EBA/GL/2017/05

11/09/2017

Orientations

Orientations sur l'évaluation du risque lié aux TIC dans le cadre du processus de contrôle et d'évaluation prudentiels (Supervisory Review and Evaluation process – SREP)

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° 1093/20101. 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 13.11.2017. 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/2017/05». 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, établies conformément à l'article 107, paragraphe 3, de la directive 2013/36/UE [2], visent à assurer la convergence des pratiques prudentielles lors de l'évaluation du risque lié aux technologies de l'information et de la communication (TIC) dans le cadre du processus de contrôle et d'évaluation prudentiels (*Supervisory Review and Evaluation process* – SREP) visé à l'article 97 de la directive 2013/36/UE et également précisé dans les orientations de l'Autorité bancaire européenne (ABE) sur les procédures et les méthodologies communes à appliquer dans le cadre du processus de contrôle et d'évaluation prudentiels (SREP)[3]. Les présentes orientations précisent en particulier les critères d'évaluation que les autorités compétentes devraient appliquer lors de l'évaluation prudentielle de la gouvernance et de la stratégie des établissements en matière de TIC ainsi que lors de l'évaluation prudentielle de l'exposition des établissements au risque lié aux TIC et des mécanismes de contrôle de ce risque. Elles font partie intégrante des orientations de l'ABE sur le SREP.

6. Les autorités compétentes devraient appliquer ces orientations conformément au niveau d'application du SREP indiqué dans les orientations de l'ABE sur le SREP et aux exigences de modèle d'engagement minimal et de proportionnalité qui y sont définies.

Destinataires

7. Les présentes orientations sont destinées aux autorités compétentes telles que définies à l'article 4, paragraphe 2, point i), du règlement (UE) nº 1093/2010.

Définitions

8. Sauf indication contraire, les termes utilisés et définis dans la directive 2013/36/UE, dans le règlement (UE) nº 575/2013 et dans les définitions fournies dans les orientations de l'ABE sur le SREP ont la même signification dans les présentes orientations. En outre, aux fins des présentes orientations, les définitions suivantes s'appliquent:

Systèmes de TIC	TIC mises en place dans le cadre d'un mécanisme ou d'un réseau d'interconnexion qui soutient les opérations d'un établissement.

[2] Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (1) - JO L 176 du 27.6.2013.

[3] ABE/GL/2014/13

Services de TIC	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 déclaration d'informations, mais aussi les services de soutien au suivi, aux opérations et aux décisions.
Risque pour la disponibilité et la continuité des TIC	Risque que les performances et la disponibilité des systèmes et des données TIC soient compromises, y compris l'incapacité de rétablir rapidement les services de l'établissement en raison d'une défaillance des composants TIC matériels ou logiciels, de dysfonctionnements dans la gestion du système de TIC ou de tout autre événement, tel que précisé dans l'annexe.
Risque pour la sécurité des TIC	Risque d'accès non autorisé aux systèmes et aux données TIC depuis l'intérieur ou l'extérieur de l'établissement (cyberattaques, par exemple), tel que précisé dans l'annexe.
Risque lié au changement des TIC	Risque découlant de l'incapacité de l'établissement à gérer rapidement et de manière contrôlée les changements apportés au système de TIC, en particulier des programmes de changement importants et complexes, tel que précisé dans l'annexe.
Risque pour l'intégrité des données TIC	Risque que les données stockées et traitées par les systèmes de TIC soient incomplètes, inexactes ou incohérentes d'un système de TIC à l'autre, par exemple en raison de contrôles laxistes ou inexistants des TIC au cours des différentes phases du cycle de vie des données TIC (c.-à-d. la conception de l'architecture des données, la construction du modèle de données et/ou des dictionnaires de données, la vérification des entrées de données, le contrôle des extractions, des transferts et du traitement des données, notamment des sorties de données restituées), nuisant à la capacité d'un établissement à rapidement fournir des services et des informations correctes sur la gestion (du risque) et la situation financière, tel que précisé dans l'annexe.
Risque lié à l'externalisation des TIC	Risque que l'engagement d'un tiers ou d'une autre entité du groupe (externalisation intragroupe) pour fournir des systèmes de TIC ou des services connexes ait une incidence négative sur la performance de l'établissement et sa gestion des risques, tel que précisé dans l'annexe.

3. Mise en œuvre

Date d'entrée en vigueur

9. Les présentes orientations s'appliquent à compter du 1er janvier 2018.

4. Exigences en matière d'évaluation du risque lié aux TIC

Titre 1 – Dispositions générales

10. Les autorités compétentes devraient évaluer les risques liés aux TIC, le dispositif de gouvernance et la stratégie en matière de TIC dans le cadre du SREP en suivant le modèle d'engagement minimal et les critères de proportionnalité indiqués au titre 2 des orientations de l'ABE sur le SREP. Cela signifie en particulier que:

    a. la fréquence de l'évaluation du risque lié aux TIC dépendra du modèle d'engagement minimal correspondant à la catégorie de SREP dont un établissement relève et de son programme de contrôle prudentiel spécifique; et

    b. l'ampleur, le détail et l'intensité de l'évaluation des TIC devraient être proportionnés à la taille, à la structure et à l'environnement opérationnel de l'établissement, ainsi qu'à la nature, à l'échelle et à la complexité de ses activités.

11. Le principe de proportionnalité s'applique tout au long des présentes orientations à la portée, à la fréquence et à l'intensité de l'engagement et du dialogue prudentiels avec un établissement ainsi qu'aux attentes prudentielles des normes auxquelles l'établissement devrait répondre.

12. Les autorités compétentes peuvent s'appuyer sur les travaux déjà entrepris par l'établissement ou par l'autorité compétente dans le cadre des évaluations d'autres risques ou éléments du SREP et prendre en considération ces travaux afin de mettre à jour l'évaluation. Plus précisément, lorsqu'elles effectuent les évaluations décrites dans les présentes orientations, les autorités compétentes devraient choisir l'approche et la méthode d'évaluation prudentielle la mieux adaptée et proportionnée à l'établissement et utiliser la documentation disponible en vigueur [par exemple les rapports pertinents et autres documents, les réunions avec les responsables (notamment ceux chargés de la gestion du risque), les résultats des contrôles sur place] pour la prendre en considération dans leur évaluation.

13. Les autorités compétentes devraient résumer les constatations de leurs évaluations des critères spécifiés dans les présentes orientations et les utiliser pour parvenir à des conclusions sur l'évaluation des éléments du SREP tels qu'ils sont décrits dans les orientations de l'ABE sur le SREP.

14. En particulier, l'évaluation de la gouvernance et de la stratégie en matière de TIC effectuée conformément au titre 2 des présentes orientations devrait aboutir à des constatations qui sont prises en considération dans le résumé des constatations de l'évaluation de la gouvernance interne et des mécanismes de maîtrise du risque dans l'ensemble de l'établissement (élément SREP visé au titre 5 des orientations de l'ABE sur le SREP), et se traduire dans la notation correspondant à cet élément du SREP.

En outre, les autorités compétentes devraient prendre en compte le fait que toute incidence négative majeure de l'évaluation de la stratégie en matière de TIC sur la stratégie d'entreprise de l'établissement et toute inquiétude quant à une éventuelle insuffisance de ressources et de capacités en matière de TIC dans l'établissement pour réaliser et soutenir les grands changements stratégiques prévus devraient être prises en considération dans l'analyse du modèle d'entreprise effectuée conformément au titre 4 des orientations de l'ABE sur le SREP.

15. Le résultat de l'évaluation du risque lié aux TIC, comme indiqué au titre 3 des présentes orientations, devrait être pris en considération dans les constatations de l'évaluation du risque opérationnel et devrait être considéré comme un facteur influençant la note attribuée, comme il est indiqué au titre 6.4 des orientations de l'ABE sur le SREP.

16. Il est à noter que, si les autorités compétentes devraient généralement évaluer les sous-catégories de risques dans le cadre des catégories principales (c'est à dire le risque lié aux TIC qui sera évalué dans le cadre du risque opérationnel), elles peuvent également évaluer individuellement les sous-catégories qu'elles jugent significatives. À cette fin, si l'autorité compétente estimait que le risque lié aux TIC est significatif, les présentes orientations fournissent également un tableau de notes (tableau 1) qui devrait être utilisé pour attribuer une note de sous-catégorie distincte pour le risque lié aux TIC en suivant l'approche globale de notation des risques pesant sur le capital définie dans les orientations de l'ABE sur le SREP.

17. Pour déterminer si le risque lié aux TIC devrait être considéré comme significatif et, par conséquent, la possibilité d'évaluer et de noter ce risque comme une sous-catégorie individuelle de risque opérationnel, les autorités compétentes peuvent utiliser les critères indiqués à la section 6.1 des orientations de l'ABE sur le SREP.

18. Lors de l'application des présentes orientations, les autorités compétentes devraient, le cas échéant, prendre en considération la liste non exhaustive des sous-catégories de risques liés aux TIC et des scénarios de risque qui est présentée à l'annexe, sachant que l'annexe se concentre sur les risques liés aux TIC susceptibles d'entraîner des pertes présentant un degré élevé de gravité. Les autorités compétentes peuvent exclure certains risques liés aux TIC inclus dans la taxonomie si ces risques ne sont pas pertinents pour leur évaluation. Il est attendu des établissements qu'ils établissent leurs propres taxonomies des risques plutôt que d'utiliser celle qui est présentée en annexe.

19. Lorsque les présentes orientations sont appliquées aux groupes bancaires transfrontaliers et à leurs entités et qu'un collège des autorités de surveillance a été mis en place, les autorités compétentes concernées devraient, dans le cadre de leur coopération pour l'évaluation du SREP conformément à la section 11.1 des orientations de l'ABE sur le SREP, coordonner autant que possible la portée exacte et détaillée de chaque élément d'information, de manière cohérente pour toutes les entités du groupe.

