DOC 56 **0610/009**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

10 april 2025

WETSVOORSTEL

houdende het toezicht op aanbieders van financiële berichtendiensten

Tekst aangenomen in tweede lezing

door de commissie voor Financiën en Begroting

Zie:

Doc 56 **0610/ (2024/2025)**:
001: Wetsvoorstel van de heer Van den Heuvel c.s.
002: Advies van de Raad van State.
003: Amendementen.
004: Verslag van de eerste lezing.
005: Artikelen aangenomen in eerste lezing.
006 en 007: Amendementen.
008: Verslag van de tweede lezing.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

10 avril 2025

PROPOSITION DE LOI

relative à la surveillance des fournisseurs de services de messagerie financière

Texte adopté en deuxième lecture

par la commission des Finances et du Budget

Voir:

Doc 56 **0610/ (2024/2025)**:
001: Proposition de loi de M. Van den Heuvel et consorts.
002: Avis du Conseil d'État.
003: Amendements.
004: Rapport de la première lecture.
005: Articles adoptés en première lecture.
006 et 007: Amendements.
008: Rapport de la deuxième lecture.

01407

N-VA	:	*Nieuw-Vlaamse Alliantie*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
PS	:	*Parti Socialiste*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Les Engagés	:	*Les Engagés*
Vooruit	:	*Vooruit*
cd&v	:	*Christen-Democratisch en Vlaams*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Open Vld	:	*Open Vlaamse liberalen en democraten*
DéFI	:	*Démocrate Fédéraliste Indépendant*

Afkorting bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 56 0000/000	*Parlementair document van de 56e zittingsperiode + basisnummer en volgnummer*	*DOC 56 0000/000*	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*
QRVA	*Schriftelijke Vragen en Antwoorden*	*QRVA*	*Questions et Réponses écrites*
CRIV	*Voorlopige versie van het Integraal Verslag*	*CRIV*	*Version provisoire du Compte Rendu Intégral*
CRABV	*Beknopt Verslag*	*CRABV*	*Compte Rendu Analytique*
CRIV	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*	*CRIV*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN	*Plenum*	*PLEN*	*Séance plénière*
COM	*Commissievergadering*	*COM*	*Réunion de commission*
MOT	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT*	*Motions déposées en conclusion d'interpellations (papier beige)*

HOOFDSTUK 1

Doel – definities – toepassingsgebied

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2

§ 1. Met het oog op de bescherming van de goede werking, de soliditeit en de doelmatigheid van de verrekenings-, vereffenings- en betalingssystemen evenals van de soliditeit van het financieel stelsel in het algemeen, regelt deze wet de activiteiten van en het toezicht door de Nationale Bank van België op in België gevestigde aanbieders van financiële berichtendiensten.

§ 2. De opdrachten die deze wet aan de Nationale Bank van België toevertrouwt, maken een taak uit zoals bedoeld in artikel 8 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België.

§ 3. Onverminderd het bepaalde in artikel 8, § 2, van de wet van 22 februari 1998 tot vastelling van het organiek statuut van de Nationale Bank van België, kan de Nationale Bank van België de verwachtingen inzake naleving van deze wet en van de ter uitvoering ervan genomen besluiten en reglementen verduidelijken aan de hand van mededelingen, richtsnoeren en circulaires.

Art. 3

Voor de toepassing van deze wet wordt verstaan onder:

1° wet van 22 februari 1998: de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België;

2° wet van 25 april 2014: de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen;

3° de Bank: de Nationale Bank van België, namelijk de instelling waarvan het statuut beheerst wordt door de wet van 22 februari 1998, hierna “de Bank”;

4° financiële berichtendiensten: diensten die financiële entiteiten en overheden toelaten om berichten met informatie betreffende financiële transacties, zoals betalings- en effectentransacties, te verzenden en ontvangen, met inbegrip van operationele diensten en

CHAPITRE 1ER

Objectif – définitions – champ d’application

Article 1er

La présente loi règle une matière visée à l’article 74 de la Constitution.

Art. 2

§ 1er. La présente loi règle, dans un but de protection du bon fonctionnement, de la solidité et de l’efficacité des systèmes de compensation, de règlement et de paiements ainsi que de la solidité du système financier en général, les activités et la surveillance par la Banque nationale de Belgique des fournisseurs de services de messagerie financière établis en Belgique.

§ 2. Les missions dévolues à la Banque nationale de Belgique par la présente loi relèvent des missions visées à l’article 8 de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique.

§ 3. Sans préjudice des dispositions de l’article 8, § 2, de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique, la Banque nationale de Belgique peut clarifier les attentes concernant le respect de la présente loi et des arrêtés et règlements adoptés aux fins de son exécution au moyen de communications, de recommandations et de circulaires.

Art. 3

Aux fins de l’application de la présente loi, il y a lieu d’entendre par:

1° loi du 22 février 1998: la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique;

2° loi du 25 avril 2014: la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit;

3° la Banque: la Banque nationale de Belgique, à savoir l’organisme dont le statut est régi par la loi du 22 février 1998, ci-après désignée “la Banque”;

4° services de messagerie financière: services qui permettent aux entités financières et aux autorités publiques d’envoyer et de recevoir des messages contenant des informations relatives à des transactions financières, telles que les paiements et les transactions sur titres, y

nevendiensten die er nauw mee samenhangen, in het verlengde ervan liggen of er een aanvulling op vormen;

5° aanbieder: iedere in België gevestigde natuurlijke persoon of rechtspersoon die financiële berichtendiensten aanbiedt;

6° systeemrelevante aanbieder: iedere aanbieder aan wie een kennisgeving is gedaan op grond van artikel 7, § 1;

7° effectieve leiding: de personen die lid zijn van de directieraad en de personen die belast zijn met het dagelijks bestuur;

8° leidinggevend personeel: leidinggevend personeel in de zin van artikel 4, 4°, van de wet van 4 december 2007 betreffende de sociale verkiezingen;

9° verbonden vennootschap of persoon: een met een aanbieder verbonden vennootschap of persoon in de zin van artikel 1:20 van het Wetboek van Vennootschappen en Verenigingen;

10° onafhankelijke controlefuncties: de interne auditfunctie, de compliancefunctie of de risicobeheerfunctie;

11° strategische beslissing:

a) een beslissing genomen door een systeemrelevante aanbieder of door een entiteit waarover zij controle heeft, die een significante impact kan hebben op het risicoprofiel van de aanbieder;

b) elke beslissing die gelijkaardige gevolgen heeft voor de systeemrelevante aanbieder en die genomen wordt door een aandeelhouder die controle uitoefent over die aanbieder;

12° uitbesteding: een overeenkomst van om het even welke vorm tussen een systeemrelevante aanbieder en een dienstverrichter, waaronder derde aanbieders van ICT-diensten, op grond waarvan deze dienstverrichter een proces, een dienst of een activiteit verricht die de systeemrelevante aanbieder toelaat financiële berichtendiensten aan te bieden en die anders door die aanbieder zelf zou worden verricht;

13° kritieke of belangrijke functie: een functie waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een systeemrelevante aanbieder, aan de soliditeit of de continuïteit van zijn diensten en activiteiten of aan de uitvoering van nationale of internationale

inclus des services opérationnels et des services auxiliaires qui y sont étroitement liés, se situent dans leur prolongement direct ou en constituent le complément;

5° fournisseur: toute personne physique ou morale établie en Belgique qui fournit des services de messagerie financière;

6° fournisseur d'importance systémique: tout fournisseur à qui une notification a été donnée en vertu de l'article 7, § 1er;

7° direction effective: les personnes qui sont membres du conseil de direction et les personnes auxquelles la gestion journalière est déléguée;

8° personnel de direction: personnel de direction au sens de l'article 4, 4°, de la loi du 4 décembre 2007 relative aux élections sociales;

9° société ou personne liée: toute société ou personne liée à un fournisseur au sens de l'article 1:20 du Code des sociétés et des associations;

10° fonctions de contrôle indépendantes: la fonction d'audit interne, la fonction de conformité (compliance) ou la fonction de gestion des risques;

11° décision stratégique:

a) une décision prise par un fournisseur d'importance systémique ou par une entité sous son contrôle, qui peut avoir un impact significatif sur le profil de risque du fournisseur;

b) tout type de décision produisant des effets similaires dans le chef du fournisseur d'importance systémique, prise par un actionnaire qui exerce le contrôle sur ce fournisseur;

12° externalisation: tout accord, quelle que soit sa forme, entre un fournisseur d'importance systémique et un prestataire de services, y compris les prestataires tiers de services TIC, en vertu duquel ce prestataire de services prend en charge un processus, un service ou une activité aux fins de permettre au fournisseur d'importance systémique la fourniture de services de messagerie financière et qui aurait autrement été pris en charge par ce fournisseur lui-même;

13° fonction critique ou importante: une fonction dont la perturbation est susceptible de nuire sérieusement à la performance financière d'un fournisseur d'importance systémique, à la solidité ou à la continuité de ses services et activités ou à l'exécution de transactions financières

financiële transacties, of waarvan de onderbreking of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door een systeemrelevante aanbieder van de verplichtingen uit hoofde van deze wet;

14° digitale operationele weerbaarheid: het vermogen van een systeemrelevante aanbieder om zijn operationele integriteit en betrouwbaarheid op te bouwen, te waarborgen en te evalueren, door direct of indirect via gebruik van diensten die door derde aanbieders van ICT-diensten worden verleend te voorzien in het volledige scala van ICT-gerelateerde capaciteiten die nodig zijn voor de beveiliging van de netwerk- en informatiesystemen waarvan een systeemrelevante aanbieder gebruikmaakt, en die de permanente verlening van financiële berichtendiensten en de kwaliteit ervan, onder meer gedurende storingen, ondersteunen;

15° netwerk- en informatiesysteem: een netwerk- en informatiesysteem als bedoeld in artikel 8, 1°, van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

16° beveiliging van netwerk- en informatiesystemen: het vermogen van netwerk- en informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen, met inbegrip van de beveiliging van de fysieke infrastructuur;

17° ICT-risico: elke redelijkerwijs aan te wijzen omstandigheid met betrekking tot het gebruik van netwerk- en informatiesystemen die, indien zij zich voordoet, de beveiliging van het netwerk- en informatiesysteem, van technologieafhankelijke instrumenten of processen, van verrichtingen en processen, of van de levering van de diensten in gevaar kan brengen, door schadelijke effecten met zich mee te brengen in de digitale of fysieke omgeving;

18° ICT-activa: software- of hardware-activa in de netwerk- en informatiesystemen die door een systeemrelevante aanbieder worden gebruikt;

19° incident: elke gebeurtenis die het verlenen van financiële berichtendiensten kan verstoren of verstoort, waaronder, in voorkomend geval, een ICT-gerelateerd incident;

20° ICT-gerelateerd incident: een gebeurtenis of een reeks gekoppelde gebeurtenissen die niet door

nationales ou internationales, ou dont l'interruption, l'anomalie ou la défaillance est susceptible de nuire sérieusement à la capacité d'un fournisseur d'importance systémique de respecter en permanence les obligations découlant des dispositions de la présente loi;

14° résilience opérationnelle numérique: la capacité d'un fournisseur d'importance systémique à développer, garantir et évaluer son intégrité et sa fiabilité opérationnelles en assurant directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC, l'intégralité des capacités liées aux TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'il utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité, y compris en cas de perturbations;

15° réseau et système d'information: un réseau et système d'information visé à l'article 8, 1°, de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;

16° sécurité des réseaux et des systèmes d'information: la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles, y inclus la protection de l'infrastructure physique;

17° risque lié aux TIC: toute circonstance raisonnablement identifiable liée à l'utilisation des réseaux et des systèmes d'information qui, si elle se concrétise, peut compromettre la sécurité des réseaux et des systèmes d'information, de tout outil ou processus dépendant de la technologie, du fonctionnement et des processus ou de la fourniture de services en produisant des effets préjudiciables dans l'environnement numérique ou physique;

18° actifs de TIC: les actifs logiciel ou matériel dans les réseaux et les systèmes d'information utilisés par un fournisseur d'importance systémique;

19° incident: un événement qui perturbe ou est susceptible de perturber la fourniture de services de messagerie financière, y compris, le cas échéant, un incident lié aux TIC;

20° incident lié aux TIC: un événement ou une série d'événements liés entre eux que le fournisseur

de systeemrelevante aanbieder zijn gepland en die de beveiliging van netwerk- en informatiesystemen in gevaar brengen en een nadelig effect hebben op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of op de door de aanbieder verleende diensten;

21° ernstig incident: een incident met grote nadelige gevolgen voor de werking van een systeemrelevante aanbieder of voor de activa of de netwerk- en informatiesystemen die zijn kritieke of belangrijke functies ondersteunen, waaronder iedere niet-beschikbaarheid van de dienstverlening;

22° cyberdreiging: een cyberdreiging in de zin van artikel 2, punt 8), van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013;

23° ernstige cyberdreiging: een cyberdreiging waarvan de technische kenmerken erop wijzen dat zij kan leiden tot een ernstig incident;

24° cyberaanval: een kwaadwillig ICT-gerelateerd incident dat het gevolg is van een door een dreigingsactor gepleegde poging om een actief te vernietigen, bloot te stellen, te veranderen, buiten werking te stellen, te stelen of er ongeoorloofde toegang toe te verkrijgen of er ongeoorloofd gebruik van te maken;

25° dreigingsgestuurde penetratietest (*threat led penetration testing* – TLPT): een kader waarin de tactiek, technieken en procedures van levensechte, als een reële cyberdreiging ervaren dreigingsactoren worden nagebootst en waarin een gecontroleerde, op maat gesneden, door inlichtingen gestuurde test van de kritieke reëel bestaande productiesystemen van een systeemrelevante aanbieder wordt voorgebracht;

26° derde aanbieder van ICT-diensten: een onderneming die ICT-diensten verleent;

27° ICT-diensten: digitale en gegevensdiensten die doorlopend via ICT-systemen aan een of meer interne of externe gebruikers worden verleend, waaronder hardware als dienst en hardwarediensten, met inbegrip van het verlenen van technische ondersteuning via software- of firmware-updates door de hardwareaanbieder, met uitzondering van traditionele analoge telefoondiensten;

d'importance systémique n'a pas prévu qui compromet la sécurité des réseaux et des systèmes d'information, et a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou sur les services fournis par le fournisseur;

21° incident majeur: un incident qui a une incidence négative élevée sur le fonctionnement du fournisseur d'importance systémique ou sur les actifs ou les réseaux et les systèmes d'information qui soutiennent ses fonctions critiques ou importantes, y compris toute indisponibilité des services;

22° cybermenace: une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013;

23° cybermenace majeure: une cybermenace dont les caractéristiques techniques indiquent qu'elle pourrait donner lieu à un incident majeur;

24° cyberattaque: un incident lié aux TIC malveillant causé par une tentative de destruction, d'exposition, de modification, de désactivation, de vol, d'utilisation non autorisée d'un actif ou d'accès non autorisé à celui-ci, perpétrée par un acteur de la menace;

25° tests de pénétration fondés sur la menace (*threat led penetration testing* – TLPT): un cadre simulant les tactiques, les techniques et les procédures d'acteurs de la menace réels perçus comme représentant une véritable cybermenace, qui permet de tester de manière contrôlée, sur mesure et en fonction des renseignements les systèmes critiques en environnement de production du fournisseur d'importance systémique;

26° prestataire tiers de services TIC: une entreprise qui fournit des services TIC;

27° services TIC: les services numériques et de données fournis de manière permanente par l'intermédiaire des systèmes de TIC à un ou plusieurs utilisateurs internes ou externes, dont le matériel en tant que service et les services matériels qui englobent la fourniture d'assistance technique au moyen de mises à jour de logiciels ou de micrologiciels réalisées par le fournisseur de matériel, à l'exclusion des services de téléphonie analogique traditionnels;

28° nauwe banden:

a) een situatie waarin een deelnemingsverhouding bestaat, of;

b) een situatie waarin ondernemingen verbonden ondernemingen zijn, of;

c) een band van dezelfde aard als bedoeld in de bepalingen onder a) en b) tussen een natuurlijke persoon en een rechtspersoon.

Art. 4

Deze wet is van toepassing op in België gevestigde aanbieders van financiële berichtendiensten.

HOOFDSTUK 2

Drempel en kennisgevingsverplichtingen

Art. 5

Indien een aanbieder per jaar minimum 1 miljard financiële berichten heeft verwerkt, gemeten als het gemiddelde over de drie voorgaande kalenderjaren, wordt deze aanbieder beschouwd als een systeemrelevante aanbieder vanaf het ogenblik waarop de kennisgeving bedoeld in artikel 7, § 1, uitwerking heeft.

Op advies van de Bank, kan de Koning:

1° het bedrag van de drempel bedoeld in het eerste lid wijzigen;

2° nadere regels vastleggen voor de berekening van de drempel bedoeld in het eerste lid.

Art. 6

§ 1. Iedere aanbieder verstrekt jaarlijks, vóór 1 april, aan de Bank de informatie die zij nodig acht om te bepalen of de in artikel 5 bedoelde drempel is overschreden.

§ 2. Iedere aanbieder is ertoe gehouden om de Bank onverwijld in te lichten wanneer hij de drempel bedoeld in artikel 5 overschrijdt.

28° liens étroits:

a) une situation dans laquelle il existe un lien de participation, ou;

b) une situation dans laquelle des entreprises sont des entreprises liées, ou;

c) une relation de même nature que sous les a) et b) entre une personne physique et une personne morale.

Art. 4

La présente loi s'applique aux fournisseurs de services de messagerie financière établis en Belgique.

CHAPITRE 2

Seuil et obligations de notification

Art. 5

Si un fournisseur a traité au minimum 1 milliard de messages financiers par an, calculés comme la moyenne des trois années civiles antérieures, ce fournisseur est considéré comme un fournisseur d'importance systémique à partir du moment où la notification visée à l'article 7, § 1er, prend effet.

Sur avis de la Banque, le Roi est habilité à:

1° modifier le montant du seuil visé à l'alinéa 1er;

2° fixer des règles plus précises pour le calcul du seuil visé à l'alinéa 1er.

Art. 6

§ 1er. Tout fournisseur transmet chaque année à la Banque, avant le 1er avril, les informations qu'elle estime nécessaires pour déterminer s'il a dépassé le seuil visé à l'article 5.

§ 2. Tout fournisseur est tenu d'immédiatement informer la Banque en cas de dépassement du seuil visé à l'article 5.

Art. 7

§ 1. Wanneer een aanbieder de drempel bedoeld in artikel 5 heeft overschreden, neemt de Bank een beslissing over diens kwalificatie als systeemrelevante aanbieder.

De Bank brengt haar beslissing ter kennis van de aanbieder met een ter post aangetekende brief of een brief met ontvangstbewijs. Die kennisgeving heeft uitwerking vanaf de datum bepaald door de Bank, doch ten vroegste zes maand na datum van de kennisgeving.

§ 2. Wanneer een systeemrelevante aanbieder niet langer de drempel in artikel 5 overschrijdt, neemt de Bank een beslissing over de intrekking van diens kwalifiatie als systeemrelevante aanbieder. De Bank neemt die beslissing op eigen initiatief dan wel op verzoek van de systeemrelevante aanbieder, in welk geval de aanbieder de nodige cijfergegevens en uitleg toevoegt aan zijn verzoek.

De Bank brengt haar beslissing ter kennis van de aanbieder met een ter post aangetekende brief of een brief met ontvangstbewijs. Die kennisgeving heeft uitwerking vanaf de datum bepaald door de Bank.

§ 3. Bij het nemen van een beslissing op grond van dit artikel houdt de Bank rekening met de informatie die zij ontvangt in toepassing van dit artikel en van artikel 6, evenals met alle informatie waarover zij beschikt in de uitoefening van haar taken.

Art. 8

De Bank houdt een lijst bij van alle systeemrelevante aanbieders. De Bank maakt deze lijst bekend op haar website en actualiseert deze wanneer nodig.

De in het eerste lid bedoelde lijst vermeldt voor iedere systeemrelevante aanbieder minstens de volgende informatie:

1° de datum waarop de kennisgeving van kwalificatie als systeemrelevante aanbieder uitwerking heeft, zoals bepaald in artikel 7, § 1;

2° de maatschappelijke benaming, de rechtsvorm en het adres van de zetel van de systeemrelevante aanbieder.

Art. 7

§ 1er. Lorsqu'un fournisseur a dépassé le seuil visé à l'article 5, la Banque prend une décision sur sa qualification de fournisseur d'importance systémique.

La Banque porte sa décision à la connaissance du fournisseur, soit par courrier recommandé, soit par courrier avec accusé de réception. Cette notification prend effet à compter de la date arrêtée par la Banque et au plus tôt six mois après la date de la notification.

§ 2. Lorsqu'un fournisseur d'importance systémique ne dépasse plus le seuil visé à l'article 5, la Banque prend une décision sur le retrait de sa qualification de fournisseur d'importance systémique. La Banque prend cette décision soit de sa propre initiative, soit sur demande du fournisseur d'importance systémique, auquel cas le fournisseur joint à sa demande toutes les explications et données nécessaires.

La Banque porte sa décision à la connaissance du fournisseur, soit par courrier recommandé, soit par courrier avec accusé de réception. Cette notification prend effet à compter de la date arrêtée par la Banque.

§ 3. Lors de la prise d'une décision sur la base de cet article, la Banque tient compte de toute information qu'elle reçoit en vertu de cet article et de l'article 6, ainsi que de toute information dont elle dispose dans l'exercice de ses missions.

Art. 8

La Banque conserve une liste de tous les fournisseurs d'importance systémique. La Banque publie cette liste sur son site internet et la met à jour si besoin en est.

La liste visée à l'alinéa 1er mentionne au minimum les informations suivantes concernant chaque fournisseur d'importance systémique:

1° la date à laquelle la notification de qualification de fournisseur d'importance systémique prend effet, conformément à l'article 7, § 1er;

2° la dénomination sociale, la forme juridique et l'adresse du siège du fournisseur d'importance sytémique.

HOOFDSTUK 3

Organisatie en bestuur

Afdeling I

Vennootschapsvorm

Art. 9

Iedere systeemrelevante aanbieder is opgericht in de vorm van een coöperatieve vennootschap of een naamloze vennootschap naar Belgisch recht, met inachtneming van de specifieke vereisten die neergelegd zijn in deze wet of in de Europese regelgeving.

Afdeling II

Vennootschapsorganen

Art. 10

§ 1. Het bestuur van een systeemrelevante aanbieder die als naamloze vennootschap is opgericht, wordt waargenomen door een raad van toezicht en een directieraad. Onverminderd de bepalingen van deze wet of de rechtstreeks toepasselijke normen van het Europees recht, zijn de bepalingen inzake duaal bestuur zoals bedoeld in boek 7, titel 4, hoofdstuk 1, afdeling 3, van het Wetboek van Vennootschappen en Verenigingen van toepassing.

§ 2. De statuten van een systeemrelevante aanbieder die anders dan als coöperatieve vennootschap is opgericht, voorzien in de oprichting van een raad van toezicht en een directieraad. Onverminderd de bepalingen van deze wet of de rechtstreeks toepasselijke normen van het Europees recht, zijn de bepalingen inzake duaal bestuur zoals bedoeld in boek 7, titel 4, hoofdstuk 1, afdeling 3, van het Wetboek van Vennootschappen en Verenigingen van overeenkomstige toepassing.

§ 3. Wanneer het Wetboek van Vennootschappen en Verenigingen voor de betrokken vennootschapsvorm in een dagelijks bestuur voorziet, mag dat niet worden opgedragen aan een lid van de raad van toezicht.

Art. 11

§ 1. Minstens één derde maar niet minder dan drie van de leden van de raad van toezicht, waaronder de voorzitter, zijn onafhankelijke bestuurders.

CHAPITRE 3

Organisation et administration

Section Ire

Forme de société

Art. 9

Chaque fournisseur d'importance systémique est constitué sous la forme d'une société coopérative ou d'une société anonyme de droit belge, moyennant le respect des exigences spécifiques prévues par la présente loi ou par la réglementation européenne.

Section II

Organes sociétaires

Art. 10

§ 1er. L'administration d'un fournisseur d'importance systémique constitué sous la forme de société anonyme est assurée par un conseil de surveillance et un conseil de direction. Sans préjudice des dispositions prévues par la présente loi ou par les normes de droit européen directement applicables, les dispositions relatives à l'administration duale visées au livre 7, titre 4, chapitre 1er, section 3,du Code des sociétés et associations sont d'application.

§ 2. Les statuts d'un fournisseur d'importance systémique constitué sous la forme d'une société coopérative prévoient la constitution d'un conseil de surveillance et d'un conseil de direction. Sans préjudice des dispositions prévues par la présente loi ou par les normes de droit européen directement applicables, les dispositions relatives à l'administration duale visées au livre 7, titre 4, chapitre 1er, section 3, du Code des sociétés et associations sont d'application par analogie.

§ 3. La gestion journalière, lorsqu'elle est prévue par le Code des sociétés et des associations pour la forme sociétaire concernée, ne peut pas être confiée à un membre du conseil de surveillance.

Art. 11

§ 1er. Au moins un tiers mais pas moins de trois des membres du conseil de surveillance, dont le président, sont des administrateurs indépendants.

§ 2. Een bestuurder wordt geacht onafhankelijk te zijn wanneer hij of zij:

1° de vaardigheid heeft om een gedegen en objectief oordeel te vormen op basis van een eerlijke en proportionele afweging van de belangen van alle betrokken interne en externe partijen, rekening houdend met alle relevante informatie;

2° de vaardigheid heeft om ongepaste beïnvloeding vanwege de effectieve leiding of het leidinggevend personeel van de systeemrelevante aanbieder of vanwege externe partijen te voorkomen, en om daar in voorkomend geval aan te weerstaan;

3° gedurende een tijdvak van vijf jaar voorafgaand aan zijn of haar benoeming, bij de systeemrelevante aanbieder geen mandaat heeft uitgeoefend van persoon belast met de effectieve leiding, en bij een verbonden vennootschap of persoon geen mandaat heeft uitgeoefend van lid van de raad van toezicht of van het bestuursorgaan, noch belast was met de effectieve leiding;

4° gedurende een tijdvak van drie jaar voorafgaand aan zijn of haar benoeming, geen deel heeft uitgemaakt van het personeel van de systeemrelevante aanbieder;

5° met de systeemrelevante aanbieder of met een verbonden vennootschap of persoon geen significante zakelijke relatie heeft of heeft gehad gedurende een tijdvak van een jaar voorafgaand aan zijn of haar benoeming;

6° gedurende een tijdvak van drie jaar voorafgaand aan zijn of haar benoeming, geen vennoot of lid van het auditteam is geweest van de huidige of vorige revisor van de systeemrelevante aanbieder of van een verbonden vennootschap of persoon;

7° geen echtgenoot, wettelijk samenwonende partner of bloed- of aanverwanten tot de tweede graad heeft die bij de systeemrelevante aanbieder of een verbonden vennootschap of persoon een mandaat uitoefent van lid van de raad van toezicht of van het bestuursorgaan, belast is met de effectieve leiding of deel uitmaakt van het leidinggevend personeel, of die zich in een van de andere in de bepalingen onder 3° tot 6° beschreven gevallen bevinden.

