cssf

Commission de Surveillance
du Secteur Financier

Circulaire CSSF 20/750

Exigences en matière de gestion des risques liés aux technologies de l'information et de la communication et à la sécurité

Commission de Surveillance du Secteur Financier

Circulaire CSSF 20/750

Concerne : Exigences en matière de gestion des risques liés aux technologies de l'information et de la communication et à la sécurité

Luxembourg, le 25 août 2020

À tous les établissements de crédit et à tous les PSF

À tous les établissements de paiement et à tous les établissements de monnaie électronique

Mesdames, Messieurs,

Cette circulaire met en œuvre les orientations de l'Autorité Bancaire Européenne EBA/GL/2019/04 relative à la gestion des risques liés aux technologies de l'information et de la communication (« TIC ») et à la sécurité (ci-après « orientations TIC »).

Par ailleurs, la circulaire précise que le contenu des orientations TIC correspond également aux attentes de la CSSF concernant les mesures de gestion des risques et les mécanismes de contrôle et de sécurité mentionnés dans la loi du 5 avril 1993 relative au secteur financier (« LSF ») et dans la loi du 10 novembre 2009 relative aux services de paiement (« LSP »).

1. Exigences en matière de gestion des risques liés aux technologies de l'information et de la communication (TIC) et à la sécurité

Mise en œuvre des orientations de l'Autorité Bancaire Européenne EBA/GL/2019/04

1. Par la présente circulaire, la CSSF, en sa qualité d'autorité compétente, se conforme aux orientations (ci-après « les orientations TIC ») de l'Autorité Bancaire Européenne (ci-après « ABE ») sur la gestion des risques liés aux TIC et à la sécurité (référence : EBA/GL/2019/04), et les applique. Par conséquent, la CSSF a intégré les orientations TIC dans sa pratique administrative et son approche réglementaire en vue de promouvoir la convergence des pratiques de surveillance dans ce domaine au niveau européen.

Mesures de gestion des risques et mécanismes de contrôle et de sécurité

2. La CSSF considère que le contenu des orientations TIC correspond à ses attentes en ce qui concerne les mesures de gestion des risques et les mécanismes de contrôle et de sécurité mentionnés dans la LSF aux articles 5(1bis), 17(1bis), 36(1) et 37-1(4) et dans la LSP aux articles 11(2) et 105-1.
3. Ainsi, la CSSF attend de toutes les entités agréées selon la LSF et la LSP - qu'elles soient également ou non dans le champ d'application des orientations TIC - qu'elles mettent en œuvre le contenu de ces orientations TIC afin de gérer leurs risques liés aux TIC et à la sécurité.

Précisions quant au contenu des orientations TIC

4. Aux fins de la présente circulaire, les termes suivants employés dans les orientations TIC sont à comprendre comme suit :
   a. Le terme « organe de direction » employé au paragraphe 50 de l'orientation « 1.5 Gestion des opérations de TIC »[1] est à comprendre comme « organe de direction ou par les responsables autorisés par l'organe de direction ».

[1] *Paragraphe 50 de l'orientation « 3.5 ICT operations management » dans la version anglaise.*

b. Le terme « direction générale » employé au point 60.d)i) de l'orientation « 3.5.1 Gestion des problèmes et incidents liés aux TIC »[2] est à comprendre comme « direction ».

2. Modification de la circulaire CSSF 12/552

5. Cette circulaire modifie la circulaire CSSF 12/552, telle que modifiée[3], comme suit :

   a. Au chapitre 2 de la partie II, le 4ème paragraphe du point 9 est remplacé par : « *La seconde ligne est formée par les fonctions de support, y compris la fonction financière et comptable (section 5.2.2 de la présente circulaire), et les fonctions compliance et de contrôle des risques (sous-chapitre 6.2 et sections 6.2.5 et 6.2.6 de la présente circulaire, et orientations 1.3*[4] *mises en œuvre par la circulaire CSSF 20/750 pour le cadre de gestion des risques liés aux technologies de l'information et de la communication et à la sécurité) qui contribuent au contrôle indépendant des risques.* »

   b. Au chapitre 5 de la partie II :

      i. le point 85 de la section 5.2.3 est remplacé par : « *Les établissements organisent leur fonction informatique de manière à en avoir le contrôle et à en assurer la robustesse, l'efficacité, la cohérence et l'intégrité conformément au point 12. Pour ce faire, ils respectent les exigences de la circulaire CSSF 20/750 relative aux exigences en matière de gestion des risques liés aux technologies de l'information et de la communication et à la sécurité* ».

      ii. le point 86 de la section 5.2.3 est supprimé.

[2] *Point 60.d)i) de l'orientation « 3.5.1 ICT incident and problem management » dans la version anglaise.*

[3] *Par les circulaires CSSF 13/563, CSSF 14/597, CSSF 16/642, CSSF 16/647 et CSSF 17/655.*

[4] *Orientations 3.3 dans la version anglaise.*

3. Abrogation et remplacement de la circulaire CSSF 19/713

6. Les orientations TIC transposées par la présente circulaire abrogent les orientations EBA/GL/2017/17 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 (PSD2). De la même manière, la présente circulaire abroge et remplace la circulaire CSSF 19/713 qui transposait les orientations EBA/GL/2017/17.

7. Il est d'ailleurs rappelé que le terme « risques liés aux TIC et à la sécurité » couvre les risques opérationnels et de sécurité visés à l'article 105-1 de la LSP.

4. Exigence additionnelle pour les prestataires de services de paiement (PSP)[5]

8. Ainsi qu'en dispose le paragraphe 24 de l'orientation « 1.3.5 Rapport à l'organe de direction »[6] et conformément à l'article 105-1(2) de la LSP, les PSP ont l'obligation de fournir à la CSSF une évaluation des risques à jour et exhaustive en matière de services de paiement (ci-après « PSP ICT Assessment »).

   La CSSF a développé un formulaire standardisé pour le PSP ICT Assessment à utiliser par tous les PSP.

   L'objectif de ce modèle standardisé du PSP ICT Assessment est de présenter des lignes directrices aux PSP quant aux attentes de la CSSF par rapport aux informations à fournir par le biais du PSP ICT Assessment, et ainsi atteindre un certain degré d'harmonisation et de comparabilité entre les différents PSP ICT Assessments.

   En ce qui concerne le champ d'application du PSP ICT Assessment, il est à noter que :

[5] *Tels que définis à l'article 1(37) de la LSP.*

[6] *Paragraphe 24 de l'orientation « 3.3.5 Reporting » dans la version anglaise.*

- Les établissements dont le modèle d'affaires n'inclut pas la prestation de services de paiement (tels que définis à l'article 1 (38) de la LSP) n'ont pas à fournir de PSP ICT Assessment. À partir du moment où le modèle d'affaires d'un établissement inclut la prestation de services de paiement, l'établissement doit soumettre à la CSSF, pour l'année civile en question, un PSP ICT Assessment.
- Les succursales originaires d'un autre État membre de l'EEE établies au Luxembourg, qui offrent des services de paiement, n'ont pas à fournir de PSP ICT Assessment à la CSSF. Par contre, les PSP luxembourgeois qui ont établi des succursales dans d'autres pays de l'EEE, qui fournissent des services de paiement, doivent inclure ces succursales dans leur PSP ICT Assessment. Dans le cas de figure où l'évaluation des risques liés aux TIC et à la sécurité pour ces succursales s'écarte de celle du PSP, ceci est à préciser dans le PSP ICT Assessment[7].

Tous les PSP devront soumettre le formulaire « PSP ICT Assessment », dûment complété, à la CSSF sur une base annuelle, au plus tard le 31 mars de chaque année et couvrant l'année civile précédente.

Le modèle du PSP ICT Assessment est disponible sur le site Internet de la CSSF à l'adresse suivante :

https://edesk.apps.cssf.lu/

Le PSP ICT Assessment doit être validé par l'organe de direction du PSP, c'est-à-dire au moins par le membre de l'organe de direction responsable de la fonction TIC. Cette validation est à préciser dans la section y relative du PSP ICT Assessment.

Le PSP ICT Assessment, dûment complété et validé, doit être soumis sur une base annuelle par un membre de l'organe de direction à la CSSF exclusivement par le portail eDesk de la CSSF.

5. Entrée en vigueur

9. La présente circulaire entre en vigueur à compter du 25 août 2020.
10. Les orientations sont annexées à la présente circulaire et sont disponibles sur le site de l'ABE à l'adresse suivante : https://eba.europa.eu/regulation-

[7] *cf. Questions/Réponses de l'EBA, ID number 2018_4176*

and-policy/internal-governance/guidelines-on-ict-and-security-risk-management.

