établissements de paiement ou des établissements de monnaie électronique, ce terme signifie les directeurs ou personnes responsables de la gestion du PSP et, le cas échéant, les personnes responsables de la gestion des activités de services de paiement du PSP; – Pour les PSP visés aux points c), e) et f) de l'article 1, paragraphe 1, de la directive (UE) 2015/2366, ce terme a la signification lui étant conférée par le droit de l'UE ou le droit national applicable.
Incident opérationnel ou de sécurité	Un événement unique ou une série d'événements liés non planifiés par le PSP, qui a ou aura probablement une incidence négative sur l'intégrité, la disponibilité, la confidentialité, l'authenticité et/ou la continuité des services liés au paiement.
Direction générale	(a) Pour les PSP qui sont des établissements de crédit, ce terme a la même signification que la définition au point 9) de l'article 3, paragraphe 1, de la directive 2013/36/UE; (b) Pour les PSP qui sont des établissements de paiement ou des établissements de monnaie électronique, ce terme signifie les personnes physiques qui exercent des fonctions exécutives dans un établissement, et qui sont responsables de la gestion quotidienne du PSP à l'égard de l'organe de direction et rendent des comptes à celui-ci en ce qui concerne cette gestion; (c) Pour les PSP visés aux points c), e) et f) de l'article 1, paragraphe 1, de la directive (UE) 2015/2366, ce terme a la signification lui étant conférée par le droit de l'UE ou le droit national applicable.
Risque de sécurité	Risque qui survient en cas d'échec ou d'inadéquation des procédures internes ou encore à la suite d'événements extérieurs qui ont ou pourraient avoir une incidence négative sur la disponibilité, l'intégrité, la confidentialité des systèmes de technologies de l'information et de la communication (TIC) et/ou des informations utilisées pour la fourniture de services de paiement. Cela comprend le risque de cyberattaques ou de sécurité physique inadaptée.
Appétit pour le risque	Le niveau et les types agrégés de risque qu'un établissement est prêt à accepter dans le cadre de sa capacité à prendre des

[5] Directive 2013/36/UE du Parlement européen et du Conseil concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338).

	risques, conformément à son modèle d'entreprise, afin d'atteindre ses objectifs stratégiques.

3. Mise en œuvre

Date d'entrée en vigueur

9. Les présentes orientations entrent en vigueur à compter du 13 janvier 2018.

4. Orientations

Orientation 1: Principes généraux

1.1 Tous les PSP devraient respecter l'ensemble des dispositions définies dans les présentes orientations. Le niveau de détail devrait être proportionnel à la taille du PSP ainsi qu'à la nature, à la portée, à la complexité et au risque des services particuliers que le PSP fournit ou a l'intention de fournir.

Orientation 2: Gouvernance

Cadre de gestion des risques opérationnels et de sécurité

2.1 Les PSP devraient établir un cadre de gestion des risques opérationnels et de sécurité (ci-après «cadre de gestion des risques») efficace, qui devrait être approuvé et réexaminé, au moins une fois par an, par l'organe de direction et, le cas échéant, par la direction générale. Ce cadre devrait se concentrer sur les mesures de sécurité visant à atténuer les risques opérationnels et de sécurité et être entièrement intégré aux procédures globales de gestion des risques du PSP.

2.2 Le cadre de gestion des risques devrait:

a) comprendre un document relatif à la politique de sécurité détaillé tel que visé à l'article 5, paragraphe 1, point j), de la directive (UE) 2015/2366;

b) être cohérent avec l'appétence au risque du PSP;

c) définir et attribuer les principaux rôles et responsabilités ainsi que le système de déclaration pertinent nécessaires pour faire appliquer les mesures de sécurité et pour gérer les risques opérationnels et de sécurité;

d) établir les procédures et les systèmes nécessaires pour identifier, mesurer, suivre et gérer l'ensemble des risques résultant des activités liées au paiement du PSP, et auxquels est exposé le PSP, notamment les dispositions en matière de continuité des activités.

2.3 Les PSP devraient veiller à ce que le cadre de gestion des risques soit correctement documenté et mis à jour avec des «enseignements tirés» documentés au cours de sa mise en œuvre et de son suivi.

2.4 Les PSP devraient, avant toute modification majeure d'infrastructure, de procédés ou de procédures et après chaque incident opérationnel ou de sécurité majeur ayant une incidence sur la sécurité des services de paiement qu'ils fournissent, veiller à réexaminer le cadre de gestion des risques pour déterminer si des modifications ou des améliorations sont nécessaires sans retard injustifié.