§ 3. Een onafhankelijk bestuurder mag geen deel uitmaken van het personeel van een systeemrelevante aanbieder. Een onafhankelijk bestuurder mag evenwel deel uitmaken van het personeel van een verbonden vennootschap of persoon, mits de systeemrelevante aanbieder afdoende garanties kan bieden dat zulks de onafhankelijke uitoefening van zijn of haar bestuursmandaat niet bemoeilijkt of belemmert.

§ 2. Un administrateur est considéré être indépendant lorsqu'il ou elle:

1° a la capacité de former un jugement approfondi et objectif fondé sur une évaluation juste et proportionnée des intérêts de toutes les parties internes et externes impliquées, en tenant compte de toutes les informations pertinentes;

2° a la capacité de prévenir et, le cas échéant, de résister à toute influence indue de la part de la direction effective ou du personnel de direction du fournisseur d'importance systémique ou de parties externes;

3° durant une période de cinq années précédant sa nomination, n'a pas exercé auprès du fournisseur d'importance systémique un mandat de personne chargée de la direction effective, et n'a pas exercée auprès d'une société ou personne liée un mandat de membre du conseil de surveillance ou de l'organe d'administration, ni un mandat de personne chargée de la direction effective;

4° durant une période de trois années précédant sa nomination, n'a pas fait partie du personnel du fournisseur d'importance systémique;

5° n'entretient pas, ni a entretenu durant une période d'un an avant sa nomination, une relation d'affaires significative avec le fournisseur d'importance systémique ou avec une société ou personne liée;

6° n'a pas été au cours des trois dernières années, membre de l'équipe d'audit du réviseur, actuel ou précédent, du fournisseur d'importance systémique ou d'une société ou personne liée;

7° n'a au sein du fournisseur d'importance systémique ou au sein d'une société ou personne liée, ni conjoint ni cohabitant légal, ni parents ni alliés jusqu'au deuxième degré exerçant un mandat de membre du conseil de surveillance ou de l'organe d'administration, un mandat de personne chargée de la direction effective ou de personnel de direction, ou se trouvant dans un des autres cas définis aux 3° à 6°.

§ 3. Un administrateur indépendant ne peut pas faire partie du personnel d'un fournisseur d'importance systémique. Cependant, un administrateur indépendant peut faire partie du personnel d'une société ou personne liée, à condition que le fournisseur d'importance systémique puisse fournir des garanties suffisantes que ceci ne complique pas ou n'entrave pas l'exercice indépendant de son mandat d'administrateur.

De in het eerste lid bedoelde onafhankelijkheid wordt geacht niet in het gedrang te komen wanneer:

1° noch de betrokken persoon in zijn of haar dagdagelijkse taken als personeelslid, noch diens directe verantwoordelijke, bij de verbonden vennootschap of persoon betrokken zijn bij de voorbereiding van of het proces inzake strategische beslissingen die betrekking hebben op de systeemrelevante aanbieder;

2° de betrokken persoon bij de verbonden vennootschap of persoon geen commerciële functie uitoefent, noch taken in verband met een betalingsactiviteit;

3° de systeemrelevante aanbieder iedere andere, gefundeerde en voor de Bank aanvaardbare waarborg kan bieden.

§ 4. Een systeemrelevante aanbieder kan van de criteria bedoeld in paragraaf 2, 3° tot 7°, afwijken, mits hiervoor een terdege onderbouwde rechtvaardiging wordt verstrekt en op voorwaarde dat de Bank niet anders oordeelt.

§ 5. Het besluit tot benoeming van een onafhankelijk bestuurder maakt melding van de motieven op grond waarvan die hoedanigheid wordt toegekend aan de bestuurder. De statuten van de systeemrelevante aanbieder kunnen in bijkomende of strengere criteria voorzien.

Art. 12

De leden van de raad van toezicht mogen dat mandaat in totaal maximaal gedurende twaalf jaar uitoefenen. De statuten van de systeemrelevante aanbieder kunnen in strengere termijnen voorzien.

Afdeling III

Oprichting van comités

Art. 13

§ 1. Onverminderd de taken van de raad van toezicht richt iedere systeemrelevante aanbieder binnen dat orgaan minstens de volgende comités op:

1° een auditcomité;

2° een risicocomité;

3° een bestuurs- en benoemingscomité.

L'indépendance visée à l'alinéa 1er est réputée non compromise lorsque:

1° ni la personne concernée dans ses fonctions quotidiennes de membre du personnel, ni son supérieur direct, au sein de la société ou personne liée ne sont impliqués dans la préparation ou le processus des décisions stratégiques relatives au fournisseur d'importance systémique;

2° la personne concernée n'exerce pas de fonction commerciale ou de tâches liées à une activité de paiement au sein de la société ou personne liée;

3° le fournisseur d'importance systémique peut offrir toute autre garantie fondée et acceptable pour la Banque.

§ 4. Moyennant justification dûment motivée et sous réserve d'une appréciation contraire de la Banque, qui vérifie le bien-fondé de cette justification, un fournisseur d'importance systémique peut déroger aux critères visés au paragraphe 2, 3° à 7°.

§ 5. La décision de nomination d'un administrateur indépendant fait mention des motifs sur la base desquels est octroyée cette qualité à l'administrateur. Les statuts du fournisseur d'importance systémique peuvent prévoir des critères additionnels ou plus sévères.

Art. 12

Les membres du conseil de surveillance ne peuvent exercer ce mandat plus de douze ans au total. Les statuts du fournisseur d'importance systémique peuvent prévoir des délais plus stricts.

Section III

Mise en place de comités

Art. 13

§ 1er. Sans préjudice des missions du conseil de surveillance, tout fournisseur d'importance systémique constitue, au sein de cet organe, au moins les comités suivants:

1° un comité d'audit;

2° un comité des risques;

3° un comité de gouvernance et de nomination.

Deze comités zijn uitsluitend samengesteld uit leden van de raad van toezicht; een lid mag niet in meer dan twee van de voornoemde comités zetelen.

§ 2. De voorzitter van ieder comité is onafhankelijk en mag slechts van één enkel comité de voorzitter zijn.

§ 3. De voorzitter van een comité wordt geacht onafhankelijk te zijn wanneer hij of zij voldoet aan de criteria bedoeld in artikel 11, § 2. De systeemrelevante aanbieder kan niet van deze criteria afwijken.

§ 4. De onafhankelijk voorzitter van een comité mag onder geen beding deel uitmaken van het personeel van de systeemrelevante aanbieder of van een vennootschap waarmee een deelnemingsverhouding bestaat in de zin van artikel 1:23 van het Wetboek van Vennootschappen en Verenigingen.

§ 5. Het besluit tot benoeming van een onafhankelijk voorzitter van een comité maakt melding van de motieven op grond waarvan die hoedanigheid wordt toegekend aan de voorzitter. De statuten van de systeemrelevante aanbieder kunnen in bijkomende of strengere criteria voorzien.

Art. 14

§ 1. De voorzitter van het auditcomité wordt benoemd door de raad van toezicht, op aanbeveling van het bestuurs- en benoemingscomité.

§ 2. De leden van het auditcomité beschikken over een collectieve deskundigheid op het gebied van de activiteiten van de systeemrelevante aanbieder. Ten minste één lid van het auditcomité beschikt over de nodige deskundigheid op het gebied van boekhouding en audit.

§ 3. Het auditcomité heeft minstens de in artikel 7:99, § 4, van het Wetboek van Vennootschappen en Verenigingen bepaalde taken.

Het auditcomité brengt bij de raad van toezicht geregeld verslag uit over de uitoefening van zijn taken.

§ 4. Dit artikel doet geen afbreuk aan de bepalingen van het Wetboek van Vennootschappen en Verenigingen over het auditcomité in genoteerde vennootschappen in de zin van artikel 1:11 van dat Wetboek.

Ces comités sont exclusivement composés de membres du conseil de surveillance, un membre ne pouvant pas siéger dans plus de deux des comités précités.

§ 2. Le président de chaque comité est indépendant et ne peut être le président que d'un seul comité.

§ 3. Le président d'un comité est considéré être indépendant lorsqu'il ou elle satisfait aux critères visés à l'article 11, § 2. Le fournisseur d'importance systémique ne peut pas déroger à ces critères.

§ 4. Le président indépendant d'un comité ne peut en aucun cas faire partie du personnel d'un fournisseur d'importance systémique ou d'une société avec laquelle il existe un lien de participation au sens de l'article 1:23 du Code des sociétés et des associations.

§ 5. La décision de nomination d'un président indépendant d'un comité fait mention des motifs sur la base desquels cette qualité est octroyée au président. Les statuts du fournisseur d'importance systémique peuvent prévoir des critères additionnels ou plus sévères.

Art. 14

§ 1er. Le président du comité d'audit est désigné par le conseil de surveillance, sur recommandation du comité de gouvernance et de nomination.

§ 2. Les membres du comité d'audit disposent d'une compétence collective dans le domaine d'activités du fournisseur d'importance systémique. Au moins un membre du comité d'audit justifie de la compétence nécessaire en matière de comptabilité et d'audit.

§ 3. Le comité d'audit est au moins chargé des missions prévues par l'article 7:99, § 4, du Code des sociétés et des associations.

Le comité d'audit fait régulièrement rapport au conseil de surveillance sur l'exercice de ses missions.

§ 4. Cet article est sans préjudice des dispositions du Code des sociétés et des associations relatives au comité d'audit au sein de sociétés cotées au sens de l'article 1:11 de ce Code.

Art. 15

§ 1. De voorzitter van het risicocomité wordt benoemd door de raad van toezicht, op aanbeveling van het bestuurs- en benoemingscomité.

§ 2. De leden van het risicocomité bezitten individueel de nodige kennis, deskundigheid, ervaring en vaardigheden om de strategie en de risicotolerantie van de systeemrelevante aanbieder te begrijpen en te bevatten.

§ 3. Het risicocomité verstrekt advies aan de raad van toezicht over de huidige en toekomstige risicotolerantie en risicostrategie. Het staat de raad van toezicht bij in de tenuitvoerlegging van deze strategie en het toezicht daarop.

§ 4. Het risicocomité bepaalt de aard, omvang, vorm en frequentie van de informatie over de risico's die aan het comité moet worden overgemaakt. Het heeft rechtstreeks toegang tot de risicobeheerfunctie van de systeemrelevante aanbieder en tot het advies van externe deskundigen.

Art. 16

§ 1. De voorzitter van het bestuurs- en benoemingscomité wordt benoemd door de raad van toezicht, op aanbeveling van het bestuurs-en benoemingscomité.

§ 2. Het bestuurs- en benoemingscomité is zodanig samengesteld dat het een gedegen en onafhankelijk oordeel kan geven over de corporate governance en de samenstelling en efficiënte werking van de bestuurs- en beleidsorganen van de systeemrelevante aanbieder, in het bijzonder over de individuele en collectieve deskundigheid van hun leden, en over hun integriteit, reputatie, diversiteit, onafhankelijkheid van geest en beschikbaarheid.

§ 3. Het bestuurs- en benoemingscomité is belast met:

1° het aanwijzen en aanbevelen, voor goedkeuring door de algemene vergadering, of, in voorkomend geval, door de raad van toezicht, van geschikte kandidaten voor het invullen van vacatures in de raad van toezicht, de comités en de directieraad, het nagaan hoe de kennis, vaardigheden, diversiteit en ervaring in de raad van toezicht en de directieraad zijn verdeeld, en het opstellen van een beschrijving van de taken en bekwaamheden

Art. 15

§ 1er. Le président du comité de risque est désigné par le conseil de surveillance, sur recommandation du comité de gouvernance et de nomination.

§ 2. Les membres du comité des risques disposent individuellement des connaissances, des compétences, de l'expérience et des aptitudes nécessaires pour leur permettre de comprendre et d'appréhender la stratégie et le niveau de tolérance au risque du fournisseur d'importance systémique.

§ 3. Le comité des risques conseille le conseil de surveillance pour les aspects concernant la stratégie et le niveau de tolérance en matière de risques, tant actuels que futurs. Il assiste le conseil de surveillance lors de la mise en œuvre de cette stratégie et lors de sa supervision.

§ 4. Le comité des risques détermine la nature, le volume, la forme et la fréquence des informations concernant les risques à lui transmettre. Il dispose d'un accès direct à la fonction de gestion des risques du fournisseur d'importance systémique et aux conseils d'experts extérieurs.

Art. 16

§ 1er. Le président du comité de gouvernance et de nomination est désigné par le conseil de surveillance, sur recommandation du comité de gouvernance et de nomination.

§ 2. Le comité de gouvernance et de nomination est composé de manière à lui permettre d'exercer un jugement pertinent et indépendant sur la gouvernance d'entreprise et la composition et le fonctionnement efficace des organes d'administration et de gestion du fournisseur d'importance systémique, en particulier sur l'expertise individuelle et collective de leurs membres et sur l'intégrité, la réputation, la diversité, l'indépendance d'esprit et la disponibilité de ceux-ci.

§ 3. Le comité de gouvernance et de nomination:

1° identifie et recommande, pour approbation par l'assemblée générale ou, le cas échéant, par le conseil de surveillance, des candidats aptes à occuper des sièges vacants au sein du conseil de surveillance, des comité et du conseil de direction, évalue l'équilibre de connaissances, de compétences, de diversité et d'expérience au sein du conseil de surveillance et du conseil de direction, élabore une description des missions et des

die voor een bepaalde benoeming zijn vereist, alsmede het beoordelen van hoeveel tijd er aan de functie moet worden besteed;

2° het periodiek, en minimaal jaarlijks, evalueren van de structuur, omvang, samenstelling en prestaties van de raad van toezicht, de comités en de directieraad en het formuleren van aanbevelingen aan de raad van toezicht met betrekking tot eventuele wijzigingen;

3° het periodiek, en minimaal jaarlijks, beoordelen van de kennis, vaardigheden, ervaring, mate van betrokkenheid, met name de regelmatige aanwezigheid, van de individuele leden van de raad van toezicht, de comités en de directieraad, en van de raad van toezicht, de comités en de directieraad als geheel, en daar verslag over uitbrengen aan de raad van toezicht;

4° het periodiek toetsen van het beleid van de raad van toezicht voor de selectie en benoeming van de leden van de directieraad, en het formuleren van aanbevelingen aan de raad van toezicht;

5° het ontwikkelen en aanbevelen van bestuursbeleid en -procedures ter goedkeuring door de algemene vergadering, met inbegrip van de statuten en bedrijfsregels, en ter goedkeuring door de raad van toezicht, met inbegrip van de gedragscode;

6° het voorbereiden en periodiek toetsen van de naleving van de in artikel 30, § 1, 3°, bedoelde procedures met betrekking tot herkenning, behandeling en beheersing van belangenconflicten, met inbegrip van het bijhouden van een centraal register van mogelijke belangenconflicten en van alle externe mandaten van leden van de raad van toezicht;

7° het promoten van een cultuur van permanente opleiding van de leden van de raad van toezicht;

8° het identificeren van mogelijke hiaten in de bestuursprocessen en het voorstellen van veranderingen op basis van best practices.

§ 4. Bij de uitoefening van zijn bevoegdheden ziet het bestuurs- en benoemingscomité erop toe dat één persoon of een kleine groep van personen de besluitvorming van de besluitvormingsorganen niet domineert op een wijze die de collegialiteit van die organen aantast of die de belangen van de systeemrelevante aanbieder in haar geheel schaadt.

§ 5. Het bestuurs- en benoemingscomité kan gebruikmaken van alle vormen van hulpmiddelen die het

qualifications liées à une nomination donnée et évalue le temps à consacrer à ces fonctions;

2° évalue périodiquement, et à tout le moins une fois par an, la structure, la taille, la composition et les performances du conseil de surveillance, des comités et du conseil de direction et soumet au conseil de surveillance des recommandations en ce qui concerne des changements éventuels;

3° évalue périodiquement, et à tout le moins une fois par an, les connaissances, les compétences, l'expérience, le degré d'implication, notamment l'assiduité, des membres du conseil de surveillance, des comités et du conseil de direction, tant individuellement que collectivement, et en rend compte au conseil de surveillance;

4° examine périodiquement les politiques du conseil de surveillance en matière de sélection et de nomination des membres du conseil de direction, et formule des recommandations à l'intention du conseil de surveillance;

5° élaborer et recommander des politiques et des procédures de gouvernance pour approbation par l'assemblée générale, y compris les statuts et les règles d'entreprise, et pour approbation par le conseil de surveillance, y compris le code de conduite;

6° prépare et examine périodiquement le respect des procédures visées à l'article 30, § 1er, 3°, servant à identifier, à gérer et à régler les conflits d'intérêts, y compris la tenue d'un registre central des conflits potentiels et des mandats externes des membres du conseil de surveillance;

7° promeut une culture de formation continue des membres du conseil de surveillance;

8° identifie des lacunes potentielles dans les processus de gouvernance et propose des changements basés sur les meilleures pratiques.

§ 4. Dans l'exercice de ses attributions, le comité de gouvernance et de nomination veille à ce que la prise de décision au sein des organes décisionnels ne soit pas dominée par une personne ou un petit groupe de personnes, d'une manière qui porte atteinte à la collégialité de ces organes ou qui soit préjudiciable aux intérêts du fournisseur d'importance systémique dans son ensemble.

§ 5. Le comité de gouvernance et de nomination peut recourir à tout type de ressource qu'il considère comme

geschikt acht voor de uitvoering van zijn opdracht, zoals het inwinnen van extern advies, en ontvangt hiertoe toereikende financiële middelen.

Art. 17

De Bank kan, bij reglement vastgesteld in toepassing van artikel 8, § 2, van de wet van 22 februari 1998, de elementen bedoeld in de artikelen 14, 15 en 16 preciseren en aanvullen.

Afdeling IV

Operationele onafhankelijke controlefuncties

Art. 18

§ 1. Iedere systeemrelevante aanbieder neemt de nodige maatregelen om blijvend te beschikken over de volgende passende onafhankelijke controlefuncties:

1° compliance;

2° risicobeheer;

3° interne audit.

Deze controlefuncties worden uitgeoefend door personen die onafhankelijk zijn van de bedrijfseenheden van de systeemrelevante aanbieder en over de nodige bevoegdheden beschikken om hun functie naar behoren te kunnen uitoefenen. De beloning van deze personen wordt vastgesteld volgens de verwezenlijking van de doelstellingen waar hun functie op gericht is, onafhankelijk van de resultaten van de werkzaamheden waarop toezicht wordt gehouden.

§ 2. Bij haar beoordeling van het passende karakter van de in paragraaf 1 bedoelde functies houdt de Bank rekening met de aard, schaal en complexiteit van de risico's die inherent zijn aan het bedrijfsmodel en aan de werkzaamheden van de systeemrelevante aanbieder.

Art. 19

§ 1. Iedere systeemrelevante aanbieder beschikt over een passende compliancefunctie om de naleving door de systeemrelevante aanbieder, de leden van zijn raad van toezicht, de personen belast met de effectieve leiding, de werknemers en gevolmachtigden te verzekeren van

étant appropriée à l'exercice de sa mission, y compris à des conseils externes, et reçoit les moyens financiers appropriés à cet effet.

Art. 17

La Banque peut, par voie de règlement pris en application de l'article 8, § 2, de la loi du 22 février 1998, préciser et compléter les éléments visés aux articles 14, 15 et 16.

Section IV

Fonctions de contrôle indépendantes opérationnelles

Art. 18

§ 1er. Chaque fournisseur d'importance systémique prend les mesures nécessaires pour disposer en permanence des fonctions de contrôle indépendantes adéquates suivantes:

1° conformité (compliance);

2° gestion des risques;

3° audit interne.

Les personnes qui assurent l'exercice de ces fonctions de contrôle sont indépendantes des unités opérationnelles du fournisseur d'importance systémique et disposent des prérogatives nécessaires au bon accomplissement de leurs fonctions. La rémunération de ces personnes est fixée en fonction de la réalisation des objectifs liés à leurs fonctions, indépendamment des performances des domaines d'activités contrôlés.

§ 2. Dans son évaluation du caractère adéquat des fonctions visées au paragraphe 1er, la Banque tient compte de la nature, de l'échelle et de la complexité des risques inhérents au modèle d'entreprise et aux activités du fournisseur d'importance systémique.

Art. 19

§ 1er. Chaque fournisseur d'importance systémique dispose d'une fonction de conformité (compliance) adéquate destinée à assurer le respect, par le fournisseur d'importance systémique, les membres de son conseil de surveillance, les personnes chargées de la direction

de wettelijke en reglementaire regels inzake integriteit en gedrag die van toepassing zijn op zijn activiteit.

§ 2. De personen die belast zijn met de compliancefunctie brengen minstens eenmaal per jaar verslag uit aan de raad van toezicht.

De raad van toezicht bezorgt aan de Bank jaarlijks een verslag over de beoordeling van de compliancefunctie die hij met toepassing van artikel 33, § 2, 2°, verricht.

Art. 20

§ 1. Iedere systeemrelevante aanbieder beschikt over een passende risicobeheerfunctie die onafhankelijk is van de operationele functies en die voldoende gezag, status en middelen heeft en rechtstreeks toegang heeft tot de raad van toezicht.

§ 2. De personen die belast zijn met de risicobeheerfunctie zorgen ervoor dat alle significante risico's worden gedetecteerd en gemeten en naar behoren worden gemeld. Zij zijn actief betrokken bij de uitstippeling van de risicostrategie van de systeemrelevante aanbieder en bij alle beleidsbeslissingen die een significante invloed hebben op de risico's en zijn in staat een volledig beeld te geven van het hele scala van risico's die de systeemrelevante aanbieder loopt.

Art. 21

De verantwoordelijken voor de risicobeheerfunctie en de compliancefunctie rapporteren rechtstreeks aan de raad van toezicht en kunnen het over hun bezorgdheid inlichten en in voorkomend geval waarschuwen indien specifieke risico-ontwikkelingen een negatieve invloed op de systeemrelevante aanbieder hebben of zouden kunnen hebben.

Het eerste lid doet geen afbreuk aan de verantwoordelijkheden van de raad van toezicht krachtens deze wet.

Art. 22

§ 1. Iedere systeemrelevante aanbieder waarborgt in een auditcharter ten minste dat de interne auditfunctie onafhankelijk is en dat haar taken betrekking hebben op alle werkzaamheden en entiteiten van de aanbieder, ook in geval van uitbesteding.

effective, ses salariés et ses mandataires des règles légales et réglementaires d'intégrité et de conduite qui s'appliquent à son activité.

§ 2. Les personnes qui assurent la fonction de conformité (compliance) font rapport au conseil de surveillance au moins une fois par an.

Le conseil de surveillance transmet annuellement à la Banque un rapport relatif à l'évaluation qu'il effectue de la fonction de conformité en application de l'article 33, § 2, 2°.

Art. 20

§ 1er. Chaque fournisseur d'importance systémique dispose d'une fonction de gestion des risques adéquate, indépendante des fonctions opérationnelles et qui dispose d'une autorité, d'un statut et de ressources suffisants, ainsi que d'un accès direct au conseil de surveillance.

§ 2. Les personnes qui assurent la fonction de gestion des risques veillent à ce que tous les risques significatifs soient détectés, mesurés et correctement déclarés. Elles participent activement à l'élaboration de la stratégie en matière de risque du fournisseur d'importance systémique ainsi qu'à toutes les décisions de gestion ayant une incidence significative en matière de risque et peuvent fournir une vue complète de toute la gamme des risques auxquels est exposé le fournisseur d'importance systémique.

Art. 21

Les responsables des fonctions de gestion des risques et de conformité (compliance) rendent directement compte au conseil de surveillance et peuvent lui faire part de préoccupations et l'avertir, le cas échéant, en cas d'évolution des risques affectant ou susceptible d'affecter le fournisseur.

L'alinéa 1er ne porte pas préjudice aux responsabilités du conseil de surveillance en vertu de la présente loi.

Art. 22

§ 1er. Chaque fournisseur d'importance systémique garanti dans une charte d'audit, au minimum, l'indépendance de la fonction d'audit interne et l'étendue de ses missions à toute activité et entité du fournisseur, y compris en cas de sous-traitance.

§ 2. De interne auditfunctie bezorgt aan de raad van toezicht een onafhankelijke beoordeling van de kwaliteit en de doeltreffendheid van de interne controle, het risicobeheer en de governanceregeling van de aanbieder.

§ 3. De interne auditfunctie rapporteert rechtstreeks aan de raad van toezicht, in voorkomend geval via het auditcomité.

Art. 23

De personen die verantwoordelijk zijn voor de onafhankelijke controlefuncties kunnen niet zonder voorafgaande goedkeuring van de raad van toezicht uit hun functie worden verwijderd.

De systeemrelevante aanbieder stelt de Bank voorafgaandelijk in kennis hiervan.

Art. 24

De Bank kan bij reglement vastgesteld in toepassing van artikel 8, § 2, van de wet van 22 februari 1998, preciseren en aanvullen wat dient verstaan te worden onder een passende onafhankelijke interne auditfunctie, een passende onafhankelijke risicobeheerfunctie en een passende onafhankelijke compliancefunctie.

Afdeling V

Leiding, professionele betrouwbaarheid en passende deskundigheid

Art. 25

§ 1. De leden van de raad van toezicht van de systeemrelevante aanbieder, de personen belast met de effectieve leiding evenals de verantwoordelijken voor de onafhankelijke controlefuncties, zijn uitsluitend natuurlijke personen.

§ 2. De in paragraaf 1 bedoelde personen moeten permanent over de voor de uitoefening van hun functie vereiste professionele betrouwbaarheid en passende deskundigheid beschikken, met inbegrip op het vlak van de naleving van de vereiste bedoeld in artikel 26.

Art. 26

§ 1. De functie van lid van de raad van toezicht, persoon belast met de effectieve leiding of verantwoordelijke

§ 2. La fonction d'audit interne a pour objet de fournir au conseil de surveillance une évaluation indépendante de la qualité et de l'efficience du contrôle interne, de la gestion des risques et du dispositif de gouvernance du fournisseur.