Titre 2 – Évaluation de la gouvernance et de la stratégie en matière de TIC des établissements

2.1 Principes généraux

20. Les autorités compétentes devraient évaluer si le cadre général de gouvernance et de contrôle interne de l'établissement couvre correctement les systèmes de TIC et les risques qui y sont liés et si l'organe de direction traite et gère adéquatement ces aspects, les TIC faisant partie intégrante du bon fonctionnement d'un établissement.

21. Lors de cette évaluation, les autorités compétentes devraient se référer aux exigences et aux normes de bonne gouvernance interne et aux dispositions de maîtrise des risques telles qu'elles sont spécifiées dans les orientations de l'ABE sur la gouvernance interne (GL 44)[4] et les orientations internationales dans ce domaine, dans la mesure où elles sont applicables aux spécificités des systèmes de TIC et des risques liés aux TIC.

22. Dans le présent titre, l'évaluation ne couvre pas les éléments spécifiques de la gouvernance, de la gestion et de la maîtrise des risques du système de TIC qui sont axés sur la gestion de certains risques liés aux TIC abordés au titre 3 des présentes orientations, mais se concentre sur les domaines suivants:

    a. la stratégie en matière de TIC – si l'établissement dispose d'une stratégie en matière de TIC qui relève d'une bonne gouvernance et est conforme à la stratégie d'entreprise de l'établissement;

    b. la gouvernance interne globale – si les mécanismes généraux de gouvernance interne de l'établissement sont adéquats par rapport aux systèmes de TIC de l'établissement ; et

    c. le risque lié aux TIC dans le cadre de gestion des risques de l'établissement – si le cadre de gestion des risques et de contrôle interne de l'établissement protège adéquatement les systèmes de TIC de l'établissement.

23. Le point a) visé au paragraphe 22, tout en fournissant des informations sur des éléments de la gouvernance de l'établissement, devrait principalement alimenter l'évaluation du modèle d'entreprise abordé au titre 4 des orientations de l'ABE sur le SREP. Les points b) et c) complètent les évaluations des sujets couverts par le titre 5 des orientations de l'ABE sur le SREP et l'évaluation décrite dans les présentes orientations devrait alimenter les différentes évaluations présentées au titre 5 des orientations de l'ABE sur le SREP.

[4] Orientations de l'ABE sur la gouvernance interne, GL 44, 27 septembre 2011.

24. Le résultat de cette évaluation devrait être pris en considération, quand cela est pertinent, pour évaluer la gestion du risque et les mécanismes de maîtrise du risque visés au titre 3 des présentes orientations.

2.2 Stratégie en matière de TIC

25. En vertu de la présente section, les autorités compétentes devraient évaluer si l'établissement a mis en place une stratégie en matière de TIC qui soit soumise à une surveillance adéquate par l'organe de direction de l'établissement, cohérente avec la stratégie d'entreprise, en particulier pour maintenir les TIC à jour et pour planifier ou mettre en œuvre des changements importants et complexes en matière de TIC, et qui soutienne le modèle d'entreprise de l'établissement.

2.2.1 Elaboration et adéquation de la stratégie en matière de TIC

26. Les autorités compétentes devraient évaluer si l'établissement dispose d'un cadre proportionné à la nature, à l'échelle et à la complexité de ses activités de TIC pour la préparation et l'élaboration de la stratégie en matière de TIC de l'établissement. Lors de cette évaluation, les autorités compétentes devraient examiner si:

    a. la direction générale[5] de la ou des lignes d'activité est dûment associée à la définition des priorités stratégiques de l'établissement en matière de TIC et si, pour sa part, la direction générale de la fonction TIC est au courant de l'évolution, de la conception et du lancement des stratégies et des initiatives d'entreprise majeures afin d'assurer un alignement permanent entre les systèmes de TIC, les services de TIC et la fonction TIC (c'est-à-dire les responsables de la gestion et du déploiement de ces systèmes et services) et la stratégie d'entreprise de l'établissement, et si les TIC sont effectivement mises à jour;

    b. la stratégie en matière de TIC est documentée et soutenue par des plans concrets de mise en œuvre, en particulier en ce qui concerne les échéances importantes et la planification des ressources (y compris les ressources financières et humaines) afin de s'assurer qu'ils sont réalistes et permettent la mise en œuvre de la stratégie en matière de TIC;

    c. l'établissement met à jour périodiquement sa stratégie en matière de TIC, en particulier lorsqu'il modifie sa stratégie d'entreprise, afin d'assurer la conformité permanente entre les TIC et les objectifs de moyen à long terme, les plans et les activités de l'entreprise; et

    d. l'organe de direction de l'établissement approuve la stratégie en matière de TIC et les plans de mise en œuvre et surveille sa mise en œuvre.

2.2.2 Mise en œuvre de la stratégie en matière de TIC

27. Si la stratégie en matière de TIC de l'établissement requiert la mise en œuvre de changements importants et complexes en matière de TIC, ou de changements ayant des implications significatives pour le modèle d'entreprise de l'établissement, les autorités compétentes devraient évaluer si l'établissement dispose d'un cadre de contrôle adapté à sa taille, à ses activités TIC ainsi qu'au niveau

[5] «Direction générale» et «organe de direction» tels que définis dans la directive 2013/36/UE du 26 juin 2013, à l'article 3, paragraphe 1, point 7) pour «organe de direction» et à l'article 3, paragraphe 1, point 9) pour «direction générale».

des activités de changement, afin de soutenir la mise en œuvre effective de la stratégie en matière de TIC de l'établissement. Lors de cette évaluation, les autorités compétentes devraient examiner si le cadre de contrôle:

a. comprend des processus de gouvernance (par exemple suivi des progrès et du budget, et rapports dédiés) et des organes pertinents (par exemple un service de gestion des projets, un groupe de pilotage des TIC ou équivalent) pour soutenir efficacement la mise en œuvre des programmes stratégiques en matière de TIC;

b. a défini et attribué les rôles et les responsabilités pour la mise en œuvre des programmes stratégiques en matière de TIC, en accordant une attention particulière à l'expérience des acteurs clés dans l'organisation, le pilotage et le suivi des changements importants et complexes en matière de TIC et la gestion des incidences plus générales sur les ressources organisationnelles et humaines (par exemple la gestion de la résistance au changement, la formation, la communication);

c. associe les fonctions indépendantes de contrôle et d'audit interne afin d'assurer que les risques associés à la mise en œuvre de la stratégie en matière de TIC ont été recensés, évalués et efficacement atténués et que le cadre de gouvernance en place pour mettre en œuvre la stratégie TIC est efficace; et

d. comporte un processus de planification et de contrôle de la planification qui offre une marge de manœuvre pour répondre aux problèmes importants constatés (par exemple aux problèmes de mise en œuvre rencontrés ou aux retards) ou aux évolutions externes (par exemple des changements importants dans l'environnement de l'entreprise, des problèmes technologiques ou des innovations) de façon à assurer l'adaptation en temps voulu du plan de mise en œuvre stratégique.

2.3 Gouvernance interne globale

28. Conformément au titre 5 des orientations de l'ABE sur le SREP, les autorités compétentes devraient évaluer si l'établissement dispose d'une structure d'entreprise appropriée et transparente adaptée à l'objectif et si elle a mis en place des mécanismes de gouvernance appropriés. En ce qui concerne les systèmes de TIC et conformément aux orientations de l'ABE sur la gouvernance interne, cette évaluation devrait comprendre une évaluation du fait que l'établissement témoigne :

a. d'une structure organisationnelle robuste et transparente qui prévoie des responsabilités claires en matière de TIC, notamment l'organe de direction et ses comités, et du fait que les personnes clés responsables des TIC (par exemple le directeur des systèmes d'information, le directeur des opérations ou un rôle équivalent) ont un accès indirect ou direct approprié à l'organe de direction afin de s'assurer que les informations ou les questions importantes relatives aux TIC sont correctement signalées, discutées et tranchées au niveau de l'organe de direction ; et

b. du fait que l'organe de direction connaisse et traite les risques liés aux TIC.

29. Conformément à la section 5.2 des orientations de l'ABE sur le SREP, les autorités compétentes devraient évaluer si la politique et la stratégie d'externalisation des TIC de l'établissement tiennent

compte, le cas échéant, de l'incidence de l'externalisation des TIC sur les affaires et le modèle d'entreprise de l'établissement.

2.4 Le risque lié aux TIC dans le cadre de gestion des risques de l'établissement

30. En évaluant la gestion du risque et les mécanismes internes de maîtrise du risque dans l'ensemble de l'établissement, conformément au titre 5 des orientations de l'ABE sur le SREP, les autorités compétentes devraient se demander si le cadre de gestion des risques et de contrôle interne de l'établissement protège de manière adéquate les systèmes de TIC de l'établissement, c'est-à-dire d'une manière proportionnelle à la taille et aux activités de l'établissement et à son profil de risque lié aux TIC tel que défini au titre 3. Les autorités compétentes devraient en particulier déterminer si:

    a. l'appétit pour le risque et l'ICAAP couvrent les risques liés aux TIC, dans le cadre de la catégorie plus large des risques opérationnels, pour la définition de la stratégie globale en matière de risque et la détermination du capital interne; et si

    b. les risques liés aux TIC relèvent des cadres de gestion du risque et de contrôle interne de l'ensemble de l'établissement.

31. Les autorités compétentes devraient effectuer l'évaluation définie au point a) ci-dessus en tenant compte à la fois des scénarios attendus et des scénarios défavorables, par exemple des scénarios compris dans le test de résistance spécifique à l'établissement ou dans le test de résistance prudentiel.

32. En ce qui concerne spécifiquement le point b), les autorités compétentes devraient évaluer si les fonctions indépendantes de contrôle et d'audit interne, telles qu'elles sont détaillées au paragraphe 104, points a) et d), et au paragraphe 105, points a) et c), des orientations de l'ABE sur le SREP, sont appropriées pour assurer un niveau suffisant d'indépendance entre les TIC et les fonctions de contrôle et d'audit, compte tenu de la taille et du profil de risque lié aux TIC de l'établissement.