Gestion des risques et modèles de contrôle

2.5 Les PSP devraient établir trois lignes de défense efficaces, ou un modèle équivalent de gestion et de contrôle des risques internes, pour identifier et gérer les risques opérationnels et de sécurité. Les PSP devraient veiller à ce que le modèle de contrôle interne susmentionné dispose de suffisamment d'autorité, d'indépendance, de ressources et d'un système de déclaration direct à l'organe de direction et, le cas échéant, à la direction générale.

2.6 Les mesures de sécurité définies dans les présentes orientations devraient faire l'objet d'un audit par des auditeurs disposant d'une expertise en matière de sécurité informatique et de paiements et qui sont indépendants d'un point de vue opérationnel au sein ou vis-à-vis du PSP. La fréquence et l'objectif de ces audits devraient tenir compte des risques de sécurité correspondants.

Externalisation

2.7 Les PSP devraient veiller à l'efficacité des mesures de sécurité définies dans les présentes orientations lorsque des fonctions opérationnelles des services de paiement, y compris des systèmes informatiques, sont externalisées.

2.8 Les PSP devraient veiller à ce que des objectifs de sécurité appropriés et proportionnés ainsi que des mesures et des objectifs de performance soient intégrés aux contrats et aux accords sur les niveaux de service passés avec les fournisseurs auprès desquels ils ont externalisé ces fonctions. Les PSP devraient veiller au suivi et à la garantie du niveau de conformité de ces fournisseurs avec leurs objectifs de sécurité, leurs mesures et leurs objectifs de performance.

Orientation 3: Évaluation des risques

Identification des fonctions, procédés et ressources

3.1 Les PSP devraient identifier, établir et tenir régulièrement à jour un inventaire de leurs fonctions commerciales, de leurs fonctions essentielles et procédés de support afin de répertorier l'importance de chaque fonction, rôle et procédé de support, ainsi que leurs interdépendances en matière de risques opérationnels et de sécurité.

3.2 Les PSP devraient identifier, établir et tenir régulièrement à jour un inventaire des actifs du système d'information, tels que les systèmes TIC, leurs configurations, d'autres infrastructures, ainsi que les interconnexions avec d'autres systèmes internes et externes pour parvenir à gérer les ressources qui soutiennent leurs fonctions commerciales et procédés essentiels.

Classification des fonctions, procédés et ressources

3.3 Les PSP devraient classer les fonctions commerciales, procédés de support et actifs du système d'information identifiés en fonction de leur niveau de risque.

Évaluation des risques des fonctions, procédés et ressources

3.4 Les PSP devraient veiller à assurer un suivi continu des menaces et des vulnérabilités et à régulièrement réexaminer les scénarios de risque ayant une incidence sur leurs fonctions commerciales, leurs processus critiques et les actifs du système d'information. Dans le cadre de l'obligation de mener et de fournir à l'AC une évaluation à jour et exhaustive des risques opérationnels et de sécurité liés aux services de paiement qu'ils fournissent et des informations sur le caractère adéquat des mesures d'atténuation et des mécanismes de contrôle mis en œuvre pour faire face à ces risques, telle que prévue à l'article 95, paragraphe 2, de la directive (UE) 2015/2366, les PSP devraient effectuer et documenter des évaluations des risques, au moins chaque année ou à des intervalles plus rapprochés fixés par l'AC, des fonctions, procédés et actifs du système d'information qu'ils ont identifiés et classés, afin d'identifier et d'évaluer les principaux risques opérationnels et de sécurité. Ces évaluations des risques devraient également être réalisées avant toute modification majeure d'infrastructure, de procédé ou de procédures ayant une incidence sur la sécurité des services de paiement.

3.5 Sur la base des évaluations des risques, les PSP devraient déterminer si et dans quelle mesure des modifications des mesures de sécurité existantes, technologies employées et procédures ou services de paiement proposés sont nécessaires. Les PSP devraient tenir compte du temps nécessaire à la mise en œuvre de ces modifications et du temps nécessaire pour prendre des mesures de sécurité intermédiaires appropriées pour limiter autant que possible les incidents opérationnels ou de sécurité, la fraude ou tous effets potentiellement perturbateurs dans la fourniture de services de paiement.

