boulevard de Berlaimont 14 – BE-1000 Bruxelles
tél. +32 2 221 48 66
numéro d'entreprise : 0203.201.340
RPM Bruxelles
www.nbb.be

BanqueNationaleBank
DE BELGIQUE VAN BELGIË
Eurosystem

Circulaire

Bruxelles, le 23 novembre 2021

Référence : NBB_2021_26

votre correspondant :
Thomas Plomteux
tél. +32 2 221 21 97
thomas.plomteux@nbb.be

Reporting en matière de risques opérationnels et de sécurité liés aux services de paiement pour les établissements de paiement et les établissements de monnaie électronique

Champ d'application

Les établissements de paiement de droit belge, les établissements de paiement agrégateurs de compte enregistrés de droit belge, les établissements de paiement limités de droit belge, les établissements de monnaie électronique de droit belge, les établissements de monnaie électronique limités de droit belge.

Résumé/Objectif

La présente circulaire définit les modalités de respect de l'obligation de reporting imposée aux établissements de paiement et aux établissements de monnaie électronique par l'article 50, § 2, de la loi du 11 mars 2018[1]. La présente circulaire entre en vigueur le 1er janvier 2022 et remplace la circulaire NBB_2020_24, qui sera abrogée à cette même date.

1 La loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement, *Moniteur belge* du 26 mars 2018 (ci-après « la loi du 11 mars 2018 »).

Madame,
Monsieur,

Par la présente circulaire, la Banque nationale de Belgique (ci-après la «Banque») entend préciser l'obligation de reporting imposée par l'article 50, § 2, de la loi du 11 mars 2018.

Conformément à l'article 50, § 2, de la loi du 11 mars 2018, il est requis d'adresser un reporting à l'autorité de contrôle concernant «une évaluation à jour et exhaustive des risques opérationnels et de sécurité liés aux services de paiement que les établissements fournissent et des informations sur le caractère adéquat des mesures d'atténuation de ces risques ainsi que les mécanismes de contrôle mis en œuvre pour faire face à ces risques».

Par la présente circulaire, la Banque entend préciser aux établissements de paiement de droit belge, aux établissements de paiement agrégateurs de compte enregistrés de droit belge, aux établissements de paiement limités de droit belge, aux établissements de monnaie électronique de droit belge et aux établissements de monnaie électronique limités de droit belge, ses attentes concernant le rapport à transmettre chaque année.

Ces établissements doivent remettre une évaluation détaillée et motivée des risques opérationnels et de sécurité liés tant aux services de paiement déjà existants qu'aux services de paiement qui devraient être disponibles dans l'année à venir. Ceci implique ce qui suit.

1. L'évaluation de chaque risque décelé doit comprendre les éléments suivants:

   - une description du risque décelé, y compris ses conséquences pour l'établissement et ses clients s'il se concrétise;
   - les niveaux de risque inhérents, avec une estimation de leur probabilité et de leur incidence sur l'établissement;
   - les contrôles d'atténuation du risque décelé déjà en place, y compris une description de leur effet sur le niveau de risque de l'établissement;
   - le niveau de risque résiduel une fois que les mesures d'atténuation sont mises en œuvre;
   - les mesures détectées qui restent à mettre en œuvre pour améliorer l'efficacité des contrôles, le cas échéant, et la planification de leur mise en œuvre.

2. Les établissements fournissent une évaluation de leur respect des orientations de l'ABE sur la gestion des risques liés aux TIC et à la sécurité qui ont été introduites dans la circulaire NBB_2020_23[2]. Cette évaluation doit présenter une description des dispositions de ces orientations avec lesquelles l'établissement n'est pas en conformité et une évaluation de l'effet de cette non-conformité sur le niveau de risque de l'établissement.
3. Les établissements décrivent les évolutions qui ont eu lieu depuis la présentation précédente du rapport (ou depuis l'octroi de l'agrément par la Banque).

2 Les directives de l'ABE auxquelles renvoie cette circulaire précisent du reste que les risques opérationnels dans le contexte des services de paiement peuvent être intérprétés comme étant principalement des risques liés aux TIC et à la sécurité, étant donné le caractère généralement électronique de ces services de paiement.

Afin que ce reporting soit d'une qualité suffisamment élevée et en vue de soutenir au mieux les établissements dans l'accomplissement de leur obligation de reporting, la Banque mettra chaque année à la disposition des établissements relevant du champ d'application des questionnaires standardisés sur les risques IT ainsi qu'une instruction pratique. Les questionnaires porteront plus précisément sur l'exposition inhérente de ces établissements à plusieurs catégories de risque lié aux TIC[3] ainsi que sur les mesures d'atténuation et les contrôles correspondants dans une série de domaines de contrôle du risque lié aux TIC[4]. De plus, compte tenu du principe de proportionnalité, ces questionnaires pourront différer d'un établissement à l'autre, par exemple en fonction de la taille et de l'organisation interne de l'établissement ainsi que de l'ampleur, de la complexité et du degré de risque des services et des produits que les établissements financiers proposent ou prévoient de proposer.

Les établissements sont censés remplir ces questionnaires chaque année de façon suffisamment complète et critique. Le cas échéant, et si les établissements donnent suite de manière adéquate aux éventuelles demandes d'information et/ou de documentation complémentaires, la Banque considérera que les réponses à ce questionnaire sont suffisantes pour satisfaire à l'obligation légale de reporting.

La présente circulaire sera d'application à partir du 1er janvier 2022.

Une copie de la présente circulaire est adressée au(x) commissaire(s), réviseur(s) agréé(s) de votre établissement.

Je vous prie d'agréer, Madame, Monsieur, l'assurance de ma considération très distinguée.

p.p. Pierre Wunsch
Gouverneur

Steven Vanackere
Vice-gouverneur

3 Cela peut inclure les catégories suivantes : risque pour la disponibilité et la continué des TIC, risque pour la sécurité des TIC, risque lié au changement des TIC, risque pour l'intégrité des données TIC et risque lié à l'externalisation des TIC.

4 Cela peut inclure les domaines suivants : gouvernance des TIC, organisation des TIC et externalisation des TIC, gestion des risques liés aux TIC, gestion de la sécurité des TIC, gestion des activités de TIC, acquisition et développement de logiciels et gestion de projets, gestion de la qualité des données, gestion de la continuité des TIC, reporting sur les TIC et audit interne des TIC.