§ 3. La fonction d'audit interne fait directement rapport au conseil de surveillance, le cas échéant via le comité d'audit.

Art. 23

Les personnes qui sont responsables des fonctions de contrôle indépendantes ne peuvent être démises de leur fonction sans l'accord préalable du conseil de surveillance.

Le fournisseur d'importance systémique en informe préalablement la Banque.

Art. 24

La Banque peut, par voie de règlement pris en application de l'article 8, § 2, de la loi du 22 février 1998, préciser et compléter ce qu'il y a lieu d'entendre par fonction d'audit interne indépendante adéquate, fonction de gestion des risques indépendante adéquate et fonction de conformité (compliance) indépendante adéquate.

Section V

Direction, honorabilité professionnelle et expertise adéquate

Art. 25

§ 1er. Les membres du conseil de surveillance du fournisseur d'importance systémique, les personnes chargées de la direction effective ainsi que les responsables des fonctions de contrôle indépendantes sont exclusivement des personnes physiques.

§ 2. Les personnes visées au paragraphe 1er doivent disposer en permanence de l'honorabilité professionnelle nécessaire et de l'expertise adéquate à l'exercice de leur fonction, y compris en ce qui concerne le respect de l'exigence visée à l'article 26.

Art. 26

§ 1er. Ne peuvent exercer les fonctions de membre du conseil de surveillance, de personne chargée de la

voor een onafhankelijke controlefunctie mag niet worden uitgeoefend door personen die werden veroordeeld tot een straf bedoeld in artikel 20, § 1, van de wet van 25 april 2014.

§ 2. De in paragraaf 1 bedoelde verbodsbepalingen gelden voor een termijn:

1° van twintig jaar ingeval de gevangenisstraf meer dan twaalf maanden bedraagt;

2° van tien jaar voor de overige gevangenisstraffen of geldboetes, alsook in geval van een veroordeling met uitstel.

Art. 27

§ 1. Iedere systeemrelevante aanbieder brengt de Bank voorafgaandelijk op de hoogte van het voorstel tot benoeming van:

1° de voorzitter van de raad van toezicht;

2° de voorzitter van de directieraad;

3° de voorzitter van ieder comité bedoeld in artikel 13, § 1;

4° de verantwoordelijke voor de risicobeheerfunctie;

5° de verantwoordelijke voor de interne auditfunctie.

In het kader van de krachtens het eerste lid vereiste informatieverstrekking deelt de systeemrelevante aanbieder aan de Bank alle documenten en informatie mee die haar toelaten te beoordelen of de personen waarvan de benoeming wordt voorgesteld, overeenkomstig artikel 25, § 2, over de voor de uitoefening van hun functie vereiste professionele betrouwbaarheid en passende deskundigheid beschikken.

Het eerste lid is eveneens van toepassing op het voorstel tot hernieuwing van de benoeming van de in het eerste lid bedoelde personen, evenals op de niet-hernieuwing van hun benoeming, hun afzetting of hun ontslag.

§ 2. De benoeming van de in paragraaf 1 bedoelde personen wordt voorafgaandelijk ter goedkeuring voorgelegd aan de Bank.

§ 3. De systeemrelevante aanbieder informeert de Bank over de eventuele taakverdeling tussen de leden

direction effective ou de responsable d'une fonction de contrôle indépendante, les personnes qui ont été condamnées à une peine visée à l'article 20, § 1er, de la loi du 25 avril 2014.

§ 2. Les interdictions mentionnées au paragraphe 1er ont une durée:

1° de vingt ans pour les peines d'emprisonnement supérieure à douze mois;

2° de dix ans pour les autres peines d'emprisonnement ou d'amende ainsi qu'en cas de condamnation assortie d'un sursis.

Art. 27

§ 1er. Chaque fournisseur d'importance systémique informe préalablement la Banque de la proposition de nomination:

1° du président du conseil de surveillance;

2° du président du conseil de direction;

3° du président de chaque comité visé à l'article 13, § 1er;

4° du responsable de la fonction de la gestion des risques;

5° le responsable de la fonction d'audit interne.

Dans le cadre de l'information requise en vertu de l'alinéa 1er, le fournisseur d'importance systémique communique à la Banque tous les documents et informations lui permettant d'évaluer si les personnes dont la nomination est proposée disposent de l'honorabilité professionnelle nécessaire et de l'expertise adéquate à l'exercice de leur fonction conformément à l'article 25, § 2.

L'alinéa 1er est également applicable à la proposition de renouvellement de la nomination des personnes qui y sont visées ainsi qu'au non-renouvellement de leur nomination, à leur révocation ou à leur démission.

§ 2. La nomination des personnes visées au paragraphe 1er est soumise à l'approbation préalable de la Banque.

§ 3. Le fournisseur d'importance systémique informe la Banque de la répartition éventuelle des tâches entre

van de raad van toezicht en tussen de personen die belast zijn met de effectieve leiding.

Belangrijke wijzigingen in de taakverdeling als bedoeld in het eerste lid geven in voorkomend geval aanleiding tot de toepassing van de paragrafen 1 en 2.

§ 4. Naast het bepaalde bij paragraaf 1 brengen de systeemrelevante aanbieder en de in paragraaf 1 bedoelde personen de Bank onverwijld op de hoogte van elk feit of element dat een wijziging inhoudt van de bij de benoeming verstrekte informatie en een invloed kan hebben op de voor de uitoefening van de betrokken functie vereiste professionele betrouwbaarheid of passende deskundigheid.

De Bank kan de naleving van de in artikel 25, § 2, bedoelde vereisten herbeoordelen wanneer zij in het kader van de uitvoering van haar toezichtsopdracht op de hoogte is van een dergelijk feit of element, dat al dan niet met toepassing van het eerste lid is verkregen.

Art. 28

De leden van de raad van toezicht en de personen belast met de effectieve leiding, alsook de personen die verantwoordelijk zijn voor de onafhankelijke controlefuncties besteden de nodige tijd aan de uitoefening van hun functies bij de systeemrelevante aanbieder.

Art. 29

De Bank kan, bij reglement vastgesteld in toepassing van artikel 8, § 2, van de wet van 22 februari 1998, de elementen bedoeld in de artikelen 25, 27 en 28 preciseren en aanvullen.

Afdeling VI

Bedrijfsorganisatie

Art. 30

§ 1. Iedere systeemrelevante aanbieder beschikt over een solide en passende regeling voor de bedrijfsorganisatie, waaronder toezichtsmaatregelen, om een doeltreffend en voorzichtig beleid van de systeemrelevante aanbieder te garanderen, die met name berust op:

1° schriftelijk vastgelegde doelstellingen waarin een hoge prioriteit wordt gegeven aan de veiligheid en de efficiëntie van het verlenen van financiële berichtendiensten,

les membres du conseil de surveillance et entre les personnes chargées de la direction effective.

Les modifications importantes intervenues dans la répartition des tâches visée à l'alinéa 1er, donnent le cas échéant lieu à l'application des paragraphes 1er et 2.

§ 4. Outre les dispositions du paragraphe 1er, le fournisseur d'importance systémique et les personnes visées au paragraphe 1er communiquent sans délai à la Banque tout fait ou élément qui implique une modification des informations fournies lors de la nomination et qui pourrait avoir une incidence sur l'honorabilité professionnelle nécessaire ou l'expertise adéquate à l'exercice de la fonction concernée.

La Banque peut effectuer une réévaluation du respect des exigences visées à l'article 25, § 2, lorsqu'elle a connaissance, dans le cadre de l'exercice de sa mission de contrôle, d'un tel fait ou élément, obtenu ou non en application de l'alinéa 1er.

Art. 28

Les membres du conseil de surveillance et les personnes chargées de la direction effective, ainsi que les personnes qui sont responsables des fonctions de contrôle indépendantes consacrent le temps nécessaire à l'exercice de leurs fonctions au sein du fournisseur d'importance systémique.

Art. 29

La Banque peut, par voie de règlement pris en application de l'article 8, § 2, de la loi du 22 février 1998, préciser et compléter les éléments visés aux articles 25, 27 et 28.

Section VI

Organisation d'entreprise

Art. 30

§ 1er. Tout fournisseur d'importance systémique doit disposer d'un dispositif solide et adéquat d'organisation d'entreprise, dont des mesures de surveillance, en vue de garantir une gestion efficace et prudente du fournisseur d'importance systémique, reposant notamment sur:

1° des objectifs consignés par écrit qui accordent une priorité élevée à la sécurité et l'efficacité de la fourniture de services de messagerie financière, et qui renforcent

en die expliciet financiële stabiliteit en andere relevante overwegingen van publiek belang, in het bijzonder open en efficiënte markten, bevorderen;

2° een passende beleidsstructuur die op het hoogste niveau gebaseerd is op een duidelijk onderscheid tussen, enerzijds, de effectieve leiding van de systeemrelevante aanbieder en, anderzijds, het toezicht op die leiding, en die binnen de systeemrelevante aanbieder voorziet in een passende functiescheiding en in een duidelijk omschreven, transparante en coherente regeling voor de toewijzing van verantwoordelijkheden;

3° de vaststelling van schriftelijke procedures met betrekking tot het functioneren en de evaluatie van de bestuursorganen, inclusief procedures met betrekking tot herkenning, behandeling en beheersing van belangenconflicten van hun leden;

4° een passende en effectieve administratieve organisatie en interne controle, waaronder met name controles die een redelijke mate van zekerheid verschaffen over de effectiviteit van de maatregelen ter verwezenlijking van een hoog niveau van digitale operationele weerbaarheid en over de betrouwbaarheid van het operationele en financiële verslaggevingsproces;

5° passende onafhankelijke controlefuncties;

6° een integraal risicobeheerskader als bedoeld in artikel 47;

7° de invoering van passende maatregelen met het oog op de bedrijfscontinuïteit en de beschikbaarheid van de dienstverlening, in het bijzonder zoals bedoeld in artikel 51;

8° een effectief kader voor het beheer van het ICT-risico als bedoeld in artikel 52, § 1;

9° een passend intern waarschuwingssysteem dat in overeenstemming is met de wet van 28 november 2022 betreffende de bescherming van melders van inbreuken op het Unie- of nationale recht vastgesteld binnen een juridische entiteit in de private sector en dat met name voorziet in een specifieke onafhankelijke en autonome melding van inbreuken op de normen en de gedragscodes van de systeemrelevante aanbieder.

§ 2. De Bank kan, bij reglement vastgesteld in toepassing van artikel 8, § 2, van de wet van 22 februari 1998, het bepaalde in paragraaf 1 preciseren en aanvullen.

explicitement la stabilité du système financier et d'autres considérations d'intérêt public, en particulier des marchés financiers ouverts et efficaces;

2° une structure de gestion adéquate basée, au plus haut niveau, sur une distinction claire entre la direction effective du fournisseur d'importance systémique d'une part, et le contrôle sur cette direction d'autre part, et prévoyant, au sein du fournisseur d'importance systémique, une séparation adéquate des fonctions et un dispositif d'attribution des responsabilités qui est bien défini, transparent et cohérent;

3° une définition des procédures formalisées par écrit régissant le fonctionnement et l'évaluation des organes d'administration, notamment les procédures servant à identifier, à gérer et à régler les conflits d'intérêts de ses membres;

4° une organisation administrative et un contrôle interne adéquats et efficaces, impliquant notamment des contrôles procurant un degré de certitude raisonnable quant à l'effectivité des mesures prises pour atteindre un niveau élevé de résilience opérationnelle numérique et quant à la fiabilité du processus de reporting opérationnel et financier;

5° des fonctions de contrôle indépendantes adéquates;

6° un cadre de gestion global des risques tel que visé à l'article 47;

7° la mise en place de mesures adéquates en vue de la continuité de l'activité et de la disponibilité de la fourniture des services, en particulier tel que visé à l'article 51;

8° un cadre efficace pour la gestion du risque TIC tel que visé à l'article 52, § 1er;

9° un système adéquat d'alerte interne conforme à la loi du 28 novembre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé, prévoyant notamment un mode de transmission spécifique, indépendant et autonome, des infractions aux normes et aux codes de conduite du fournisseur d'importance systémique.

§ 2. La Banque peut, par voie de règlement pris en application de l'article 8, § 2, de la loi du 22 février 1998, préciser et compléter les éléments visés au paragraphe 1er.

Art. 31

De in artikel 30 bedoelde organisatieregeling is exhaustief en passend voor de aard, schaal en complexiteit van de risico's die inherent zijn aan het bedrijfsmodel en aan de werkzaamheden van de systeemrelevante aanbieder. De organisatieregeling houdt in het bijzonder, doch niet uitsluitend, rekening met de verplichtingen inzake bedrijfsvoering en risicobeheer bedoeld in hoofdstuk 7.

Art. 32

Als de systeemrelevante aanbieder nauwe banden heeft met andere natuurlijke of rechtspersonen, mogen die banden of de voor die personen geldende wettelijke en bestuursrechtelijke bepalingen of de tenuitvoerlegging ervan geen belemmering vormen voor het toezicht op de aanbieder door de Bank.

Afdeling VII

Toezicht en leiding

Art. 33

§ 1. De raad van toezicht beoordeelt periodiek en minstens eenmaal per jaar de doeltreffendheid van de in artikel 30 bedoelde organisatieregeling van de systeemrelevante aanbieder en de overeenstemming ervan met de wettelijke en reglementaire bepalingen. Het ziet erop toe dat de nodige maatregelen worden genomen om eventuele tekortkomingen aan te pakken.

§ 2. De raad van toezicht:

1° oefent effectief toezicht uit op de effectieve leiding en op de beslissingen die door de effectieve leiding worden genomen;

2° beoordeelt de goede werking van de onafhankelijke controlefuncties;

3° ziet erop toe dat de systeemrelevante aanbieder voldoende personele en financiële middelen wijdt aan de permanente opleiding van de leden van de raad van toezicht;

4° rechtvaardigt in het jaarlijks verslag de individuele en collectieve deskundigheid van de leden van de in artikel 13, § 1, bedoelde comités.

Art. 31

Les dispositifs organisationnels visés à l'article 30 sont exhaustifs et appropriés à la nature, à l'échelle et à la complexité des risques inhérents au modèle d'entreprise et aux activités du fournisseur d'importance systémique. Les dispositifs organisationnels tiennent en particulier, mais pas exclusivement, compte des obligations de conduite des activités et de gestion de risque visées au chapitre 7.

Art. 32

S'il existe des liens étroits entre le fournisseur d'importance systémique et d'autres personnes physiques ou morales, ces liens ou les dispositions légales, réglementaires et administratives applicables à ces personnes ou leur mise en œuvre ne peuvent pas entraver l'exercice du contrôle du fournisseur par la Banque.

Section VII

Contrôle et direction

Art. 33

§ 1er. Le conseil de surveillance évalue périodiquement, et au moins une fois par an, l'efficacité des dispositifs d'organisation du fournisseur d'importance systémique visés à l'article 30 et leur conformité aux obligations légales et réglementaires. Il veille à ce que les mesures nécessaires pour remédier aux éventuels manquements soient prises.

§ 2. Le conseil de surveillance:

1° exerce un contrôle effectif sur la direction effective et assure la surveillance des décisions prises par la direction effective;

2° évalue le bon fonctionnement des fonctions de contrôle indépendantes;

3° s'assure que le fournisseur d'importance systémique consacre des ressources humaines et financières adéquates à la formation continue des membres du conseil de surveillance;

4° justifie dans le rapport annuel la compétence individuelle et collective des membres des comités visés à l'article 13, § 1er.

Art. 34

De leden van de raad van toezicht hebben passende toegang tot alle informatie en documenten die nodig zijn om de opdrachten uit te voeren waarmee ze belast zijn met toepassing van de bepalingen van deze wet en haar uitvoeringsbesluiten.

Art. 35

§ 1. Onverminderd de bevoegdheden van de raad van toezicht neemt de directieraad de nodige maatregelen voor de naleving en de tenuitvoerlegging van de bepalingen van artikel 30.

§ 2. De directieraad rapporteert jaarlijks aan de raad van toezicht en aan de Bank over de beoordeling van de doeltreffendheid van de in artikel 30 bedoelde organisatieregeling en over de maatregelen die in voorkomend geval worden genomen om eventuele tekortkomingen aan te pakken. Het verslag rechtvaardigt waarom deze maatregelen voldoen aan de wettelijke en reglementaire bepalingen.

Art. 36

De Bank kan, bij reglement vastgesteld in toepassing van artikel 8, § 2, van de wet van 22 februari 1998, de elementen bedoeld in de artikelen 33, 34 en 35 preciseren en aanvullen.

HOOFDSTUK 4

Kapitaalvereisten

Art. 37

§ 1. Het kapitaal samen met het overgedragen resultaat en de reserves van een systeemrelevante aanbieder is evenredig met de risico's die uit de activiteiten van de aanbieder voortkomen. Het is te allen tijde voldoende om:

1° te waarborgen dat de systeemrelevante aanbieder adequaat wordt beschermd tegen operationele, juridische en zakelijke risico's zodat de systeemrelevante aanbieder diensten kan blijven verrichten als *going concern*;

2° in een reeks stressscenario's het herstel te verzekeren opgelegd overeenkomstig het plan bepaald in artikel 48.

Art. 34

Les membres du conseil de surveillance disposent d'un accès adéquat à toutes les informations et tous les documents nécessaires pour assurer les missions dont ils sont chargés en application des dispositions de la présente loi et des arrêtés pris pour son exécution.

Art. 35

§ 1er. Sans préjudice des pouvoirs dévolus au conseil de surveillance, le conseil de direction prend les mesures nécessaires pour assurer le respect et la mise en œuvre des dispositions de l'article 30.

§ 2. Le conseil de direction fait une fois par an rapport au conseil de surveillance et à la Banque concernant l'évaluation de l'efficacité des dispositifs d'organisation visés à l'article 30 et les mesures prises le cas échéant pour remédier aux déficiences qui auraient été constatées. Le rapport justifie en quoi ces mesures satisfont aux dispositions légales et réglementaires.

Art. 36

La Banque peut, par voie de règlement pris en application de l'article 8, § 2, de la loi du 22 février 1998, préciser et compléter les éléments visés aux articles 33, 34 et 35.

CHAPITRE 4

Exigences de capital

Art. 37

§ 1er. Le capital, complété par les résultats reportés et les réserves du fournisseur d'importance systémique, est proportionnel au risque découlant des activités du fournisseur. Il doit être suffisant, à tout moment, pour;

1° garantir que le fournisseur d'importance systémique bénéficie d'une protection adéquate à l'égard du risque opérationnel, juridique, économique, de telle manière que le fournisseur d'importance systémique peut assurer la continuité de l'exploitation;

2° assurer, dans le cadre d'un éventail de scénarios de crise, un redressement conformément au plan visé à l'article 48.

§ 2. Bij reglement vastgesteld in toepassing van artikel 8, § 2, van de wet van 22 februari 1998 kan de Bank de vereisten bedoeld in paragraaf 1 preciseren.

Art. 38

Iedere systeemrelevante aanbieder houdt een plan aan voor:

1° het aantrekken van extra kapitaal voor het geval dat zijn aandelenkapitaal de in artikel 37 neergelegde drempels nadert of daaronder daalt;

2° het verzekeren van het herstel of ordelijke liquidatie van zijn bedrijfsactiviteiten en diensten indien de aanbieder niet in staat is nieuw kapitaal aan te trekken.

Het plan wordt door de raad van toezicht of door een ter zake bevoegd comité van dit orgaan goedgekeurd, en regelmatig, waaronder minstens jaarlijks, geactualiseerd. Telkens wanneer het plan is geactualiseerd, wordt het toegezonden aan de Bank. De Bank kan de systeemrelevante aanbieder verzoeken aanvullende maatregelen te nemen of andere voorzieningen te treffen indien zij het plan van de aanbieder ontoereikend acht.

HOOFDSTUK 5

Strategische beslissingen

Art. 39

§ 1. De voorafgaande toestemming van de Bank is vereist voor strategische beslissingen.

§ 2. De Bank beslist binnen twee maanden na ontvangst van een volledig dossier van de voorgenomen strategische beslissing. Zij mag haar toestemming enkel weigeren om redenen die verband houden met het vermogen van de systeemrelevante aanbieder om te voldoen aan de bepalingen die door of krachtens deze wet zijn vastgelegd of die verband houden met een gezond en voorzichtig beleid van de aanbieder of indien de beslissing de continuïteit en stabiliteit van het uitvoeren van nationale en internationale financiële transacties of de soliditeit van het financieel stelsel ernstig zou kunnen aantasten. Als zij niet binnen de voornoemde termijn optreedt, wordt de toestemming geacht te zijn verkregen.

§ 3. De Bank kan, bij reglement vastgesteld in toepassing van artikel 8, § 2, van de wet van 22 februari 1998 nader bepalen welke beslissingen als strategisch moeten worden beschouwd in de zin van artikel 3, 11°, met name rekening houdend met het risicoprofiel en

§ 2. La Banque, par voie de règlement pris en application de l'article 8, § 2, de la loi du 22 février 1998, peut préciser les exigences visées au paragraphe 1er.

Art. 38

Chaque fournisseur d'importance systémique tient à jour un plan pour:

1° lever des capitaux propres supplémentaires, pour le cas où son capital approcherait du seuil énoncé à l'article 37 ou tomberait sous ce seuil;

2° assurer le redressement ou la cessation ordonnée de ses activités et services au cas où il ne serait pas en mesure de lever de nouveaux capitaux.

Le plan est approuvé par le conseil de surveillance ou un comité compétent à cet égard de cet organe et est régulièrement, et au moins chaque année, mis à jour. Chaque mise à jour du plan est transmise à la Banque. La Banque peut demander que le fournisseur d'importance systémique prenne des mesures supplémentaires ou prévoie d'autres dispositions si elle estime le plan du fournisseur insuffisant.

CHAPITRE 5

Décisions stratégiques

Art. 39

§ 1er. Les décisions stratégiques sont soumises à l'autorisation préalable de la Banque.

§ 2. La Banque se prononce dans les deux mois de la réception d'un dossier complet de la décision stratégique prévue. Elle ne peut refuser son autorisation que pour des motifs tenant à la capacité du fournisseur d'importance systémique à satisfaire aux dispositions prévues par ou en vertu de la présente loi ou tenant à la gestion saine et prudente du fournisseur ou si la décision est susceptible d'affecter de façon significative la continuité et la stabilité de l'exécution de transactions financières nationales et internationales ou la solidité du système financier. Si elle n'intervient pas dans le délai fixé ci-dessus, l'autorisation est réputée acquise.

§ 3. La Banque peut, par voie de règlement pris en application de l'article 8, § 2, de la loi du 22 février 1998, préciser les décisions qui sont à considérer comme stratégiques au sens de l'article 3, 11°, en tenant notamment compte du profil de risque et de la nature des activités

de aard van de werkzaamheden van systeemrelevante aanbieders, of, in voorkomend geval, de groep waartoe ze behoren.

HOOFDSTUK 6

Uitbesteding

Art. 40

§ 1. Indien een systeemrelevante aanbieder activiteiten aan een derde, met inbegrip van derde aanbieders van ICT-diensten, uitbesteedt, blijft hij volledig verantwoordelijk voor het vervullen van al zijn verplichtingen uit hoofde van deze wet en neemt hij te allen tijde de volgende voorwaarden in acht:

1° de uitbesteding leidt er niet toe dat de systeemrelevante aanbieder zijn verantwoordelijkheden voor het vervullen van zijn verplichtingen uit hoofde van deze wet delegeert;

2° de relatie en verplichtingen van de systeemrelevante aanbieder ten opzichte van zijn dienstafnemers worden niet gewijzigd;

3° de naleving van de vereisten waaraan de systeemrelevante aanbieder krachtens deze wet moet voldoen, mag niet worden ondermijnd;

4° de uitbesteding mag geen wezenlijke afbreuk doen aan de kwaliteit van de interne controle van de systeemrelevante aanbieder en aan het vermogen van de Bank om de naleving door de systeemrelevante aanbieder van zijn verplichtingen te controleren;

5° de systeemrelevante aanbieder heeft directe toegang tot de relevante informatie over de uitbestede diensten;

6° de dienstverrichter werkt in verband met de uitbestede activiteiten met de Bank samen.

§ 2. De systeemrelevante aanbieder bepaalt in een schriftelijke overeenkomst zijn rechten en verplichtingen en die van de dienstverrichter. De uitbestedingsovereenkomst staat toe dat de systeemrelevante aanbieder de overeenkomst beëindigt.

Art. 41

§ 1. Een systeemrelevante aanbieder mag kritieke of belangrijke functies met betrekking tot financiële

des fournisseurs d'importance systémique, ou, le cas échéant, le groupe auxquels ils appartiennent.

CHAPITRE 6

Externalisation

Art. 40

§ 1er. Si un fournisseur d'importance systémique externalise des activités vers un prestataire tiers, y compris en cas d'externalisation vers un prestataire tiers de services TIC, il reste pleinement responsable du respect de toutes les obligations qui lui incombent en vertu de la présente loi et se conforme à tout moment aux conditions suivantes:

1° l'externalisation n'entraîne aucune délégation de la responsabilité du fournisseur d'importance systémique pour respecter les obligations qui lui incombent en vertu de la présente loi;

2° la relation et les obligations du fournisseur d'importance systémique vis-à-vis de ses acheteurs de service ne sont pas modifiées;

3° le respect des exigences que le fournisseur d'importance systémique est tenu de remplir en vertu de la présente loi n'est pas altéré;

4° l'externalisation ne peut pas être faite d'une manière qui nuise sérieusement à la qualité du contrôle interne du fournisseur d'importance systémique et qui empêche la Banque de contrôler le respect, par le fournisseur d'importance systémique, de ses obligations;

5° le fournisseur d'importance systémique a un accès direct aux informations pertinentes concernant les services externalisés;

6° le prestataire de services coopère avec la Banque en ce qui concerne les activités externalisées.

§ 2. Le fournisseur d'importance systémique définit par un accord écrit ses droits et obligations et ceux du prestataire de services. L'accord d'externalisation comporte la possibilité pour le fournisseur d'importance systémique d'y mettre un terme.

Art. 41

§ 1er. Un fournisseur d'importance systémique ne peut externaliser des fonctions critiques ou importantes

berichtendiensten slechts uitbesteden aan een dienstverrichter nadat de Bank haar toestemming heeft verleend.