Orientation 4: Protection

4.1 Les PSP devraient établir et mettre en œuvre des mesures de sécurité préventives contre des risques opérationnels et de sécurité identifiés. Ces mesures devraient garantir un niveau approprié de sécurité correspondant aux risques identifiés.

4.2 Les PSP devraient établir et mettre en œuvre une méthode de «défense en profondeur» en instituant des contrôles à plusieurs niveaux visant les personnes, les procédés et la technologie, chaque niveau servant de filet de sécurité aux niveaux précédents. L'expression «Défense en profondeur» devrait être comprise comme un ensemble de plusieurs contrôles visant à couvrir le même risque, comme le principe des quatre yeux, l'authentification à deux facteurs, la segmentation en réseaux et de multiples pare-feu.

4.3 Les PSP devraient veiller à la confidentialité, l'intégrité et la disponibilité de leurs actifs logiques et physiques critiques, ressources et données de paiement sensibles de leurs USP qu'elles soient stockées, en transit ou en cours d'utilisation. Si ces données comportent des données à caractère

personnel, ces mesures devraient être mises en œuvre conformément au règlement (UE) 2016/6796 ou, le cas échéant, au règlement (CE) 45/2001.7

4.4 Les PSP devraient déterminer, de manière continue, si les changements dans l'environnement opérationnel existant influencent les mesures de sécurité existantes ou nécessitent l'adoption de mesures supplémentaires pour atténuer le risque impliqué. Ces changements devraient faire partie du processus de gestion des changements formel du PSP, qui devrait veiller à ce que les changements soient dûment planifiés, testés, documentés et autorisés. Sur base des menaces observées pour la sécurité et des changements apportés, des tests devraient être réalisés pour inclure des scénarios d'attaques potentielles pertinentes et connues.

4.5 Dans la conception, le développement et la fourniture de services de paiement, les PSP devraient veiller à l'application des principes de la séparation des fonctions et du «moindre privilège». Les PSP devraient accorder une attention spécifique à la séparation des environnements informatiques, notamment des environnements de développement, de test et de production.

Intégrité et confidentialité des données et systèmes

4.6 Dans la conception, le développement et la fourniture de services de paiement, les PSP devraient s'assurer que la collecte, l'acheminement, le traitement, le stockage et/ou l'archivage et la visualisation des données de paiement sensibles des USP sont appropriés, pertinents et limités au strict nécessaire pour la fourniture de leurs services de paiement.

4.7 Les PSP devraient vérifier régulièrement que le logiciel utilisé pour la fourniture de services de paiement, y compris le logiciel de paiement de l'utilisateur, soit à jour et que des correctifs de sécurité critique soient déployés. Les PSP devraient veiller à ce que des mécanismes de vérification de l'intégrité soient en place afin de vérifier l'intégrité des logiciels, microprogrammes et informations relatifs à leurs services de paiement.

Sécurité physique

4.8 Les PSP devraient disposer de mesures de sécurité physique appropriées, notamment pour protéger les données de paiement sensibles des USP ainsi que les systèmes TIC utilisés pour fournir des services de paiement.

Contrôle d'accès

[6] Règlement (UE) du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119, 4.5.2016, p. 1).

[7] Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes de la Communauté et la libre circulation de ces données (JO L 8, 12.1.2001, p. 1).

4.9 L'accès physique et logique aux systèmes TIC devrait uniquement être autorisé aux personnes agréées. L'agrément devrait être accordé en fonction des tâches et responsabilités du personnel, en se limitant aux personnes correctement formées et contrôlées. Les PSP devraient instaurer des contrôles qui limitent de manière fiable cet accès aux systèmes TIC aux personnes dont l'activité l'exige légitimement. L'accès électronique sur demande aux données et systèmes devrait se limiter au minimum requis pour fournir le service concerné.

4.10 Les PSP devraient effectuer des contrôles rigoureux des accès privilégiés au système en limitant strictement et en supervisant étroitement le personnel dont les droits d'accès au système sont élevés. Les contrôles tels que les contrôles d'accès fondés sur les rôles, la production de journaux d'événements, l'analyse des activités des utilisateurs privilégiés sur les systèmes, l'authentification forte et le suivi des anomalies devraient être mis en œuvre. Les PSP devraient gérer les droits d'accès aux actifs du système d'information et à leurs systèmes de support sur la base du «besoin d'en connaître». Les droits d'accès devraient être réexaminés périodiquement.