2.5 Résumé des constatations

33. Ces résultats devraient être reflétés dans le résumé des constatations visé au titre 5 des orientations de l'ABE sur le SREP et devraient faire partie des notations attribuées conformément aux considérations du tableau 3 des orientations de l'ABE sur le SREP.

34. Pour l'évaluation de la stratégie en matière de TIC, les points suivants devraient être pris en considération lors de l'achèvement de l'évaluation susmentionnée:

    a. si les autorités compétentes concluent que le cadre de gouvernance de l'établissement est inadéquat pour élaborer et mettre en œuvre la stratégie en matière de TIC de l'établissement conformément à la section 2.2, il faudrait en tenir compte dans l'évaluation de la gouvernance interne de l'établissement visée au titre 5, paragraphe 87, point a), des orientations de l'ABE sur le SREP;

b. si, à l'issue des évaluations susmentionnées à la section 2.2 ci-dessus, les autorités compétentes concluent à l'existence probable d'un déséquilibre important entre la stratégie en matière de TIC et la stratégie d'entreprise qui pourrait avoir une incidence négative majeure sur les objectifs commerciaux et/ou financiers à long terme de l'établissement, la durabilité et/ou le modèle d'entreprise de l'établissement, ou les domaines/lignes d'activité de l'établissement qui ont été déterminés comme étant les plus significatifs au paragraphe 62, point a), des orientations de l'ABE sur le SREP, il faudrait en tenir compte dans l'évaluation du modèle d'entreprise visée au titre 4 desdites orientations, paragraphes 70, points b) et c); et

c. si, à l'issue des évaluations susmentionnées à la section 2.2 ci-dessus, les autorités compétentes concluent que l'établissement pourrait ne pas disposer des ressources en TIC et des capacités de mise en œuvre des TIC suffisantes pour réaliser et soutenir les grands changements stratégiques prévus, il faudrait en tenir compte dans l'évaluation du modèle d'entreprise visée au titre 4, paragraphe 70, point b), des orientations de l'ABE sur le SREP.

Titre 3 – Évaluation des expositions des établissements aux risques liés aux TIC et des mécanismes de maîtrise de ces risques

3.1 Considérations générales

35. Les autorités compétentes devraient évaluer si l'établissement a correctement recensé, évalué et atténué les risques liés aux TIC auxquels il est exposé. Ce processus devrait faire partie du cadre de gestion du risque opérationnel et être conforme à l'approche applicable aux risques opérationnels.

36. Les autorités compétentes devraient d'abord déceler les risques significatifs inhérents liés aux TIC auxquels l'établissement est ou pourrait être exposé, puis effectuer une évaluation de l'efficacité du cadre de gestion des risques liés aux TIC, des procédures et des contrôles de l'établissement pour atténuer ces risques. Le résultat de l'évaluation devrait se refléter dans un résumé des constatations qui sert de base à la note du risque opérationnel dans les orientations de l'ABE sur le SREP. Lorsque le risque lié aux TIC est considéré comme significatif et que les autorités compétentes souhaitent lui attribuer une note individuelle, le tableau 1 devrait être utilisé pour lui attribuer une note en tant que sous-risque du risque opérationnel.

37. Lors de l'évaluation décrite sous le présent titre, les autorités compétentes devraient utiliser toutes les sources d'information disponibles, comme indiqué au paragraphe 127 du titre 6 des orientations de l'ABE sur le SREP, par exemple les activités de gestion des risques de l'établissement, les rapports et les résultats, comme base pour définir leurs priorités d'évaluation prudentielle. Les autorités compétentes devraient également utiliser d'autres sources d'information pour mener cette évaluation, notamment, le cas échéant, les sources suivantes:

    a. auto-évaluations du risque lié aux TIC et des mécanismes de maîtrise (si elles sont fournies dans les informations de l'ICAAP);
    b. les informations de gestion relatives au risque lié aux TIC transmises à l'organe de direction de l'établissement, par exemple les rapports en matière de risque lié aux TIC, qu'ils soient périodiques ou consécutifs à un incident (notamment dans la base de données sur les pertes opérationnelles), les données sur l'exposition au risque lié aux TIC provenant de la fonction de gestion des risques de l'établissement;
    c. les constatations des audits internes et externes liés aux TIC rapportées au comité d'audit de l'établissement.

3.2 Détection des risques significatifs liés aux TIC

38. Les autorités compétentes devraient détecter les risques significatifs liés aux TIC auxquels l'établissement est ou pourrait être exposé en suivant les étapes décrites ci-dessous.

3.2.1 Examen du profil de risque lié aux TIC de l'établissement

39. Lors de l'examen du profil de risque lié aux TIC de l'établissement, les autorités compétentes devraient prendre en considération toutes les informations pertinentes sur les expositions aux risques liés aux TIC de l'établissement, notamment les informations visées au paragraphe 37 et les lacunes ou faiblesses significatives constatées dans l'organisation des TIC et les mécanismes de maîtrise du risque dans l'ensemble de l'établissement décrits au titre 2 des présentes orientations, et, le cas échéant, examiner ces informations de manière proportionnée. Dans le cadre de cet examen, les autorités compétentes devraient prendre en considération:

    a. l'incidence potentielle d'une perturbation importante des systèmes de TIC de l'établissement sur le système financier, soit au niveau national, soit au niveau international;
    b. le fait de savoir si l'établissement peut être exposé à des risques pour la sécurité des TIC ou à des risques pour la disponibilité et la continuité des TIC s'il est tributaire d'internet, du recours important à des solutions innovantes de TIC ou d'autres canaux de distribution économiques qui peuvent en faire une cible privilégiée de cyberattaques;
    c. le fait de savoir si l'établissement pourrait être plus exposé aux risques pour la sécurité des TIC, aux risques pour la disponibilité et la continuité des TIC, aux risques pour l'intégrité des données des TIC ou aux risques liés au changement des TIC en raison de la complexité (par exemple à la suite de fusions ou d'acquisitions) ou de l'obsolescence de ses systèmes de TIC;
    d. le fait de savoir si l'établissement apporte des changements significatifs dans ses systèmes de TIC et/ou la fonction TIC (par exemple en raison de fusions, d'acquisitions, de cessions ou de remplacement de ses systèmes principaux de TIC), ce qui peut avoir une incidence négative sur la stabilité ou le bon fonctionnement des systèmes de TIC et entraîner des risques significatifs pour la disponibilité et la continuité des TIC, des risques pour la sécurité des TIC, des risques liés au changement des TIC ou des risques liés à l'intégrité des données TIC;
    e. le fait de savoir si l'établissement a externalisé des services de TIC ou des systèmes de TIC à l'intérieur ou à l'extérieur du groupe, ce qui pourrait l'exposer à des risques significatifs liés à l'externalisation des TIC;
    f. le fait de savoir si l'établissement prend des mesures radicales pour réduire le coût des TIC, ce qui pourrait entraîner la réduction des investissements, des ressources et de l'expertise nécessaires en matière de TIC et pourrait accroître l'exposition à tous les types de risques liés aux TIC définis dans la taxonomie;
    g. le fait de savoir si l'emplacement des centres d'opérations des TIC ou des centres de données importants (par exemple, régions, pays) risque d'exposer l'établissement à des catastrophes naturelles (par exemple inondations, séismes), à une instabilité politique ou à des conflits du travail et à des désordres civils susceptibles d'entraîner un accroissement significatif des risques pour la disponibilité et la continuité des TIC et des risques pour la sécurité des TIC.

3.2.2 Examen des systèmes et services de TIC essentiels

40. Dans le cadre du processus visant à détecter les risques liés aux TIC susceptibles d'avoir une incidence prudentielle significative sur l'établissement, les autorités compétentes devraient examiner la documentation de l'établissement et formuler un avis précisant quels systèmes et services de TIC sont

essentiels au bon fonctionnement, à la disponibilité, à la continuité et à la sécurité des activités premières de l'établissement.

41. À cette fin, les autorités compétentes devraient examiner la méthodologie et les processus appliqués par l'établissement pour identifier les systèmes et les services de TIC qui sont essentiels, en tenant compte du fait que certains systèmes et services peuvent être considérés par l'établissement comme essentiels du point de vue de la continuité et de la disponibilité de l'activité, de la sécurité (par exemple la prévention de la fraude) et/ou de la confidentialité (par exemple les données confidentielles). Lors de l'examen, les autorités compétentes devraient le mener en prenant en compte le fait que les systèmes et services de TIC essentiels devraient remplir au moins une des conditions suivantes:

    a. ils soutiennent le cœur de métier de l'établissement (opérations et canaux de distribution, par exemple les guichets automatiques, les services bancaires en ligne et mobiles);

    b. ils soutiennent des processus de gouvernance et des fonctions d'entreprise essentiels, notamment la gestion du risque (par exemple les systèmes de gestion du risque et de gestion de la trésorerie);

    c. ils sont soumis à des exigences juridiques ou réglementaires spéciales (le cas échéant) qui imposent des conditions plus strictes en matière de disponibilité, de résilience, de confidentialité ou de sécurité [par exemple la législation sur la protection des données, éventuellement un «temps de reprise admissible» (RTO, *Recovery Time Objective*, soit le délai maximal de redémarrage d'un système ou d'un processus après un incident) et une «perte de données maximale admissible» (RPO, *Recovery Point Objective*, soit la durée maximale pendant laquelle des données peuvent être perdues en cas d'incident)] pour certains services d'importance systémique (le cas échéant);

    d. ils traitent ou stockent des données confidentielles ou sensibles pour lesquelles un accès non autorisé pourrait avoir une incidence significative sur la réputation, les résultats financiers ou la solidité et la continuité des activités de l'établissement (par exemple les bases de données contenant des données confidentielles sur les clients); et

    e. ils fournissent des fonctionnalités de base qui sont vitales pour le bon fonctionnement de l'établissement (par exemple les services de télécommunications et de connectivité, des services de TIC et de cybersécurité).