§ 2. Gelet op de noodzaak van een gezond en voorzichtig beleid, een passende risicobeheersing en de continuïteit en stabiliteit van de uitvoering van nationale en internationale financiële transacties en de soliditeit van het financieel stelsel, kan de Bank de uitbesteding van kritieke of belangrijke functies aan bijkomende voorwaarden onderwerpen, waaronder op het vlak van exitstrategieën en exitplanning.

Art. 42

De Bank kan, bij reglement vastgesteld in toepassing van artikel 8, § 2, van de wet van 22 februari 1998, de elementen bedoeld in de artikelen 40 en 41 preciseren en aanvullen.

HOOFDSTUK 7

Bedrijfsvoering en risicobeheersing

Afdeling I

Algemene bepalingen

Art. 43

Een systeemrelevante aanbieder heeft welomschreven doelstellingen die haalbaar zijn, onder meer op het gebied van minimumdienstniveaus, risicomanagementverwachtingen en zakelijke prioriteiten.

Art. 44

Een systeemrelevante aanbieder zorgt voor solide beheers- en controlesystemen voor het vaststellen, bewaken en beheren van algemene bedrijfsrisico's, waaronder verliezen die voortvloeien uit slechte uitoefening van de bedrijfsstrategie, negatieve cashflows of onverwachte en excessief hoge exploitatiekosten.

Art. 45

De Bank kan bij reglement vastgesteld in toepassing van artikel 8, § 2, van de wet van 22 februari 1998, de inhoud en de nadere regels van de toepassing van de vereisten van dit hoofdstuk preciseren en aanvullen.

relatives aux services de messagerie financière à un prestataire de services qu'avec l'autorisation préalable de la Banque.

§ 2. En vue d'une gestion saine et prudente, d'une maîtrise adéquate des risques et de la continuité et de la stabilité de l'exécution de transactions financières nationales et internationales et de la solidité du système financier, la Banque peut soumettre l'externalisation des fonctions critiques ou importantes à des conditions additionnelles, y inclus dans le domaine des stratégies et plans de sortie.

Art. 42

La Banque peut, par voie de règlement pris en application de l'article 8, § 2, de la loi du 22 février 1998, préciser et compléter les éléments visés aux articles 40 et 41.

CHAPITRE 7

Conduite des activités et gestion des risques

Section Ire

Dispositions générales

Art. 43

Un fournisseur d'importance systémique a des objectifs clairement définis et réalisables, notamment en ce qui concerne les niveaux de service minimum, les perspectives en matière de gestion des risques et les priorités économiques.

Art. 44

Un fournisseur d'importance systémique établit des systèmes de gestion et de contrôle solides afin d'identifier, de surveiller et de gérer les risques d'activité, y compris les pertes dues à une mauvaise exécution de la stratégie commerciale, à des flux de trésorerie négatifs ou à des charges d'exploitation inattendues et excessivement élevées.

Art. 45

La Banque peut, par voie de règlement pris en application de l'article 8, § 2, de la loi du 22 février 1998, préciser et compléter le contenu et les modalités d'application des exigences définies dans ce chapitre.

Afdeling II

Juridische risico's

Art. 46

§ 1. Een systeemrelevante aanbieder stelt regels en procedures vast en gaat overeenkomsten aan, welke helder zijn en consistent met het toepasselijke recht van alle relevante jurisdicties.

§ 2. Een systeemrelevante aanbieder stelt zijn regels, procedures en overeenkomsten zo op dat zij in alle relevante jurisdicties afdwingbaar zijn.

§ 3. Een systeemrelevante aanbieder die zijn bedrijfsactiviteiten in meer dan één jurisdictie uitoefent, stelt de risico's die voortvloeien uit enig mogelijk wetsconflict vast en beperkt deze.

Afdeling III

Integraal risicobeheerskader

Art. 47

§ 1. Een systeemrelevante aanbieder zet een solide risicobeheerskader op dat hem in staat stelt om de risico's die zich voordoen of door hem gedragen worden te identificeren, meten, opvolgen en beheersen. Hij herziet het risicobeheerskader tenminste eenmaal per jaar. Het risicobeheerskader:

1° omvat het beleid inzake risicobereidheid van de systeemrelevante aanbieder en passende risicobeheersinstrumenten;

2° omvat de interne verslaggeving over de risico's die de systeemrelevante aanbieder kan lopen, met inbegrip van de voorkoming van belangenconflicten;

3° wijst verantwoordelijkheden en verantwoordingsplichten toe met betrekking tot risicobeslissingen;

4° behandelt besluitvorming in buitengewone omstandigheden met betrekking tot de systeemrelevante aanbieder, inclusief ontwikkelingen op de financiële markten die een schadelijk effect hebben op de stabiliteit van het uitvoeren van nationale en internationale financiële transacties.

§ 2. Een systeemrelevante aanbieder stimuleert zijn dienstafnemers, en waar van toepassing hun klanten, om de risico's die zij vormen voor het verlenen van financiële

Section II

Risques juridiques

Art. 46

§ 1er. Un fournisseur d'importance systémique définit des règles et des procédures et conclut des contrats, qui sont clairs et conformes à la législation en vigueur dans tous les systèmes juridiques pertinents.

§ 2. Un fournisseur d'importance systémique conçoit ses règles, procédures et contrats de telle manière qu'ils soient exécutoires dans tous les systèmes juridiques pertinents.

§ 3. Un fournisseur d'importance systémique qui opère dans plus d'un système juridique identifie et atténue les risques résultant de tout conflit de lois éventuel.

Section III

Cadre de gestion globale des risques

Art. 47

§ 1er. Un fournisseur d'importance systémique met en place un cadre solide de gestion des risques lui permettant d'identifier, de mesurer, de suivre et de maîtriser les risques qui surviennent ou qu'il supporte. Il réexamine le cadre de gestion des risques au moins une fois par an. Le cadre de gestion des risques:

1° inclut la politique de tolérance aux risques du fournisseur d'importance systémique ainsi que des outils appropriés de gestion des risques;

2° inclut le reporting interne des risques auxquels le fournisseur d'importance systémique est susceptible d'être exposé, y compris la prévention des conflits d'intérêts;

3° assigne la responsabilité et l'obligation de rendre compte des décisions relatives aux risques;

4° traite de la prise de décision dans les situations d'urgence concernant le fournisseur d'importance systémique, y compris les évolutions sur les marchés financiers susceptibles de nuire à la stabilité de l'exécution de transactions financières nationale et internationales.

§ 2. Un fournisseur d'importance systémique met en place des dispositifs incitant ses acheteurs de services et, le cas échéant, leurs clients à gérer et à contenir les

berichtendiensten evenals de risico's waaraan zij zelf blootstaan door een systeemrelevante aanbieder, te beheersen en te beperken. Met betrekking tot dienstafnemers kunnen dergelijke stimulerende maatregelen een effectief, proportioneel en afschrikwekkend boetesysteem en/of regelingen voor deling van verlies omvatten.

§ 3. Een systeemrelevante aanbieder toetst ten minste eenmaal per jaar de materiële risico's die het verlenen van financiële berichtendiensten loopt en zelf vormt voor andere entiteiten, als gevolg van onderlinge afhankelijkheden. De systeemrelevante aanbieder ontwikkelt risicobeheersinstrumenten die solide zijn en in verhouding staan tot het vastgestelde risiconiveau.

§ 4. Een systeemrelevante aanbieder identificeert zijn kritieke of belangrijke functies. Hij identificeert specifieke scenario's waardoor hij deze kritieke of belangrijke functies als going concern mogelijkerwijze niet zou kunnen leveren en beoordeelt de effectiviteit van alle herstelacties en een ordelijke liquidatie. Hij beoordeelt de kritieke of belangrijke functies tenminste eenmaal per jaar.

Afdeling IV

Herstel en ordelijke liquidatie

Art. 48

§ 1. Op basis van de in artikel 47, § 4, bedoelde beoordeling stelt een systeemrelevante aanbieder een uitvoerbaar herstelplan of een ordelijke liquidatieplan op. Het herstel- of ordelijke liquidatieplan bevat onder meer een inhoudelijke samenvatting van de cruciale herstel- of ordelijke liquidatiestrategieën, een herformulering van de kritieke of belangrijke functies en een beschrijving van de benodigde maatregelen voor het uitvoeren van de cruciale strategieën.

§ 2. Een systeemrelevante aanbieder stelt het bedrag aan activa vast dat nodig is om het in paragraaf 1 bedoelde herstel- of ordelijke liquidatieplan te implementeren. Het bedrag van deze activa wordt bepaald door het algemene bedrijfsrisicoprofiel en de duur van de periode die vereist is om, indien nodig, een herstel of ordelijke liquidatie tot stand te brengen van zijn kritieke of belangrijke functies. Dit bedrag is minstens gelijk aan het equivalent van exploitatiekosten over zes maanden.

§ 3. Om het in paragraaf 2 bedoelde bedrag af te dekken, houdt een systeemrelevante aanbieder liquide

risques qu'ils font courir à la fourniture de services de messagerie financière et que le fournisseur d'importance systémique leur fait supporter. En ce qui concerne les acheteurs de services, ces dispositifs incitatifs peuvent inclure un régime de sanctions pécuniaires efficaces, proportionnées et dissuasives ou des dispositifs de répartition des pertes, ou les deux.

§ 3. Un fournisseur d'importance systémique réexamine au moins annuellement les risques importants que d'autres entités font courir à la fourniture de services de messagerie financière ou qu'il fait courir à d'autres entités, en raison d'interdépendances. Le fournisseur d'importance systémique conçoit des outils de gestion des risques qui sont solides et proportionnés au niveau déterminé de risque.

§ 4. Un fournisseur d'importance systémique identifie ses fonctions critiques ou importantes. Il identifie les scénarios spécifiques susceptibles de l'empêcher d'assurer sans interruption ces fonctions critiques ou importantes, et évalue l'efficacité d'un éventail complet de solutions permettant le redressement ou la liquidation ordonnée de ses activités. Il évalue les fonctions critiques ou importantes au moins une fois par an.

Section IV

Redressement et liquidation ordonnée

Art. 48

§ 1er. Sur la base de l'évaluation visée à l'article 47, § 4, un fournisseur d'importance systémique élabore un plan viable de redressement ou de liquidation ordonnée de ses activités. Ce plan de redressement ou de liquidation ordonnée comporte, entre autres, une synthèse détaillée des stratégies clés de redressement ou de liquidation ordonnée des activités, une redéfinition des fonctions critiques ou importantes et une description des mesures nécessaires pour la mise en œuvre de ces stratégies clés.

§ 2. Un fournisseur d'importance systémique détermine le montant d'actifs nécessaire pour mettre en œuvre le plan de redressement ou de liquidation ordonnée visé au paragraphe 1er. Le montant de ces actifs est déterminé en fonction du profil général de risque d'activité et du temps nécessaire pour procéder, si besoin, à un redressement ou à la liquidation ordonnée de ses fonctions critiques ou importantes. Ce montant représente au moins six mois de charges d'exploitation courantes.

§ 3. Afin de couvrir le montant visé au paragraphe 2, un fournisseur d'importance systémique détient des

netto-activa aan die worden verschaft middels deelnemingen, zoals gewone aandelen, reserves of overgedragen resultaten, zodat hij de bedrijfsvoering en de diensten kan voortzetten als een going concern.

§ 4. Activa die worden aangehouden ter afdekking van het algemene bedrijfsrisico zijn dermate liquide en van hoge kwaliteit dat deze tijdig beschikbaar zijn. De systeemrelevante aanbieder moet deze activa met weinig of geen nadelig prijseffect kunnen verkopen, zodat hij de bedrijfsvoering kan voortzetten als going concern wanneer algemene bedrijfsverliezen worden geleden.

Afdeling V

Beleggingsrisico's

Art. 49

§ 1. Een systeemrelevante aanbieder heeft een investeringsstrategie die consistent is met zijn algehele risicobeheerstrategie. De systeemrelevante aanbieder herziet deze investeringsstrategie tenminste eenmaal per jaar.

§ 2. De investeringen van een systeemrelevante aanbieder op basis van zijn investeringsstrategie worden gedekt door debiteuren van hoge kwaliteit of vorderingen op deze. Een systeemrelevante aanbieder stelt criteria voor debiteuren van hoge kwaliteit vast. Investeringen worden gedaan in instrumenten met een minimaal krediet-, markt- en liquiditeitsrisico.

Afdeling VI

Operationeel risico

Art. 50

§ 1. Een systeemrelevante aanbieder zet een solide kader op met toepasselijke systemen, beleidslijnen, procedures en controles voor het vaststellen, bewaken en beheren van exploitatierisico's.

Regelmatig, en na iedere significante verandering, toetst, herbeoordeelt en test een systeemrelevante aanbieder de systemen evenals het operationeel beleid en de operationele procedures en controles.

§ 2. Een systeemrelevante aanbieder stelt doelstellingen vast met betrekking tot het dienstverleningsniveau en de betrouwbaarheid van de exploitatie, evenals

actifs nets liquides financés par des fonds propres, par exemple des actions ordinaires, des réserves ou des résultats reportés, de façon à pouvoir assurer la continuité de ses opérations et de ses services.

§ 4. Les actifs détenus pour couvrir le risque général d'activité sont de qualité élevée et suffisamment liquides pour être disponibles en temps utile. Le fournisseur d'importance systémique peut liquider ces actifs sans effets négatifs sur les prix, ou avec des effets minimes, de sorte qu'il peut assurer la continuité de ses opérations si ces pertes d'activité se matérialisent.

Section V

Risques d'investissement

Art. 49

§ 1er. Un fournisseur d'importance systémique définit sa stratégie d'investissement de manière compatible avec sa stratégie globale de gestion du risque. Il réexamine la stratégie d'investissement au moins une fois par an.

§ 2. Les placements effectués par le fournisseur d'importance systémique en vertu de sa stratégie d'investissement sont garantis par, ou sont des créances sur, des débiteurs de haute qualité. Le fournisseur d'importance systémique définit les critères auxquels répondent les débiteurs de haute de qualité. Les instruments d'investissement présentent des risques minimes de crédit, de marché et de liquidité.

Section VI

Risque opérationnel

Art. 50

§ 1er. Un fournisseur d'importance systémique met en place un cadre solide, doté de systèmes, de politiques, de procédures et de contrôles appropriés pour identifier, surveiller et gérer les risques opérationnels.

Un fournisseur d'importance systémique réexamine, vérifie et teste les systèmes ainsi que les politiques, procédures et contrôles opérationnels de manière régulière et après tout changement important.

§ 2. Un fournisseur d'importance systémique définit des objectifs en termes de niveau de service et de fiabilité opérationnelle, ainsi que des politiques conçues

beleidslijnen om die doelstellingen te bereiken. De systeemrelevante aanbieder herziet de doelstellingen en beleidslijnen tenminste eenmaal per jaar.

§ 3. Een systeemrelevante aanbieder zet een integraal beleid op met betrekking tot fysieke veiligheid en beveiliging, beschikbaarheid, confidentialiteit, authenticiteit en integriteit van informatie waarmee alle mogelijke zwakheden en bedreigingen genoegzaam kunnen worden vastgesteld, beoordeeld en beheerst. De systeemrelevante aanbieder herbeoordeelt het beleid tenminste eenmaal per jaar.

§ 4. Een systeemrelevante aanbieder stelt vast wie de kritieke dienstafnemers zijn, met name op basis van volumes van afgenomen financiële berichtendiensten en de waarde daarvan, alsmede hun potentiële invloed op andere dienstafnemers en op de dienstverlening door de systeemrelevante aanbieder indien die kritieke dienstafnemers te maken krijgen met een aanzienlijk exploitatieprobleem.

§ 5. Een systeemrelevante aanbieder stelt de risico's vast, bewaakt en beheert deze, die kritieke dienstafnemers, andere financiële marktinfrastructuren en dienstverleners kunnen vormen voor de operaties van de systeemrelevante aanbieder.

Afdeling VII

Bedrijfscontinuïteit en beschikbaarheid van de dienstverlening

Art. 51

§ 1. Onverminderd het bepaalde in artikel 50, zet een systeemrelevante aanbieder een bedrijfscontinuïteitsplan op met betrekking tot gebeurtenissen die het verlenen van financiële berichtendiensten aanzienlijk kunnen verstoren. Dit plan wordt goedgekeurd door de raad van toezicht en:

1° streeft naar een snel herstel van de activiteiten en de naleving van zijn verplichtingen in het geval van een storing in het verstrekken van financiële berichtendiensten;

2° is zodanig opgezet dat de systeemrelevante aanbieder in staat is om alle verstoorde financiële berichtendiensten zo snel mogelijk te hernemen.

De systeemrelevante aanbieder test het plan tenminste eenmaal per jaar en herziet het. Naar gelang het geval nemen dienstafnemers en derde aanbieders

pour atteindre ces objectifs. Il réexamine ces objectifs et politiques au moins une fois par an.

§ 3. Un fournisseur d'importance systémique dispose de politiques détaillées en termes de sécurité physique et de sécurité, disponibilité, confidentialité, authenticité et intégrité de l'information, qui identifient, évaluent et gèrent de façon adéquate toutes les vulnérabilités et menaces potentielles. Il réexamine ces politiques au moins une fois par an.

§ 4. Un fournisseur d'importance systémique identifie les acheteurs de services critiques en fonction, notamment, des volumes de services de messagerie financière achetés et de leur valeur, ainsi que de leur impact potentiel sur d'autres acheteurs de services et sur la fourniture de services par le fournisseur d'importance systémique, en cas de problème opérationnel significatif rencontré par ces acheteurs de services critiques.

§ 5. Un fournisseur d'importance systémique identifie, surveille et gère les risques auxquels les acheteurs de services critiques, d'autres infrastructures de marché financières et des prestataires de services pourraient exposer les opérations du fournisseur d'importance systémique.

Section VII

Continuité d'activité et disponibilité des services

Art. 51

§ 1er. Sans préjudice de l'article 50, un fournisseur d'importance systémique élabore un plan de continuité d'activité qui remédie aux événements constituant un risque important pour le bon fonctionnement de la fourniture de services de messagerie financière. Ce plan est approuvé par le conseil de surveillance et:

1° tend vers une reprise rapide des activités et le respect de ses obligations en cas de perturbation de la fourniture de services de messagerie financière;

2° est conçu de manière à ce que que le fournisseur d'importance systémique soit toujours en mesure de reprendre le plus vite possible tous les services de messagerie financière perturbés.

Le fournisseur d'importance systémique teste et réexamine le plan au moins une fois par an. Selon le cas, les acheteurs de services et les prestataires tiers de

van ICT-diensten die diensten verlenen die kritieke of belangrijke functies ondersteunen deel aan het testen van het plan.

§ 2. Een systeemrelevante aanbieder brengt de Bank onmiddellijk op de hoogte wanneer er aanwijzingen zijn dat het bedrijfscontinuïteitsplan geheel of gedeeltelijk moet worden toegepast.

§ 3. Een systeemrelevante aanbieder verzekert dat hij zijn capaciteit voor het verlenen van financiële berichtendiensten te allen tijde kan uitbreiden in geval van toename van de te behandelen volumes ingevolge stress-evenementen. Tevens verzekert hij dat het nagestreefde dienstverleningsniveau kan behouden blijven.

Afdeling VIII

Digitale operationele weerbaarheid

Art. 52

§ 1. Een systeemrelevante aanbieder zet een effectief kader voor het beheer van het ICT-risico op met passende governancemaatregelen teneinde een hoog niveau van digitale operationele weerbaarheid te verkrijgen. Na alle operaties en onderliggende activa geïdentificeerd te hebben, treft de systeemrelevante aanbieder passende maatregelen om ze te beschermen tegen cyberaanvallen, deze op te sporen, erop te reageren en ervan te herstellen. Deze maatregelen worden regelmatig getest.

§ 2. De raad van toezicht van een systeemrelevante aanbieder bepaalt alle regelingen met betrekking tot het in paragraaf 1 bedoelde beheerskader, keurt deze goed, houdt toezicht op de uitvoering ervan en is ervoor verantwoordelijk. Daartoe is de raad van toezicht belast met:

1° de eindverantwoordelijkheid voor het beheer van het ICT-risico van de systeemrelevante aanbieder;

2° de invoering van beleidslijnen die erop gericht zijn de handhaving van hoge normen inzake beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens te waarborgen;

3° de vaststelling van duidelijke taken en verantwoordelijkheden voor alle ICT-gerelateerde functies en van passende governanceregelingen om te zorgen voor doeltreffende en tijdige communicatie, samenwerking en coördinatie tussen die functies;

4° de algemene verantwoordelijkheid voor het vaststellen en goedkeuren van de strategie voor digitale

services TIC qui fournissent des services qui soutiennent des fonctions critiques ou importantes participent dans le test du plan.

§ 2. Un fournisseur d'importance systémique informe immédiatement la Banque lorsqu'il existe des indications selon lesquelles le plan de continuité d'activité doit être appliqué en tout ou en partie.

§ 3. Un fournisseur d'importance systémique veille à ce qu'il peut à tout moment étendre sa capacité à fournir des services de messagerie financière en cas d'augmentation des volumes à traiter en raison d'événements de crise. Il assure également qu'il peut atteindre ses objectifs de niveau de service.

Section VIII

Résilience opérationnelle numérique

Art. 52

§ 1er. Un fournisseur d'importance systémique met en place un cadre efficace pour la gestion du risque TIC, ainsi que des mesures de gouvernance appropriées, afin d'atteindre un niveau élevé de résilience opérationnelle numérique. Après avoir identifié toutes ses opérations et les actifs sous-jacents, le fournisseur d'importance systémique instaure des mesures appropriées afin de les protéger des cyber-attaques, de les détecter de réagir à celles-ci et de les surmonter. Ces mesures sont régulièrement testées.

§ 2. Le conseil de surveillance du fournisseur d'importance systémique définit, approuve, supervise et est responsable de la mise en œuvre de toutes les dispositions relatives au cadre de gestion visé au paragraphe 1er. À ces fins, le conseil de surveillance:

1° assume la responsabilité ultime de la gestion du risque lié aux TIC du fournisseur d'importance systémique;

2° met en place des stratégies visant à garantir le maintien de normes élevées en matière de disponibilité, d'authenticité, d'intégrité et de confidentialité des données;

3° définit clairement les rôles et les responsabilités pour toutes les fonctions liées aux TIC et met en place des dispositifs de gouvernance appropriés pour assurer une communication, une coopération et une coordination efficaces et en temps utile entre ces fonctions;

4° assume la responsabilité globale de la définition et de l'approbation de la stratégie de résilience

operationele weerbaarheid als bedoeld in artikel 54, § 4, met inbegrip van de bepaling van een passend risicotolerantieniveau voor het ICT-risico van de systeemrelevante aanbieder;

5° de goedkeuring van, het toezicht op en de periodieke evaluatie van de uitvoering van het beleid inzake ICT-bedrijfscontinuïteit en van de ICT-respons- en herstelplannen van de systeemrelevante aanbieder, als bedoeld in respectievelijk artikel 59, § 1 en § 2, die een integrerend onderdeel mogen uitmaken van het ruimere beleid inzake bedrijfscontinuïteit bedoeld in artikel 51 en het herstelplan bedoeld in artikel 48;

6° de goedkeuring en de periodieke evaluatie van de interne ICT-auditplannen en ICT-audits van de systeemrelevante aanbieder en significante wijzigingen daarvan;

7° de toewijzing en de periodieke evaluatie van een passend budget om te voldoen aan de behoeften inzake digitale operationele weerbaarheid met betrekking tot alle soorten middelen, waaronder relevante bewustmakingsprogramma's op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele weerbaarheid zoals bedoeld in artikel 61, § 5, en ICT-vaardigheden voor al het personeel;

8° de goedkeuring en de periodieke evaluatie van het beleid van de systeemrelevante aanbieder inzake regelingen betreffende het gebruik van ICT-diensten die door derde aanbieders van ICT-diensten worden verleend;

9° het opzetten van meldingskanalen op bedrijfsniveau die het in staat stellen informatie in te winnen over:

a) overeenkomsten met derde aanbieders van ICT-diensten inzake het gebruik van ICT-diensten;

b) elke relevante geplande significante wijziging betreffende de derde aanbieders van ICT-diensten;

c) de potentiële effecten van deze veranderingen voor de kritieke of belangrijke functies die onder die overeenkomsten vallen, inclusief door middel van een samenvatting van de risicoanalyse om het effect te beoordelen van die veranderingen en op zijn minst ernstige ICT-gerelateerde incidenten en de gevolgen daarvan, alsook respons-, herstel- en corrigerende maatregelen.

§ 3. De leden van de raad van toezicht onderhouden actief voldoende kennis en vaardigheden om ICT-risico en de gevolgen daarvan voor de verrichtingen van de systeemrelevante aanbieder te begrijpen en te beoordelen, onder meer door regelmatig specifieke opleidingen

opérationnelle numérique visée à l'article 54, § 4, y compris la détermination d'un niveau approprié de tolérance au risque lié aux TIC du fournisseur d'importance systémique;

5° approuve, supervise et examine périodiquement la mise en œuvre de la politique de continuité des activités de TIC du fournisseur d'importance systémique et des plans de réponse et de rétablissement des TIC visés, respectivement, à l'article 59, § 1er et § 2, qui peuvent faire partie intégrante de la politique globale de continuité d'activité visée à l'article 51 et du plan de redressement visé à l'article 48;

6° approuve et examine périodiquement les plans internes d'audit des TIC et les audits des TIC du fournisseur d'importance systémique ainsi que les modifications significatives qui y sont apportées;

7° alloue et réexamine périodiquement un budget approprié pour satisfaire les besoins en matière de résilience opérationnelle numérique pour tous les types de ressources, y compris les programmes pertinents de sensibilisation à la sécurité des TIC et les formations pertinentes à la résilience opérationnelle numérique visés à l'article 61, § 5, et les compétences en matière de TIC pour l'ensemble du personnel;

8° approuve et examine périodiquement la politique du fournisseur d'importance systémique concernant les modalités d'utilisation des services TIC fournis par des prestataires tiers de services TIC;

9° met en place, au niveau de l'entreprise, des canaux de notification lui permettant d'être dûment informé des éléments suivants:

a) des accords conclus avec des prestataires tiers de services TIC sur l'utilisation des services TIC;

b) de tout changement significatif pertinent prévu concernant les prestataires tiers de services TIC;

c) des incidences potentielles de ces changements sur les fonctions critiques ou importantes faisant l'objet de ces accords, notamment un résumé de l'analyse des risques visant à évaluer les incidences de ces changements, et au minimum des incidents majeurs liés aux TIC et de leur incidence, ainsi que des mesures de réponse, de rétablissement et de correction.