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur général

Annexe

Orientations

EBA/GL/2019/04

28 novembre 2019

Orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité

Obligations de conformité et de déclaration

Statut des présentes orientations

1. Le présent document contient des orientations formulées conformément à l'article 16 du règlement (UE) nº 1093/2010[1]. Conformément à l'article 16, paragraphe 3, du règlement (UE) nº 1093/2010, les autorités compétentes et les établissements financiers doivent tout mettre en œuvre pour respecter ces orientations.

2. Les orientations exposent le point de vue de l'ABE concernant les pratiques de surveillance appropriées au sein du système européen de surveillance financière ou les modalités d'application de la législation de l'Union européenne dans un domaine particulier. Les autorités compétentes, telles que définies à l'article 4, paragraphe 2, du règlement (UE) nº 1093/2010, auxquelles s'appliquent les orientations, devraient les respecter en les intégrant de manière appropriée dans leurs pratiques (par exemple en modifiant leur cadre juridique ou leurs processus de surveillance), y compris lorsque les orientations s'adressent en priorité à des établissements.

Obligations de déclaration

3. Conformément à l'article 16, paragraphe 3, du règlement (UE) nº 1093/2010, les autorités compétentes doivent indiquer à l'ABE si elles respectent ou entendent respecter les présentes orientations, ou indiquer les raisons de tout non-respect, le cas échéant, avant le ([jj.mm.aaaa]). En l'absence de toute notification dans ce délai, les autorités compétentes seront considérées par l'ABE comme ne respectant pas 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/2019/04». Les notifications doivent être envoyées par des personnes dûment habilitées à rendre compte du respect des orientations au nom des autorités compétentes qu'elles représentent. Toute modification du statut de conformité avec les orientations doit également 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) nº 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (JO L 331 du 15.12.2010, p. 12).

Objet, champ d'application et définitions

Objet

5. Les présentes orientations sont fondées sur les dispositions de l'article 74 de la directive 2013/36/UE (directive sur les exigences de fonds propres, ou CRD) concernant la gouvernance interne et procèdent du mandat visant à formuler des orientations tel que prévu à l'article 95, paragraphe 3, de la directive (UE) 2015/2366 (deuxième directive sur les services de paiement, ou DSP2).

6. Les présentes orientations précisent les mesures de gestion des risques que les établissements financiers (tels que définis au paragraphe 9 ci-dessous) doivent prendre, conformément à l'article 74 de la CRD, afin de gérer les risques liés aux technologies de l'information et de la communication (TIC) et à la sécurité dans le cadre de toutes leurs activités, ainsi que les mesures de gestion des risques que les prestataires de services de paiement («PSP», tels que définis au paragraphe 9 ci-dessous) doivent prendre, conformément à l'article 95, paragraphe 1, de la DSP2, pour gérer les risques opérationnels et de sécurité (au sens de «risques liés aux TIC et à la sécurité») liés aux services de paiement qu'ils fournissent. Les orientations incluent des exigences en matière de sécurité de l'information, y compris de cybersécurité, dans la mesure où les informations sont conservées sur des systèmes de TIC.

Champ d'application

7. Les présentes orientations s'appliquent à la gestion des risques liés aux TIC et à la sécurité au sein des établissements financiers (tels que définis au paragraphe 9). Aux fins des présentes orientations, le terme «risques liés aux TIC et à la sécurité» couvre les risques opérationnels et de sécurité visés à l'article 95 de la DSP2 concernant la prestation de services de paiement.

8. Pour les PSP (tels que définis au paragraphe 9), les présentes orientations s'appliquent à la prestation de services de paiement, conformément au champ d'application et au mandat visés à l'article 95 de la DSP2. Pour les établissements (tels que définis au paragraphe 9), les présentes orientations s'appliquent à toutes les activités qu'ils fournissent.

Destinataires

9. Les présentes orientations s'adressent aux établissements financiers, terme qui, aux fins des présentes orientations, couvre (1) les PSP au sens de l'article 4, paragraphe 11, de la DSP2 et (2) les établissements, terme couvrant les établissements de crédit et les entreprises d'investissement au sens de l'article 4, paragraphe 1, point 3), du règlement (UE) nº 575/2013. Les orientations s'appliquent également aux autorités compétentes au sens de l'article 4, paragraphe 1, point 40), du règlement (UE) nº 575/2013, y compris à la Banque centrale européenne en ce qui concerne les questions se rapportant aux tâches qui lui sont confiées en

vertu du règlement (UE) nº 1024/2013, et aux autorités compétentes au sens de la DSP2, comme indiqué à l'article 4, paragraphe 2, point i) du règlement (UE) nº 1093/2010.

Définitions

10. Sauf indication contraire, les termes utilisés et définis dans la directive 2013/36/UE (directive sur les exigences de fonds propres, ou CRD), dans le règlement (UE) nº 575/2013 (règlement sur les exigences de fonds propres, ou CRR) et dans la directive (UE) 2015/2366 (deuxième directive sur les services de paiement, ou DSP2) ont la même signification dans les présentes orientations. En outre, aux fins de ces orientations, les définitions suivantes s'appliquent:

Risque lié aux TIC et à la sécurité	Risque de perte découlant d'une violation de la confidentialité, d'une défaillance de l'intégrité des systèmes et des données, de l'inadéquation ou de l'indisponibilité des systèmes et des données, ou de l'impossibilité de modifier les technologies de l'information dans un délai et pour des coûts raisonnables, lorsque l'environnement ou les exigences «métiers» changent (agilité)[2]. Cela inclut les risques de sécurité découlant de processus internes insuffisants ou de défaillance de ces processus, ou bien d'événements externes, tels que des cyberattaques ou une sécurité physique insuffisante.
Organe de direction	(a) Pour les établissements de crédit et les entreprises d'investissement, ce terme a la même signification que la définition prévue à l'article 3, paragraphe 1, point 7), de la directive 2013/36/UE. (b) Pour les établissements de paiement et les établissements de monnaie électronique, ce terme signifie les dirigeants ou les personnes responsables de la gestion de l'établissement concerné et, le cas échéant, les personnes responsables de la gestion des activités de services de paiement de l'établissement concerné. (c) Pour les PSP visés à l'article premier, paragraphe 1, points c), e) et f), de la directive (UE) 2015/2366, ce terme a la signification qui lui est donnée 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 l'établissement financier, qui a ou aura probablement une incidence négative sur l'intégrité, la disponibilité, la confidentialité et/ou l'authenticité des services.
Direction générale	(a) Pour les établissements de crédit et les entreprises d'investissement, ce terme a la même signification que la

[2] Définition tirée des orientations de l'ABE sur les procédures et les méthodologies communes à appliquer dans le cadre du processus de contrôle et d'évaluation prudentiels du 19 décembre 2014 (EBA/GL/2014/13), modifiées par les orientations EBA/GL/2018/03.

	définition prévue à l'article 3, paragraphe 1, point 9), de la directive 2013/36/UE. (b) Pour les établissements de paiement et les établissements de monnaie électronique, ce terme désigne les personnes physiques qui exercent des fonctions exécutives dans l'établissement concerné, et qui sont responsables de la gestion quotidienne de l'établissement 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 à l'article premier, paragraphe 1, points c), e) et f), de la directive (UE) 2015/2366, ce terme a la signification qui lui est donnée par le droit de l'UE ou le droit national applicable.
Appétit pour le risque	Le niveau et les types agrégés de risque que les PSP et les établissements sont prêts à accepter dans le cadre de leur capacité à prendre des risques, conformément à leur modèle d'entreprise, afin d'atteindre leurs objectifs stratégiques.
Fonction d'audit	(a) Pour les établissements de crédit et les entreprises d'investissement, la fonction d'audit correspond à celle présentée à la section 22 des orientations de l'ABE sur la gouvernance interne (EBA/GL/2017/11). (b) Pour les PSP autres que les établissements de crédit, la fonction d'audit doit exercer ses activités de façon indépendante au sein du PSP ou en dehors de celui-ci, et peut être une fonction interne et/ou externe.
Projets de TIC	Tout projet, ou toute partie d'un projet, dans le cadre duquel les services et les systèmes de TIC sont modifiés, remplacés, supprimés ou mis en œuvre. Les projets de TIC peuvent faire partie de programmes plus larges de TIC ou de transformation des activités.
Tiers	Toute organisation ayant conclu un contrat ou une relation d'affaires avec une entité dans le but de fournir un produit ou un service[3].
Actifs informationnels	Ensemble d'informations, tangibles ou non, suffisamment importantes pour être protégées.
Actifs informatiques	Logiciels ou équipement informatique présents dans l'environnement de l'entreprise.
Systèmes de TIC[4]	TIC mises en place dans le cadre d'un mécanisme ou d'un réseau d'interconnexion qui soutient les opérations d'un établissement financier.
Services de TIC[5]	Services fournis par des systèmes de TIC à un ou plusieurs utilisateurs internes ou externes. Les services de TIC comprennent par exemple la saisie de données, le stockage de données, le traitement de données et les services de communication

[3] Définition tirée des «éléments fondamentaux pour la cybersécurité du secteur financier» établis par le G7.
[4] Définition tirée des orientations sur l'évaluation du risque lié aux TIC dans le cadre du processus de contrôle et d'évaluation prudentiels (SREP) (EBA/GL/ 2017/05).
[5] ibid.

d'informations, ainsi que les services de soutien au suivi, aux opérations et aux décisions.