3.2.3 Détection des risques significatifs liés aux TIC relatifs aux systèmes et services de TIC essentiels

42. Compte tenu des examens effectués sur le profil de risque lié aux TIC de l'établissement et sur les systèmes et services de TIC essentiels susmentionnés, les autorités compétentes devraient se prononcer sur les risques significatifs pour les TIC qui, selon leur jugement prudentiel, peuvent avoir une incidence prudentielle significative sur les systèmes et services de TIC essentiels de l'établissement.

43. Lors de l'évaluation de l'incidence potentielle des risques liés aux TIC sur les systèmes et les services de TIC essentiels d'un établissement, les autorités compétentes devraient prendre en considération:

    a. l'incidence financière, notamment (mais sans s'y limiter) la perte de fonds ou d'actifs, la compensation éventuelle des clients, les frais juridiques et les frais liés aux mesures correctives, les dommages contractuels, les pertes de revenus;

    b. le potentiel de perturbation des activités, compte tenu (mais sans s'y limiter) de l'importance des services financiers touchés; le nombre de clients et/ou de succursales et de employés potentiellement concernés;

    c. l'incidence potentielle sur la réputation de l'établissement en fonction de l'importance des services bancaires ou des activités opérationnelles touchés (par exemple le vol de données des clients); le profil/la visibilité externe des systèmes et services de TIC touchés (par exemple les systèmes bancaires mobiles ou en ligne, les points de vente, les guichets automatiques ou les systèmes de paiement);

    d. l'incidence réglementaire, notamment le risque de sanction par le régulateur avec publication de la décision, les amendes ou même l'éventualité d'un retrait d'autorisation d'exercer;

    e. l'incidence stratégique sur l'établissement, par exemple, si des produits stratégiques ou des plans d'entreprise sont compromis ou volés.

44. Les autorités compétentes devraient ensuite cartographier les risques liés aux TIC détectés qui sont considérés comme significatifs dans les catégories de risque lié aux TIC suivantes, pour lesquelles une description supplémentaire et des exemples de risques sont fournis en annexe. Les autorités compétentes devraient se pencher sur les risques liés aux TIC dans l'annexe dans le cadre de l'évaluation présentée au titre 3:

    a. Risque pour la disponibilité et la continuité des TIC
    b. Risque pour la sécurité des TIC
    c. Risque lié au changement des TIC
    d. Risque pour l'intégrité des données TIC
    e. Risque lié à l'externalisation des TIC

    La cartographie doit aider les autorités compétentes à déterminer quels risques sont significatifs (le cas échéant) et devraient donc être soumis à un examen plus attentif et plus approfondi lors des étapes d'évaluation suivantes.

3.3 Évaluation des contrôles visant à atténuer les risques significatifs liés aux TIC

45. Pour évaluer l'exposition résiduelle de l'établissement aux risques liés aux TIC, les autorités compétentes devraient examiner comment l'établissement détecte, surveille, évalue et atténue les risques significatifs détectés par les autorités compétentes lors de l'évaluation décrite ci-dessus.

46. À cette fin, pour les risques significatifs liés aux TIC détectés, les autorités compétentes devraient examiner les éléments suivants:

    a. politique et processus de gestion des risques liés aux TIC et seuils de tolérance aux risques;

    b. cadre de gestion organisationnelle et de surveillance;

    c. étendue et constatations des audits internes; et

    d. contrôles des risques liés aux TIC qui sont spécifiques au risque significatif lié aux TIC détecté.

47. L'évaluation devrait tenir compte des résultats de l'analyse du cadre général de gestion des risques et de contrôle interne visé au titre 5 des orientations de l'ABE sur le SREP, ainsi que de la gouvernance et de la stratégie de l'établissement visées au titre 2 des présentes orientations, car la détection de lacunes significatives dans ces domaines peut influencer la capacité de l'établissement à gérer et à atténuer son exposition aux risques liés aux TIC. Le cas échéant, les autorités compétentes devraient également utiliser les sources d'informations évoquées au paragraphe 37 des présentes orientations.

48. Les autorités compétentes devraient suivre les étapes d'évaluation suivantes d'une manière proportionnée à la nature, à l'échelle et à la complexité des activités de l'établissement et en appliquant un contrôle prudentiel adapté au profil de risque lié aux TIC de l'établissement.

3.3.1 Politique et processus de gestion du risque lié aux TIC et seuils de tolérance

49. Les autorités compétentes devraient examiner si l'établissement dispose de politiques, de processus et de seuils de tolérance appropriés pour les risques significatifs liés aux TIC détectés. Ceux-ci peuvent faire partie du cadre de gestion du risque opérationnel ou d'un document distinct. Lors de cette évaluation, les autorités compétentes devraient examiner si :

    a. la politique de gestion du risque est formalisée et approuvée par l'organe de direction et contient des orientations suffisantes sur l'appétit pour le risque lié aux TIC de l'établissement et sur les principaux objectifs de gestion du risque lié aux TIC poursuivis et/ou sur les seuils de tolérance appliqués au risque lié aux TIC. La politique applicable de gestion du risque lié aux TIC devrait également être notifiée à toutes les parties prenantes concernées;

    b. la politique applicable couvre tous les éléments importants pour la gestion des risques significatifs liés aux TIC détectés;

    c. l'établissement a mis en place un processus et des procédures sous-jacentes pour la détection (par exemple, les «auto-évaluations du risque et des mécanismes de maîtrise», l'analyse des scénarios de risque) et le suivi des risques significatifs liés aux TIC concernés; et

    d. l'établissement dispose d'un système de notification des risques liés aux TIC qui fournisse des informations en temps utile à la direction générale et à l'organe de direction et qui permette à la direction générale et/ou à l'organe de direction d'évaluer et de surveiller si les plans et les mesures pris par l'établissement pour atténuer les risques liés aux TIC sont cohérents avec l'appétit pour le risque et/ou les seuils de tolérance approuvés (le cas échéant) et de surveiller les changements de risques significatifs liés aux TIC.

3.3.2 Cadre de gestion organisationnelle et de surveillance

50. Les autorités compétentes devraient évaluer la manière dont les rôles et les responsabilités applicables en matière de gestion des risques sont intégrés dans l'organisation interne pour gérer et surveiller les risques significatifs liés aux TIC détectés. À cet égard, les autorités compétentes devraient évaluer:

    a. si l'établissement a prévu des rôles et des responsabilités clairs pour la détection, l'évaluation, le suivi, l'atténuation, la déclaration et la surveillance du risque significatif lié aux TIC concerné;
    b. si les responsabilités et les rôles concernant le risque sont clairement notifiés, attribués et intégrés dans les secteurs (par exemple les lignes d'activité, l'informatique) et les processus concernés de l'organisation, notamment les rôles et responsabilités pour la collecte et le regroupement des informations sur les risques et leur déclaration à la direction générale et/ou à l'organe de direction;
    c. si les activités de gestion du risque lié aux TIC sont réalisées au moyen de ressources humaines et techniques suffisantes et à la hauteur de la mission. Pour évaluer la crédibilité des plans d'atténuation des risques applicables, les autorités compétentes devraient également évaluer si l'établissement a alloué des budgets suffisants et/ou d'autres ressources requises pour leur mise en œuvre;
    d. si l'organe de direction apporte un suivi et une réponse adéquats aux constatations importantes des fonctions de contrôle indépendant concernant le(s) risque(s) lié(s) aux TIC, en tenant compte de la délégation éventuelle de certains aspects à un comité, le cas échéant; et
    e. si les exceptions aux règlements et aux politiques applicables en matière de TIC sont enregistrées et font l'objet d'un contrôle et de rapports documentés par la fonction de contrôle indépendant en mettant l'accent sur les risques connexes.

3.3.3 Étendue et constatations des audits internes

51. Les autorités compétentes devraient évaluer si la fonction d'audit interne est efficace en ce qui concerne l'audit du cadre de contrôle du risque lié aux TIC applicable en examinant si :

    a. l'audit du cadre de contrôle du risque lié aux TIC respecte la qualité, le niveau de détail et la fréquence requis et est proportionnel à la taille, aux activités et au profil de risque lié aux TIC de l'établissement;
    b. le plan d'audit comprend des audits des risques essentiels liés aux TIC détectés par l'établissement;
    c. les constatations importantes de l'audit des TIC, notamment les mesures convenues, sont signalées à l'organe de direction; et
    d. les constatations des audits des TIC, notamment les mesures convenues, font l'objet d'un suivi et de rapports d'avancement examinés périodiquement par la direction générale et/ou le comité d'audit.

3.3.4 Contrôles des risques liés aux TIC qui sont spécifiques aux risques significatifs liés aux TIC détectés

52. En ce qui concerne les risques significatifs liés aux TIC détectés, les autorités compétentes devraient évaluer si l'établissement dispose de contrôles spécifiques pour y faire face. Les sections suivantes fournissent une liste non exhaustive des contrôles spécifiques à envisager lors de l'évaluation des risques significatifs détectés visés au point 3.2.3 qui ont été cartographiés dans les catégories de risque lié aux TIC suivantes:

a. risques pour la disponibilité et la continuité des TIC;
b. risques pour la sécurité des TIC;
c. risques liés au changement des TIC;
d. risques pour l'intégrité des données TIC;
e. risque lié à l'externalisation des TIC.

(a) Contrôles visant à gérer les risques significatifs pour la disponibilité et la continuité des TIC

53. En plus de vérifier les exigences visées dans les orientations de l'ABE sur le SREP (paragraphes 279 à 281), les autorités compétentes devraient évaluer si l'établissement dispose d'un cadre approprié pour détecter, comprendre, mesurer et atténuer les risques pour la disponibilité et la continuité des TIC.