§ 3. Les membres du conseil de surveillance maintiennent activement à jour des connaissances et des compétences suffisantes pour comprendre et évaluer le risque lié aux TIC et son incidence sur les opérations du fournisseur d'importance systémique, notamment en

te volgen die in verhouding staan tot het te beheren ICT-risico.

Art. 53

§ 1. Iedere systeemrelevante aanbieder beschikt over een passende functie van beveiliging van de netwerk- en informatiesystemen die zorgt voor de ontwikkeling, implementatie en controle door de systeemrelevante aanbieder van een beleid en procedures die, in overeenstemming met de bepalingen van deze afdeling, een passende beveiliging bieden van de netwerk- en informatiesystemen en een passend beheer van de daaraan verbonden ICT-risico's.

Deze functie monitort bovendien de overeenkomsten met derde aanbieders van ICT-diensten met betrekking tot het gebruik van deze diensten en is verantwoordelijk voor het toezicht op de desbetreffende risicoblootstelling en de relevante documentatie.

§ 2. De functie van beveiliging van de netwerk- en informatiesystemen:

1° is onafhankelijk van de operationele functies, in het bijzonder van de diensten die verantwoordelijk zijn voor de exploitatie en de ontwikkeling van ICT-systemen;

2° wordt niet betrokken bij interne auditactiviteiten;

3° heeft een gedegen kennis van logische en fysieke beveiligingsoplossingen evenals een grondig begrip van het bedrijfsmodel en de organisatiestructuur van de systeemrelevante aanbieder;

4° heeft rechtstreeks toegang tot de raad van toezicht en de directieraad.

§ 3. De personen die belast zijn met de functie van beveiliging van de netwerk- en informatiesystemen brengen minstens tweemaal per jaar verslag uit aan de directieraad.

Art. 54

§ 1. Iedere systeemrelevante aanbieder beschikt over een solide, alomvattend en goed gedocumenteerd kader voor ICT-risicobeheer, als onderdeel van het integraal risicobeheerskader bedoeld in artikel 47, dat hem in staat stelt ICT-risico snel, efficiënt en zo volledig mogelijk aan te pakken en een hoog niveau van digitale operationele weerbaarheid te waarborgen.

suivant régulièrement une formation spécifique proportionnée au risque lié aux TIC géré.

Art. 53

§ 1er. Chaque fournisseur d'importance systémique dispose d'une fonction de sécurité des réseaux et systèmes d'information adéquate qui assure le développement, la mise en œuvre et le contrôle, par le fournisseur d'importance systémique, de politiques et procédures offrant une protection adéquate des réseaux et systèmes d'information et une gestion adéquate des risques liés aux TIC y afférents, conformément aux dispositions de la section présente.

En plus, cette fonction fait le suivi des accords conclus avec des prestataires tiers de services TIC sur l'utilisation des services TIC et est chargée de superviser l'exposition aux risques connexe et la documentation pertinente.

§ 2. La fonction de sécurité des réseaux et systèmes d'information:

1° est indépendante des fonctions opérationnelles, notamment des services responsables de l'exploitation et du développement des systèmes TIC;

2° n'est pas impliqué dans des activités d'audit interne;

3° possède une solide connaissance des solutions de sécurité logique et physique, ainsi qu'une compréhension approfondie du modèle d'entreprise et de la structure organisationnelle du fournisseur d'importance systémique;

4° a un accès direct au conseil de surveillance et au conseil de direction.

§ 3. Les personnes qui assurent la fonction de sécurité des réseaux et systèmes d'information font rapport au conseil de direction au moins deux fois par an.

Art. 54

§ 1er. Chaque fournisseur d'importance systémique dispose d'un cadre de gestion du risque lié aux TIC solide, complet et bien documenté, faisant partie de son cadre de gestion global des risques visé à l'article 47, qui lui permet de parer au risque lié aux TIC de manière rapide, efficiente et exhaustive et de garantir un niveau élevé de résilience opérationnelle numérique.

§ 2. Het kader voor ICT-risicobeheer omvat ten minste strategieën, beleidslijnen, procedures, ICT-protocollen en instrumenten die nodig zijn om alle informatie- en ICT-activa, met inbegrip van computersoftware, hardware en servers, naar behoren en toereikend te beschermen, en om alle relevante fysieke elementen en infrastructuur, zoals gebouwen en terreinen, datacentra en als gevoelig aangewezen gebieden te beschermen, teneinde te waarborgen dat alle informatie- en ICT-activa toereikend worden beschermd tegen risico's, waaronder schade, ongeoorloofde toegang en ongeoorloofd gebruik.

§ 3. Het kader voor ICT-risicobeheer wordt ten minste eenmaal per jaar gedocumenteerd en geëvalueerd, alsook wanneer zich ernstige ICT-gerelateerde incidenten voordoen en ingevolge conclusies die voortvloeien uit relevante tests of auditprocessen op het gebied van digitale operationele weerbaarheid. Het wordt voortdurend verbeterd op basis van de lessen die uit de uitvoering en de monitoring naar voren komen.

§ 4. Het kader voor ICT-risicobeheer verduidelijkt via welke methoden de strategie voor digitale operationele weerbaarheid wordt uitgevoerd en specifieke ICT-doelstellingen worden verwezenlijkt.

Art. 55

§ 1. Om ICT-risico aan te pakken en te beheren, gebruiken en onderhouden systeemrelevante aanbieders geactualiseerde ICT-systemen, -protocollen en -instrumenten die:

1° geschikt zijn gezien de omvang van de verrichtingen ter ondersteuning van hun activiteiten;

2° betrouwbaar zijn;

3° voldoende capaciteit hebben voor een nauwkeurige verwerking van de gegevens die nodig zijn voor de uitvoering van activiteiten en de tijdige verlening van diensten, en om zo nodig volumepieken in orders, orderberichten of transacties op te vangen, onder meer wanneer nieuwe technologie wordt ingevoerd;

4° technologisch gezien voldoende weerbaar zijn om indien nodig in gespannen marktomstandigheden of andere ongunstige situaties naar behoren te voorzien in bijkomende gegevensverwerking.

§ 2. Systeemrelevante aanbieders beschikken over robuuste methodologieën teneinde te kunnen plannen

§ 2. Le cadre de gestion du risque lié aux TIC englobe au moins les stratégies, les politiques, les procédures, les protocoles et les outils de TIC qui sont nécessaires pour protéger dûment et de manière appropriée tous les actifs informationnels et les actifs de TIC, y compris les logiciels, le matériel informatique, les serveurs, ainsi que toutes les composantes et infrastructures physiques pertinentes, telles que les locaux, centres de données et zones sensibles désignées, afin de garantir que tous les actifs informationnels et actifs de TIC sont correctement protégés contre les risques, y compris les dommages et les accès ou utilisations non autorisés.

§ 3. Le cadre de gestion du risque lié aux TIC est documenté et réexaminé au moins une fois par an, ainsi qu'en cas de survenance d'incidents majeurs liés aux TIC, et conformément aux conclusions tirées des tests de résilience opérationnelle numérique ou des processus d'audit pertinents. Il est amélioré en permanence sur la base des enseignements tirés de la mise en œuvre et du suivi.

§ 4. Le cadre de gestion du risque lié aux TIC précise les méthodes pour mettre en œuvre la stratégie de résilience opérationnelle numérique et pour atteindre les objectifs spécifiques en matière de TIC.

Art. 55

§ 1er. Afin d'atténuer et de gérer le risque lié aux TIC, les fournisseurs d'importance systémique utilisent et tiennent à jour des systèmes, protocoles et outils de TIC qui sont:

1° adaptés à l'ampleur des opérations qui sous-tendent l'exercice de leurs activités;

2° fiables;

3° équipés d'une capacité suffisante pour traiter avec exactitude les données nécessaires à l'exécution des activités et à la fourniture des services en temps utile, et pour faire face aux pics de volume d'ordres, de messages ou de transactions, selon les besoins, y compris lorsque de nouvelles technologies sont mises en place;

4° suffisamment résilients sur le plan technologique pour répondre de manière adéquate aux besoins supplémentaires de traitement de l'information qui apparaissent en situation de tensions sur les marchés ou dans d'autres situations défavorables.

§ 2. Les fournisseurs d'importance systémique disposent de méthodologies robustes afin de pouvoir planifier

voor de gehele levensloop van de gebruikte technologieën en de selectie van technologische standaarden.

Art. 56

§ 1. In het kader van het in artikel 54, § 1, bedoelde kader voor ICT-risicobeheer identificeren, classificeren en documenteren systeemrelevante aanbieders naar behoren alle door ICT ondersteunde bedrijfsfuncties, taken en verantwoordelijkheden, de informatie- en ICT-activa die deze functies ondersteunen, en hun taken en afhankelijkheden met betrekking tot ICT-risico's.

§ 2. Systeemrelevante aanbieders identificeren permanent alle bronnen van ICT-risico, met name de wederzijdse risicoblootstelling ten aanzien van andere financiële entiteiten, en beoordelen de cyberdreigingen en ICT-kwetsbaarheden die relevant zijn voor hun door ICT ondersteunde bedrijfsfuncties en informatie- en ICT-activa. Zij evalueren regelmatig en ten minste eenmaal per jaar de risicoscenario's die op hen van invloed zijn.

§ 3. Systeemrelevante aanbieders verrichten een risicobeoordeling bij elke belangrijke wijziging in de netwerk- en informatiesysteeminfrastructuur en in de processen of procedures die van invloed zijn op hun door ICT ondersteunde bedrijfsfuncties en informatie- of ICT-activa.

§ 4. Systeemrelevante aanbieders identificeren alle informatie- en ICT-activa en inventariseren die welke zij cruciaal achten en de verbanden en onderlinge afhankelijkheden tussen de verschillende informatie- en ICT-activa.

§ 5. Systeemrelevante aanbieders identificeren en documenteren alle processen die afhankelijk zijn van derde aanbieders van ICT-diensten en identificeren interconnecties met derde aanbieders van ICT-diensten die diensten verlenen die kritieke of belangrijke functies ondersteunen.

Art. 57

§ 1. Om ICT-systemen op passende wijze te beschermen en met het oog op de organisatie van responsmaatregelen monitoren en controleren systeemrelevante aanbieders voortdurend de beveiliging en werking van de ICT-systemen en -instrumenten en beperken zij de effecten van ICT-risico op ICT-systemen door de inzet

l'ensemble de la durée de vie des technologies utilisées et la sélection de normes technologiques.

Art. 56

§ 1er. Aux fins du cadre de gestion du risque lié aux TIC visé à l'article 54, § 1er, les fournisseurs d'importance systémique identifient, classent et documentent de manière adéquate toutes les fonctions "métiers", tous les rôles et toutes les responsabilités s'appuyant sur les TIC, les actifs informationnels et les actifs de TIC qui soutiennent ces fonctions, ainsi que leurs rôles et dépendances en ce qui concerne le risque lié aux TIC.

§ 2. Les fournisseurs d'importance systémique identifient, de manière continue, toutes les sources de risque lié aux TIC, en particulier l'exposition au risque vis-à-vis d'autres entités financières et émanant de celles-ci, et évaluent les cybermenaces et les vulnérabilités des TIC qui concernent leurs fonctions "métiers" s'appuyant sur les TIC, leurs actifs informationnels et leurs actifs de TIC. Ils examinent régulièrement, et au moins une fois par an, les scénarios de risque qui ont des incidences sur elles.

§ 3. Les fournisseurs d'importance systémique procèdent à une évaluation des risques à chaque modification importante de l'infrastructure du réseau et du système d'information, des processus ou des procédures, qui affecte leurs fonctions "métiers" s'appuyant sur les TIC, leurs actifs informationnels ou leurs actifs de TIC.

§ 4. Les fournisseurs d'importance systémique identifient tous les actifs informationnels et actifs de TIC et répertorient ceux considérés comme critiques et les liens et interdépendances entre les différents actifs informationnels et actifs de TIC.

§ 5. Les fournisseurs d'importance systémique identifient et documentent tous les processus qui dépendent de prestataires tiers de services TIC, et identifient les interconnexions avec des prestataires tiers de services TIC qui fournissent des services qui soutiennent des fonctions critiques ou importantes.

Art. 57

§ 1er. Aux fins de la protection adéquate des systèmes de TIC et en vue d'organiser les mesures de réponse, les fournisseurs d'importance systémique assurent un suivi et un contrôle permanents de la sécurité et du fonctionnement des systèmes et outils de TIC et réduisent au minimum l'incidence du risque lié aux TIC

van passende ICT-beveiligingsinstrumenten, -beleidslijnen en -procedures.

§ 2. Systeemrelevante aanbieders zorgen voor het ontwerp, de aanbesteding en de uitvoering van ICT-beveiligingsbeleidslijnen, -procedures, -protocollen en -instrumenten die er op gericht zijn de weerbaarheid, continuïteit en beschikbaarheid van ICT-systemen, met name die welke kritieke of belangrijke functies ondersteunen, te waarborgen alsmede hoge normen inzake beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens, zowel in rusttoestand, bij gebruik als bij doorvoer, te handhaven.

§ 3. In het kader van het in artikel 54, § 1, bedoelde kader voor ICT-risicobeheer zorgen systeemrelevante aanbieders voor het volgende:

1° zij ontwikkelen en documenteren een beleid inzake informatiebeveiliging waarin regels worden vastgesteld ter bescherming van de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens, informatie- en ICT-activa, inclusief die van hun gebruikers, in voorkomend geval;

2° zij voeren op grond van een op risico's gebaseerde aanpak een degelijke structuur voor netwerk- en infrastructuurbeheer in met gebruik van passende technieken, methoden en protocollen, eventueel met toepassing van geautomatiseerde mechanismen om in geval van cyberaanvallen de getroffen informatieactiva te isoleren;

3° zij voeren een beleid waarbij de fysieke of logische toegang tot informatie- en ICT-activa wordt beperkt tot hetgeen alleen voor legitieme en goedgekeurde functies en activiteiten noodzakelijk is, en voeren daartoe een reeks beleidslijnen, procedures en controles in om toegangsrechten en een degelijk beheer daarvan te waarborgen;

4° zij voeren beleidslijnen en protocollen in voor strenge authenticatiemechanismen die gebaseerd zijn op relevante normen, specifieke controlesystemen en beschermingsmaatregelen voor cryptografische sleutels, waarbij gegevens worden versleuteld uitgaande van de resultaten van goedgekeurde processen van gegevensclassificatie en ICT-risicobeoordeling;

5° zij voeren gedocumenteerde beleidslijnen, procedures en controles in voor het beheer van veranderingen in ICT, met inbegrip van veranderingen in software, hardware, firmwarecomponenten, systemen of beveiligingsparameters, die uitgaan van een op risicobeoordeling gebaseerde aanpak en integrerend deel uitmaken

sur les systèmes de TIC par le déploiement d'outils, de stratégies et de procédures appropriés en matière de sécurité des TIC.

§ 2. Les fournisseurs d'importance systémique conçoivent, acquièrent et mettent en œuvre des stratégies, des politiques, des procédures, des protocoles et des outils de sécurité de TIC qui visent à garantir la résilience, la continuité et la disponibilité des systèmes de TIC, en particulier ceux qui soutiennent des fonctions critiques ou importantes, et à maintenir des normes élevées en matière de disponibilité, d'authenticité, d'intégrité et de confidentialité des données, que ce soit au repos, en cours d'utilisation ou en transit.

§ 3. Aux fins du cadre de gestion du risque lié aux TIC visé à l'article 54, § 1er, les fournisseurs d'importance systémique:

1° élaborent et documentent une politique de sécurité de l'information qui définit des règles visant à protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, des actifs informationnels et des actifs de TIC, y compris ceux de leurs utilisateurs, le cas échéant;

2° instaurent, selon une approche fondée sur les risques, une gestion solide des réseaux et des infrastructures en recourant aux techniques, aux méthodes et aux protocoles appropriés, qui peuvent inclure la mise en œuvre de mécanismes automatisés pour isoler les actifs informationnels affectés en cas de cyberattaques;

3° mettent en œuvre des politiques qui limitent l'accès physique ou logique aux actifs informationnels et aux actifs de TIC, à ce qui est nécessaire pour les fonctions et les activités légitimes et approuvées uniquement, et définissent à cette fin un ensemble de politiques, de procédures et de contrôles qui portent sur les droits d'accès et veillent à leur bonne administration;

4° mettent en œuvre des politiques et des protocoles pour des mécanismes d'authentification forte, fondés sur des normes pertinentes et des systèmes de contrôle spécifiques, et des mesures de protection des clés de chiffrement par lesquelles les données sont chiffrées sur la base des résultats des processus approuvés de classification des données et d'évaluation du risque lié aux TIC;

5° mettent en œuvre des politiques, des procédures et des contrôles documentés pour la gestion des changements dans les TIC, y compris les changements apportés aux logiciels, au matériel, aux composants de micrologiciels, aux systèmes ou aux paramètres de sécurité, qui sont fondés sur une approche d'évaluation

van het algemene veranderingsbeheerproces van de systeemrelevante aanbieder, teneinde te garanderen dat alle veranderingen in ICT-systemen op gecontroleerde wijze worden geregistreerd, getest, beoordeeld, goedgekeurd, ingevoerd en geverifieerd;

6°zij beschikken over een passend en alomvattend gedocumenteerd beleid voor patches en updates.

Art. 58

§ 1. Systeemrelevante aanbieders beschikken over mechanismen om overeenkomstig artikel 66 afwijkende activiteiten zo spoedig mogelijk te detecteren, met inbegrip van kwesties op het gebied van ICT-netwerkprestaties en ICT-gerelateerde incidenten, en om potentiële zwakke fysieke punten ("*single points of failure*") te identificeren. Al deze detectiemechanismen worden regelmatig getest.

§ 2. De in paragraaf 1 bedoelde detectiemechanismen maken meerdere controlelagen mogelijk en bepalen waarschuwingsdrempels en criteria om processen voor respons op ICT-gerelateerde incidenten in werking te stellen, met inbegrip van automatische waarschuwingsmechanismen voor de betrokken personeelsleden die belast zijn met de respons op ICT-gerelateerde incidenten.

§ 3. Systeemrelevante aanbieders zetten voldoende middelen en capaciteiten in om toezicht te houden op activiteiten van gebruikers en het optreden van ICT-anomalieën en ICT-gerelateerde incidenten, met name cyberaanvallen.

Art. 59

§ 1. Systeemrelevante aanbieders voeren een alomvattend doch specifiek ICT-bedrijfscontinuïteitsbeleid dat een integrerend onderdeel vormt van het ruimere beleid inzake bedrijfscontinuïteit als bedoeld in artikel 51, en dat uitgevoerd wordt via specifieke, aangepaste en gedocumenteerde regelingen, plannen, procedures en mechanismen die erop gericht zijn:

1° de continuïteit van de kritieke of belangrijke functies van de systeemrelevante aanbieder te verzekeren;

2° op een snelle, passende en doeltreffende wijze een respons en een oplossing te bieden voor alle ICT-gerelateerde incidenten waarbij de schade wordt beperkt en prioriteit wordt verleend aan de hervatting van de activiteiten en aan herstelmaatregelen;

des risques et font partie intégrante du processus global de gestion des changements du fournisseur d'importance systémique, afin de garantir que tous les changements apportés aux systèmes de TIC sont consignés, testés, évalués, approuvés, mis en œuvre et vérifiés de manière contrôlée;

6° disposent de stratégies documentées appropriées et globales en matière de correctifs et de mises à jour.

Art. 58

§ 1er. Les fournisseurs d'importance systémique mettent en place des mécanismes permettant de détecter rapidement les activités anormales, conformément à l'article 66, y compris les problèmes de performance des réseaux de TIC et les incidents liés aux TIC, ainsi que de repérer les points uniques de défaillance potentiellement significatifs. Tous ces mécanismes de détection sont régulièrement testés.

§ 2. Les mécanismes de détection visés au paragraphe 1er permettent la mise en place de plusieurs niveaux de contrôle, définissent des seuils d'alerte et des critères de déclenchement et de lancement des processus de réponse en cas d'incident lié aux TIC, y compris des mécanismes d'alerte automatique destinés au personnel compétent chargé de la réponse aux incidents liés aux TIC.

§ 3. Les fournisseurs d'importance systémique consacrent des ressources et des capacités suffisantes pour surveiller l'activité des utilisateurs, l'apparition d'anomalies liées aux TIC et d'incidents liés aux TIC, en particulier les cyberattaques.

Art. 59

§ 1er. Les fournisseurs d'importance systémique se dotent d'une politique de continuité des activités de TIC complète mais spécifique, qui forme une partie intégrante de leur politique globale de continuité d'activité visé à l'article 51, et qui est mise en œuvre au moyen de dispositifs, de plans, de procédures et de mécanismes spécifiques, appropriés et documentés visant à:

1° garantir la continuité des fonctions critiques ou importantes du fournisseur d'importance systémique;

2° répondre aux incidents liés aux TIC et les résoudre rapidement, dûment et efficacement de manière à limiter les dommages et à donner la priorité à la reprise des activités et aux mesures de rétablissement;

3° onverwijld specifieke plannen in werking te stellen om inperkingsmaatregelen, -processen en -technologieën mogelijk te maken die aangepast zijn aan elk type ICT-gerelateerd incident en waarmee verdere schade kan worden voorkomen, alsmede op maat gesneden respons- en herstelprocedures in overeenstemming met artikel 60;

4° de voorlopige effecten, schade en verliezen te ramen;

5° maatregelen voor communicatie en crisisbeheersing op te stellen die garanderen dat aan alle betrokken personeelsleden en externe belanghebbenden geactualiseerde informatie wordt verstrekt overeenkomstig artikel 62, en verslag uit te brengen aan de Bank.

§ 2. Binnen het kader voor ICT-risicobeheer voeren systeemrelevante aanbieders bijbehorende ICT-respons- en herstelplannen in.

§ 3. Systeemrelevante aanbieders voeren passende ICT-bedrijfscontinuïteitsplannen in, handhaven deze en zorgen voor periodieke tests, met name wat betreft kritieke of belangrijke functies die zijn uitbesteed of via contractuele overeenkomsten met derde aanbieders van ICT-diensten zijn overeengekomen.

§ 4. In het kader van het algemene bedrijfscontinuiteitsbeleid voeren systeemrelevante aanbieders een bedrijfsimpactanalyse (business impact analysis – BIA) uit van hun blootstelling aan ernstige verstoringen van de bedrijfsactiviteiten. In het kader van de BIA beoordelen zij de potentiële gevolgen van ernstige verstoringen van de bedrijfsactiviteiten aan de hand van kwantitatieve en kwalitatieve criteria, in voorkomend geval met behulp van interne en externe gegevens en scenarioanalyse. In de BIA wordt rekening gehouden met de kritieke aard van geïdentificeerde en in kaart gebrachte bedrijfsfuncties, ondersteuningsprocessen, afhankelijkheden van derden en informatieactiva, en hun onderlinge afhankelijkheden. ICT-activa en ICT-diensten worden ontworpen en gebruikt in volledige overeenstemming met de BIA, met name om de redundantie van alle kritieke onderdelen adequaat te waarborgen.

§ 5. Systeemrelevante aanbieders testen:

1° de ICT-bedrijfscontinuïteitsplannen en de ICT-respons- en herstelplannen met betrekking tot ICT-systemen die kritieke of belangrijke functies ondersteunen, ten minste jaarlijks evenals in geval van substantiële wijzigingen in ICT-systemen die kritieke of belangrijke functies ondersteunen;

3° activer, sans retard, des plans spécifiques permettant de déployer des mesures, des processus et des technologies d'endiguement adaptés à chaque type d'incident lié aux TIC et de prévenir tout dommage supplémentaire, ainsi que des procédures sur mesure de réponse et de rétablissement, définies conformément à l'article 60;

4° estimer les incidences, les dommages et les pertes préliminaires;

5° définir des mesures de communication et de gestion des crises qui garantissent la transmission d'informations actualisées à tous les membres du personnel et à toutes les parties prenantes externes concernés, conformément à l'article 62, et leur déclaration à la Banque.

§ 2. Aux fins du cadre de gestion du risque lié aux TIC, les fournisseurs d'importance systémique mettent en œuvre des plans de réponse et de rétablissement des TIC.

§ 3. Les fournisseurs d'importance systémique mettent en place, maintiennent et testent périodiquement des plans de continuité des activités de TIC appropriés, notamment en ce qui concerne les fonctions critiques ou importantes externalisées ou sous-traitées dans le cadre d'accords avec des prestataires tiers de services TIC.

§ 4. Dans le cadre de la politique globale de continuité d'activité, les fournisseurs d'importance systémique procèdent à une analyse des incidences sur les activités de leurs expositions à de graves perturbations de leurs activités. Dans le cadre de cette analyse, ils évaluent l'incidence potentielle de graves perturbations de leurs activités au moyen de critères quantitatifs et qualitatifs, à l'aide de données internes et externes et d'une analyse de scénarios, le cas échéant. L'analyse des incidences sur les activités tient compte du caractère critique des fonctions "métiers", des processus de soutien, des dépendances de tiers et des actifs informationnels identifiés et cartographiés, ainsi que de leurs interdépendances. Les actifs de TIC et les services TIC sont conçus et utilisés dans le respect total de l'analyse des incidences sur les activités, en particulier en garantissant de manière adéquate la redondance de toutes les composantes critiques.

§ 5. Les fournisseurs d'importance systémique testent:

1° les plans de continuité des activités de TIC et les plans de réponse et de rétablissement des TIC concernant les systèmes de TIC soutenant toutes les fonctions, au moins une fois par an ainsi qu'en cas de modifications substantielles apportées aux systèmes de TIC qui soutiennent des fonctions critiques ou importantes;

2° de overeenkomstig artikel 62 opgestelde crisiscommunicatieplannen.

Voor de toepassing van het bepaalde onder 1°, nemen systeemrelevante aanbieders in de testplannen scenario's op van cyberaanvallen en omschakelingen tussen de primaire ICT-infrastructuur en de reservecapaciteit, backups en reservefaciliteiten die noodzakelijk zijn om te voldoen aan de in artikel 60 bedoelde verplichtingen.

Systeemrelevante aanbieders evalueren regelmatig hun ICT-bedrijfscontinuïteitsbeleid en hun ICT-respons- en herstelplannen, rekening houdend met de resultaten van de overeenkomstig het eerste lid uitgevoerde tests en de aanbevelingen die voortvloeien uit audits of beoordelingen door de Bank.