4.11 Les journaux d'événements des accès devraient être conservés pour une période proportionnée au niveau de risque des fonctions commerciales, des procédés de support d'accompagnement et des actifs du système d'information identifiés, conformément aux points GL 3.1 et GL 3.2, sans préjudice des exigences de rétention définies dans la législation de l'UE et des États membres. Les PSP devraient utiliser ces informations pour faciliter l'identification et l'analyse d'activités anormales détectées lors de la fourniture de services de paiement.

4.12 Afin de garantir une communication sûre et de réduire les risques, l'accès administratif à distance aux composants critiques des systèmes TIC ne devrait être accordé que sur la base du «besoin d'en connaître» et lorsque des solutions d'authentification renforcée sont appliquées.

4.13 Le fonctionnement des produits, des outils et des procédures relatifs aux procédés de contrôle d'accès devrait empêcher que ces processus soient compromis ou contournés. Cela comprend la phase d'enrôlement, de fourniture, de révocation et de retrait des produits, outils et procédures correspondants.

Orientation 5: Détection

Suivi continu et détection

5.1 Les PSP devraient établir et mettre en œuvre des processus et des dispositions pour suivre de manière continue les fonctions commerciales, les procédés de support et les actifs du système d'information afin de détecter les activités anormales lors de la fourniture de services de paiement. Dans le cadre de ce suivi continu, les PSP devraient disposer de capacités adaptées et efficaces pour détecter les intrusions physiques ou logiques ainsi que les violations de confidentialité, d'intégrité et de disponibilité des actifs du système d'information utilisés lors de la fourniture de services de paiement.

5.2 Le suivi en continu et les procédés de détection devraient couvrir:

a) les facteurs internes et externes pertinents, notamment les fonctions administratives commerciales et des systèmes TIC;

b) les transactions afin de détecter tout abus d'accès par les prestataires de services ou autres entités; et

c) les menaces internes et externes potentielles.

5.3 Les PSP devraient mettre en œuvre des mesures de détection pour identifier de possibles fuites d'informations, codes malveillants et autres menaces pour la sécurité, ainsi que les vulnérabilités notoires des logiciels et matériels, et s'informer des nouvelles mises à jour de sécurité correspondantes.

Suivi et signalement des incidents opérationnels ou de sécurité

5.4 Les PSP devraient déterminer les critères et seuils adaptés pour considérer un événement comme incident opérationnel ou de sécurité, tel que défini dans la section «Définitions» des présentes orientations, ainsi que les indicateurs d'avertissement précoce devant servir d'alerte au PSP afin de permettre la détection précoce d'incidents opérationnels ou de sécurité.

5.5 Les PSP devraient établir les procédés et structures organisationnelles adaptés pour garantir le contrôle, la gestion et le suivi cohérents et intégrés des incidents opérationnels ou de sécurité.

5.6 Les PSP devraient établir une procédure de signalement de leurs incidents opérationnels ou de sécurité ainsi que des réclamations de leurs clients relatives à la sécurité à leur direction générale.

Orientation 6: Continuité d'activité

6.1 Les PSP devraient mettre en place une gestion saine de leur continuité d'activité, afin de maximiser leur capacité de fournir des services de paiement sans interruption et de limiter les pertes en cas de perturbation grave de leurs activités.

6.2 Afin de mettre en place une gestion saine de la continuité d'activité, les PSP devraient analyser soigneusement leur exposition à des interruptions graves de leur activités et évaluer, tant sur le plan quantitatif que qualitatif, leurs impacts potentiels au moyen d'une analyse interne et/ou externe de données et de scénarios. Sur la base des fonctions critiques, des procédés, des systèmes, des transactions et des interdépendances identifiés et classés conformément aux points GL 3.1 à GL 3.3, les PSP devraient organiser les mesures de continuité d'activité selon une méthode fondée sur les risques, qui peut être basée sur les évaluations des risques réalisées au titre du point GL 3. Selon le modèle d'entreprise du PSP, cela peut, par exemple, faciliter le traitement ultérieur des transactions critiques tout en poursuivant le rétablissement du service.

6.3 Sur base de l'analyse réalisée au point GL 6.2, les PSP devraient mettre en place:

a) des PCA afin de garantir leur capacité à réagir de manière appropriée aux urgences et de poursuivre leurs activités commerciales majeures; et

b) des mesures d'atténuation à adopter dans l'éventualité d'une cessation de leurs services de paiement et de la résiliation des contrats existants, pour éviter toute incidence négative sur les systèmes de paiement et sur les USP et pour garantir l'exécution des transactions de paiement en cours.