54. Pour cette évaluation, les autorités compétentes devraient notamment examiner si le cadre:

a. recense les processus de TIC essentiels et les systèmes de TIC sous-jacents liés et qui devraient faire partie des programmes de résilience et de continuité de l'entreprise avec:

   i. une analyse complète des dépendances entre les processus opérationnels clés et les systèmes sous-jacents;

   ii. des objectifs de rétablissement pour les systèmes de TIC sous-jacents (généralement déterminés par l'entreprise et/ou la réglementation en matière de RTO et de RPO);

   iii. une planification d'urgence appropriée pour permettre la disponibilité, la continuité et le rétablissement des systèmes et services de TIC essentiels afin de réduire les perturbations des opérations de l'établissement dans un délai raisonnable;

b. tient compte de la résilience de l'entreprise, prévoit des politiques et des normes de continuité des activités et des contrôles opérationnels qui incluent:

   i. des mesures visant à éviter qu'un seul scénario, incident ou catastrophe ait une incidence à la fois sur les systèmes de production et sur les systèmes de rétablissement des TIC;

   ii. des procédures de sauvegarde et de rétablissement du système de TIC pour les logiciels et les données essentiels, qui garantissent que ces sauvegardes sont stockées dans un lieu sécurisé et suffisamment éloigné, de sorte qu'un incident ou une catastrophe ne puisse pas détruire ou corrompre ces données essentielles;

   iii. des solutions de surveillance pour détecter en temps utile les incidents portant atteinte à la disponibilité ou la continuité des TIC;

iv. un processus documenté de gestion et de remontée d'informations relatives aux incidents, qui fournisse également des orientations sur les différents rôles et responsabilités relatifs à la gestion et à la remontée des informations relatives aux incidents aux membres du ou des comités de crise et à la chaîne de commandement en cas d'urgence;

v. des mesures physiques visant à protéger l'infrastructure essentielle des TIC de l'établissement (par exemple les centres de données) contre les risques environnementaux (par exemple les inondations ou d'autres catastrophes naturelles) et à assurer un environnement d'exploitation approprié pour les systèmes de TIC (par exemple la climatisation);

vi. des processus, des rôles et des responsabilités afin de garantir que les systèmes et services de TIC externalisés soient également couverts par des solutions et des plans adéquats de résilience et de continuité de l'entreprise;

vii. des solutions de planification et de suivi des performance et des capacités des TIC pour les systèmes et services de TIC essentiels avec des exigences de disponibilité définies, de façon à détecter en temps utile les problèmes importants de performance et de capacité;

viii. des solutions pour protéger les activités ou les services essentiels liés à l'internet (par exemple les services bancaires électroniques), lorsque cela est approprié, contre le déni de service et d'autres cyberattaques visant à empêcher ou à perturber l'accès à ces activités et services.

c. teste des solutions de disponibilité et de continuité des TIC contre un certain nombre de scénarios réalistes, notamment les cyberattaques, les tests de commutation et les tests de sauvegarde pour les logiciels et les données essentiels qui:

i. soient planifiées, formalisés et documentés, et qui prévoient que les résultats des tests seront utilisés pour renforcer l'efficacité des solutions de disponibilité et de continuité des TIC;

ii. associent des parties prenantes et des fonctions au sein de l'organisation, telles que la direction des lignes d'activité, notamment les équipes responsables de la continuité des activités, des incidents et des interventions en cas de crise, ainsi que des parties prenantes externes concernées dans l'écosystème;

iii. associent de manière appropriée l'organe de direction et la direction générale (par exemple dans le cadre d'équipes de gestion de crise) et les informent des résultats des tests.

(b) Contrôles visant à gérer les risques significatifs pour la sécurité des TIC

55. Les autorités compétentes devraient évaluer si l'établissement dispose d'un cadre efficace pour détecter, comprendre, mesurer et atténuer les risques pour la sécurité des TIC. Lors de cette évaluation, les autorités compétentes devraient notamment examiner si ce cadre prévoit:

a. des rôles et des responsabilités clairement définis concernant:

i. la (les) personne(s) et/ou les comités qui sont responsables de la gestion quotidienne de la sécurité des TIC et de l'élaboration des politiques générales de sécurité des TIC, ou qui doivent

en rendre compte, en prêtant attention au besoin d'indépendance de ces personnes ou comités;

ii. la conception, la mise en œuvre, la gestion et le suivi des contrôles de sécurité des TIC;

iii. la protection des systèmes et des services de TIC essentiels en adoptant, par exemple, un processus d'évaluation de la vulnérabilité, une gestion des correctifs logiciels, une protection des points de terminaison (par exemple contre les virus malveillants), des outils de détection et de prévention des intrusions;

iv. la surveillance, la classification et la gestion des incidents de sécurité des TIC externes ou internes, notamment la réaction face aux incidents ainsi que le redémarrage et le rétablissement des systèmes et des services de TIC;

v. les évaluations régulières et préventives des menaces pour maintenir des contrôles de sécurité appropriés;

b. une politique de sécurité des TIC qui prend en considération les normes et les principes de sécurité des TIC internationalement reconnus et, le cas échéant, y adhère (par exemple le «principe du moindre privilège», qui consiste à limiter l'accès au niveau minimal qui permettra un fonctionnement normal de la gestion des droits d'accès, et le principe de la «défense en profondeur», qui consiste à concevoir une architecture de sécurité avec des mécanismes de sécurité sur plusieurs niveaux pour augmenter la sécurité du système dans son ensemble);

c. un processus visant à recenser les systèmes et les services de TIC et les exigences de sécurité proportionnelles qui reflètent les éventuels risques de fraude et/ou mauvais usages et/ou abus de données confidentielles ainsi que les attentes de sécurité documentées à respecter pour ces systèmes, services et données TIC recensés, alignés sur la tolérance au risque de l'établissement et surveillés pour une mise en œuvre correcte;

d. un processus documenté de gestion et de remontée d'informations relatives aux incidents de sécurité, qui fournit des orientations sur les différents rôles et responsabilités relatifs à la gestion et à la remontée des informations relatives aux incidents, aux membres du ou des comités de crise et à la chaîne de commandement en cas d'urgence pour la sécurité;

e. l'enregistrement des activités des utilisateurs et des administrateurs pour permettre un suivi efficace et la détection en temps utile des activités non autorisées ainsi qu'une intervention rapide face à de telles activités; pour mener des enquêtes techniques sur les incidents de sécurité ou y participer. L'établissement devrait avoir mis en place des politiques d'enregistrement qui définissent les types de journaux appropriés à garder et leur période de conservation;

f. des campagnes ou des initiatives de sensibilisation et d'information pour informer tous les niveaux de l'établissement sur l'utilisation sans risque et la protection des systèmes de TIC de l'établissement et les principaux risques liés à la sécurité des TIC (et autres) dont ils devraient avoir connaissance, en particulier en ce qui concerne les menaces cybernétiques existantes et évolutives (par exemple les virus informatiques, les éventuels abus ou attaques internes ou externes, les cyberattaques), et leur rôle dans l'atténuation des atteintes à la sécurité;

g. des mesures de sécurité physique adéquates (par exemple vidéosurveillance, alarme antieffraction, portes de sécurité) pour empêcher l'accès physique non autorisé aux systèmes de TIC essentiels et sensibles (par exemple les centres de données);

h. des mesures visant à protéger les systèmes de TIC contre les attaques perpétrées depuis l'internet (cyberattaques) ou d'autres réseaux externes (par exemple, les connexions télécom traditionnelles ou les connexions avec des partenaires fiables). Les autorités compétentes devraient examiner si le cadre de l'établissement prévoit:

   i. un processus et des solutions pour garder un inventaire complet et actualisé et une vue d'ensemble de tous les points de connexion du réseau offrant un accès vers l'extérieur (par exemple, les sites internet, les applications internet, le wifi, l'accès à distance) par lesquels des tiers pourraient entrer dans les systèmes internes des TIC;

   ii. des mesures de sécurité soigneusement gérées et étroitement surveillées (par exemple pare-feu, serveurs proxy, relais de courriers électroniques, antivirus et scanners de contenu) pour sécuriser le trafic entrant et sortant sur le réseau (par exemple le courrier électronique) et les connexions réseau externes par lesquelles des tiers pourraient entrer dans les systèmes internes des TIC;

   iii. des processus et des solutions pour sécuriser les sites web et les applications qui peuvent être directement attaqués depuis l'internet et/ou de l'extérieur, qui peuvent servir de point d'entrée dans les systèmes internes des TIC. En général, cela comprend une combinaison de pratiques reconnues de développement sécurisé, de durcissement du système de TIC et d'examen des points faibles et/ou la mise en œuvre de solutions de sécurité supplémentaires, comme par exemple les pare-feu d'applications, les systèmes de détection des intrusions (IDS) ou de prévention des intrusions (IPS);

   iv. des tests périodiques d'attaques contre la sécurité pour évaluer l'efficacité des mesures et des processus de sécurité des TIC externes et internes mis en œuvre. Ces tests devraient être effectués par du personnel et/ou des experts externes possédant les connaissances nécessaires et leurs résultats et conclusions être documentés et rapportés à la direction générale et/ou à l'organe de direction. Lorsque cela est nécessaire l'établissement devrait tirer des enseignements de ces tests afin d'améliorer davantage les contrôles et les processus de sécurité et/ou d'obtenir une meilleure assurance de leur efficacité.