Mise en œuvre

Date d'entrée en vigueur

11. Les présentes orientations s'appliquent à compter du 30 juin 2020.

Abrogation

12. Les orientations relatives aux mesures de sécurité pour les risques opérationnels et de sécurité (EBA/GL/2017/17) formulées en 2017 seront abrogées par les présentes orientations à la date d'entrée en vigueur de ces dernières.

Orientations sur les TIC et la gestion des risques de sécurité

1.1. Proportionnalité

1. Tous les établissements financiers devraient respecter les dispositions stipulées dans les présentes orientations d'une façon qui, d'une part, soit proportionnée à la taille et à l'organisation interne des établissements financiers, à la nature, la portée et la complexité des produits et services que ces établissements fournissent ou comptent fournir et au risque qu'ils présentent, et qui, d'autre part, tienne compte de ces facteurs.

1.2. Gouvernance et stratégie

1.2.1. Gouvernance

2. L'organe de direction devrait veiller à ce que les établissements financiers disposent d'un cadre de gouvernance interne et de contrôle interne adéquat compte tenu de leurs risques liés aux TIC et à la sécurité. L'organe de direction devrait définir des rôles et responsabilités clairs pour les fonctions de TIC, la gestion des risques liés à la sécurité de l'information et la continuité des activités, y compris ceux de l'organe de direction et de ses comités.

3. L'organe de direction devrait veiller à ce que les établissements financiers disposent d'un nombre d'employés suffisant, aux compétences adéquates, pour répondre à leurs besoins opérationnels en termes de TIC et soutenir leurs processus de gestion des risques liés aux TIC et à la sécurité, en continu, ainsi que pour assurer la mise en œuvre de leur stratégie en matière de TIC. L'organe de direction devrait veiller à ce que le budget alloué soit suffisant pour

répondre aux besoins susmentionnés. En outre, les établissements financiers devraient veiller à ce que tous les membres du personnel, y compris les titulaires de postes clés, reçoivent une formation appropriée consacrée aux risques liés aux TIC et à la sécurité, portant notamment sur la sécurité de l'information, une fois par an ou plus fréquemment si nécessaire (voir également la section 1.4.7).

4. L'organe de direction a la responsabilité globale de la définition, de l'approbation et de la supervision de la mise en œuvre de la stratégie des établissements financiers en matière de TIC, dans le cadre de leur stratégie générale, ainsi que de la mise en œuvre d'un cadre de gestion des risques efficace pour les risques liés aux TIC et à la sécurité.

1.2.2. Stratégie

5. La stratégie en matière de TIC devrait être alignée sur la stratégie générale des établissements financiers, et devrait définir:

   a) la façon dont les TIC des établissements financiers devraient évoluer pour soutenir la stratégie et y participer, s'agissant notamment de l'évolution de la structure organisationnelle, des changements apportés au système de TIC et des principales dépendances à l'égard de tiers;
   b) la stratégie et l'évolution de l'architecture des TIC qu'il est prévu de mettre en œuvre, y compris pour les dépendances à l'égard de tiers;
   c) des objectifs clairs en matière de sécurité de l'information, donnant la priorité aux systèmes de TIC ainsi qu'aux services, au personnel et processus des TIC.

6. Les établissements financiers devraient définir des plans d'action prévoyant les mesures à prendre pour réaliser les objectifs de la stratégie en matière de TIC. Ces plans devraient être communiqués à tous les membres du personnel concernés (y compris aux contractants et aux fournisseurs tiers, le cas échéant et si cela est pertinent). Les plans d'action devraient être réexaminés périodiquement afin de veiller à ce qu'ils restent pertinents et appropriés. Les établissements financiers devraient également mettre en œuvre des processus permettant de surveiller et de mesurer l'efficacité de la mise en œuvre de leur stratégie en matière de TIC.

1.2.3. Recours à des fournisseurs tiers

7. Sans préjudice des orientations de l'ABE sur les accords d'externalisation (EBA/GL/2019/02) et de l'article 19 de la DSP2, les établissements financiers devraient assurer l'efficacité des mesures de maîtrise des risques définies dans leur cadre de gestion des risques, y compris des mesures définies dans les présentes orientations, lorsque les fonctions opérationnelles des services de paiement et/ou les services et systèmes de TIC de toute activité sont externalisés, y compris vers des entités du même groupe, ou lors du recours à des tiers.

8. Afin d'assurer la continuité des services et systèmes de TIC, les établissements financiers devraient veiller à ce que les contrats et les accords de niveau de service (dans des conditions normales ou en cas de perturbation des services – voir également la section 1.7.2) conclus avec des fournisseurs (prestataires de services d'externalisation, entités du groupe ou fournisseurs tiers) incluent les éléments suivants:

a) objectifs et mesures appropriés et proportionnés en matière de sécurité de l'information, y compris des exigences telles qu'un niveau de cybersécurité minimal; spécifications relatives au cycle de vie des données de l'établissement financier concerné; exigences relatives aux processus de chiffrement des données, à la sécurité des réseaux et aux processus de surveillance de la sécurité, ainsi qu'à l'emplacement des centres de données;
b) procédures de traitement des incidents opérationnels et liés à la sécurité, notamment pour la communication et la remontée des informations.

9. Les établissements financiers devraient surveiller le niveau de conformité de ces fournisseurs avec les objectifs, les mesures et les niveaux de performance définis par l'établissement financier concerné en matière de sécurité, et s'assurer de ce niveau de conformité.

1.3. Cadre de gestion des risques liés aux TIC et à la sécurité

1.3.1. Organisation et objectifs

10. Les établissements financiers devraient identifier et gérer leurs risques liés aux TIC et à la sécurité. La ou les fonction(s) de TIC chargée(s) des systèmes de TIC, des processus et des opérations liées à la sécurité devraient disposer des processus et des contrôles appropriés pour veiller, d'une part, à ce que tous les risques soient identifiés, analysés, mesurés, surveillés, gérés, communiqués et maintenus dans les limites de l'appétit pour le risque de l'établissement financier concerné et, d'autre part, à ce que les projets et systèmes qu'elle(s) fournit/fournissent et les activités qu'elle(s) exécute(nt) respectent les exigences externes et internes.

11. Les établissements financiers devraient attribuer la responsabilité de la gestion et de la supervision des risques liés aux TIC et à la sécurité à une fonction de contrôle respectant les exigences de la section 19 des orientations de l'ABE sur la gouvernance interne (EBA/GL/2017/11). Les établissements financiers devraient assurer l'indépendance et l'objectivité de cette fonction de contrôle en la séparant de manière appropriée des processus liés aux opérations de TIC. Cette fonction de contrôle devrait rendre compte directement à l'organe de direction, et devrait être chargée de surveiller et de contrôler le respect du cadre de gestion des risques liés aux TIC et à la sécurité. Elle devrait veiller à ce que les risques liés aux TIC et à la sécurité soient identifiés, mesurés, évalués, gérés, surveillés et communiqués. Les établissements financiers devraient veiller à ce que cette fonction de contrôle ne soit responsable d'aucun audit interne.

    La fonction d'audit interne devrait, selon une approche fondée sur les risques, pouvoir examiner de façon indépendante toutes les activités et unités d'un établissement financier liées aux TIC et à la sécurité, et garantir en toute objectivité qu'elles respectent les politiques et procédures de cet établissement, ainsi que les exigences externes, en respectant les exigences de la section 22 des orientations de l'ABE sur la gouvernance interne (EBA/GL/2017/11).

12. Les établissements financiers devraient définir et attribuer les principaux rôles et responsabilités, ainsi que les lignes hiérarchiques pertinentes, pour assurer l'efficacité du cadre de gestion des risques liés aux TIC et à la sécurité. Ce cadre devrait être entièrement intégré aux processus de gestion des risques généraux des établissements financiers, et aligné sur ces processus.