§ 6. Systeemrelevante aanbieders beschikken over een functie voor crisisbeheer die in geval van activering van hun ICT-bedrijfscontinuïteitsplannen of ICT-respons- en herstelplannen onder meer duidelijke procedures bepaalt voor het beheer van interne en externe crisiscommunicatie in overeenstemming met artikel 62.

§ 7. Systeemrelevante aanbieders verstrekken de Bank kopieën van de resultaten van de ICT-bedrijfscontinuïteitstests of van soortgelijke oefeningen.

Art. 60

§ 1. Teneinde het terugzetten van ICT-systemen en gegevens te verzekeren met een minimale uitval en een beperkte verstoring en beperkt verlies, ontwikkelen en documenteren systeemrelevante aanbieders als onderdeel van hun kader voor ICT-risicobeheer:

1° een back-upbeleid en back-upprocedures;

2° procedures en methoden voor terugzetting en herstel.

§ 2. Systeemrelevante aanbieders zetten back-upsystemen op die kunnen worden geactiveerd in overeenstemming met het back-upbeleid, de back-upprocedures, en de procedures en methoden voor terugzetting en herstel. De activering van back-upsystemen mag de beveiliging van de netwerk- en informatiesystemen of de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens niet in gevaar brengen. De back-upprocedures en de terugzettings- en herstelprocedures en -methoden worden periodiek getest.

2° les plans de communication en situation de crise établis conformément à l'article 62.

Aux fins du 1°, les fournisseurs d'importance systémique incluent dans les plans de test des scénarios de cyberattaques et de basculement entre l'infrastructure de TIC principale et la capacité redondante, les sauvegardes et les installations redondantes nécessaires pour satisfaire aux obligations énoncées à l'article 60.

Les fournisseurs d'importance systémique réexaminent régulièrement leur politique de continuité des activités de TIC et leurs plans de réponse et de rétablissement des TIC en tenant compte des résultats des tests effectués conformément à l'alinéa 1er, et des recommandations découlant des contrôles d'audit ou des examens de la Banque.

§ 6. Les fournisseurs d'importance systémique disposent d'une fonction de gestion de crise qui, en cas d'activation de leurs plans de continuité des activités de TIC ou de leurs plans de réponse et de rétablissement des TIC, définit, entre autres, des procédures claires pour gérer les communications internes et externes en situation de crise, conformément à l'article 62.

§ 7. Les fournisseurs d'importance systémique fournissent à la Banque des copies des résultats des tests de continuité des activités de TIC ou d'exercices similaires.

Art. 60

§ 1er. Dans le but de veiller à la restauration des systèmes et des données des TIC en limitant au maximum la durée d'indisponibilité, les perturbations et les pertes, aux fins de leur cadre de gestion du risque lié aux TIC, les fournisseurs d'importance systémique définissent et documentent:

1° des politiques et procédures de sauvegarde;

2° des procédures et méthodes de restauration et de rétablissement.

§ 2. Les fournisseurs d'importance systémique mettent en place des systèmes de sauvegarde qui peuvent être activés conformément aux politiques et procédures de sauvegarde, ainsi qu'aux procédures et méthodes de restauration et de rétablissement. L'activation de systèmes de sauvegarde ne compromet pas la sécurité du réseau et des systèmes d'information ni la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données. Des tests des procédures de sauvegarde et des procédures et méthodes de restauration et de rétablissement sont effectués périodiquement.

§ 3. Systeemrelevante aanbieders handhaven ten minste één secundaire verwerkingslocatie, met adequate middelen, capaciteiten, functies en personeelsvoorziening om te voorzien in de zakelijke behoeften.

De secundaire verwerkingslocatie is:

1° fysiek gevestigd op een bepaalde afstand van de primaire verwerkingslocatie om te verzekeren dat de locatie een ander risicoprofiel heeft en om te voorkomen dat deze wordt getroffen door de gebeurtenis die de primaire locatie heeft getroffen;

2° in staat de continuïteit van kritieke of belangrijke functies op dezelfde manier te waarborgen als de primaire locatie of het niveau van diensten te leveren dat noodzakelijk is om ervoor te zorgen dat de systeemrelevante aanbieder zijn kritieke activiteiten verricht binnen het kader van de hersteldoelstellingen;

3° onmiddellijk toegankelijk voor het personeel van de systeemrelevante aanbieder om de continuïteit van kritieke of belangrijke functies te waarborgen ingeval de primaire verwerkingslocatie niet langer beschikbaar is.

§ 4. Bij het bepalen van de doelstellingen inzake hersteltijd en herstelpunt voor elke functie houden systeemrelevante aanbieders rekening met de vraag of het een kritieke of belangrijke functie betreft. Deze tijdsdoelstellingen zorgen ervoor dat de overeengekomen niveaus in extreme scenario's worden gehaald.

§ 5. Bij herstel van een ICT-gerelateerd incident verrichten systeemrelevante aanbieders de benodigde controles, ook meerdere controles, waaronder afstemmingen, om ervoor te zorgen dat het hoogste niveau van gegevensintegriteit wordt gehandhaafd. Deze controles worden ook verricht bij het reconstrueren van gegevens van externe belanghebbenden om te waarborgen dat alle gegevens consistent zijn tussen de systemen.

Art. 61

§ 1. Systeemrelevante aanbieders beschikken over capaciteiten en personele middelen om informatie te verzamelen over kwetsbaarheden en cyberdreigingen, ICT-gerelateerde incidenten, met name cyberaanvallen, en om de waarschijnlijke gevolgen ervan voor hun digitale operationele weerbaarheid te analyseren.

§ 2. Systeemrelevante aanbieders verrichten ICT-gerelateerde post-incidentevaluaties na verstoringen van hun kernactiviteiten ten gevolge van een ICT-gerelateerd

§ 3. Les fournisseurs d'importance systémique maintiennent au moins un site de traitement secondaire doté de ressources, de capacités, de fonctions et d'effectifs adéquats pour répondre à leurs besoins.

Le site de traitement secondaire:

1° est situé à une certaine distance géographique du site de traitement primaire afin de veiller à ce qu'il présente un profil de risque distinct et d'éviter qu'il ne soit affecté par l'événement qui a touché le site primaire;

2° est capable d'assurer la continuité des fonctions critiques ou importantes de la même manière que le site primaire, ou de fournir le niveau de services dont le fournisseur d'importance systémique a besoin pour effectuer ses opérations critiques dans le cadre des objectifs de rétablissement;

3° est immédiatement accessible au personnel de du fournisseur d'importance systémique afin d'assurer la continuité des fonctions critiques ou importantes en cas d'indisponibilité du site de traitement primaire.

§ 4. Lorsqu'elles déterminent les objectifs en matière de délai de rétablissement et de point de rétablissement pour chaque fonction, les fournisseurs d'importance systémique tiennent compte du caractère critique ou important de la fonction. Ces objectifs temporels permettent d'assurer, dans des scénarios extrêmes, le respect des niveaux de service convenus.

§ 5. Lorsqu'elles opèrent un rétablissement à la suite d'un incident lié aux TIC, les fournisseurs d'importance systémique effectuent les contrôles nécessaires, y compris tout contrôle multiple et rapprochement, afin de garantir le niveau d'intégrité des données le plus haut possible. Ces contrôles sont également effectués lors de la reconstitution des données provenant de parties prenantes externes, afin que toutes les données soient cohérentes entre les systèmes.

Art. 61

§ 1er. Les fournisseurs d'importance systémique disposent de capacités et d'effectifs pour recueillir des informations sur les vulnérabilités et les cybermenaces, et sur les incidents liés aux TIC, en particulier les cyberattaques, et analyser leurs incidences probables sur leur résilience opérationnelle numérique.

§ 2. Les fournisseurs d'importance systémique réalisent des examens post-incident lié aux TIC après qu'un incident majeur lié aux TIC a perturbé leurs activités

incident, analyseren daarbij de oorzaken van de verstoring en identificeren de verbeteringen die moeten worden aangebracht.

Systeemrelevante aanbieders delen aan de Bank de wijzigingen mee die na de in het eerste lid bedoelde ICT-gerelateerde post-incidentevaluaties zijn doorgevoerd.

De ICT-gerelateerde post-incidentevaluaties hebben onder meer betrekking op het verrichten van forensische analyses, de doeltreffendheid van incidentescalatie binnen de systeemrelevante aanbieder en de doeltreffendheid van interne en externe communicatie.

§ 3. In het ICT-risicobeoordelingsproces wordt voortdurend naar behoren rekening gehouden met lessen die voortspruiten uit de overeenkomstig de artikelen 63 en 65 uitgevoerde tests op de digitale operationele weerbaarheid en uit ICT-gerelateerde incidenten die zich in het reële leven hebben voorgedaan, met name cyberaanvallen, alsmede met problemen die zich voordoen bij de activering van ICT-bedrijfscontinuïteitsplannen en ICT-respons- en -herstelplannen, samen met relevante informatie die met tegenpartijen wordt uitgewisseld.

§ 4. Systeemrelevante aanbieders zien erop toe dat hun strategie voor digitale operationele weerbaarheid als bedoeld in artikel 54, § 4, op doeltreffende wijze wordt uitgevoerd. Zij inventariseren de ontwikkeling van ICT-risico's in de tijd, analyseren de frequentie, de types, de omvang en de evolutie van ICT-gerelateerde incidenten, met name cyberaanvallen en de patronen daarvan, teneinde inzicht te krijgen in het niveau van blootstelling aan ICT-risico's, met name met betrekking tot kritieke of belangrijke functies, en de maturiteit en paraatheid van de financiële entiteit ten aanzien van deze risico's te verhogen.

§ 5. Systeemrelevante aanbieders ontwikkelen bewustmakingsprogramma's op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele weerbaarheid als verplichte modules in de opleidingsprogramma's voor het personeel. Die programma's en opleidingen zijn van toepassing op alle werknemers en het leidinggevend personeel, en hebben een niveau van complexiteit dat in verhouding staat tot hun takenpakket. In voorkomend geval nemen systeemrelevante aanbieders ook derde aanbieders van ICT-diensten op in hun relevante opleidingsprogramma's.

§ 6. Systeemrelevante aanbieders houden voortdurend toezicht op relevante technologische ontwikkelingen, ook om inzicht te krijgen in de mogelijke effecten van de invoering van deze nieuwe technologieën op de

principales, afin d'analyser les causes de la perturbation et de déterminer les améliorations à apporter aux opérations de TIC ou dans le cadre de la politique de continuité d'activité.

Les fournisseurs d'importance systémique communiquent à la Banque les changements qui ont été apportés à la suite des examens post-incident lié aux TIC visés à l'alinéa premier.

Les examens post-incident lié aux TIC concernent entre autres l'analyse technico-légale, l'efficacité de la remontée des incidents au sein du fournisseur d'importance systémique et l'efficacité de la communication interne et externe.

§ 3. Les enseignements tirés des tests de résilience opérationnelle numérique effectués conformément aux articles 63 et 65 et des incidents liés aux TIC en situation réelle, en particulier les cyberattaques, ainsi que les difficultés rencontrées lors de l'activation des plans de continuité des activités de TIC et des plans de réponse et de rétablissement des TIC, de même que les informations pertinentes échangées avec les contreparties, sont dûment intégrés, de manière continue, dans le processus d'évaluation du risque lié aux TIC.

§ 4. Les fournisseurs d'importance systémique contrôlent l'efficacité de la mise en œuvre de leur stratégie de résilience opérationnelle numérique définie à l'article 54, § 4. Ils retracent l'évolution du risque lié aux TIC dans le temps, analysent la fréquence, les types, l'ampleur et l'évolution des incidents liés aux TIC, en particulier les cyberattaques et leurs caractéristiques, afin de cerner le niveau d'exposition au risque lié aux TIC, en particulier en ce qui concerne les fonctions critiques ou importantes, et de renforcer la maturité et la préparation des TIC.

§ 5. Les fournisseurs d'importance systémique élaborent des programmes de sensibilisation à la sécurité des TIC et des formations à la résilience opérationnelle numérique qu'elles intègrent à leurs programmes de formation du personnel sous forme de modules obligatoires. Ces programmes et formations sont destinés à tous les employés et au personnel de direction et présentent un niveau de complexité proportionné à leurs fonctions. Le cas échéant, les fournisseurs d'importance systémique incluent également les prestataires tiers de services TIC dans leurs programmes de formation pertinents.

§ 6. Les fournisseurs d'importance systémique assurent un suivi continu des évolutions technologiques pertinentes, notamment en vue de déterminer l'incidence que le déploiement de ces nouvelles technologies pourrait

ICT-beveiligingsvereisten en de digitale operationele weerbaarheid. Zij blijven op de hoogte van de meest recente processen voor ICT-risicobeheer, om bestaande of nieuwe vormen van cyberaanvallen doeltreffend aan te pakken.

Art. 62

§ 1. Als onderdeel van het kader voor ICT-risicobeheer beschikken systeemrelevante aanbieders over crisiscommunicatieplannen die het mogelijk maken ten minste ernstige ICT-gerelateerde incidenten of kwetsbaarheden op verantwoordelijke wijze bekend te maken aan dienstafnemers en tegenpartijen en, in voorkomend geval, aan het publiek.

§ 2. Als onderdeel van het kader voor ICT-risicobeheer voeren systeemrelevante aanbieders een communicatiebeleid in voor het personeel en voor externe belanghebbenden. In het communicatiebeleid voor het personeel wordt rekening gehouden met de noodzaak om een onderscheid te maken tussen personeel dat betrokken is bij het ICT-risicobeheer, met name het personeel dat verantwoordelijk is voor respons en herstel, en personeel dat moet worden geïnformeerd.

Art. 63

§ 1. Voor de beoordeling van de paraatheid ten aanzien van de behandeling van ICT-gerelateerde incidenten, de omschrijving van zwakheden, gebreken en lacunes in de digitale operationele weerbaarheid, en de snelle uitvoering van corrigerende maatregelen zorgen systeemrelevante aanbieders voor het vaststellen, handhaven en evalueren van een degelijk en alomvattend programma voor het testen van de digitale operationele weerbaarheid als integrerend onderdeel van het kader voor ICT-risicobeheer als bedoeld in artikel 54.

§ 2. Het testprogramma voor digitale operationele weerbaarheid omvat een reeks beoordelingen, tests, methodologieën, praktijken en instrumenten die overeenkomstig de artikelen 64 en 65 worden toegepast.

§ 3. Bij de uitvoering van het testprogramma voor digitale operationele weerbaarheid volgen systeemrelevante aanbieders een risicogebaseerde benadering, rekening houdend met het veranderende landschap van het ICT-risico, eventuele specifieke risico's waaraan de systeemrelevante aanbieder wordt of kan worden blootgesteld, de kritieke aard van informatieactiva en verleende diensten, alsmede alle andere factoren die de systeemrelevante aanbieder passend acht.

avoir sur les exigences en matière de sécurité des TIC et la résilience opérationnelle numérique. Ils se tiennent informés des processus de gestion du risque lié aux TIC les plus récents, afin de lutter efficacement contre les formes actuelles ou émergentes de cyberattaques.

Art. 62

§ 1er. Aux fins du cadre de gestion du risque lié aux TIC, les fournisseurs d'importance systémique mettent en place des plans de communication en situation de crise qui favorisent une divulgation responsable, au minimum, des incidents majeurs liés aux TIC ou des vulnérabilités majeures aux acheteurs de services et aux contreparties ainsi qu'au public, le cas échéant.

§ 2. Aux fins du cadre de gestion du risque lié aux TIC, les fournisseurs d'importance systémique mettent en œuvre des politiques de communication à l'intention des membres du personnel et des parties prenantes externes. Les politiques de communication à l'intention du personnel tiennent compte de la nécessité d'établir une distinction entre le personnel participant à la gestion du risque lié aux TIC, en particulier le personnel responsable de la réponse et du rétablissement, et le personnel qui doit être informé.

Art. 63

§ 1er. Afin d'évaluer l'état de préparation en vue du traitement d'incidents liés aux TIC, de recenser les faiblesses, les défaillances et les lacunes en matière de résilience opérationnelle numérique et de mettre rapidement en œuvre des mesures correctives, les fournisseurs d'importance systémique établissent, maintiennent et réexaminent un programme solide et complet de tests de résilience opérationnelle numérique, qui fait partie intégrante du cadre de gestion du risque lié aux TIC visé à l'article 54.

§ 2. Le programme de tests de résilience opérationnelle numérique comprend une série d'évaluations, de tests, de méthodologies, de pratiques et d'outils à appliquer conformément aux articles 64 et 65.

§ 3. Lorsqu'ils exécutent le programme de tests de résilience opérationnelle numérique, les fournisseurs d'importance systémique adoptent une approche fondée sur le risque en prenant dûment en considération l'évolution du risque lié aux TIC, tout risque spécifique auquel le fournisseur d'importance systémique est ou pourrait être exposée, la criticité des actifs informationnels et des services fournis, ainsi que tout autre facteur que le fournisseur d'importance systémique juge approprié.

§ 4. Systeemrelevante aanbieders zorgen ervoor dat de tests worden uitgevoerd door interne of externe onafhankelijke partijen. Wanneer tests worden uitgevoerd door een interne tester, zetten zij voldoende middelen in en zorgen zij ervoor dat belangenconflicten gedurende de hele ontwerp- en uitvoeringsfase van de test worden voorkomen.

§ 5. Systeemrelevante aanbieders stellen procedures en beleidslijnen vast om alle problemen die tijdens de uitvoering van de tests aan het licht zijn gekomen, te prioriteren, te classificeren en te verhelpen, en stellen interne valideringsmethoden vast om na te gaan of alle vastgestelde zwakheden, gebreken of lacunes volledig worden aangepakt.

Art. 64

Het testprogramma voor digitale operationele weerbaarheid bedoeld in artikel 63 voorziet in de uitvoering van passende tests, zoals kwetsbaarheidsbeoordelingen en -scans, opensourceanalyses, netwerkbeveiligingsbeoordelingen, kloofanalyses, beoordelingen van fysieke beveiliging, vragenlijsten en scanningsoftwareoplossingen, beoordelingen van broncodes indien mogelijk, scenariogebaseerde tests, compatibiliteitstests, prestatietests, eind-tot-eindtests en penetratietests.

Art. 65

§ 1. Systeemrelevante aanbieders voeren ten minste om de drie jaar geavanceerde tests uit door middel van TLPT. Die tests vinden plaats overeenkomstig het TLPT-kader dat de Bank vaststelt.

§ 2. Elke dreigingsgestuurde penetratietest heeft betrekking op meerdere of alle kritieke of belangrijke functies van een systeemrelevante aanbieder en worden uitgevoerd op systemen die prestaties in het reële leven verrichten ter ondersteuning van deze functies.

Systeemrelevante aanbieders bepalen alle relevante onderliggende ICT-systemen, -processen en technologieën ter ondersteuning van kritieke of belangrijke functies en ICT-diensten, met inbegrip van die ter ondersteuning van uitbestede of met derde aanbieders van ICT-diensten contractueel overeengekomen kritieke of belangrijke functies.

§ 4. Les fournisseurs d'importance systémique veillent à ce que les tests soient effectués par des parties indépendantes internes ou externes. Lorsque les tests sont effectués par un testeur interne, ils leur accordent des ressources suffisantes et veillent à éviter les conflits d'intérêts pendant les phases de conception et d'exécution du test.

§ 5. Les fournisseurs d'importance systémique définissent des procédures et des stratégies destinées à hiérarchiser, classer et résoudre tous les problèmes mis en évidence au cours des tests et élaborent des méthodes de validation interne pour veiller à ce que toutes les faiblesses, défaillances ou lacunes recensées soient entièrement corrigées.

Art. 64

Le programme de tests de résilience opérationnelle numérique visé à l'article 63 prévoit l'exécution de tests appropriés, tels que des évaluations et des analyses de vulnérabilité, des analyses de sources ouvertes, des évaluations de la sécurité des réseaux, des analyses des écarts, des examens de la sécurité physique, des questionnaires et des solutions logicielles de balayage, des examens du code source lorsque cela est possible, des tests fondés sur des scénarios, des tests de compatibilité, des tests de performance, des tests de bout en bout et des tests de pénétration.

Art. 65

§ 1er. Les fournisseurs d'importance systémique effectuent au moins tous les trois ans des tests avancés au moyen d'un test de pénétration fondé sur la menace. Ces tests se déroulent conformément au cadre pour les tests de pénétration fondé sur la menace que la Banque établit.

§ 2. Chaque test de pénétration fondé sur la menace couvre plusieurs, voire la totalité, des fonctions critiques ou importantes d'un fournisseur d'importance systémique et est effectué sur des systèmes en environnement de production en direct qui soutiennent ces fonctions.

Les fournisseurs d'importance systémique recensent tous les systèmes, processus et technologies de TIC sous-jacents pertinents qui soutiennent des fonctions critiques ou importantes et des services TIC, y compris ceux qui soutiennent des fonctions critiques ou importantes qui ont été externalisés ou sous-traités à des prestataires tiers de services TIC.

Systeemrelevante aanbieders beoordelen voor welke kritieke of belangrijke functies TLPT moeten worden verricht. Het resultaat van die beoordeling bepaalt het exacte toepassingsgebied van TLPT en wordt gevalideerd door de Bank.

§ 3. Wanneer derde aanbieders van ICT-diensten binnen het toepassingsgebied van de TLPT vallen, neemt de systeemrelevante aanbieder de nodige maatregelen en waarborgen om de deelname van deze derde aanbieders van ICT-diensten aan de TLPT te waarborgen en behoudt hij de volledige verantwoordelijkheid voor het waarborgen van de naleving van deze wet.

§ 4. Systeemrelevante verwerkers passen doeltreffende risicobeheerscontroles toe om de risico's van potentiële effecten op gegevens, schade aan activa en verstoring van kritieke of belangrijke functies, diensten of activiteiten bij henzelf, bij hun tegenhangers of in de financiële sector te mitigeren.

§ 5. Na afloop van de tests, nadat overeenstemming is bereikt over verslagen en correctieplannen, verstrekken de systeemrelevante aanbieder en, waar van toepassing, de externe testers aan de Bank een samenvatting van de relevante bevindingen, de correctieplannen en de documentatie waaruit blijkt dat de TLPT in overeenstemming met de vereisten is verricht.

Afdeling IX

Beheer, classificatie en melding van incidenten

Art. 66

§ 1. Systeemrelevante aanbieders leggen een incidentbeheerproces vast dat gericht is op het detecteren, beheren en melden van incidenten en leggen dit ten uitvoer.

§ 2. Systeemrelevante aanbieders registreren alle incidenten en ernstige cyberdreigingen. Zij stellen passende procedures en processen vast voor een consistente en geïntegreerde monitoring, behandeling en follow-up van incidenten, teneinde ervoor te zorgen dat onderliggende oorzaken worden opgespoord, gedocumenteerd en weggenomen om dergelijke incidenten te voorkomen.

Les fournisseurs d'importance systémique évaluent quelles fonctions critiques ou importantes doivent être couvertes par les tests de pénétration fondés sur la menace. Le résultat de cette évaluation détermine la portée précise de ces tests et est validé par la Banque.

§ 3. Lorsque des prestataires tiers de services TIC sont inclus dans le champ d'application du test de pénétration fondé sur la menace, le fournisseur d'importance systémique prend les mesures et garanties nécessaires pour assurer la participation de ces prestataires tiers de services TIC à ce test, et conserve à tout moment l'entière responsabilité de veiller au respect de la présente loi.

§ 4. Les fournisseurs d'importance systémique procèdent à des contrôles efficaces de la gestion des risques afin d'atténuer les risques d'incidence potentielle sur les données, de dommages aux actifs et de perturbation des fonctions, services ou opérations critiques ou importants au sein de lui-même, de ses contreparties ou du secteur financier.

§ 5. À l'issue du test, une fois que les rapports et les plans de mesures correctives ont été approuvés, le fournisseur d'importance systémique et, s'il y a lieu, les testeurs externes fournissent à la Banque une synthèse des conclusions pertinentes, les plans de mesures correctives et la documentation démontrant que le test de pénétration fondé sur la menace a été effectué conformément aux exigences.

Section IX

Gestion, classification et notification des incidents

Art. 66

§ 1er. Les fournisseurs d'importance systémique établissent un processus de gestion des incidents afin de détecter, de gérer et de notifier les incidents, et le mettent en œuvre.

§ 2. Les fournisseurs d'importance systémique enregistrent tous les incidents et les cybermenaces majeures. Ils mettent en place des procédures et des processus adéquats pour assurer une surveillance, un traitement et un suivi cohérents et intégrés des incidents, pour veiller à ce que les causes originelles soient identifiées et documentées et qu'il y soit remédié pour éviter que de tels incidents ne se produisent.

Art. 67

Systeemrelevante aanbieders classificeren alle incidenten en ernstige cyberdreigingen en bepalen de effecten daarvan minstens op basis van de volgende criteria:

1° het aantal en/of de relevantie van getroffen dienstafnemers;

2° de mate waarin dienstafnemers getroffen zijn;

3° het aantal getroffen transacties;

4° de duur van het incident, waaronder de uitvaltijd van de dienst;

5° de impact op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens;

6° de mate waarin de getroffen diensten als cruciaal kunnen worden aangemerkt.

Art. 68

Onverminderd het bepaalde in artikel 69, melden systeemrelevante aanbieders alle incidenten aan de Bank.

Art. 69

§ 1. Systeemrelevante aanbieders melden ernstige incidenten en ernstige cyberdreigingen onverwijld en in geen geval later dan op de dag waarop het incident of de dreiging zich voordoet, aan de Bank.

§ 2. Systeemrelevante aanbieders houden de Bank na de initiële kennisgeving op de hoogte van nieuwe informatie over het incident of de dreiging en over de vooruitgang in de implementatie van respons-, herstel- en corrigerende maatregelen.

§ 3. Systeemrelevante aanbieders maken over ieder ernstig incident en iedere ernstige cyberdreiging een eindverslag over aan de Bank.

Het eindverslag bevat minstens:

1° een analyse van de onderliggende oorzaken van het incident of de dreiging;

2° een voorstel van plan of maatregelen om te vermijden dat het incident of de dreiging zich opnieuw voordoet;

Art. 67

Les fournisseurs d'importance systémique classent tous les incidents et les cybermenaces majeures et déterminent leur incidence au moins sur la base des critères suivants:

1° le nombre et/ou l'importance des acheteurs de services touchés;

2° la mesure dans laquelle les acheteurs de services sont touchés;

3° le nombre de transactions touchées;

4° la durée de l'incident, y compris les interruptions de service;

5° l'impact sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données;

6° la criticité des services touchés.