(c) Contrôles visant à gérer les risques significatifs liés aux changements des TIC

56. Les autorités compétentes devraient évaluer si l'établissement dispose d'un cadre efficace pour détecter, comprendre, mesurer et atténuer les risques liés aux changements des TIC, proportionnel à la nature, à l'échelle et à la complexité des activités de l'établissement ainsi qu'au profil de risque lié aux TIC de l'établissement. Le cadre de l'établissement doit couvrir les risques liés au développement, au test et à l'approbation des changements intervenus dans les systèmes de TIC, notamment le développement ou la modification de logiciels avant leur migration vers l'environnement de production, et assurer une gestion adéquate du cycle de vie des TIC. Lors de cette évaluation, les autorités compétentes devraient notamment examiner si ce cadre prévoit:

   a. des processus documentés pour la gestion et le contrôle des changements apportés aux systèmes de TIC (par exemple la configuration et la gestion des correctifs) et des données (par exemple la correction des erreurs ou les corrections de données), assurant une gestion adéquate des risques liés aux TIC lors des changements importants des TIC susceptibles d'avoir une incidence significative sur le profil de risque ou l'exposition au risque de l'établissement;

b. un cahier des charges concernant la séparation des tâches requise pendant les différentes phases des processus de changement de TIC mis en œuvre (par exemple la conception et le développement de solutions, le test et l'approbation de nouveaux logiciels et/ou des changements de logiciels, la migration et la mise en œuvre dans l'environnement de production et la correction des bogues), avec un accent particulier sur les solutions mises en œuvre et la séparation des tâches établie pour gérer et contrôler les changements apportés aux systèmes et données TIC de production par le personnel responsable des TIC (par exemple les développeurs, les administrateurs du système des TIC, les administrateurs des bases de données) ou par toute autre partie (par exemple les utilisateurs commerciaux, les prestataires de services);

c. des environnements de test qui ressemblent adéquatement les environnements de production;

d. un inventaire des ressources des applications et des systèmes de TIC existants dans l'environnement de production, ainsi que l'environnement de test et de développement, de sorte que les changements requis (par exemple les mises à jour ou mises à niveau de versions, correctifs de systèmes, modifications de la configuration) puissent être correctement gérés, mis en œuvre et surveillés pour les systèmes de TIC concernés;

e. un processus de suivi et de gestion du cycle de vie des systèmes de TIC utilisés, afin de garantir qu'ils continuent de répondre aux exigences réelles en matière de gestion des risques et d'activités et de veiller à ce que les solutions et les systèmes de TIC utilisés soient toujours pris en charge par leurs fournisseurs; et que ce processus soit assorti de procédures appropriées de cycle de vie du développement logiciel (SDLC);

f. un système de contrôle du code source des logiciels et des procédures appropriées pour empêcher les modifications non autorisées du code source du logiciel développé en interne;

g. un processus visant à effectuer un examen de la sécurité et de la vulnérabilité des systèmes de TIC et des logiciels nouveaux ou ayant subi des modifications significatives, avant de les rendre disponibles dans l'environnement de production et de les exposer à d'éventuelles cyberattaques;

h. un processus et des solutions pour empêcher la divulgation non autorisée ou involontaire de données confidentielles lors du remplacement, de l'archivage, de la mise au rebut ou de la destruction des systèmes de TIC;

i. un processus indépendant de contrôle et de validation pour réduire les risques d'erreurs humaines lors des modifications des systèmes de TIC susceptibles d'avoir un effet négatif important sur la disponibilité, la continuité ou la sécurité de l'établissement (par exemple les changements importants à la configuration du pare-feu) ou sur la sécurité de l'établissement (par exemple les changements apportés aux pare-feu).

(d) Contrôles visant à gérer les risques significatifs pour l'intégrité des données TIC

57. Les autorités compétentes devraient évaluer si l'établissement dispose d'un cadre efficace pour détecter, comprendre, mesurer et atténuer le risque pour l'intégrité des données TIC, proportionnel à la nature, à l'échelle et à la complexité des activités de l'établissement ainsi qu'au profil de risque lié aux TIC de l'établissement. Le cadre de l'établissement devrait tenir compte des risques associés à la préservation de l'intégrité des données stockées et traitées par les systèmes de TIC. Lors de cette évaluation, les autorités compétentes devraient notamment examiner si le cadre prévoit:

    a. une politique qui définit les rôles et les responsabilités pour gérer l'intégrité des données dans les systèmes de TIC (par exemple un architecte de données, des délégués aux données[6], des dépositaires de données[7], des propriétaires/gestionnaires de données[8]) et fournit des orientations sur les données qui sont essentielles du point de vue de l'intégrité des données et qui devraient faire l'objet de contrôles spécifiques des TIC (par exemple des contrôles automatiques de validation des entrées, des contrôles de transfert de données, des rapprochements, etc.) ou d'examens (par exemple une vérification de la compatibilité avec l'architecture des données) dans les différentes phases du cycle de vie des données TIC;

    b. une architecture des données documentée, un modèle et/ou un dictionnaire de données qui a été validé par les parties prenantes concernées responsables des activités et de l'informatique pour favoriser la cohérence nécessaire des données dans tous les systèmes de TIC et pour veiller à ce que l'architecture des données, le modèle et/ou le dictionnaire de données restent alignés sur les besoins de l'entreprise et les besoins en matière de gestion des risques;

    c. une stratégie concernant l'utilisation autorisée du *End-User Computing* (EUC), en particulier en ce qui concerne l'identification, l'enregistrement et la documentation de solutions EUC importantes (par exemple lors du traitement de données importantes) et les niveaux de sécurité attendus pour empêcher des modifications non autorisées, à la fois dans l'outil lui-même, ainsi que dans les données stockées dans celui-ci;

    d. des processus documentés de traitement des exceptions pour résoudre les problèmes d'intégrité des données TIC observés, en fonction de leur importance et de leur sensibilité.

58. Pour les établissements sous contrôle qui relèvent des «Principes aux fins de l'agrégation des données sur les risques et de la notification des risques» du Comité de Bâle[9], les autorités compétentes devraient contrôler l'analyse des risques par les établissements de leurs pratiques de notification des risques et de leurs capacités d'agrégation des données par rapport aux principes et à la documentation préparée à ce sujet, en prenant en considération le délai de mise en œuvre et les dispositions transitoires prévus dans ces principes.

[6] Un délégué aux données est responsable du traitement et de l'utilisation des données.

[7] Un dépositaire de données est responsable de la conservation, du transport et du stockage des données en toute sécurité.

[8] Un gestionnaire de données est responsable de la gestion et de l'adéquation des éléments de données – à la fois du contenu et des métadonnées.

[9] Comité de Bâle sur le contrôle bancaire, «Principes aux fins de l'agrégation des données sur les risques et de la notification des risques», janvier 2013, accessible à l'adresse suivante: http://www.bis.org/publ/bcbs239.pdf.

(e) Contrôles visant à gérer les risques significatifs liés à l'externalisation des TIC

59. Les autorités compétentes devraient évaluer si la stratégie d'externalisation de l'établissement, répondant aux exigences énoncées dans les orientations du CECB relatives à l'externalisation (2006) et dans la lignée de l'exigence énoncée au paragraphe 85, point d), des orientations de l'ABE sur le SREP, s'applique de manière adéquate à l'externalisation des TIC, y compris à l'externalisation intragroupe (fourniture de services de TIC au sein du groupe). Lors de l'évaluation des risques d'externalisation des TIC, les autorités compétentes devraient prendre en considération le fait que ces risques peuvent également être couverts dans le cadre de l'évaluation des risques opérationnels inhérents visés au paragraphe 240, point j), des orientations de l'ABE sur le SREP afin d'éviter toute duplication du travail et tout double comptage.

60. En particulier, les autorités compétentes devraient évaluer si l'établissement dispose d'un cadre efficace pour détecter, comprendre et mesurer le risque d'externalisation des TIC et, en particulier, d'un environnement de contrôle pour atténuer les risques liés aux services de TIC significatifs externalisés , qui sont proportionnels à la taille, aux activités et au profil de risque lié aux TIC de l'établissement et comprennent:

    a. une évaluation de l'incidence de l'externalisation des TIC sur la gestion des risques de l'établissement liée au recours à des prestataires de services (par exemple les prestataires de services dans le nuage) et à leurs services pendant le processus de passation de marché, qui est documentée et prise en considération par la direction générale ou l'organe de direction avant de décider d'externaliser les services ou non. L'établissement devrait examiner les politiques de gestion des risques liés aux TIC ainsi que les contrôles et l'environnement de contrôle des TIC du prestataire de services afin de s'assurer qu'ils respectent les objectifs internes de gestion des risques et l'appétit pour le risque de l'établissement. Cet examen devrait être périodiquement actualisé au cours de la période d'externalisation contractuelle, en tenant compte des caractéristiques des services externalisés;

    b. un suivi des risques liés aux TIC associés aux services externalisés pendant la période d'externalisation contractuelle dans le cadre de la gestion des risques de l'établissement, qui alimente les notifications de l'établissement sur sa gestion des risques liés aux TIC (par exemple les rapports sur la continuité des activités, les rapports de sécurité);

    c. un suivi et une comparaison des niveaux de service reçus avec les niveaux de service contractuellement convenus qui devraient faire partie du contrat d'externalisation ou de l'accord sur le niveau de service (ANS); et

    d. du personnel, des ressources et des compétences nécessaires pour surveiller et gérer les risques liés aux TIC associés aux services externalisés.

3.4 Résumé des constatations et notation

61. À la suite de l'évaluation susvisée, les autorités compétentes devraient se former un avis sur le risque lié aux TIC de l'établissement. Cet avis devrait être reflété dans un résumé des constatations que les autorités compétentes devraient prendre en considération lors de l'attribution de la note de risque opérationnel, conformément au tableau 6 des orientations de l'ABE sur le SREP. Les autorités compétentes devraient fonder leur opinion sur les risques significatifs liés aux TIC en tenant compte des éléments suivants dans l'évaluation des risques opérationnels:

a. Considérations concernant le risque

   i. profil de risque lié aux TIC et expositions de l'établissement à ce risque;
   ii. systèmes et services de TIC essentiels recensés; et
   iii. importance du risque lié aux TIC concernant les systèmes de TIC essentiels.

b. Considérations concernant la gestion et les mécanismes de maîtrise

   i. la politique et la stratégie de l'établissement en matière de gestion du risque lié aux TIC sont cohérentes avec sa stratégie globale et son appétence au risque;
   ii. le cadre organisationnel relatif à la gestion du risque lié aux TIC est solide et doté de responsabilités claires et d'une séparation des tâches claire entre preneurs de risques et fonctions de gestion et de contrôle;
   iii. les systèmes de mesure, de suivi et de déclaration du risque lié aux TIC sont appropriés; et
   iv. les cadres de contrôle du risque lié aux TIC sont sains.