13. Le cadre de gestion des risques liés aux TIC et à la sécurité devrait inclure des processus visant à:

    a) déterminer l'appétit pour les risques liés aux TIC et à la sécurité, conformément à l'appétit pour le risque de l'établissement financier;
    b) identifier et évaluer les risques liés aux TIC et à la sécurité auxquels un établissement financier est exposé;
    c) définir des mesures de maîtrise, y compris des contrôles, permettant de maîtriser les risques liés aux TIC et à la sécurité;
    d) surveiller l'efficacité de ces mesures et le nombre d'incidents communiqués, y compris, s'agissant des PSP, des incidents notifiés conformément à l'article 96 de la DSP2 concernant les activités liées aux TIC, et prendre les dispositions nécessaires pour corriger ces mesures si besoin;
    e) communiquer les risques liés aux TIC et à la sécurité et les contrôles afférents à l'organe de direction;
    f) identifier et évaluer les éventuels risques liés aux TIC et à la sécurité découlant de toute modification majeure du système de TIC ou des services, processus et procédures relatifs aux TIC et/ou survenus après tout incident important lié aux opérations ou à la sécurité.

14. Les établissements financiers devraient veiller à ce que le cadre de gestion des risques liés aux TIC et à la sécurité soit documenté et amélioré en continu en fonction des enseignements tirés de sa mise en œuvre et de sa surveillance. Le cadre de gestion des risques liés aux TIC et à la sécurité devrait être approuvé et réexaminé, au moins une fois par an, par l'organe de direction.

1.3.2. Identification des fonctions, processus et actifs informationnels

15. Les établissements financiers devraient identifier, établir, tenir à jour une cartographie de leurs fonctions et métiers, et de leurs processus «supports», afin de déterminer l'importance de chacun d'entre eux et leur interdépendance avec les risques liés aux TIC et à la sécurité.

16. Les établissements financiers devraient également identifier, établir, tenir à jour une cartographie des actifs informationnels soutenant leurs fonctions «métiers» et les processus «supports» afférents, comme les systèmes de TIC, le personnel, les prestataires, les tiers et les dépendances à l'égard d'autres systèmes et processus internes ou externes, afin de pouvoir, au minimum, gérer les actifs informationnels soutenant leurs fonctions et processus «métiers» revêtant une importance critique.

1.3.3. Classification et évaluation des risques

17. Les établissements financiers devraient classifier les fonctions «métiers», processus «supports» et actifs informationnels identifiés, mentionnés aux paragraphes 15 et 16, en fonction de leur niveau de criticité.

18. Pour définir le niveau de criticité de ces fonctions «métiers», processus «supports» et actifs informationnels identifiés, les établissements financiers devraient tenir compte, au minimum, des exigences de confidentialité, d'intégrité et de disponibilité. Les actifs informationnels devraient faire l'objet d'obligations de rendre compte et de responsabilités clairement attribuées.

19. Les établissements financiers devraient examiner l'adéquation du classification des actifs informationnels et des documents pertinents lors de toute évaluation des risques.

20. Les établissements financiers devraient identifier les risques liés aux TIC et à la sécurité ayant une incidence sur les fonctions «métiers», les processus «supports» et les actifs informationnels identifiés et classifiés, en fonction de leur niveau de criticité. L'évaluation des risques devrait être effectuée et documentée une fois par an, ou plus souvent si cela est nécessaire. Les risques devraient également être évalués lors de toute modification majeure de l'infrastructure, des processus ou des procédures ayant une incidence sur les fonctions «métiers», les processus «supports» ou les actifs informationnels, après quoi l'évaluation des risques applicable aux établissements financiers devrait être mise à jour.

21. Les établissements financiers devraient veiller à surveiller en continu les menaces et vulnérabilités relatives à leurs processus «métiers», fonctions «supports» et actifs informationnels, et devraient régulièrement réexaminer les scénarios de risque ayant une incidence en la matière.

1.3.4. Maîtrise des risques

22. Suite à l'évaluation des risques, les établissements financiers devraient déterminer les mesures à prendre pour ramener les risques liés aux TIC et à la sécurité à des niveaux acceptables et déterminer s'il est nécessaire de modifier les processus «métiers», mesures de contrôle, systèmes de TIC et services de TIC existants. Un établissement financier devrait évaluer le temps requis pour mettre ces modifications en œuvre et pour prendre les mesures compensatoires appropriées pour maîtriser les risques liés aux TIC et à la sécurité, afin de rester dans les limites de l'appétit pour les risques liés aux TIC et à la sécurité de l'établissement financier concerné.

23. Les établissements financiers devraient définir et mettre en œuvre des mesures permettant de maîtriser les risques liés aux TIC et à la sécurité qui ont été identifiés et de protéger les actifs informationnels en fonction de leur classification.

1.3.5. Rapport à l'organe de direction

24. Les établissements financiers devraient communiquer les résultats de l'évaluation des risques à l'organe de direction, clairement et en temps utile. Ce rapport est sans préjudice de l'obligation des PSP de fournir aux autorités compétentes une évaluation des risques à jour et exhaustive, comme stipulé à l'article 95, paragraphe 2, de la directive (UE) 2015/2366.

1.3.6. Audit

25. La gouvernance, les systèmes et les processus d'un établissement financier dans le cadre de ses risques liés aux TIC et à la sécurité devraient être audités, de façon périodique, par des auditeurs ayant des connaissances, des compétences et une expertise suffisantes concernant ces risques et les paiements (pour les PSP), afin de fournir à l'organe de direction, en toute indépendance, l'assurance qu'ils sont efficaces. Les auditeurs devraient exercer leurs activités de façon indépendante au sein de l'établissement financier ou être indépendants de l'établissement financier. La fréquence et les priorités de ces audits devraient être proportionnées aux risques liés aux TIC et à la sécurité.

26. L'organe de direction d'un établissement financier devrait approuver le plan d'audit, y compris tout audit des TIC et toute modification majeure y afférente. Le plan d'audit et sa mise en œuvre, y compris la fréquence des audits, devraient refléter les risques liés aux TIC et à la sécurité inhérents à l'établissement financier, être proportionnés à ces risques et être mis à jour régulièrement.

27. Un processus de suivi formel, comprenant des dispositions pour la vérification et la résolution, en temps utile, des conclusions déterminantes de l'audit des TIC, devrait être établi.

1.4. Sécurité de l'information

1.4.1. Politique relative à la sécurité de l'information

28. Les établissements financiers devraient élaborer et documenter une politique relative à la sécurité de l'information qui devrait définir des règles et principes de haut niveau visant à protéger la confidentialité, l'intégrité et la disponibilité des données et informations des établissements financiers et de leurs clients. Pour les PSP, cette politique est identifiée dans le document relatif à la politique de sécurité devant être adopté conformément à l'article 5, paragraphe 1, point j), de la directive (UE) 2015/2366. La politique relative à la sécurité de l'information devrait correspondre aux objectifs de l'établissement financier en matière de sécurité de l'information et devrait être fondée sur les résultats pertinents du processus d'évaluation des risques. Cette politique devrait être approuvée par l'organe de direction.

29. Cette politique devrait inclure une description des principaux rôles et responsabilités en matière de gestion de la sécurité de l'information, définir les exigences applicables au personnel et aux prestataires, ainsi qu'aux processus et aux technologies, en matière de sécurité de l'information, en reconnaissant que le personnel et les prestataires, à tous les niveaux, sont responsables d'assurer la sécurité de l'information au sein des établissements

financiers. La politique devrait veiller à la confidentialité, l'intégrité et la disponibilité des actifs logiques et physiques ayant une importance critique, des ressources et des données sensibles d'un établissement financier, qu'ils soient au repos, en transit ou en cours d'utilisation. La politique relative à la sécurité de l'information devrait être communiquée à tous les membres du personnel et à tous les prestataires de l'établissement financier.

30. En fonction de la politique relative à la sécurité de l'information, les établissements financiers devraient établir et mettre en œuvre des mesures de sécurité visant à maîtriser les risques liés aux TIC et à la sécurité auxquels ils sont exposés. Ces mesures devraient inclure les éléments suivants:

    a) organisation et gouvernance, conformément aux paragraphes 10 et 11;
    b) sécurité logique (section 1.4.2);
    c) sécurité physique (section 1.4.3);
    d) sécurité des opérations de TIC (section 1.4.4);
    e) surveillance de la sécurité (section 1.4.5);
    f) examens, évaluations et tests de la sécurité de l'information (section 1.4.6);
    g) formation et sensibilisation en matière de sécurité de l'information (section 1.4.7).