Art. 68

Sans préjudice des dispositions de l'article 69, les fournisseurs d'importance systémique notifient à la Banque tous les incidents.

Art. 69

§ 1er. Les fournisseurs d'importance systémique notifient à la Banque les incidents majeurs et les cybermenaces majeures sans délai et au plus tard le jour où l'incident ou la menace se produit.

§ 2. Après la notification initiale, les fournisseurs d'importance systémique tiennent la Banque informée des nouvelles informations sur l'incident ou la menace et du progrès réalisé dans la mise en œuvre des mesures de réponse, de rétablissement et de correction.

§ 3. Les fournisseurs d'importance systémique soumettent à la Banque un rapport final sur chaque incident majeur et chaque cybermenace majeure.

Le rapport final contient au minimum:

1° une analyse des causes originelles de l'incident ou de la menace;

2° une proposition de plan ou de mesures pour éviter que l'incident ou la menace ne se reproduise;

3° een uiterste datum voor implementatie van elk onderdeel van het plan of van elke maatregel.

Art. 70

§ 1. Wanneer een ernstig incident optreedt en gevolgen heeft voor de financiële belangen van cliënten, stellen systeemrelevante aanbieders, zodra zij het incident hebben opgemerkt, hun dienstafnemers onverwijld in kennis van het ernstig incident en van de maatregelen die zijn genomen om de negatieve gevolgen van een dergelijk incident te beperken.

§ 2. In het geval van een ernstige cyberdreiging stellen systeemrelevante aanbieders hun dienstafnemers die mogelijk getroffen kunnen worden in kennis van de passende beschermingsmaatregelen die zij kunnen nemen.

Afdeling X

Dienstverleningscriteria

Art. 71

§ 1. Een systeemrelevante aanbieder stelt non-discriminatoire criteria vast voor het aanbieden van zijn diensten aan alle dienstafnemers, en maakt deze openbaar. De systeemrelevante aanbieder herziet de criteria tenminste eenmaal per jaar.

§ 2. De in paragraaf 1 bedoelde criteria worden gerechtvaardigd door de eisen van veiligheid en efficiëntie van het verlenen van financiële berichtendiensten en de markten die daardoor worden bediend en worden afgestemd op, en staan in verhouding tot, de specifieke risico's daarvan. In overeenstemming met het proportionaliteitsprincipe stelt een systeemrelevante aanbieder vereisten vast die zijn dienstverlening zo min mogelijk beperken. Indien een systeemrelevante aanbieder zijn diensten weigert aan een entiteit, geeft hij hiervoor schriftelijke redenen aan die zijn gebaseerd op een integrale risicoanalyse.

§ 3. Een systeemrelevante aanbieder bewaakt voortdurend of de dienstafnemers voldoen aan de in paragraaf 1 bedoelde criteria. Hij stelt non-discriminatoire procedures vast, en maakt deze openbaar, op basis waarvan het mogelijk is het beroep op de diensten van de systeemrelevante aanbieder te schorsen of ordelijk te beëindigen wanneer de dienstafnemer niet voldoet aan de in paragraaf 1 bedoelde criteria. De systeemrelevante aanbieder herziet de procedures tenminste eenmaal per jaar.

3° un délai de mise en œuvre de chaque partie du plan ou de chaque mesure.

Art. 70

§ 1er. Lorsqu'un incident majeur survient et a une incidence sur les intérêts financiers des clients, les fournisseurs d'importance systémique informent leurs acheteurs de services de cet incident majeur et des mesures qui ont été prises pour atténuer les effets préjudiciables de cet incident sans retard injustifié, dès qu'ils en ont connaissance.

§ 2. En cas de cybermenace majeure, les fournisseurs d'importance systémique informent leurs acheteurs de services susceptibles d'être affectés de toute mesure de protection appropriée que ces derniers pourraient envisager de prendre.

Section X

Critères de fourniture de services

Art. 71

§ 1er. Un fournisseur d'importance systémique définit et rend publics des critères non discriminatoires pour la fourniture de ses services à tous les acheteurs de services. Il réexamine ces critères au moins une fois par an.

§ 2. Les critères mentionnés au paragraphe 1er sont justifiés en termes de sécurité et d'efficience de la fourniture de services de messagerie financière et des marchés qu'il dessert, et sont adaptés et proportionnels aux risques spécifiques y afférents. Conformément au principe de proportionnalité, un fournisseur d'importance systémique fixe des exigences restreignant le moins possible la fourniture de ses services. Si un fournisseur d'importance systémique refuse à une entité l'accès à ses services, il donne par écrit les raisons de ce refus, en se fondant sur une analyse générale du risque.

§ 3. Un fournisseur d'importance systémique contrôle en permanence si les acheteurs de services respectent les critères mentionnés au paragraphe 1er. Il définit et rend publiques des procédures non discriminatoires afin de faciliter la suspension ou la cessation ordonnée de la fourniture des services lorsqu'un acheteur de services ne satisfait plus aux critères mentionnés au paragraphe 1er. Il réexamine ces procédures au moins une fois par an.

Afdeling XI

Communicatieprocedures en normen

Art. 72

Een systeemrelevante aanbieder gebruikt relevante internationaal geaccepteerde communicatieprocedures en -normen, of accommodeert deze, teneinde efficiënte financiële berichtendiensten en financiële transacties te faciliteren.

Afdeling XII

Openbaarmaking van regels, cruciale procedures en marktgegevens

Art. 73

§ 1. Een systeemrelevante aanbieder stelt heldere en integrale regels en procedures vast die volledig openbaar worden gemaakt aan dienstafnemers. Toepasselijke regels en cruciale procedures worden ook openbaar gemaakt.

§ 2. Een systeemrelevante aanbieder maakt heldere beschrijvingen openbaar van de dienstverlening alsmede van de rechten en verplichtingen van de systeemrelevante aanbieder en de dienstafnemers, zodat zij de risico's kunnen beoordelen die zij zouden lopen bij het afnemen van diensten.

§ 3. Een systeemrelevante aanbieder verschaft alle benodigde en toepasselijke documentatie en training zodat de dienstafnemers de regels en procedures begrijpen evenals de risico's die zij lopen bij het afnemen van diensten.

§ 4. Een systeemrelevante aanbieder maakt zijn tarieven bekend met betrekking tot elke financiële berichtendienst die hij aanbiedt, evenals het beleid inzake kortingen. De systeemrelevante aanbieder geeft heldere beschrijvingen van de betaalde diensten, zodat vergelijking mogelijk is.

Section XI

Procédures et normes de communication

Art. 72

Un fournisseur d'importance systémique utilise des procédures et des normes de communication internationalement acceptées, ou s'y adapte, afin d'assurer l'efficience des services de messagerie financière et des transactions financières.

Section XII

Communication de règles, procédures clés et données de marché

Art. 73

§ 1er. Un fournisseur d'importance systémique adopte un ensemble de règles et de procédures claires et exhaustives, qui sont entièrement communiquées aux acheteurs de services. Les règles et procédures clés applicables sont également rendues publiques.

§ 2. Un fournisseur d'importance systémique communique des descriptions claires de la fourniture de services, ainsi que de ses droits et obligations et de ceux des acheteurs de services, afin que ces derniers puissent évaluer les risques liés à leur achat de services.

§ 3. Un fournisseur d'importance systémique fournit toute la documentation et la formation nécessaires et appropriées pour permettre aux acheteurs de services de comprendre facilement les règles et procédures, ainsi que les risques auxquels ils sont confrontés du fait de leur achat de services.

§ 4. Un fournisseur d'importance systémique rend publiques les commissions qu'il perçoit pour chaque service de messagerie financière qu'il propose, ainsi que sa politique de remises. Le fournisseur d'importance systémique fournit des descriptions claires des services facturés, à des fins de comparaison.

HOOFDSTUK 8

Toezicht op aanbieders van financiële berichtendiensten

Afdeling I

Toezicht door de Bank

Art. 74

§ 1. Aanbieders zijn onderworpen aan het toezicht van de Bank.

§ 2. De Bank ziet erop toe dat iedere aanbieder doorlopend werkt overeenkomstig de bepalingen van deze wet die op hem van toepassing zijn en de ter uitvoering ervan genomen besluiten en reglementen. Het toezicht door de Bank dient evenredig en passend te zijn, in het licht van de aard, de omvang en de complexiteit van de door de aanbieder verrichte activiteiten, en de eraan verbonden risico's.

Art. 75

De Bank kan zich door iedere aanbieder alle inlichtingen doen verstrekken die zij nodig acht volgens de nadere regels die zij bepaalt.

De Bank kan de in het eerste lid bedoelde inlichtingen opvragen om na te gaan of de voorschriften van deze wet of de ter uitvoering ervan genomen besluiten en reglementen zijn nageleefd, evenals om bij te dragen tot de doelstellingen bedoeld in artikel 2, § 1.

Met dat doel kan de Bank zich ook inlichtingen doen verstrekken door agenten van aanbieders of door entiteiten waaraan een systeemrelevante aanbieder activiteiten heeft uitbesteed. Systeemrelevante aanbieders leggen aan deze agenten en entiteiten een contractuele verplichting op om volledige medewerking te verlenen aan de Bank wanneer zij de in dit artikel bedoelde inlichtingen opvraagt.

In zoverre de in dit artikel bedoelde inlichtingen betrekking hebben op natuurlijke personen kan de Bank deze inlichtingen enkel opvragen indien dat noodzakelijk is voor controle van de naleving van de bepalingen van Hoofdstuk 3 of indien de Bank hiertoe uitdrukkelijk gemachtigd is op grond van een andere bepaling van het nationaal of Europees recht die de essentiële elementen van deze verwerking van persoonsgegevens vastlegt.

CHAPITRE 8

Surveillance des fournisseurs de services de messagerie financière

Section Ire

Surveillance par la Banque

Art. 74

§ 1er. Les fournisseurs sont soumis au contrôle de la Banque.

§ 2. La Banque veille à ce que chaque fournisseur fonctionne en permanence en conformité avec les dispositions de la présente loi qui lui sont applicables, ainsi que des arrêtés et règlements pris pour son exécution. La surveillance exercée par la Banque doit être proportionnée et adaptée à la nature, à l'étendue et à la complexité des activités exercées par le fournisseur, et aux risques qui y sont liés.

Art. 75

La Banque peut se faire transmettre par chaque fournisseur tous les renseignements dont elle a besoin selon les modalités qu'elle détermine.

La Banque peut demander les renseignements visés à l'alinéa 1er afin de vérifier si les prescriptions de la présente loi ou des arrêtés et règlements pris pour son application sont respectées, ainsi que pour contribuer aux objectifs visés à l'article 2, § 1er.

À cette fin, la Banque peut également se faire communiquer des informations par les agents de fournisseurs ou par des entités auprès desquelles un fournisseur d'importance systémique a externalisé des activités. Les fournisseurs d'importance systémique imposent à ces agents et entités une obligation contractuelle de coopérer pleinement avec la Banque lorsque celle-ci demande les renseignements visés par cet article.

Dans la mesure où les informations visées au présent article concernent des personnes physiques, la Banque ne peut demander ces informations que si cela est nécessaire pour vérifier le respect des dispositions du Chapitre 3 ou si la Banque y est expressément autorisée en vertu d'une autre disposition de droit national ou européen déterminant les éléments essentiels de ce traitement de données à caractère personnel.

Art. 76

§ 1. De Bank kan bij iedere aanbieder ter plaatse inspecties verrichten en ter plaatse kennisnemen en een kopie maken van elk gegeven in het bezit van de aanbieder, met inbegrip van de informatie bedoeld in artikel 75, om na te gaan of de bepalingen van deze wet zijn nageleefd en of de haar voorgelegde staten en andere inlichtingen juist en waarheidsgetrouw zijn, en om bij te dragen tot de doelstellingen bedoeld in artikel 2, § 1.

In zoverre de in dit artikel bedoelde gegevens betrekking hebben op natuurlijke personen kan de Bank er enkel kennis van nemen en kopie van maken indien dat noodzakelijk is voor de controle van de naleving van de bepalingen van Hoofdstuk 3 of indien de Bank hiertoe uitdrukkelijk gemachtigd is op grond van een andere bepaling van het nationaal of Europees recht die de essentiële elementen van deze verwerking van persoonsgegevens vastlegt.

§ 2. De in dit artikel bedoelde prerogatieven omvatten ook de toegang tot de agenda's en de notulen van de vergaderingen van de verschillende organen van de aanbieders en van hun interne comités, evenals tot de bijbehorende documenten en tot de resultaten van de interne en/of externe beoordeling van de werking van de genoemde organen.

§ 3. Met het oog op het bepaalde in paragraaf 1 kan de Bank ook ter plaatse inspecties verrichten bij agenten van aanbieders of bij entiteiten waaraan een systeemrelevante aanbieder activiteiten heeft uitbesteed, en ter plaatse kennisnemen en een kopie maken van alle gegeven waarover zij beschikken. Systeemrelevante aanbieders leggen aan deze agenten en entiteiten een contractuele verplichting op om volledig mee te werken tijdens de door de Bank ter plaatse uitgevoerde inspecties.

§ 4. Artikel 36/20 van de wet van 22 februari 1998 is van toepassing wanneer de uitoefening door de Bank van de haar krachtens dit artikel toegekende prerogatieven verhinderd wordt of wanneer haar bewust onjuiste of onvolledige informatie wordt verstrekt.

Art. 77

In het kader van het toezicht en met name van de inspecties zijn de personeelsleden van de Bank gemachtigd om van de leiders en de werknemers van de aanbieder, de agenten of de entiteiten waaraan activiteiten zijn uitbesteed alle inlichtingen en uitleg op te vragen die zij nodig achten voor de uitvoering van hun opdrachten

Art. 76

§ 1er. La Banque peut procéder auprès de chaque fournisseur à des inspections sur place et prendre connaissance et copie, sur place également, de toute information détenue par le fournisseur, y inclus l'information visée à l'article 75, en vue de vérifier le respect des dispositions de la présente loi ainsi que l'exactitude et la sincérité des états et autres informations qui lui sont fournis, et pour contribuer aux objectifs visés à l'article 2, § 1er.

Dans la mesure où l'information visée au présent article concerne des personnes physiques, la Banque ne peut en prendre connaissance et copie que si cela est nécessaire pour vérifier le respect des dispositions du Chapitre 3 ou si la Banque y est expressément autorisée en vertu d'une autre disposition de droit national ou européen déterminant les éléments essentiels de ce traitement de données à caractère personnel.

§ 2. Les prérogatives visées au présent article couvrent également l'accès aux ordres du jour et aux procès-verbaux des réunions des différents organes des fournisseurs et de leurs comités internes, ainsi qu'aux documents y afférents et aux résultats de l'évaluation interne et/ou externe du fonctionnement desdits organes.

§ 3. Aux fins visées au paragraphe 1er, la Banque peut également procéder à des inspections sur place auprès des agents de fournisseurs ou des entités auprès desquelles un fournisseur d'importance systémique a externalisé l'exécution des activités et prendre connaissance et copie, sans déplacement, de toutes informations détenues par ces derniers. Les fournisseurs d'importance systémique imposent à ces agents et entités une obligation contractuelle de coopérer pleinement lors des inspections sur place effectuées par la Banque.

§ 4. L'article 36/20 de la loi du 22 février 1998 est applicable lorsque la Banque est empêchée d'exercer les prérogatives qui lui sont accordées en vertu du présent article ou lorsque des informations inexactes ou incomplètes lui sont sciemment fournies.

Art. 77

Dans le cadre du contrôle et notamment des inspections, les agents de la Banque sont habilités à demander des dirigeants et des employés du fournisseur, des agents et des entités auprès desquelles des activités sont externalisées toutes informations et explications qu'ils estiment nécessaires pour l'exercice de leurs missions

en kunnen zij te dien einde gesprekken eisen met de leiders of personeelsleden die zij aanduiden.

Art. 78

Voor de uitvoering van haar toezichtsopdracht mag de Bank een beroep doen op deskundigen die zij aanstelt om de nuttige controles en onderzoeken te verrichten. De Bank kan de kost van deze deskundigen aanrekenen aan de betrokken aanbieder.

Art. 79

De inspectieverslagen en meer in het algemeen alle documenten die uitgaan van de Bank, waarvan zij aangeeft dat ze vertrouwelijk zijn, mogen niet openbaar worden gemaakt door de aanbieder zonder haar uitdrukkelijke toestemming.

De niet-naleving van deze verplichting wordt bestraft met de straffen waarin voorzien is in artikel 458 van het Strafwetboek.

Art. 80

§ 1. Een systeemrelevante aanbieder bewaart al haar vastleggingen over de verrichte diensten en activiteiten voor zo lang als nodig om de Bank toe te laten de naleving van deze wet te controleren.

§ 2. Systeemrelevante aanbieders leggen aan hun agenten en entiteiten waaraan zij activiteiten uitbesteden een gelijkwaardige contractuele verplichting op om toe te laten dat de Bank de naleving van deze wet kan controleren.

§ 3. De Bank preciseert bij reglement vastgesteld in toepassing van artikel 8, § 2, van de wet van 22 februari 1998, welke vastleggingen moeten bewaard worden voor de doelstellingen als bedoeld in paragraaf 1 evenals de termijn, die 10 jaar niet zal overschrijden, gedurende dewelke die vastleggingen moeten bewaard worden.

Afdeling II

Coöperatief toezicht

Art. 81

§ 1. In voorkomend geval kan de Bank niet-bindende samenwerkingsregelingen sluiten met autoriteiten van de

et peuvent, à cette fin, requérir la tenue d'entretiens avec les dirigeants ou membres du personnel qu'ils désignent.

Art. 78

La Banque peut, pour l'exécution de sa mission de contrôle, recourir à des experts qu'elle désigne en vue d'effectuer les vérifications et expertises utiles. La Banque peut répercuter le coût de ces experts sur le fournisseur concerné.

Art. 79

Les rapports d'inspection et plus généralement tous les documents émanant de la Banque dont elle indique qu'ils sont confidentiels ne peuvent être divulgués par les fournisseurs sans son consentement exprès.

Le non-respect de cette obligation est puni des peines prévues par l'article 458 du Code pénal.

Art. 80

§ 1er. Un fournisseur d'importance systémique conserve tous les enregistrements relatifs aux services fournis et aux activités exercées, aussi longtemps que nécessaire pour permettre à la Banque de contrôler le respect de la présente loi.

§ 2. Les fournisseurs d'importance systémique imposent à leurs agents et entités auprès desquelles des activités sont externalisées une obligation contractuelle équivalente pour permettre à la Banque de contrôler le respect de la présente loi.

§ 3. La Banque précise, par voie de règlement pris en application de l'article 8, § 2, de la loi du 22 février 1998, quels enregistrements doivent être conservés aux fins visées au paragraphe 1er, ainsi que la durée, qui ne peut excéder dix ans, pendant laquelle ils doivent être conservés.

Section II

Surveillance coopérative

Art. 81

§ 1er. Le cas échéant, la Banque peut conclure des arrangements de coopération non contraignants avec

Europese Unie, van andere lidstaten van de Europese Economische Ruimte en van derde landen wanneer hen gelijkwaardige opdrachten zijn toevertrouwd als bedoeld in artikel 8 van de wet van 22 februari 1998, evenals met de centrale banken of monetaire autoriteiten van de Europese Unie, van andere lidstaten van de Europese Economische Ruimte en van derde landen.

§ 2. Wanneer het toezicht op een systeemrelevante aanbieder het voorwerp uitmaakt van een samenwerkingsregeling bedoeld in paragraaf 1, oefent de Bank de haar door deze wet toevertrouwde opdrachten uit ter ondersteuning van die samenwerking.

§ 3. De Bank raadpleegt voorafgaand de deelnemers aan de samenwerkingsregelingen bedoeld in paragraaf 1 wanneer zij overweegt met het oog op de toepassing van deze wet een mededeling, richtsnoer of circulaire uit te vaardigen of een reglement vast te stellen in toepassing van artikel 8, § 2, van de wet van 22 februari 1998.

§ 4. De Bank mag aan de deelnemers aan de samenwerkingsregelingen bedoeld in paragraaf 1 de vertrouwelijke informatie meedelen waarvan zij kennis heeft naar aanleiding van de uitoefening van haar taken bedoeld in deze wet, onder de voorwaarden bepaald in artikel 35/1, § 2 en § 3, van de wet van 22 februari 1998.

HOOFDSTUK 9

Dwingende maatregelen

Art. 82

§ 1. Wanneer de Bank vaststelt dat of over gegevens beschikt waaruit blijkt dat:

1° een systeemrelevante aanbieder niet werkt overeenkomstig de bepalingen van deze wet of haar uitvoeringsbesluiten en reglementen;

2° het gevaar bestaat dat een systeemrelevante aanbieder in de komende 12 maanden niet meer zal werken overeenkomstig deze bepalingen;

3° de uitoefening van het bedrijf van een systeemrelevante aanbieder een bedreiging vormt voor de stabiliteit en continuïteit van nationale en internationale financiële transacties; of

4° de uitoefening van het bedrijf van een systeemrelevante aanbieder een bedreiging vormt voor het verzekeren van de doelstellingen bedoeld in artikel 2, § 1,

les autorités de l'Union européenne, d'autres États membres de l'Espace économique européen et d'États tiers chargées de missions équivalentes à celles visées à l'article 8 de la loi du 22 février 1998, ainsi qu'avec les banques centrales ou les autorités monétaires de l'Union européenne, d'autres États membres de l'Espace économique européen et d'États tiers.

§ 2. Lorsque la surveillance d'un fournisseur d'importance systémique fait l'objet d'un arrangement de coopération visé au paragraphe 1er, la Banque exerce les missions qui lui sont dévolues par la présente loi en soutien de cette coopération.

§ 3. La Banque consulte préalablement les participants aux arrangements de coopération visés au paragraphe 1er lorsqu'elle envisage, en vue de l'application de la présente loi, émettre une communication, une recommandation ou une circulaire, ou adopter un règlement en application de l'article 8, § 2, de la loi du 22 février 1998.

§ 4. La Banque peut communiquer aux participants aux arrangements de coopération visés au paragraphe 1er les informations confidentielles dont elle a connaissance en raison de l'exercice de ses compétences visées par la présente loi, sous les conditions déterminées par l'article 35/1, § 2 et § 3, de la loi du 22 février 1998.

CHAPITRE 9

Mesures contraignantes

Art. 82

§ 1er. Lorsque la Banque constate ou qu'elle dispose d'éléments indiquant:

1° qu'un fournisseur d'importance systémique ne fonctionne pas en conformité avec les dispositions de cette loi ou des arrêtés et règlements pris pour son exécution;

2° qu'un fournisseur d'importance systémique risque de ne plus fonctionner en conformité avec ces dispositions au cours des douze prochains mois;

3° que l'exercice de l'activité d'un fournisseur d'importance systémique présente une menace pour la stabilité et la continuité des transactions financières nationales et internationales; ou

4° que l'exercice de l'activité d'un fournisseur d'importance systémique présente une menace pour l'assurance des objectifs visés à l'article 2, § 1er,

stelt zij de termijn vast waarbinnen deze toestand moet worden verholpen.

§ 2. Zolang de systeemrelevante aanbieder de in paragraaf 1 bedoelde toestand niet heeft verholpen, kan de Bank te allen tijde:

1° de gehele of gedeeltelijke reservering van uitkeerbare winst opleggen;

2° kapitaalvereisten opleggen die strenger zijn of een aanvulling vormen op deze waarin voorzien is krachtens artikel 37;

3° alle dividenduitkeringen of betalingen, met name van interesten, aan aandeelhouders, beperken of verbieden, voor zover de schorsing van de betalingen die daaruit zou voortvloeien, niet leidt tot de opening van een faillissementsprocedure met toepassing van de bepalingen van boek XX, titel VI, hoofdstuk 1, van het Wetboek van Economisch Recht;

4° eisen dat de systeemrelevante aanbieder het risico dat verbonden is aan bepaalde werkzaamheden of aan zijn organisatie, beperkt, in voorkomend geval door de integrale of gedeeltelijke overdracht op te leggen van zijn bedrijf of zijn net;

5° een aanvullende rapporteringsverplichting opleggen of een frequentere rapportering opleggen dan waarin voorzien is bij of krachtens deze wet, met name voor de rapportering over risico's;

6° de openbaarmaking eisen van informatie waarvan het onderwerp wordt bepaald door de Bank.

§ 3. Wanneer de Bank van oordeel is dat de maatregelen die de systeemrelevante aanbieder binnen de met toepassing van paragraaf 1 vastgestelde termijn heeft genomen om de vastgestelde toestand te verhelpen, bevredigend zijn, heft zij volgens de modaliteiten die zij bepaalt, alle of een deel van de maatregelen op waartoe zij met toepassing van paragraaf 2 heeft besloten.

Art. 83

§ 1. Wanneer de Bank vaststelt dat een systeemrelevante aanbieder niet of niet langer voldoet aan de met toepassing van artikel 82, § 2, genomen maatregelen, of dat hij de toestand na het verstrijken van de met toepassing van artikel 82, § 1, vastgestelde termijn niet heeft verholpen, kan de Bank, onverminderd de andere bepalingen die bij of krachtens deze wet zijn vastgesteld:

elle fixe le délai dans lequel il doit être remédié à cette situation.

§ 2. Aussi longtemps qu'il n'a pas été remédié par le fournisseur d'importance systémique à la situation visée au paragraphe 1er, la Banque peut, à tout moment:

1° imposer la mise en réserve totale ou partielle de bénéfices distribuables;

2° imposer des exigences de capital plus sévères que, ou complémentaires à, celles prévues en vertu de l'article 37;

3° limiter ou interdire toute distribution de dividendes ou tout paiement, notamment d'intérêts, aux actionnaires, dans la mesure où la suspension des versements qui en résulterait n'entraîne pas les conditions d'ouverture d'une procédure de faillite en application des dispositions du livre XX, titre VI, chapitre 1er, du Code de droit économique;

4° imposer que le fournisseur d'importance systémique diminue le risque inhérent à certaines activités ou à son organisation, le cas échéant en imposant la cession de tout ou partie de ses activités ou de son réseau;

5° imposer une obligation d'information (reporting) supplémentaire ou imposer une fréquence d'information (reporting) plus élevée que ce qui est prévu par ou en vertu de cette loi, notamment en matière de risques;

6° imposer la publication d'informations dont l'objet est déterminé par la Banque.

§ 3. Lorsque la Banque estime que les mesures prises par le fournisseur d'importance systémique dans le délai fixé en application du paragraphe 1er pour remédier à la situation constatée sont satisfaisantes, elle lève, selon les modalités qu'elle détermine, tout ou partie des mesures décidées en application du paragraphe 2.