62. Si les autorités compétentes jugent que le risque lié au TIC est significatif et que l'autorité compétente décide d'évaluer et de noter ce risque en tant que sous-catégorie du risque opérationnel, les considérations relatives à la note en matière de risque lié aux TIC figurant dans le tableau ci-dessous (tableau 1) doivent être appliquées.

Tableau 1: considérations prudentielles pour l'attribution d'une note au risque lié aux TIC

Note en matière de risque	Opinion prudentielle	Considérations concernant le risque inhérent	Considérations concernant l'adéquation de la gestion et des mécanismes de maîtrise
1	Il n'existe aucun risque perceptible d'une incidence prudentielle significative sur l'établissement compte tenu du niveau de risque inhérent et de la gestion et des mécanismes de maîtrise du risque.	• Les sources d'information à prendre en considération conformément au paragraphe 37 ne révèlent aucune exposition significative au risque lié aux TIC. • La nature du profil de risque lié aux TIC de l'établissement, combinée à l'examen des systèmes de TIC essentiels et aux risques significatifs liés aux TIC pour les systèmes et services de TIC, ne révèle aucun risque significatif lié aux TIC.	• La politique et la stratégie de l'établissement en matière de risque lié aux TIC sont proportionnelles à sa stratégie globale et son appétence au risque. • Le cadre organisationnel relatif au risque lié aux TIC est solide et doté de responsabilités claires et d'une séparation des tâches claire entre preneurs de risques et fonctions de gestion et de contrôle. • Les systèmes de mesure, de suivi et de déclaration du risque lié aux TIC sont appropriés. • Le cadre de contrôle du risque lié aux TIC est sain.
2	Il existe un risque faible d'une incidence prudentielle significative sur l'établissement compte tenu du niveau de risque inhérent et de la gestion et des mécanismes de maîtrise du risque.	• Les sources d'information à prendre en considération conformément au paragraphe 37 ne révèlent aucune exposition significative au risque lié aux TIC. • La nature du profil de risque lié aux TIC de l'établissement, combinée à l'examen des systèmes de TIC essentiels et aux risques significatifs liés aux TIC pour les systèmes et services de TIC, révèle une exposition limitée au risque lié aux TIC (par exemple, pas plus de 2 sur 5 des catégories de risque lié aux TIC prédéfinies).	
3	Il existe un risque moyen d'une incidence prudentielle significative sur l'établissement compte tenu du niveau de risque inhérent et de la gestion et	• Les sources d'information à prendre en considération conformément au paragraphe 37 révèlent une possible exposition significative au risque lié aux TIC. • La nature du profil de risque lié aux TIC de l'établissement, combinée à l'examen des systèmes de TIC essentiels et aux risques significatifs liés aux TIC	

	des mécanismes de maîtrise du risque.	pour les systèmes et services de TIC, révèle une exposition accrue au risque lié aux TIC (par exemple, au moins 3 sur 5 des catégories de risque lié aux TIC prédéfinies).	
4	Il existe un risque élevé d'une incidence prudentielle significative sur l'établissement compte tenu du niveau de risque inhérent et de la gestion et des mécanismes de maîtrise du risque.	• Les sources d'information à prendre en considération conformément au paragraphe 37 révèlent de multiples indications d'une exposition significative au risque lié aux TIC. • La nature du profil de risque lié aux TIC de l'établissement, combinée à l'examen des systèmes de TIC essentiels et aux risques significatifs liés aux TIC pour les systèmes et services de TIC, révèle une exposition élevée au risque lié aux TIC (par exemple, 4 ou 5 sur 5 des catégories de risque lié aux TIC prédéfinies).	

Annexe – Taxonomie du risque lié aux TIC

5 catégories de risque lié aux TIC accompagnées d'une liste non exhaustive de risques liés aux TIC ayant potentiellement une gravité élevée et/ou une incidence sur les opérations, la réputation ou la situation financière [de l'établissement]

Catégories de risque lié aux TIC	Risques liés aux TIC (liste non exhaustive[10])	Description du risque	Exemples
Risques pour la disponibilité et la continuité des TIC	Gestion des capacités inadéquate	Un manque de ressources (par exemple de matériel, de logiciels, de personnel, de prestataires de services) peut entraîner une incapacité à adapter le service pour répondre aux besoins de l'entreprise, aux interruptions du système, à la dégradation du service et/ou aux erreurs opérationnelles.	• Un manque de capacités risque de porter atteinte à la vitesse de transmission et la disponibilité du réseau (internet) pour des services tels que la banque en ligne. • Un manque de personnel (interne ou tiers) peut entraîner des interruptions du système et/ou des erreurs opérationnelles.
	Pannes du système de TIC	Indisponibilité en raison de pannes du matériel.	• Panne/dysfonctionnement du stockage (disques durs), du serveur ou d'autres équipements TIC, en raison par exemple d'un manque de maintenance.
		Indisponibilité en raison de pannes et de bogues du logiciel.	• Une boucle fermée dans le logiciel de l'application empêche l'exécution de l'opération. • Pannes résultant de l'utilisation continue de systèmes et de solutions de TIC obsolètes qui ne répondent plus aux exigences actuelles de disponibilité et de résilience et/ou ne sont plus pris en charge par leurs fournisseurs.
	Inadéquation des plans de continuité et de rétablissement après un incident	Échec des solutions de disponibilité et/ou de continuité des TIC planifiées et/ou du rétablissement après un incident (par exemple un centre de données de rétablissement de secours) lorsqu'elles sont activées en réponse à un incident.	• Des différences de configuration entre les centres de données principal et secondaire peuvent entraîner l'incapacité du centre de données de secours à assurer la continuité planifiée du service.

[10] Les risques liés aux TIC sont répertoriés dans la catégorie de risque sur laquelle ils ont le plus d'incidence, mais ils peuvent avoir des conséquences sur d'autres catégories de risque.

Catégories de risque lié aux TIC	Risques liés aux TIC (liste non exhaustive[10])	Description du risque	Exemples
	Cyberattaques causant des perturbations ou des destructions	Attaques à des fins diverses (par exemple activisme, chantage) qui entraînent une surcharge des systèmes et du réseau, empêchant les utilisateurs légitimes d'accéder aux services informatiques en ligne.	• Des attaques de déni de service répandues sont menées au moyen d'une multitude de systèmes informatiques sur internet sous le contrôle d'un pirate informatique qui envoie une grande quantité de demandes de service apparemment légitimes à des services en ligne (par exemple la banque en ligne).
Risques pour la sécurité des TIC	Cyberattaques et autres attaques externes à partir des TIC	Attaques menées à partir d'internet ou de réseaux externes à des fins diverses (par exemple fraude, espionnage, activisme/sabotage, cyberterrorisme) en utilisant des techniques variées (par exemple l'ingénierie sociale, les tentatives d'intrusion par l'exploitation des failles, le déploiement de logiciels malveillants) entraînant une prise de contrôle des systèmes internes de TIC.	Différents types d'attaques: • APT (menace persistante avancée) pour prendre le contrôle de systèmes internes ou voler des informations (par exemple des informations liées au vol d'identité ou des informations sur les cartes de crédit). • Logiciel malveillant (par exemple rançongiciel) qui crypte les données dans un but de chantage. • Infection de systèmes de TIC internes par des chevaux de Troie pour commettre des actions malveillantes dans le système de manière dissimulée. • Exploitation des failles du système de TIC et/ou des applications (web) (par exemple injection SQL, etc.) pour accéder au système interne de TIC.
		Exécution d'opérations de paiement frauduleuses par des pirates informatiques qui cassent ou qui contournent la sécurité des services bancaires en ligne et des services de paiement et/ou qui attaquent et exploitent les failles de la sécurité dans les systèmes de paiement internes de l'établissement.	• Attaques contre les services de banque en ligne ou de paiement dans le but d'exécuter des opérations non autorisées. • Création et envoi d'opérations de paiement frauduleuses depuis les systèmes de paiement internes de l'établissement (par exemple messages SWIFT frauduleux).
		Exécution d'opérations sur titres frauduleuses par des pirates informatiques qui cassent ou qui contournent la	• Attaques «*pump and dump*» permettant aux pirates d'accéder aux comptes de titres en ligne des clients

Catégories de risque lié aux TIC	Risques liés aux TIC (liste non exhaustive[10])	Description du risque	Exemples
		sécurité des services bancaires en ligne, lesquels donnent également accès aux comptes de titres des clients.	et de placer des ordres d'achat ou de vente frauduleux pour influencer les cours et/ou réaliser des gains à partir de positions sur titres détenues dans le portefeuille.
		Attaques sur les connexions de communication et les conversations de toutes sortes ou des systèmes de TIC dans le but de collecter des informations et/ou de commettre des fraudes.	• Écoute/interception de la transmission non protégée de données d'authentification en texte clair.
	Sécurité interne inadéquate des TIC	Accès non autorisé aux systèmes de TIC essentiels de l'établissement depuis l'intérieur de celui-ci à des fins diverses (par exemple fraude, exécution et dissimulation d'activités commerciales illicites, vol de données, activisme/sabotage) à l'aide de techniques variées (par exemple abus et/ou augmentation de privilèges, vol d'identité, ingénierie sociale, exploitation des points faibles des systèmes de TIC, déploiement de logiciels malveillants).	• Installation d'enregistreurs de trajectoires de touches (enregistreurs de clés) pour voler les identifiants d'utilisateurs et les mots de passe et obtenir un accès non autorisé à des données confidentielles et/ou commettre des fraudes. • Craquer/deviner des mots de passe faciles pour obtenir des droits d'accès illégitimes ou d'un haut niveau. • L'administrateur du système utilise des systèmes d'exploitation ou des utilitaires de base de données (pour modifier directement la base de données) afin de commettre des fraudes.
		Manipulations informatiques non autorisées en raison de procédures et pratiques de gestion de l'accès aux TIC inadéquates.	• Non-désactivation ou non-suppression des comptes inutiles tels que ceux du personnel ayant changé de fonctions et/ou quitté l'établissement, notamment des invités ou des fournisseurs qui n'ont plus besoin d'accès, offrant un accès non autorisé aux systèmes de TIC. • Octroi de droits et privilèges d'accès excessifs, permettant des accès non autorisés et/ou la dissimulations d'activités illicites.
		Menaces pour la sécurité dues à un manque de sensibilisation à la sécurité, ce qui fait que les	• Employés manipulés pour apporter leur aide à une attaque (c.-à-d. ingénierie sociale).