1.4.2. Sécurité logique

31. Les établissements financiers devraient définir, documenter et mettre en œuvre des procédures de contrôle d'accès logique (gestion des identités et des accès). Ces procédures devraient être mises en œuvre, appliquées, surveillées et réexaminées à intervalles réguliers. Ces procédures devraient également inclure des contrôles permettant de surveiller les anomalies. Ces procédures devraient, au minimum, mettre les éléments suivants en œuvre (le terme «utilisateur» inclut les utilisateurs techniques):

    (a) **Principes du besoin d'en connaître, du moindre privilège et de séparation des fonctions:** les établissements financiers devraient gérer les droits d'accès aux actifs informationnels et à leurs systèmes les soutenant selon le principe du «besoin d'en connaître», y compris pour l'accès à distance. Les utilisateurs devraient recevoir les droits d'accès minimum strictement requis pour exécuter leurs fonctions (principe du «moindre privilège»), c'est-à-dire pour prévenir tout accès non justifié à un large ensemble de données ou toute allocation de droits d'accès combinés pouvant servir à contourner les contrôles (principe de «séparation des fonctions»).
    (b) **Imputabilité des utilisateurs:** les établissements financiers devraient limiter l'utilisation de comptes utilisateurs génériques et partagés, dans la mesure du possible, et veiller à ce que les actions effectuées dans les systèmes de TIC puissent être attribuées aux utilisateurs concernés.
    (c) **Droits d'accès privilégiés:** les établissements financiers devraient mettre en œuvre des contrôles solides sur l'accès privilégié aux systèmes, en limitant strictement et en surveillant étroitement les comptes assortis de droits supérieurs d'accès aux systèmes (par exemple les comptes administrateur). Afin de garantir une communication sécurisée et de réduire les risques, l'accès administratif à distance à des systèmes de TIC

ayant une importance critique devrait être accordé uniquement selon le principe du «besoin d'en connaître» et lorsque des mesures d'authentification forte sont appliquées.

(d) **Enregistrement des activités des utilisateurs:** au minimum, toutes les activités des utilisateurs privilégiés devraient être enregistrées et surveillées. Les registres d'accès devraient être sécurisés afin de prévenir toute modification ou suppression non autorisée, et conservés durant une période proportionnée au niveau de criticité des fonctions «métiers», processus de soutien et actifs informationnels identifiés, conformément à la section 1.3.3, sans préjudice des exigences de conservation définies dans le droit de l'UE ou le droit national. Un établissement financier devrait utiliser ces informations pour faciliter l'identification et l'analyse d'activités anormales ayant été détectées dans la prestation de services.

(e) **Gestion des accès:** les droits d'accès devraient être accordés, retirés ou modifiés en temps utile, conformément à des circuits d'approbation prédéfinis incluant le propriétaire fonctionnel des informations auxquelles l'utilisateur accède (propriétaire des actifs informationnels). En cas de résiliation du contrat de travail, les droits d'accès devraient être rapidement retirés.

(f) **Renouvellement des accès:** les droits d'accès devraient périodiquement être réexaminés afin de veiller à ce que les utilisateurs ne possèdent pas de privilèges excessifs et à ce que les droits d'accès soient retirés dès lors qu'ils ne sont plus requis.

(g) **Méthodes d'authentification:** les établissements financiers devraient appliquer des méthodes d'authentification forte pour assurer, de façon appropriée et efficace, que les politiques et procédures de contrôle d'accès sont respectées. Les méthodes d'authentification devraient être proportionnées au niveau de criticité des systèmes de TIC, des informations ou des processus auxquels l'utilisateur accède. Au minimum, cela devrait inclure des mots de passe complexes ou des méthodes d'authentification forte (comme l'authentification à deux facteurs), en fonction des risques pertinents.

32. L'accès électronique sur demande aux données et aux systèmes de TIC devrait se limiter au minimum requis pour fournir le service concerné.

1.4.3. Sécurité physique

33. Les mesures de sécurité physique des établissements financiers devraient être définies, documentées et mises en œuvre afin de protéger les locaux, les centres de données et les zones sensibles contre tout accès non autorisé et contre les dangers environnementaux.

34. L'accès physique aux systèmes de TIC devrait être accordé uniquement aux personnes autorisées. L'autorisation devrait être accordée en fonction des tâches et responsabilités de la personne concernée, en se limitant à des personnes correctement formées et surveillées. L'accès physique devrait être régulièrement réexaminé afin de veiller à ce que les droits d'accès qui ne sont plus nécessaires soient rapidement révoqués.

35. Des mesures adéquates de protection contre les dangers environnementaux devraient être proportionnées à l'importance des bâtiments et au niveau de criticité des opérations ou des systèmes de TIC situés dans ces bâtiments.

1.4.4. Sécurité des opérations de TIC

36. Les établissements financiers devraient mettre en œuvre des procédures visant à prévenir les problèmes de sécurité dans les systèmes et les services de TIC, et devraient minimiser leur incidence sur la prestation des services de TIC. Ces procédures devraient inclure les mesures suivantes:

    a) identification des vulnérabilités potentielles, qui devraient être évaluées et résolues en s'assurant que les logiciels et micrologiciels sont à jour, y compris les logiciels fournis par les établissements financiers à leurs utilisateurs internes et externes, en installant les correctifs de sécurité essentiels ou en mettant des contrôles compensatoires en œuvre;
    b) implémentation de configurations de référence sécurisées pour tous les équipements réseaux;
    c) segmentation réseau, systèmes de prévention des pertes de données et chiffrement du trafic du réseau (conformément à la classification des données);
    d) protection des terminaux, y compris des serveurs, des postes de travail et des appareils mobiles – les établissements financiers devraient déterminer si les terminaux sont conformes aux normes de sécurité qu'ils ont définies avant de leur permettre d'accéder au réseau d'entreprise;
    e) mise en place de mécanismes permettant de vérifier l'intégrité des logiciels, des micrologiciels et des données;
    f) chiffrement des données au repos ou en transit (conformément à la classification des données).

37. En outre, les établissements financiers devraient déterminer, en continu, si les changements intervenant dans l'environnement opérationnel existant influencent les mesures de sécurité existantes ou nécessitent d'adopter des mesures supplémentaires afin de maîtriser les risques associés de façon appropriée. Ces changements devraient faire partie du processus de gestion des changements des établissements financiers, qui devraient veiller à ce que ces changements soient dûment planifiés, testés, documentés, autorisés et déployés.

1.4.5. Surveillance de la sécurité

38. Les établissements financiers devraient établir et mettre en œuvre des politiques et procédures permettant, d'une part, de détecter les activités anormales susceptibles d'avoir une incidence sur la sécurité de l'information au sein des établissements financiers et, d'autre part, de répondre de façon appropriée à ces événements. Dans le cadre de cette surveillance continue, les établissements financiers devraient mettre en œuvre des capacités adaptées et efficaces pour détecter et communiquer les intrusions physiques ou logiques ainsi que les violations de

confidentialité, d'intégrité et de disponibilité des actifs informationnels. La surveillance continue et les processus de détection devraient couvrir:

a) les facteurs internes et externes pertinents, y compris les fonctions administratives «métiers» et liées aux TIC;
b) les opérations visant à détecter toute utilisation abusive des droits d'accès par des tiers ou autres entités, ou par des personnes internes à l'établissement;
c) les menaces internes et externes potentielles.

39. Les établissements financiers devraient établir et mettre en œuvre des processus et structures organisationnelles permettant d'identifier et de surveiller en continu les menaces pour la sécurité qui pourraient avoir une incidence importante sur leur capacité à fournir des services. Les établissements financiers devraient activement surveiller les évolutions technologiques afin de faire en sorte d'être au courant des risques de sécurité. Les établissements financiers devraient mettre en œuvre des mesures de détection, par exemple pour identifier de possibles fuites d'informations, codes malveillants et autres menaces pour la sécurité, ainsi que les vulnérabilités des logiciels et matériels informatiques qui sont connues du public, et devraient s'informer des nouvelles mises à jour de sécurité correspondantes.

40. Le processus de surveillance de la sécurité devrait également permettre à l'établissement financier de comprendre la nature des incidents opérationnels ou de sécurité, d'identifier les tendances et d'appuyer les enquêtes diligentées.