Art. 83

§ 1er. Sans préjudice des autres dispositions prévues par ou en vertu de la présente loi, lorsque la Banque constate qu'un fournisseur d'importance systémique ne se conforme pas ou cesse de se conformer aux mesures adoptées en application de l'article 82, § 2, ou qu'à l'issue du délai fixé en application de l'article 82, § 1er, il n'a pas remédié à la situation, la Banque peut:

1° een speciaal commissaris aanstellen overeenkomstig het bepaalde in artikel 84;

2° voor de duur die zij bepaalt, de rechtstreekse of onrechtstreekse uitoefening van het bedrijf van de systeemrelevante aanbieder geheel of ten dele schorsen dan wel verbieden;

3° de vervanging gelasten van alle of een deel van de leiders van de systeemrelevante aanbieder, of voorlopige bestuurders aanstellen overeenkomstig het bepaalde in artikel 85;

4° de systeemrelevante aanbieder gelasten binnen de door haar vastgestelde termijn een algemene vergadering van aandeelhouders bijeen te roepen waarvan zij de agenda vaststelt.

Een schorsing of verbod als bedoeld in het eerste lid, 2°, kan, in de door de Bank bepaalde mate, de volledige of gedeeltelijke schorsing van de uitvoering van de lopende overeenkomsten tot gevolg hebben. De leden van de raad van toezicht en de personen belast met de effectieve leiding die handelingen stellen of beslissingen nemen ondanks de schorsing of het verbod, zijn hoofdelijk aansprakelijk voor het nadeel dat hieruit voortvloeit voor de systeemrelevante aanbieder of voor derden. Indien de Bank de schorsing of het verbod in het *Belgisch Staatsblad* heeft bekendgemaakt, zijn alle hiermee strijdige handelingen en beslissingen nietig.

§ 2. Niettegenstaande de voorwaarden voor de toepassing van paragraaf 1, kan de Bank in uiterst spoedeisende gevallen of indien de ernst van de feiten dit rechtvaardigt, de maatregelen als bedoeld in de genoemde paragraaf 1 treffen zonder vooraf een termijn op te leggen.

§ 3. De in paragraaf 1 bedoelde beslissingen van de Bank hebben voor de systeemrelevante aanbieder uitwerking vanaf de datum van de kennisgeving ervan met een aangetekende brief of een brief met ontvangstbewijs en, voor derden, vanaf de datum van de bekendmaking ervan.

Art. 84

§ 1. Wanneer de Bank een speciaal commissaris aanstelt, is voor alle handelingen en beslissingen van alle organen van de systeemrelevante aanbieder, inclusief de algemene vergadering, alsook voor die van de personen die instaan voor het beleid, zijn schriftelijke, algemene of bijzondere toestemming vereist. Evenwel kan de Bank de verrichtingen waarvoor een toestemming vereist is, beperken.

1° désigner un commissaire spécial conformément à l'article 84;

2° suspendre pour la durée qu'elle détermine l'exercice direct ou indirect de tout ou partie de l'activité du fournisseur d'importance systémique ou interdire cet exercice;

3° enjoindre le remplacement de tout ou partie des dirigeants du fournisseur d'importance systémique, ou, désigner des administrateurs provisoires conformément à l'article 85;

4° enjoindre au fournisseur d'importance systémique de convoquer, dans le délai qu'elle fixe, une assemblée générale des actionnaires, dont elle établit l'ordre du jour.

Une suspension ou interdiction visée à l'alinéa 1er, 2°, peut, dans la mesure déterminée par la Banque, impliquer la suspension totale ou partielle de l'exécution des contrats en cours. Les membres du conseil de surveillance et les personnes chargées de la direction effective qui accomplissent des actes ou prennent des décisions en violation de la suspension ou de l'interdiction sont responsables solidairement du préjudice qui en est résulté pour le fournisseur d'importance systémique ou les tiers. Si la Banque a publié la suspension ou l'interdiction au *Moniteur belge*, les actes et décisions intervenus en contravention à celle-ci sont nuls.

§ 2. Nonobstant les conditions d'application du paragraphe 1er, en cas d'extrême urgence ou lorsque la gravité des faits le justifie, la Banque peut adopter les mesures visées audit paragraphe 1er sans qu'un délai soit préalablement fixé.

§ 3. Les décisions de la Banque visées au paragraphe 1er sortent leurs effets à l'égard du fournisseur d'importance systémique à dater de leur notification à celle-ci par lettre recommandée ou avec accusé de réception et, à l'égard des tiers, à dater de leur publication.

Art. 84

§ 1er. Lorsque la Banque désigne un commissaire spécial, l'autorisation écrite, générale ou spéciale de celui-ci est requise pour tous les actes et décisions de tous les organes du fournisseur d'importance systémique, y compris l'assemblée générale, et pour ceux des personnes chargées de la gestion. La Banque peut toutefois limiter le champ des opérations soumises à autorisation.

§ 2. De speciaal commissaris mag elk voorstel dat hij nuttig acht aan alle organen van de systeemrelevante aanbieder voorleggen, inclusief de algemene vergadering.

§ 3. De bezoldiging van de speciaal commissaris wordt vastgesteld door de Bank en gedragen door de systeemrelevante aanbieder.

§ 4. De leden van de bestuurs- en de beleidsorganen en de personen die instaan voor het beleid, die handelingen stellen of beslissingen nemen zonder de vereiste toestemming van de speciaal commissaris, zijn hoofdelijk aansprakelijk voor het nadeel dat hieruit voor de systeemrelevante aanbieder of voor derden voortvloeit.

§ 5. Indien de Bank de aanstelling van een speciaal commissaris in het *Belgisch Staatsblad* heeft bekendgemaakt, met opgave van de handelingen en beslissingen waarvoor zijn toestemming is vereist, zijn alle handelingen en beslissingen zonder deze vereiste toestemming nietig, tenzij de speciaal commissaris die bekrachtigt. Onder dezelfde voorwaarden zijn alle beslissingen van de algemene vergadering zonder de vereiste toestemming van de speciaal commissaris nietig, tenzij hij die bekrachtigt.

§ 6. De Bank kan een plaatsvervangend commissaris aanstellen.

Art. 85

§ 1. De Bank kan de vervanging gelasten van alle of een deel van de leden van de raad van toezicht en/of van de personen belast met de effectieve leiding van de systeemrelevante aanbieder, binnen een termijn die zij bepaalt. Indien binnen deze termijn geen vervanging geschiedt, kan de Bank één of meerdere leden van de raad van toezicht of één of meer personen belast met de effectieve leiding van de aanbieder ontslaan, of in de plaats van de voltallige bestuurs- en beleidsorganen van de aanbieder een of meer voorlopige bestuurders aanstellen die alleen of collegiaal, naargelang van het geval, de bevoegdheden hebben van de vervangen personen. De Bank maakt haar beslissing bekend in het *Belgisch Staatsblad*.

§ 2. Wanneer de omstandigheden dit rechtvaardigen, kan de Bank een of meer voorlopige bestuurders aanstellen zonder vooraf de vervanging te gelasten van alle of een deel van de leiders van de systeemrelevante aanbieder.

§ 2. Le commissaire spécial peut soumettre à la délibération de tous les organes du fournisseur d'importance systémique, y compris l'assemblée générale, toutes propositions qu'il juge opportunes.

§ 3. La rémunération du commissaire spécial est fixée par la Banque et supportée par le fournisseur d'importance systémique.

§ 4. Les membres des organes d'administration et de gestion et les personnes chargées de la gestion qui accomplissent des actes ou prennent des décisions sans avoir recueilli l'autorisation requise du commissaire spécial sont responsables solidairement du préjudice qui en est résulté pour le fournisseur d'importance systémique ou les tiers.

§ 5. Si la Banque a publié au *Moniteur belge* la désignation du commissaire spécial et spécifié les actes et décisions soumis à son autorisation, les actes et décisions intervenus sans cette autorisation alors qu'elle était requise sont nuls, à moins que le commissaire spécial ne les ratifie. Dans les mêmes conditions toute décision d'assemblée générale prise sans avoir recueilli l'autorisation requise du commissaire spécial est nulle, à moins que le commissaire spécial ne la ratifie.

§ 6. La Banque peut désigner un commissaire suppléant.

Art. 85

§ 1er. La Banque peut enjoindre le remplacement de tout ou partie des membres du conseil de surveillance et/ou des personnes chargées de la direction effective du fournisseur d'importance systémique, dans un délai qu'elle fixe. À défaut d'un tel remplacement dans ce délai, la Banque peut démettre un ou plusieurs membres du conseil de surveillance ou une ou plusieurs personnes chargées de la direction effective du fournisseur ou substituer à l'ensemble des organes d'administration et de gestion du fournisseur un ou plusieurs administrateurs provisoires qui disposent, seuls ou collégialement selon le cas, des pouvoirs des personnes remplacées. La Banque publie sa décision au *Moniteur belge*.

§ 2. Lorsque les circonstances le justifient, la Banque peut procéder à la désignation d'un ou plusieurs administrateurs provisoires sans procéder préalablement à l'injonction de remplacer tout ou partie des dirigeants du fournisseur d'importance systémique.

§ 3. Mits de Bank hiermee instemt, kan of kunnen de voorlopige bestuurder(s) een algemene vergadering bijeenroepen en de agenda ervan vaststellen.

§ 4. Het mandaat van de vervangen personen eindigt na de kennisgeving van de beslissing van de Bank om hen door een of meer voorlopige bestuurders te vervangen. De systeemrelevante aanbieder vervult de openbaarmakingsformaliteiten die vereist zijn in geval van beëindiging van de betrokken mandaten.

§ 5. De Bank kan afwijken van de door of krachtens deze wet vastgestelde rapporteringsverplichtingen voor de systeemrelevante aanbieder ten aanzien waarvan zij een maatregel bestaande in de benoeming van een of meer voorlopige bestuurders heeft genomen.

§ 6. De bezoldiging van de voorlopige bestuurder(s) wordt vastgesteld door de Bank en gedragen door de systeemrelevante aanbieder.

§ 7. De Bank kan de voorlopige bestuurder(s) te allen tijde vervangen, hetzij ambtshalve, hetzij op verzoek van een meerderheid van aandeelhouders of vennoten, wanneer zij aantonen dat het beleid van de betrokkenen niet langer de nodige waarborgen biedt.

Art. 86

§ 1. De speciaal commissaris en de voorlopige bestuurder(s) bedoeld in de artikelen 84 en 85, dragen voor rekening van de Bank bij aan de uitoefening van haar wettelijke opdracht. In het kader van deze opdracht:

1° handelen zij uitsluitend in het kader van het in artikel 2 van deze wet vastgelegde doel;

2° volgen zij de instructies van de Bank met betrekking tot de wijze waarop de hun toevertrouwde specifieke opdracht moet worden uitgevoerd;

3° zijn zij onderworpen aan dezelfde verplichtingen inzake beroepsgeheim als die welke voor de Bank gelden in het kader van de in deze wet vastgelegde toezichtsopdracht. Voor het gebruik van wettelijke uitzonderingen is de voorafgaande toestemming van de Bank vereist;

4° brengen zij op verzoek van de Bank, volgens de modaliteiten die zij bepaalt, verslag uit over de financiële positie van de systeemrelevante aanbieder en over de maatregelen die zij in het kader van hun opdracht hebben genomen, evenals over de financiële positie aan het begin en aan het einde van die opdracht.

§ 3. Moyennant l'autorisation de la Banque, le ou les administrateurs provisoires peuvent convoquer une assemblée générale et en établir l'ordre du jour.

§ 4. Le mandat des personnes remplacées prend fin dès la notification de la décision de la Banque substituant un ou plusieurs administrateurs provisoires. Le fournisseur d'importance systémique accomplit les formalités de publicité requises par la fin des mandats concernés.

§ 5. La Banque peut déroger aux obligations de reporting prévues par ou en vertu de la présente loi à l'égard du fournisseur d'importance systémique faisant l'objet d'une mesure de nomination d'un ou plusieurs administrateurs provisoires.

§ 6. La rémunération du ou des administrateurs provisoires est fixée par la Banque et supportée par le fournisseur d'importance systémique.

§ 7. La Banque peut, à tout moment, remplacer le ou les administrateurs provisoires, soit d'office, soit à la demande d'une majorité des actionnaires ou associés lorsque ceux-ci justifient que la gestion des intéressés ne présente plus les garanties nécessaires.

Art. 86

§ 1er. Le commissaire spécial et le ou les administrateurs provisoires visés aux articles 84 et 85 contribuent à l'exercice de la mission légale de la Banque, pour compte de celle-ci. Dans le cadre de cette mission,

1° ils agissent exclusivement dans le cadre de la finalité prévue par l'article 2 de la présente loi;

2° ils suivent les instructions de la Banque quant à la manière d'accomplir la mission particulière qui leur est confiée;

3° ils sont assujettis aux mêmes obligations en matière de secret professionnel que celles applicables à la Banque en ce qui concerne la mission de contrôle prévue par la présente loi, l'usage des exceptions légales étant soumis à une autorisation préalable de la Banque;

4° ils font, à la requête de la Banque, selon les modalités qu'elle détermine, rapport sur la situation financière du fournisseur d'importance systémique et sur les mesures prises dans le cadre de leur mission, ainsi que sur la situation financière au début et à la fin de cette mission.

Hun ondersteunende rol ten aanzien van de Bank impliceert dat zij als dusdanig niet als administratieve autoriteit kunnen worden beschouwd.

§ 2. De vervanging van de voltallige bestuurs- en beleidsorganen van de systeemrelevante aanbieder door voorlopige bestuurders, overeenkomstig artikel 85 impliceert niet dat deze laatsten moeten worden beschouwd als bestuurders of leden van het wettelijk bestuursorgaan in de zin van het Wetboek van Vennootschappen en Verenigingen, maar enkel dat zij de bevoegdheden hebben van de vervangen personen, met name om de handelingen te verrichten die de systeemrelevante aanbieder in staat stellen te voldoen aan zijn wettelijke en reglementaire verplichtingen, in het bijzonder deze die door of krachtens het Wetboek van Vennootschappen en Verenigingen zijn vastgesteld. Er wordt aan hen geen kwijting verleend bij een beslissing of stemming als bedoeld in het Wetboek van Vennootschappen en Verenigingen. Zij zijn voor hun opdracht uitsluitend verantwoording verschuldigd ten aanzien van de Bank, die hen in voorkomend geval kwijting verleent.

Art. 87

§ 1. De ondernemingsrechtbank spreekt op verzoek van elke belanghebbende de nietigverklaringen uit bedoeld in artikel 83, § 1, tweede lid, en in artikel 84, § 5.

§ 2. De nietigheidsvordering wordt ingesteld tegen de systeemrelevante aanbieder. Indien verantwoord om ernstige redenen, kan de eiser in kort geding de voorlopige schorsing vorderen van de gewraakte handelingen of beslissingen. Het schorsingsbevel en het vonnis van nietigverklaring hebben uitwerking ten aanzien van iedereen. Ingeval de geschorste of vernietigde handeling of beslissing bekendgemaakt is, worden het schorsingsbevel en het vonnis van nietigverklaring bij uittreksel op dezelfde wijze bekendgemaakt.

§ 3. Wanneer de nietigheid afbreuk kan doen aan de rechten die een derde te goeder trouw ten aanzien van de systeemrelevante aanbieder heeft verworven, kan de rechtbank verklaren dat die nietigheid geen uitwerking heeft ten aanzien van de betrokken rechten, onverminderd het eventuele recht van de eiser op schadevergoeding.

§ 4. De nietigheidsvordering kan niet meer worden ingesteld na afloop van een termijn van zes maanden vanaf de datum waarop de betrokken handelingen of beslissingen kunnen worden tegengeworpen aan wie hun nietigheid inroept, of hem bekend zijn.

Leur qualité d'auxiliaire de la Banque implique qu'ils ne peuvent, comme tels, être considérés comme une autorité administrative.

§ 2. La substitution de l'ensemble des organes d'administration et de gestion du fournisseur d'importance systémique par les administrateurs provisoires opérée en application de l'article 85 n'implique pas que ces derniers doivent être considérés comme des administrateurs ou membres de l'organe légal d'administration au sens du Code des sociétés et des associations mais seulement qu'ils bénéficient des pouvoirs des personnes remplacées, notamment aux fins d'accomplir les actes permettant au fournisseur d'importance systémique de satisfaire à ses obligations légales et réglementaires, en particulier celles prévues par ou en vertu du Code des sociétés et des associations. À ce titre, ils ne font pas l'objet d'une décision ou d'un vote sur la décharge tel que prévu par le Code des sociétés et des associations mais répondent de leur mission à l'égard de la Banque exclusivement qui leur donne décharge s'il y échet.

Art. 87

§ 1er. Le tribunal de l'entreprise prononce à la requête de tout intéressé, les nullités prévues à l'article 83, § 1er, alinéa 2, et à l'article 84, § 5.

§ 2. L'action en nullité est dirigée contre le fournisseur d'importance systémique. Si des motifs graves le justifient, le demandeur en nullité peut solliciter en référé la suspension provisoire des actes ou décisions attaqués. L'ordonnance de suspension et le jugement prononçant la nullité produisent leurs effets à l'égard de tous. Au cas où l'acte ou la décision suspendu ou annulé a fait l'objet d'une publication, l'ordonnance de suspension et le jugement prononçant la nullité sont publiés en extrait dans les mêmes formes.

§ 3. Lorsque la nullité est de nature à porter atteinte aux droits acquis de bonne foi par un tiers à l'égard du fournisseur d'importance systémique, le tribunal peut déclarer sans effet la nullité à l'égard de ces droits, sans préjudice du droit du demandeur à des dommages et intérêts s'il y a lieu.

§ 4. L'action en nullité ne peut plus être intentée après l'expiration d'un délai de six mois à compter de la date à laquelle les actes ou décisions intervenus sont opposables à celui qui invoque la nullité ou sont connus de lui.

HOOFDSTUK 10

Dwangsommen, administratieve sancties en andere maatregelen

Art. 88

Onverminderd de andere bij deze wet voorgeschreven maatregelen kan de Bank bekendmaken dat een systeemrelevante aanbieder geen gevolg heeft gegeven aan haar aanmaningen om zich binnen de termijn die zij bepaalt te conformeren aan de bepalingen van deze wet en haar uitvoeringsbesluiten en reglementen.

Art. 89

§ 1. Wanneer de Bank een termijn heeft opgelegd als bedoeld in artikel 82, § 1, en de toestand na het verstrijken van die termijn niet is verholpen, kan de Bank een dwangsom opleggen na de systeemrelevante aanbieder gehoord of tenminste opgeroepen te hebben. De dwangsom mag per dag niet meer bedragen dan 50.000 euro, noch in het totaal 2.500.000 euro overschrijden.

§ 2. Bij de vaststelling van het bedrag van de dwangsom wordt met name rekening gehouden met:

1° de ernst van de vastgestelde tekortkomingen en, in voorkomend geval, de potentiële impact van die tekortkomingen op de financiële stabiliteit en op de stabiliteit en continuïteit van nationale en internationale financiële transacties;

2° de financiële draagkracht van de systeemrelevante aanbieder, zoals die met name blijkt uit zijn totale omzet.

Art. 90

§ 1. Onverminderd de andere maatregelen bepaald in deze wet, kan de Bank aan de betrokken systeemrelevante aanbieder of de verantwoordelijke natuurlijke persoon een administratieve geldboete opleggen indien zij een inbreuk vaststelt op de bepalingen van deze wet of op de ter uitvoering ervan genomen besluiten en reglementen. Het bedrag van de administratieve geldboete mag voor hetzelfde feit of voor hetzelfde geheel van feiten niet meer bedragen dan 10 % van de jaarlijkse netto-omzet van het voorbije boekjaar van de systeemrelevante aanbieder.

§ 2. Wanneer de inbreuk voor de overtreder winst heeft opgeleverd of hem heeft toegelaten verlies te vermijden, mag dit maximum worden verhoogd tot het drievoud van deze winst of dit verlies.

CHAPITRE 10

Astreintes, sanctions administratives et autres mesures

Art. 88

Sans préjudice des autres mesures prévues par la présente loi, la Banque peut publier qu'un fournisseur d'importance systémique ne s'est pas conformé aux injonctions qui lui ont été faites de respecter dans le délai qu'elle détermine les dispositions de la présente loi et des arrêtés et règlements pris pour son exécution.

Art. 89

§ 1er. Lorsque la Banque a fixé un délai visé à l'article 82, § 1er, et qu'au terme de ce délai il n'a pas été remédié à la situation, la Banque peut infliger une astreinte après avoir entendu ou à tout le moins avoir dûment convoqué le fournisseur d'importance systémique. L'astreinte ne pourra excéder 50.000 euros par jour, ni 2.500.000 euros au total.

§ 2. Le montant de l'astreinte est fixé en tenant notamment compte:

1° de la gravité des manquements rencontrés et, le cas échéant, de l'impact potentiel de ces manquements sur la stabilité financière et sur la stabilité et la continuité des transactions financières nationales et internationales;

2° de l'assise financière du fournisseur d'importance systémique, telle qu'elle ressort notamment de son chiffre d'affaires total.

Art. 90

§ 1er. Sans préjudice des autres mesures prévues par la présente loi, la Banque peut imposer une amende administrative au fournisseur d'importance systémique ou à la personne physique en cause, si elle constate une infraction aux dispositions de la présente loi ou des arrêtés et règlements pris pour son exécution. Le montant de l'amende administrative, pour le même fait ou pour le même ensemble de faits, est de maximum 10 % du chiffre d'affaires annuel net au cours de l'exercice précédent du fournisseur d'importance systémique.

§ 2. Lorsque l'infraction a procuré un profit au contrevenant ou a permis à ce dernier d'éviter une perte, ce maximum peut être porté au triple du montant de ce profit ou de cette perte.

§ 3. Het bedrag van de geldboete wordt met name vastgesteld op grond van:

1° de ernst en de duur van de tekortkomingen;

2° de mate van verantwoordelijkheid van de betrokkene;

3° de financiële draagkracht van de betrokkene, zoals die met name blijkt uit de totale omzet van de betrokken rechtspersoon of uit het jaarinkomen van de betrokken natuurlijke persoon;

4° het voordeel of de winst die deze tekortkomingen eventueel opleveren;

5° het nadeel dat derden door deze tekortkomingen hebben geleden, voor zover dit kan worden bepaald;

6° de mate van medewerking van de betrokken natuurlijke of rechtspersoon met de Bank;

7° vroegere tekortkomingen van de betrokkene;

8° de potentiële negatieve impact van de tekortkomingen op de financiële stabiliteit en op de stabiliteit en continuïteit van nationale en internationale financiële transacties.

Art. 91

De met toepassing van de artikelen 89 en 90 opgelegde dwangsommen en geldboetes worden ingevorderd ten bate van de Schatkist door de Algemene Administratie van de inning en invordering van de Federale Overheidsdienst Financiën.

Art. 92

De Bank kan de overeenkomstig dit hoofdstuk opgelegde maatregelen openbaar maken nadat zij de systeemrelevante aanbieder of betrokken natuurlijke personen in kennis heeft gesteld, tenzij de bekendmaking een lopend strafrechtelijk onderzoek zou ondermijnen, de stabiliteit van de financiële markten in gevaar zou brengen of disproportionele schade zou berokkenen aan de systeemrelevante aanbieder of de betrokken natuurlijke personen.

De Bank zorgt ervoor dat op grond van dit artikel bekendgemaakte informatie gedurende ten minste vijf jaar op haar website blijft staan. Persoonsgegevens mogen alleen worden bewaard op de website van de

§ 3. Le montant de l'amende est notamment fixé en fonction:

1° de la gravité et de la durée des manquements;

2° du degré de responsabilité de la personne en cause;

3° de l'assise financière de la personne en cause, telle qu'elle ressort notamment de son chiffre d'affaires total de la personne morale en cause ou des revenus annuels de la personne physique en cause;

4° des avantages ou profits éventuellement tirés de ces manquements;

5° d'un préjudice subi par des tiers du fait des manquements, dans la mesure où il peut être déterminé;

6° du degré de coopération avec la Banque dont a fait preuve la personne physique ou morale en cause;

7° des manquements antérieurs commis par la personne en cause;

8° de l'impact négatif potentiel des manquements sur la stabilité financière et sur la stabilité et la continuité des transactions financières nationales et internationales.

Art. 91

Les astreintes et amendes imposées en application des articles 89 et 90 sont recouvrées au profit du Trésor public par l'Administration générale de la Perception et du Recouvrement du Service public fédéral Finances.

Art. 92

La Banque peut rendre publiques les mesures imposées conformément au présent Chapitre après avoir informé le fournisseur d'importance systémique ou les personnes physiques concernées, sauf si la publication compromettrait une enquête pénale en cours ou la stabilité des machés financiers, ou causerait un préjudice disproportionné au fournisseur d'importance systémique ou aux personnes physiques concernées.

La Banque veille à ce que toute information publiée en vertu du présent article demeure sur son site internet pendant au moins cinq ans. Les données à caractère personnel ne peuvent être maintenus sur le site internet

Bank indien dat is toegestaan op grond van de toepasselijke regels inzake gegevensbescherming.

HOOFDSTUK 11

Wijzigingsbepalingen en inwerkingtreding

Art. 93

Artikel 8 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, vervangen bij de wet van 24 maart 2017, wordt aangevuld met een paragraaf 4, luidende:

"§ 4. De Bank kan de werkingskosten die betrekking hebben op het toezicht bedoeld in de eerste paragraaf verhalen op de instellingen die onder haar toezicht staan, volgens de nadere regels vastgesteld door de Koning.

De Bank kan de Algemene Administratie van de inning en invordering van de Federale overheidsdienst Financiën belasten met de inning van de onbetaalde vergoedingen.".

Art. 94

Deze wet treedt in werking op 1 januari 2026.

de la Banque que si les règles applicables en matière de protection des données le permettent.

CHAPITRE 11

Modifications et entrée en vigueur

Art. 93

L'article 8 de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique, remplacé par la loi du 24 mars 2017, est complété par un paragraphe 4 rédigé comme suit:

"§ 4. La Banque peut récupérer auprès des établissements soumis à son contrôle les frais de fonctionnement qui ont trait au contrôle visé au paragraphe 1er, selon les modalités fixées par le Roi.

La Banque peut charger l'Administration générale de la perception et du recouvrement du service public fédéral Finances du recouvrement des contributions impayées.".

Art. 94

La présente loi entre en vigueur le 1er janvier 2026.

Centrale drukkerij - Imprimerie centrale