Catégories de risque lié aux TIC	Risques liés aux TIC (liste non exhaustive[10])	Description du risque	Exemples
		travailleurs ne comprennent pas, négligent ou ne respectent pas les politiques et les procédures de sécurité des TIC.	• Mauvaises pratiques concernant les informations d'identification: partage de mots de passe, utilisation de mots de passe «faciles» à deviner, utilisation du même mot de passe à de nombreuses fins différentes, etc. • Stockage de données confidentielles non cryptées sur des ordinateurs portables et des solutions de stockage de données à puce (par exemple clés USB) qui peuvent être perdus ou volés.
		Stockage ou transfert non autorisé d'informations confidentielles en dehors de l'établissement.	• Vol, divulgation délibérée ou transmission d'informations confidentielles à des personnes non autorisées ou au public.
	Inadéquation de la sécurité physique des TIC	Mauvaise utilisation ou vol de ressources TIC par un accès physique entraînant des dégâts, des pertes de ressources ou de données ou pour rendre possibles d'autres menaces.	• Entrée par effraction dans des immeubles de bureaux et/ou des centres de données pour y voler des équipements informatiques (par exemple ordinateurs, ordinateurs portables, solutions de stockage) et/ou copier des données en accédant physiquement aux systèmes de TIC.
		Dégâts volontaires ou accidentels infligés à des ressources physiques des TIC par des actes de terrorisme, des accidents ou des manipulations malheureuses/erronées provoqués par le personnel de l'établissement et/ou des tiers (fournisseurs, réparateurs).	• Terrorisme physique (bombes posées par des terroristes) ou sabotage des ressources TIC. • Destruction du centre de données par le feu, des fuites d'eau ou d'autres facteurs.
		La protection physique insuffisante contre les catastrophes naturelles entraîne une destruction partielle ou complète des systèmes de TIC/centres de données par des catastrophes naturelles.	• Tremblements de terre, vagues de chaleur, tempêtes, fortes tempêtes de neige, inondations, incendies, foudre.
Risques liés au changement	Contrôles inadéquats des changements	Incidents causés par des erreurs ou des failles non détectées à la suite de changements (par exemple effets imprévus d'un changement ou changement mal	• Mise en production de logiciels insuffisamment testés ou changements de configuration ayant des effets indésirables inattendus sur les données (par

Catégories de risque lié aux TIC	Risques liés aux TIC (liste non exhaustive[10])	Description du risque	Exemples
des TIC	apportés au système de TIC et du développement des TIC.	géré en raison d'un manque de tests ou de pratiques inappropriées de gestion du changement) apportés par exemple à des logiciels, systèmes et données TIC.	exemple la corruption, la suppression de données) et/ou sur les performances du système de TIC (par exemple panne, dégradation des performances). • Changements incontrôlés des systèmes ou des données TIC dans l'environnement de production. • Mise en production de systèmes de TIC et d'applications internet mal sécurisés, permettant aux pirates d'attaquer les services internet fournis et/ou de briser les systèmes internes de TIC. • Changements incontrôlés dans le code source d'un logiciel développé en interne. • Tests insuffisants en raison de l'absence d'environnements d'essai adéquats.
	Architecture des TIC inadéquate	Une gestion défaillante de l'architecture des TIC lors de la conception, de l'élaboration et de la maintenance des systèmes de TIC (par exemple logiciel, matériel, données) peut conduire, au fil du temps, à des systèmes complexes, difficiles, coûteux à gérer et rigides qui ne correspondent plus suffisamment aux besoins de l'entreprise et ne répondent plus aux exigences réelles de gestion des risques.	• Mauvaise gestion des changements apportés aux systèmes, aux logiciels et/ou aux données TIC sur une longue période, conduisant à des systèmes et des architectures TIC complexes, hétérogènes et difficiles à gérer, entraînant de nombreux effets négatifs sur la gestion des risques et l'entreprise (par exemple manque de flexibilité et d'agilité, incidents et pannes des TIC, coûts d'exploitation élevés, affaiblissement de la sécurité et de la résilience des TIC, réduction de la qualité des données et des capacités de notification). • Personnalisation et extension excessives des logiciels commerciaux avec des logiciels développés en interne, ce qui entraîne l'incapacité de mettre en place les futures versions et mises à niveau du logiciel commercial et le risque qu'il ne soit plus pris en charge par le vendeur.
	Gestion	Absence d'inventaire adéquat de toutes les ressources	• Systèmes TIC non corrigés et obsolètes qui risquent

Catégories de risque lié aux TIC	Risques liés aux TIC (liste non exhaustive[10])	Description du risque	Exemples
	inadéquate du cycle de vie et des correctifs	TIC qui soutiennent, et se combinent avec, des bonnes pratiques de gestion du cycle de vie et des correctifs. Cela conduit à des systèmes de TIC mal corrigés (et donc plus vulnérables) et obsolètes qui risquent de ne pas prendre en charge les besoins en matière de gestion des risques et les besoins de l'entreprise.	d'avoir une incidence négative sur la gestion de l'entreprise et des risques (par exemple manque de souplesse et d'agilité, pannes de TIC, affaiblissement de la sécurité et de la résilience des TIC).
Risques pour l'intégrité des données des TIC	Dysfonctionnement dans le traitement ou la gestion des données TIC	En cas d'erreurs ou de pannes du système, de la communication et/ou de l'application, ou bien d'exécution erronée du processus d'extraction, de transfert et de chargement (ETL), les données pourraient être corrompues ou perdues.	• Erreur du système informatique dans le traitement par lots, provoquant des soldes incorrects dans les comptes bancaires de la clientèle. • Exécution erronée de requêtes • Perte de données due à une erreur de réplication de données (sauvegarde).
	Mauvaise conception des contrôles de validation des données dans les systèmes de TIC	Erreurs dues à l'absence ou à l'inefficacité des contrôles d'entrée et d'acceptation automatiques de données (par exemple pour les données de tiers utilisées), au transfert de données, au traitement et aux contrôles de sortie dans les systèmes de TIC (par exemple les contrôles de validité des entrées, les rapprochements de données).	• Insuffisance ou invalidité du formatage/de la validation des entrées de données dans les applications et/ou les interfaces utilisateur. • Absence de contrôles de rapprochement des données sur les sorties • Absence de contrôles des processus d'extraction de données exécutés (par exemple requêtes introduites dans une base de données) produisant des données erronées. • Utilisation de données externes défectueuses.
	Modifications de données mal contrôlées dans les systèmes de TIC de production.	Erreurs de données introduites en raison du manque de contrôles de l'exactitude et de la justification des manipulations des données effectuées dans la production des systèmes de TIC	• Les développeurs ou les administrateurs de bases de données accèdent directement aux données et les modifient dans les systèmes de TIC de production de manière non contrôlée, par exemple dans le cas d'un incident de TIC.
	Mauvaise conception et/ou gestion de	Une mauvaise gestion de l'architecture des données, des modèles de données, des flux de données ou des dictionnaires de données risque d'aboutir à plusieurs	• Existence de différentes bases de données clients par produit ou par branche d'activité proposant des définitions et des champs de données différents, ce

Catégories de risque lié aux TIC	Risques liés aux TIC (liste non exhaustive[10])	Description du risque	Exemples
	l'architecture des données, des flux de données, des modèles de données ou des dictionnaires de données	versions des mêmes données dans les systèmes de TIC, sans aucune cohérence en raison de l'application différente des modèles de données ou des définitions de données, et/ou des différences dans le processus sous-jacent de génération et de modification des données.	qui rend impossible le rapprochement des données clients intégrées et complique leur comparaison au niveau de l'ensemble de l'établissement financier ou du groupe.
Risques liés à l'externalisation des TIC	Résilience insuffisante des services proposés par des tiers ou une autre entité du groupe	Indisponibilité de services de TIC , de services de télécommunication et de services publics clés externalisés. Perte ou corruption de données clés/sensibles confiées au prestataire de services	• Indisponibilité des services de base en raison de défaillances dans les systèmes ou applications de TIC (externalisés) des prestataires. • Perturbation des liaisons de télécommunication • Coupure de l'alimentation électrique
	Gouvernance inadéquate de l'externalisation	Dégradation ou pannes majeures des services en raison de processus de préparation ou de contrôle inefficaces du prestataire des services externalisés. Une gouvernance inefficace de l'externalisation risque d'entraîner un manque de compétences et de capacités nécessaires pour détecter, évaluer, atténuer et surveiller les risques liés aux TIC et peut limiter les capacités opérationnelles de l'établissement.	• Faiblesse des procédures de traitement des incidents, des mécanismes de contrôle contractuels et des garanties intégrées au contrat du prestataire de services qui augmentent la dépendance aux tiers et aux fournisseurs. • Des contrôles inadéquats de la gestion du changement concernant l'environnement des TIC du prestataire de services peuvent entraîner une dégradation ou une défaillance majeure du service.
	Sécurité insuffisante d'un tiers ou d'une autre entité du groupe	Piratage des systèmes de TIC des prestataires de services tiers, ayant une incidence directe sur les services externalisés ou sur des données clés/confidentielles stockées chez le prestataire de services. Accès non autorisé du personnel du prestataire de services à des données clés/sensibles stockées chez le prestataire de services	• Piratage des prestataires de services par des criminels ou des terroristes pour trouver un point d'accès aux systèmes de TIC de l'établissement ou pour accéder à des données clés ou sensibles stockées chez le prestataire de services ou pour détruire ces données. • Des personnes malveillantes du côté du prestataire de services essaient de voler et de vendre des données sensibles.