Planification de la continuité d'activité sur la base de scénarios

6.4 Le PSP devrait envisager un ensemble de différents scénarios, y compris extrêmes, mais plausibles, auxquels il pourrait être confronté, et évaluer l'incidence potentielle que de tels scénarios pourraient avoir.

6.5 Sur la base de l'analyse réalisée au point GL 6.2 et des scénarios vraisemblables identifiés au point GL 6.4, le PSP devrait développer des plans de réponse et de rétablissement de l'activité, qui devraient:

a) être axés sur le déroulement des fonctions, des procédés, des systèmes, des transactions et des interdépendances critiques;

b) être documentés et mis à la disposition des unités commerciales et de support et facilement accessibles en cas d'urgence; et

c) être mis à jour conformément aux enseignements tirés des tests, aux nouveaux risques identifiés, aux menaces, aux changements des objectifs de rétablissement de l'activité et aux priorités.

Test des plans de continuité d'activité

6.6 Les PSP devraient tester leurs PCA et veiller à ce que la mise en œuvre de leurs fonctions, processus, systèmes, transactions et interdépendances critiques soient testés au moins tous les ans. Ces plans devraient soutenir les objectifs visant à protéger et, le cas échéant à rétablir l'intégrité et la disponibilité des opérations, ainsi que la confidentialité de leurs actifs du système d'information.

6.7 Les plans devraient être mis à jour au moins chaque année, sur la base des résultats des tests, des renseignements relatifs aux menaces actuelles, du partage d'informations et des enseignements tirés d'événements antérieurs, et de l'évolution des objectifs de rétablissement de l'activité, ainsi que de l'analyse des scénarios opérationnels et techniques plausibles qui ne se sont pas encore réalisés et, le cas échéant, suite à des modifications des systèmes et procédés. Les PSP devraient consulter et se coordonner avec les parties concernées internes et externes lors de l'établissement de leurs PCA.

6.8 Les tests des PSP ainsi que leurs PCA devraient:

a) comprendre un ensemble adapté de scénarios, tel que visé au point GL 6.4;

b) être conçus pour remettre en question les hypothèses sur lesquelles se fondent les PCA, notamment les dispositifs de gouvernance et les plans de communication en situation de crise; et

c) comprendre des procédures visant à vérifier la capacité de leur personnel et de leurs procédés à répondre de manière adaptée aux scénarios ci-dessus.

6.9 Les PSP devraient procéder périodiquement au suivi de l'efficacité de leurs PCA, et documenter et analyser toutes les difficultés ou tous les échecs résultant des tests.

Communication en situation de crise

6.10 En cas de perturbation ou d'urgence, et au cours de la mise en œuvre des PCA, les PSP devraient veiller à disposer de mesures efficaces de communication en situation de crise, afin que toutes les parties concernées internes et externes, y compris les prestataires de services externes, soient informées en temps utile et de façon appropriée.

Orientation 7: Test des mesures de sécurité

7.1 Les PSP devraient établir et mettre en œuvre un cadre de test qui valide la solidité et l'efficacité des mesures de sécurité et veiller à ce que ce cadre de test soit adapté pour contrer des nouvelles menaces et vulnérabilités, identifiées à travers des activités de contrôle des risques.

7.2 Les PSP devraient veiller à ce que des tests soient réalisés en cas de modification d'infrastructure, de procédés ou de procédures et si des modifications sont apportées suite à des incidents opérationnels ou de sécurité majeurs.

7.3 Ce cadre de test devrait également englober les mesures de sécurité pertinentes pour i) les terminaux de paiement et dispositifs utilisés aux fins des services de paiement, ii) les terminaux de paiement et dispositifs utilisés aux fins de l'authentification des USP, et iii) les dispositifs et logiciels fournis par le PSP à l'USP pour générer/recevoir un code d'authentification.

7.4 Le cadre de test devrait garantir que les tests:

a) sont réalisés dans le cadre du processus de gestion des changements formel du PSP pour garantir leur solidité et efficacité;

b) sont réalisés par des testeurs indépendants disposant de suffisamment de connaissances, de compétences et d'expertise en matière de test de mesures de sécurité relatives aux services de paiement et n'étant pas impliqués dans l'élaboration des mesures de sécurité relatives aux services ou systèmes de paiement correspondants à tester, du moins pour les tests finaux préalablement à la mise en œuvre des mesures de sécurité; et

c) comprennent des analyses de vulnérabilité et des tests d'intrusion adaptés au niveau de risque identifié avec les services de paiement.