1.4.6. Examens, évaluations et tests en matière de sécurité de l'information

41. Les établissements financiers devraient procéder à divers examens, évaluations et tests en matière de sécurité de l'information, afin d'assurer une identification efficace des vulnérabilités au sein de leurs systèmes et services de TIC. Par exemple, les établissements financiers peuvent mener des analyses des écarts par rapport aux normes de sécurité de l'information, des examens de conformité, des audits internes et externes sur les systèmes d'information ou des examens de la sécurité physique. En outre, l'établissement concerné devrait envisager de bonnes pratiques telles que l'examen des codes sources, l'évaluation des vulnérabilités, des tests d'intrusion et des simulations de cyber-attaques avec équipe adverse (dite «rouge»).

42. Les établissements financiers devraient établir et mettre en œuvre un cadre de test de la sécurité de l'information validant la solidité et l'efficacité de leurs mesures de sécurité de l'information et veiller à ce que ce cadre tienne compte des menaces et des vulnérabilités identifiées grâce à la surveillance des menaces et au processus d'évaluation des risques liés aux TIC et à la sécurité.

43. Le cadre de test de la sécurité de l'information devrait garantir que les tests:

a) sont menés par des testeurs indépendants qui possèdent des connaissances, des compétences et une expertise suffisantes en matière de test des mesures de sécurité de l'information et qui ne participent pas à l'élaboration des mesures de sécurité de l'information;

b) incluent des analyses de vulnérabilité et des tests d'intrusion (y compris des tests d'intrusion fondés sur les menaces si cela est nécessaire et approprié) proportionnés au niveau de risque identifié pour les processus et systèmes de l'entreprise.

44. Les établissements financiers devraient tester les mesures de sécurité de façon continue et récurrente. S'agissant de tous les systèmes de TIC ayant une importance critique (paragraphe 17), ces tests devraient être effectués au moins une fois par an. Pour les PSP, ils font partie de l'évaluation exhaustive des risques de sécurité liés aux services de paiement qu'ils fournissent, conformément à l'article 95, paragraphe 2, de la DSP2. Les systèmes n'ayant pas une importance critique devraient être régulièrement testés selon une méthode fondée sur les risques, et ce au moins tous les trois ans.

45. Les établissements financiers devraient veiller à ce que les mesures de sécurité soient testées en cas de modification de l'infrastructure, des processus ou des procédures et si des changements sont apportés en raison d'incidents opérationnels ou de sécurité majeurs ou de la mise en production d'applications critiques nouvelles ou fortement modifiées exposées à internet.

46. Les établissements financiers devraient surveiller et évaluer les résultats des tests de sécurité et mettre à jour leurs mesures de sécurité en conséquence, sans retard injustifié dans le cas des systèmes de TIC ayant une importance critique.

47. Pour les PSP, ce cadre de test devrait également englober les mesures de sécurité pertinentes pour (1) les terminaux de paiement et dispositifs utilisés aux fins de la prestation des services de paiement, (2) les terminaux de paiement et dispositifs utilisés aux fins de l'authentification des utilisateurs de services de paiement (USP) et (3) les dispositifs et logiciels fournis par le PSP à l'USP pour générer/recevoir un code d'authentification.

48. Sur la base des menaces identifiées pour la sécurité et des changements apportés, des tests qui incluent des scénarios d'attaques potentielles pertinentes et connues devraient être réalisés.

1.4.7. Formation et sensibilisation en matière de sécurité de l'information

49. Les établissements financiers devraient établir un programme de formation, incluant des programmes périodiques de sensibilisation à la sécurité, à l'attention de tous leurs employés et prestataires, afin de veiller à ce qu'ils soient formés, d'une part, à l'exécution de leurs tâches et responsabilités conformément aux politiques et procédures de sécurité pertinentes afin de réduire l'erreur humaine, le vol, la fraude, les abus ou les pertes et, d'autre part, aux moyens de résolution des risques liés à la sécurité de l'information. Les établissements financiers devraient veiller à ce que tous les membres du personnel et tous les prestataires reçoivent ce programme de formation au moins une fois par an.

1.5. Gestion des opérations de TIC

50. Les établissements financiers devraient gérer leurs opérations liées aux TIC en fonction de processus et procédures documentés et mis en œuvre [qui, pour les PSP, incluent le document relatif à la politique de sécurité visé à l'article 5, paragraphe 1, point j), de la DSP2] qui ont été

approuvés par l'organe de direction. Ensemble, ces documents devraient définir la façon dont les établissements financiers exploitent, surveillent et contrôlent leurs services et systèmes de TIC, y compris la documentation des opérations de TIC revêtant une importance critique, et devraient permettre aux établissements financiers de tenir à jour un inventaire des actifs informatiques.

51. Les établissements financiers devraient veiller à ce que la performance de leurs opérations de TIC soit alignée sur leurs exigences «métiers». Les établissements financiers devraient maintenir et améliorer, dans la mesure du possible, l'efficacité de leurs opérations de TIC. Ils devraient notamment, mais sans s'y limiter, envisager des façons de minimiser les potentielles erreurs découlant de l'exécution de tâches manuelles.

52. Les établissements financiers devraient mettre en œuvre des procédures d'enregistrement et de surveillance des opérations de TIC ayant une importance critique afin de détecter, analyser et corriger les erreurs.

53. Les établissements financiers devraient tenir à jour l'inventaire de leurs actifs informatiques (y compris les systèmes de TIC, les équipements réseau, les bases de données, etc.). L'inventaire des actifs informatiques devrait contenir la configuration des actifs informatiques, ainsi que les liens et interdépendances entre eux, afin d'établir un processus de configuration et de gestion du changement approprié.

54. L'inventaire des actifs informatiques devrait être suffisamment détaillé pour permettre d'identifier rapidement un actif informatique, son emplacement, sa classification de sécurité et son propriétaire. Les interdépendances entre les actifs devraient être documentées afin de faciliter la mise en œuvre de la réponse à apporter aux incidents opérationnels et de sécurité, y compris aux cyberattaques.

55. Les établissements financiers devraient surveiller et gérer le cycle de vie des actifs informatiques, afin de s'assurer qu'ils répondent toujours aux exigences «métiers» et aux besoins en matière de gestion des risques et apportent toujours le soutien nécessaire en la matière. Les établissements financiers devraient surveiller leurs actifs informatiques afin de vérifier s'ils sont pris en charge par leurs fournisseurs et développeurs externes ou internes et si tous les correctifs et mises à jour pertinents sont appliqués conformément aux processus documentés. Les risques découlant de actifs informatiques obsolètes ou non pris en charge devraient être évalués et maîtrisés.

56. Les établissements financiers devraient mettre en œuvre des processus de planification et de surveillance des performances et des capacités permettant de prévenir, détecter et résoudre tout problème de performance important dans les systèmes de TIC, ainsi que toute pénurie de capacité, dans un délai convenable.

57. Les établissements financiers devraient définir et mettre en œuvre des procédures de sauvegarde et de restauration des données et des systèmes de TIC visant à assurer qu'ils peuvent être récupérés en cas de besoins. Le périmètre et la fréquence des sauvegardes devraient être définis conformément aux exigences de reprise des activités et au niveau de criticité des données et systèmes de TIC, et analysés en fonction de l'évaluation des risques

effectuée. Les procédures de sauvegarde et de restauration devraient être testées à intervalles réguliers.

58. Les établissements financiers devraient veiller à ce que les sauvegardes des données et systèmes de TIC soient stockées de façon sécurisée à un endroit suffisamment éloigné du site principal pour ne pas être exposées aux mêmes risques.

3.5.1 Gestion des problèmes et incidents liés aux TIC

59. Les établissements financiers devraient établir et mettre en œuvre un processus de gestion des problèmes et incidents afin, d'une part, de surveiller et consigner les incidents opérationnels et de sécurité liés aux TIC et, d'autre part, de poursuivre ou rétablir les fonctions et processus «métiers» de ces institutions ayant une importance critique, en temps utile, après une perturbation. Les établissements financiers devraient déterminer les critères et les seuils appropriés pour classifier un événement comme incident opérationnel ou incident de sécurité, selon la définition prévue à la section «Définitions» des présentes orientations, ainsi que les indicateurs d'alerte précoce devant servir d'alerte afin de permettre la détection précoce de ces incidents. Ces critères et seuils, pour les PSP, sont sans préjudice de la classification des incidents majeurs visée à l'article 96 de la DSP2 et des orientations sur la notification des incidents majeurs en vertu de la DSP2 (EBA/GL/2017/10).