7.5 Les PSP devraient procéder à des tests continus et répétés des mesures de sécurité pour leurs services de paiement. Pour les systèmes qui sont essentiels à la fourniture de leurs services de

paiement (comme décrits au point GL 3.2), ces tests devraient être réalisés au moins sur base annuelle. Les systèmes non essentiels devraient être régulièrement testés selon une méthode fondée sur les risques, mais au moins tous les trois ans.

7.6 Les PSP devraient procéder au suivi et à l'évaluation des résultats des tests réalisés, et mettre à jour leurs mesures de sécurité en conséquence et sans retard injustifié dans le cas des systèmes essentiels.

Orientation 8: Connaissances des situations et formation continue

Nature de la menace et connaissances des situations

8.1 Les PSP devraient établir et mettre en œuvre des procédés et structures organisationnelles pour identifier et suivre de manière continue les menaces opérationnelles et de sécurité qui pourraient avoir une incidence matérielle sur leur capacité de fournir des services de paiement.

8.2 Les PSP devraient analyser les incidents opérationnels ou de sécurité ayant été identifiés ou s'étant produits au sein ou en dehors de l'organisation. Les PSP devraient tenir compte des enseignements essentiels tirés de ces analyses et mettre à jour les mesures de sécurité en conséquence.

8.3 Les PSP devraient suivre activement les évolutions technologiques afin de garantir qu'ils connaissent les risques de sécurité.

Formation et programmes de sensibilisation à la sécurité

8.4 Les PSP devraient établir un programme de formation à l'intention de l'ensemble de leur personnel, pour garantir qu'il soit formé pour exécuter ses tâches et exercer ses responsabilités conformément aux politiques et procédures de sécurité pertinentes afin de réduire l'erreur humaine, le vol, la fraude, les abus ou les pertes. Les PSP devraient veiller à ce que le programme de formation du personnel soit organisé au moins annuellement, et plus fréquemment si nécessaire.

8.5 Les PSP devrait veiller à ce que le personnel occupant des fonctions essentielles identifiées au point GL 3.1 suive des formations ciblées dans le domaine de la sécurité de l'information sur base annuelle, ou plus fréquemment si nécessaire.

8.6 Les PSP devraient établir et mettre en œuvre des programmes ponctuels de sensibilisation à la sécurité afin de former leur personnel et de répondre aux risques relatifs à la sécurité de l'information. Ces programmes devraient exiger du personnel des PSP qu'ils signalent toute activité ou tous incidents inhabituels.

Orientation 9: Gestion des relations avec les utilisateurs de services de paiement

Sensibilisation des utilisateurs de services de paiement aux risques de sécurité et aux mesures d'atténuation des risques

9.1 Les PSP devraient établir et mettre en œuvre des procédés pour renforcer la sensibilisation des USP aux risques de sécurité liés aux services de paiement en leur fournissant de l'assistance et des orientations.

9.2 L'assistance et les orientations fournies aux USP devraient être mises à jour à la lumière des nouvelles menaces et vulnérabilités, et les changements devraient être communiqués aux USP.

9.3 Lorsque la fonctionnalité des produits le permet, les PSP devraient permettre aux USP de désactiver les fonctionnalités de paiement spécifiques liées aux services de paiement fournis par le PSP à l'USP.

9.4 Lorsque, conformément à l'article 68, paragraphe 1, de la directive (UE) 2015/2366, un PSP a convenu avec le payeur de plafonds de dépenses pour les opérations de paiement exécutées au moyen d'instruments spécifiques de paiement, le PSP devrait donner au payeur la possibilité d'ajuster ses plafonds à la limite maximale convenue.

9.5 Les PSP devraient offrir aux USP la possibilité de recevoir des alertes relatives à des tentatives initiées et/ou avortées de réaliser des transactions de paiement, leur permettant de détecter toute utilisation frauduleuse ou malveillante de leurs comptes.

9.6 Les PSP devraient tenir les USP informés des mises à jour des procédures de sécurité ayant une incidence sur les USP vis-à-vis de la fourniture de services de paiement.

9.7 Les PSP devraient fournir aux USP une assistance pour toutes les questions, les demandes de support et les notifications d'anomalies ou les problèmes relatifs aux questions de sécurité afférentes aux services de paiement. Les USP devraient être correctement informés de la manière dont cette assistance peut être obtenue.