60. Afin de minimiser l'impact des événements indésirables et de permettre une reprise rapide, les établissements financiers devraient établir des processus et des structures organisationnelles appropriés pour assurer une surveillance, un traitement et un suivi cohérents et intégrés des incidents opérationnels et de sécurité et pour veiller à ce que les causes originelles soient identifiées et éliminées afin d'empêcher que ces incidents ne se répètent. Le processus de gestion des incidents et des problèmes devrait établir:

    a) les procédures visant à identifier, suivre, consigner, catégoriser et classer les incidents par ordre de priorité, en fonction de leur criticité pour les métiers;
    b) les rôles et responsabilités inhérents à différents scénarios d'incidents (par exemple les erreurs, les dysfonctionnements et les cyberattaques);
    c) les procédures de gestion des problèmes permettant d'identifier, d'analyser et de résoudre la cause originelle d'un ou de plusieurs incidents – l'établissement financier devrait analyser les incidents opérationnels ou de sécurité susceptibles de l'affecter qui ont été identifiés ou qui sont survenus en son sein et/ou à l'extérieur, et devrait tenir compte des principaux enseignements tirés de ces analyses et mettre ses mesures de sécurité à jour en conséquence;
    d) des plans de communication interne efficaces, y compris pour la notification des incidents et les procédures d'escalade de l'information – couvrant également les plaintes des clients relevant de la sécurité – afin de s'assurer que:
        i) les incidents pouvant avoir une incidence négative importante sur les systèmes et services de TIC ayant une importance critique sont communiqués à la direction générale de la fonction TIC et des lignes d'activités;

ii) l'organe de direction est informé des éventuels incidents importants de façon ponctuelle et, au minimum, est informé de l'incidence des incidents, de la réponse qui leur est apportée et des contrôles supplémentaires à définir en conséquence.

e) les procédures de réponse aux incidents visant à atténuer l'incidence des incidents et à faire en sorte que le service devienne opérationnel et sécurisé dès que possible;

f) des plans de communication externe spécifiques pour les fonctions «métiers» et les processus revêtant une importance critique, afin de:

i) collaborer avec les parties prenantes concernées pour répondre en toute efficacité et rétablir les activités suite à l'incident;

ii) en temps utile, fournir des informations aux parties extérieures (par exemple des clients, d'autres participants au marché et l'autorité de supervision), le cas échéant et conformément à la réglementation applicable.

1.6. Gestion des projets de TIC et du changement

1.6.1. Gestion des projets de TIC

61. Un établissement financier devrait mettre en œuvre un programme et/ou un processus de gouvernance de projet définissant les rôles, responsabilités et obligations de rendre compte visant à soutenir la mise en œuvre de la stratégie en matière de TIC.

62. Un établissement financier devrait surveiller les risques liés à son portefeuille de projets de TIC (gestion des programmes) de façon appropriée et les maîtriser, en tenant également compte du fait que ces risques peuvent découler des interdépendances entre différents projets et des dépendances de plusieurs projets à l'égard des mêmes ressources et/ou expertises.

63. Un établissement financier devrait établir et mettre en œuvre une politique de gestion des projets de TIC incluant au minimum:

a) les objectifs du projet;
b) les rôles et responsabilités;
c) une évaluation des risques liés au projet;
d) le plan, le calendrier et les étapes du projet;
e) les principaux jalons;
f) les exigences en matière de gestion du changement.

64. La politique de gestion des projets de TIC devrait veiller à ce que les exigences en matière de sécurité de l'information soient analysées et approuvées par une fonction indépendante de la fonction de développement.

65. Un établissement financier devrait veiller à ce que les domaines affectés par un projet de TIC soient représentées au sein de l'équipe chargée du projet et à ce que cette équipe possède les connaissances requises pour assurer une implémentation sécurisée et réussie des projets.

66. La création et l'avancée des projets de TIC et des risques associés devraient être communiqués à l'organe de direction, à titre individuel ou global, en fonction de l'importance et de la taille des projets de TIC, à intervalles réguliers ou de façon ponctuelle, si nécessaire. Les établissements financiers devraient inclure les risques liés aux projets dans leur cadre de gestion des risques.

1.6.2. Acquisition et développement de systèmes de TIC

67. Les établissements financiers devraient développer et mettre en œuvre un processus régissant l'acquisition, le développement et l'entretien de systèmes de TIC. Ce processus devrait être conçu selon une approche fondée sur les risques.

68. Un établissement financier devrait veiller, avant d'acquérir ou de développer des systèmes de TIC, à ce que les exigences fonctionnelles et non fonctionnelles (y compris les exigences en matière de sécurité de l'information) soient clairement définies et approuvées par la direction de la ligne d'activité concernée.

69. Un établissement financier devrait veiller à ce que des mesures soient prises pour maîtriser le risque de modification non intentionnelle ou de manipulation intentionnelle des systèmes de TIC durant leur développement et leur implémentation dans l'environnement de production.

70. Les établissements financiers devraient mettre une méthodologie en place pour le test et l'approbation des systèmes de TIC avant leur première utilisation. Cette méthodologie devrait tenir compte du caractère critique des actifs et des processus «métiers». Les tests devraient veiller à ce que les nouveaux systèmes de TIC fonctionnent comme prévu. Ils devraient également s'effectuer dans des environnements de tests qui reflètent de manière adéquate l'environnement de production.

71. Les établissements financiers devraient tester les systèmes de TIC, les services de TIC et les mesures de sécurité de l'information afin d'identifier les faiblesses, violations et incidents potentiels en matière de sécurité.

72. Un établissement financier devrait mettre en œuvre des environnements de TIC distincts afin d'assurer une séparation des fonctions appropriée et d'atténuer l'incidence de toute modification non vérifiée sur les systèmes de production. Plus précisément, un établissement financier devrait faire en sorte que les environnements de production soient séparés du développement, du test et des autres environnements ne relevant pas de la production. Un établissement financier devrait assurer l'intégrité et la confidentialité des données de production dans les environnements autres que l'environnement de production. L'accès aux données de production est limité aux utilisateurs autorisés.

73. Les établissements financiers devraient mettre en œuvre des mesures visant à protéger l'intégrité des codes source des systèmes de TIC développés en interne. Ils devraient également documenter le développement, l'implémentation, le fonctionnement et/ou la configuration des systèmes de TIC, de façon exhaustive, afin de réduire toute dépendance inutile à l'égard d'experts en la matière. La documentation relative au système de TIC devrait inclure au

minimum, le cas échéant, la documentation «utilisateur», la documentation technique relative au système et les procédures opérationnelles.

74. Les processus d'acquisition et de développement de systèmes de TIC d'un établissement financier devraient également s'appliquer aux systèmes de TIC développés ou gérés par les utilisateurs finaux de la ligne d'activité en dehors de l'organisation responsable des TIC (par exemple, les applications informatiques de l'utilisateur final), en suivant une approche fondée sur les risques. L'établissement financier devrait tenir un registre des applications soutenant les fonctions ou processus «métiers» ayant une importance critique.

1.6.3. Gestion des changements liés aux TIC

75. Les établissements financiers devraient établir et mettre en œuvre un processus de gestion des changements liés aux TIC afin de garantir que toutes les modifications apportées aux systèmes de TIC sont enregistrées, testées, évaluées, approuvées, implémentées et vérifiées de façon contrôlée. Les établissements financiers devraient opérer les changements nécessaires en cas de situations d'urgence (c'est-à-dire les changements devant être introduits le plus rapidement possible) conformément à des procédures permettant de mettre en place des mesures de protection appropriées.

76. Les établissements financiers devraient déterminer si les changements intervenant dans l'environnement opérationnel existant influencent les mesures de sécurité existantes ou nécessitent d'adopter des mesures supplémentaires afin de maîtriser les risques concernés. Ces changements devraient respecter le processus officiel de gestion du changement des établissements financiers.

1.7. Gestion de la continuité des activités

77. Les établissements financiers devraient établir un processus adéquat pour la gestion de la continuité des activités afin de maximiser leur capacité à fournir des services en continu et à limiter les pertes en cas de perturbation grave de l'activité, conformément à l'article 85, paragraphe 2, de la directive 2013/36/UE et au titre VI des orientations de l'ABE sur la gouvernance interne (EBA/GL/2017/11).

1.7.1. Analyse des incidences sur les activités

78. Dans le cadre de leur processus adéquat pour la gestion de la continuité des activités, les établissements financiers devraient mener une analyse d'incidence sur les activités («AIA») en analysant leur exposition à toute perturbation grave de l'activité et en évaluant leur incidence potentielle (y compris sur la confidentialité, l'intégrité et la disponibilité), en termes quantitatifs comme qualitatifs, à l'aide de données internes et/ou externes (par exemple les données de fournisseurs tiers concernant une ligne d'activité ou des données qui sont dans le domaine public et peuvent être pertinentes pour l'AIA) et d'une analyse des scénarios. L'AIA devrait également prendre en compte le caractère critique des fonctions «métiers», processus «supports», tiers et actifs informationnels identifiés et classifiés, ainsi que leurs interdépendances, conformément à la section 1.3.3.

79. Les établissements financiers devraient veiller à ce que leurs systèmes et services de TIC soient conçus en fonction de l'AIA et alignés en conséquence, par exemple en assurant la duplication de certaines composantes ayant une importance critique afin de prévenir les perturbations découlant d'événements qui ont une incidence sur ces composantes.

1.7.2. Planification de la continuité des activités

80. En fonction de leurs AIA, les établissements financiers devraient établir des plans visant à assurer la continuité des activités (plans de continuité d'activités, «PCA»), qui devraient être documentés et approuvés par leur organe de direction. Ces plans devraient examiner spécifiquement les risques pouvant avoir une incidence négative sur les systèmes et services de TIC. Ces plans devraient soutenir les objectifs visant à protéger, et à restaurer si nécessaire, la confidentialité, l'intégrité et la disponibilité de leurs fonctions «métiers», processus «supports» et actifs informationnels. Les établissements financiers devraient assurer une coordination appropriée avec les parties prenantes internes et externes durant la mise en place de ces plans.

81. Les établissements financiers devraient mettre en place des PCA visant à faire en sorte qu'ils puissent réagir de façon appropriée à tout scénario de défaillance potentiel et qu'ils puissent reprendre leurs activités revêtant une importance critique après toute perturbation, dans la limite de la durée maximale d'interruption admissible (DMIA, c'est-à-dire la durée maximale au bout de laquelle un système ou un processus doit être rétabli après un incident) et en fonction d'une perte de données maximale admissible (PDMA, c'est-à-dire la période maximale pendant laquelle il est acceptable de perdre des données en cas d'incident). En cas de perturbation grave de l'activité déclenchant des plans de continuité des activités spécifiques, les établissements financiers devraient hiérarchiser les priorités des mesures de continuité des activités en utilisant une approche fondée sur les risques, qui peut se fonder sur des évaluations des risques menées en vertu de la section 1.3.3. Pour les PSP, cela peut consister, par exemple, à faciliter la poursuite du traitement des opérations ayant une importance critique durant les efforts de remise en état.

82. Un établissement financier devrait envisager plusieurs scénarios différents dans son PCA, y compris des scénarios extrêmes mais plausibles auxquels il pourrait être confronté, dont un scénario de cyberattaque, et devrait évaluer l'incidence potentielle que de tels scénarios pourraient avoir. En fonction de ces scénarios, un établissement financier devrait décrire la façon dont la continuité des systèmes et services de TIC, ainsi que la sécurité de l'information au sein de l'établissement, peuvent être assurées.

1.7.3. Plans de réponse et de reprise

83. En fonction des AIA (paragraphe 78) et des scénarios plausibles (paragraphe 82), les établissements financiers devraient définir des plans de réponse et de rétablissement. Ces plans devraient préciser les conditions pouvant déclencher l'activation des plans et les mesures à prendre pour assurer la disponibilité, la continuité et la reprise, au minimum, des systèmes et services de TIC revêtant une importance critique pour les établissements financiers. Les plans

de réponse et de rétablissement devraient viser à répondre aux objectifs de reprise des opérations des établissements financiers.

84. Les plans de réponse et de rétablissement devraient tenir compte des options de rétablissement à court terme et à long terme. Ces plans devraient:

    a) se concentrer sur le rétablissement des fonctions «métiers», processus de «supports» et actifs informationnels ayant une importance critique, ainsi que leurs interdépendances, afin d'éviter toute incidence négative sur le fonctionnement des établissements financiers et sur le système financier, y compris sur les systèmes de paiement et les utilisateurs de services de paiement, et d'assurer l'exécution des opérations de paiement en attente de traitement;
    b) être documentés et mis à la disposition des unités «métier» et de soutien, et facilement accessibles en cas d'urgence;
    c) être mis à jour conformément aux enseignements tirés des incidents, aux tests, aux nouveaux risques et nouvelles menaces identifiés, ainsi qu'aux objectifs et priorités de reprise qui ont été modifiés.

85. Les plans devraient également envisager des solutions alternatives si la reprise n'est pas possible à court terme en raison des coûts, des risques, de la logistique ou de circonstances imprévues.

86. En outre, dans le cadre des plans de réponse et de rétablissement, un établissement financier devrait envisager et mettre en œuvre des mesures de continuité permettant d'atténuer les défaillances de fournisseurs tiers ayant une importance clé pour la continuité de ses services de TIC [conformément aux dispositions prévues dans les orientations de l'ABE sur les accords d'externalisation (EBA/GL/2019/02) s'agissant des plans de continuité des activités].

1.7.4. Mesures visant à tester les plans

87. Les établissements financiers devraient périodiquement tester leurs PCA. Notamment, ils devraient veiller à ce que les PCA relatifs aux fonctions «métiers», processus «supports» et actifs informationnels revêtant une importance critique (y compris ceux fournis par des tiers, le cas échéant), ainsi que leurs interdépendances, soient testés au moins une fois par an, conformément au paragraphe 89.

88. Les PCA devraient être mis à jour au moins une fois par an, en fonction des résultats des tests, des renseignements les plus récents sur les menaces et des enseignements tirés des événements précédents. Toute modification des objectifs de rétablissement (y compris les DMIA et PDMA) et/ou des fonctions «métiers», processus «supports» et actifs informationnels devrait également être prise en compte, le cas échéant, pour mettre les PCA à jour.

89. Les tests réalisés par les établissements financiers sur leurs PCA devraient prouver qu'ils sont capables d'assurer la viabilité de leurs activités jusqu'à ce que les opérations ayant une importance critique soient rétablies. Ils devraient notamment:

    a) inclure des tests fondés sur un ensemble approprié de scénarios graves mais plausibles, y compris de ceux envisagés lors du développement des PCA (ainsi que le test des

services fournis par des tiers, le cas échéant) – cela devrait, entre autres, intégrer la commutation des fonctions «métiers», processus «supports» et actifs informationnels revêtant une importance critique avec l'environnement de rétablissement après sinistre et à prouver, d'une part, qu'ils peuvent fonctionner de cette façon pendant une période suffisamment représentative et, d'autre part, qu'un fonctionnement normal peut être rétabli par la suite;

b) être conçus pour vérifier les hypothèses sur lesquelles se fondent les PCA, y compris les dispositifs de gouvernance et les plans de communication en situation de crise; et

c) inclure des procédures permettant de vérifier la disponibilité du personnel et des prestataires, des systèmes de TIC et des services de TIC afin de répondre de façon appropriée aux scénarios définis au paragraphe 89(a).

90. Les résultats des tests devraient être documentés et toute lacune identifiée lors des tests devrait être analysée, résolue et communiquée à l'organe de direction.

1.7.5. Communication en situation de crise

91. En cas de perturbation ou d'urgence, et durant la mise en œuvre des PCA, les établissements financiers devraient veiller à disposer de mesures de communication efficaces en situation de crise, afin que toutes les parties concernées internes et externes, y compris les autorités compétentes si cela est requis par la réglementation nationale, ainsi que les fournisseurs concernés (prestataires de services d'externalisation, entités du groupe ou fournisseurs tiers), soient informés à temps et de façon appropriée.

1.8. Gestion des relations avec les utilisateurs de services de paiement

92. Les PSP devraient établir et mettre en œuvre des processus permettant de renforcer la sensibilisation des USP aux risques de sécurité liés aux services de paiement, en leur fournissant de l'assistance et des orientations.

93. L'assistance et les orientations fournies aux USP devraient être mises à jour en fonction des nouvelles menaces et vulnérabilités, et les changements devraient être communiqués aux USP.

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

95. Lorsque, conformément à l'article 68, paragraphe 1, de la directive (UE) 2015/2366, un PSP a convenu avec le payeur de limites 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 ces limites à hauteur de la limite maximale convenue.

96. Les PSP devraient offrir aux USP la possibilité de recevoir des alertes lors de tentatives initiées et/ou ratées d'initier des opérations de paiement, de manière à leur permettre de détecter toute utilisation frauduleuse ou malveillante de leurs comptes.

97. Les PSP devraient tenir les USP informés des mises à jour des procédures de sécurité ayant une incidence sur les USP s'agissant de la prestation de services de paiement.

98. Les PSP devraient fournir aux USP l'aide nécessaire pour toute question, demande de soutien et notification d'anomalies ou tout problème de sécurité relatifs aux services de paiement. Les USP devraient être correctement informés de la manière dont ils peuvent obtenir cette aide.

Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu