DOC 56 **0610/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

18 december 2024

WETSVOORSTEL

houdende het toezicht op aanbieders van financiële berichtendiensten

(ingediend door de heer Koen Van den Heuvel c.s.)

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

18 décembre 2024

PROPOSITION DE LOI

relative à la surveillance des fournisseurs de services de messagerie financière

(déposée par M. Koen Van den Heuvel et consorts)

SAMENVATTING

Dit wetsvoorstel beoogt systeemrelevante aanbieders van financiële berichtendiensten die in België gevestigd zijn, te onderwerpen aan specifieke bedrijfsuitoefeningsvoorwaarden en onder het directe toezicht van de Nationale Bank van België (NBB) te brengen. Dit is van belang omdat deze entiteiten een cruciale rol spelen in het functioneren van het verrekenings-, vereffenings- en betalingssysteem.

Het wetsvoorstel heeft als doel een juridisch afdwingbaar toezicht te implementeren voor deze systeemrelevante aanbieders van financiële berichtendiensten, met de nadruk op risicobeheer en operationele veiligheid, en is geïnspireerd op bestaande internationale normen en Europese wetgeving.

RÉSUMÉ

La présente proposition de loi vise à soumettre les fournisseurs de services de messagerie financière d'importance systémique établis en Belgique à certaines conditions d'exploitation et à les placer sous la supervision directe de la Banque nationale de Belgique. C'est important parce que les entités jouent un rôle important dans le bon fonctionnement des systèmes de compensation, de règlement en de paiement.

La proposition de loi vise à mettre en place une surveillance juridiquement contraignante pour ces fournisseurs de services de messagerie financière d'importance systémique, en mettant l'accent sur la gestion des risques et la sécurité opérationnelle, et s'inspire des normes internationales existantes et de la législation européenne.

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*

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

TOELICHTING

DAMES EN HEREN,

Inleiding

Dit wetsvoorstel heeft als doel de in België gevestigde systeemrelevante aanbieders van financiële berichtendiensten te onderwerpen aan bepaalde bedrijfsuitoefeningsvoorwaarden en om hen onder direct wettelijk toezicht van de Nationale Bank van België (hierna: de Bank) te brengen.

Entiteiten die instaan voor het verlenen van financiële berichtendiensten spelen doorgaans een belangrijke rol in het naar behoren functioneren van de verrekenings-, vereffenings- en betalingssystemen. Dit wetsvoorstel legt daarom een reeks verplichtingen op aan de in België gevestigde aanbieders van financiële berichtendiensten die van systemisch belang zijn. Er wordt voorgesteld dit systemisch belang te bepalen op basis van de overschrijding van een drempel van het aantal financiële transacties, gemeten over één kalenderjaar, met betrekking waartoe een aanbieder financiële berichtendiensten heeft verleend.

Voor een goed begrip van de doelstellingen die met dit wetsvoorstel worden nagestreefd, is het belangrijk om eerst een overzicht te bieden van de toezichtsactiviteiten die de Bank vandaag de dag reeds uitoefent ten aanzien van financiële marktinfrastructuren en aanbieders van financiële berichtendiensten, in het bijzonder ten aanzien van SWIFT. Daaruit zal blijken dat dit zogenaamde *oversight* voornamelijk gebaseerd is op normen die juridisch niet afdwingbaar zijn (*soft law*) en op morele overtuigingskracht (*moral suasion*), terwijl het juist aangewezen is om minstens een deel van dat *oversight* op systeemrelevante aanbieders van financiële berichtendiensten te baseren op een juridisch bindend en afdwingbaar kader. Hierin ligt dan ook de ware doelstelling van het voorliggend wetsvoorstel. De motieven voor het tot stand brengen van die doelstellingen worden vervolgens op algemene wijze toegelicht, alvorens een inzicht te bieden in de beleidsmatige, praktische en juridisch-technische keuzes die voorgesteld worden ter implementatie van die doelstellingen. Tot slot wordt waar nodig per artikel toelichting verstrekt bij de gemaakte keuzes en de eventuele implicaties daarvan.

Normen voor de uitoefening van het oversight op financiële marktinfrastructuren

Op Bank oefent op grond van artikel 12*bis* van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België (hierna: de

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

Introduction

Cette proposition de loi a pour objet de soumettre les fournisseurs de services de messagerie financière d'importance systémique établis en Belgique à un ensemble de conditions d'exercice de leur activité et de les placer sous la surveillance légale directe de la Banque nationale de Belgique (ci-après, "la Banque").

Les entités chargées de fournir des services de messagerie financière jouent généralement un rôle important dans le bon fonctionnement des systèmes de compensation, de règlement et de paiement. La présente proposition de loi impose donc une série d'obligations aux fournisseurs de services de messagerie financière d'importance systémique établis en Belgique. Il est proposé de définir cette importance systémique sur la base du dépassement d'un seuil quant au nombre de transactions financières, calculé au cours d'une année civile, pour lesquelles un fournisseur a offert des services de messagerie financière.

Pour bien comprendre les objectifs poursuivis par cette proposition de loi, il importe de d'abord donner un aperçu des activités de surveillance que la Banque exerce aujourd'hui à l'égard des infrastructures de marchés financiers et des fournisseurs de services de messagerie financière, en particulier à l'égard de SWIFT. Il en ressortira que cette surveillance (*oversight*) repose principalement sur des normes juridiquement non contraignantes (*soft law*) et sur la force de persuasion morale (*moral suasion*), tandis que qu'il convient précisément de fonder au moins une partie de cet *oversight* des fournisseurs de services de messagerie financière d'importance systémique sur un cadre juridiquement contraignant et exécutoire. Tel est donc le véritable objectif de la présente proposition de loi. Les raisons qui ont motivé la fixation de ces objectifs sont ensuite expliquées de manière générale, avant que ne soient passés en revue les choix politiques, pratiques et juridico-techniques qui sont proposés pour les mettre en œuvre. Enfin, là où cela s'avère nécessaire, des explications sont fournies pour chaque article quant aux choix effectués et à leurs implications éventuelles.

Normes pour l'exercice de l'oversight des infrastructures de marchés financiers

La Banque exerce le contrôle dit prudentiel des établissements financiers en vertu de l'article 12*bis* de la loi du 22 février 1998 fixant le statut organique de la Banque

organieke wet) het zogenaamd prudentieel toezicht uit op financiële instellingen. Deze instellingen dienen voor het uitoefenen van hun activiteiten een vergunning te ontvangen van de Bank en te allen tijde te voldoen aan de bij wet voorgeschreven bedrijfsuitoefeningsvoorwaarden. De Bank ziet aldus toe op de naleving van de voorwaarden voor het verkrijgen van een vergunning en de betrokken bedrijfsuitoefeningsvoorwaarden. De regels inzake het prudentieel statuut van deze instellingen, waaronder kredietinstellingen, beursvennootschappen, verzekeringsondernemingen en betalingsinstellingen, zijn vastgelegd in een in detail geregeld en juridisch afdwingbaar kader.

Daarnaast waakt de Bank op grond van artikel 8 van haar Organieke Wet ook over de goede werking van de verrekenings-, vereffenings- en betalingssystemen en vergewist ze zich van hun doelmatigheid en deugdelijkheid overeenkomstig de toepasselijke wetsbepalingen. Dit zogenaamd *oversight* onderwerpt de exploitanten van de betrokken systemen niet aan een vergunningsplicht maar enkel aan welomschreven bedrijfsuitoefeningsnormen. Het *oversight* is verder gebaseerd op vrijwilligheid en historische relaties met belangrijke spelers in de financiële markt, en impliceert dat de Bank in dialoog treedt met de entiteiten die verrekenings-, vereffenings- en betalingssystemen exploiteren (hierna: financiële marktinfrastructuren) en hen er in voorkomend geval op basis van morele overtuigingskracht of zogenaamde *moral suasion* tracht toe te brengen om de normen na te leven die de goede werking, doelmatigheid en deugdelijkheid van de betrokken systemen dienen te verzekeren. Anders dan wat het bepaalde in paragraaf 1 van artikel 8 van de Organieke Wet laat uitschijnen, zijn de normen die de exploitanten van financiële marktinfrastructuren op grond van dat artikel geacht worden na te leven doorgaans immers niet vastgelegd in een juridisch bindend kader en dus ook niet juridisch afdwingbaar.

Op internationaal en overkoepelend niveau zijn de *oversight*normen voor financiële marktinfrastructuren in de eerste plaats terug te vinden in de *Principles for Financial Market Infrastructures* (hierna: PFMI), zoals ontwikkeld in 2012 in samenwerking tussen enerzijds het in de schoot van de Bank voor Internationale Betalingen opgerichte Committee on Payment and Market Infrastructures (hierna: CPMI) en anderzijds het Technische Comité van de Internationale Organisatie van Effectentoezichthouders (hierna: IOSCO). De PFMI zijn hier terug te vinden: *https://www.bis.org/cpmi/publ/d101a.pdf.*

Op Eurosysteemniveau wordt het *oversight* op betalingssystemen die niet systeemrelevant zijn uitgeoefend op basis van de PFMI. Hetzelfde geldt onder meer wat

Nationale de Belgique (ci-après, “la loi organique”). Ces établissements doivent être agréés par la Banque pour exercer leur activité et doivent à tout moment respecter les conditions d’exercice de celle-ci prescrites par la loi. La Banque veille ainsi au respect des conditions d’obtention de l’agrément et des conditions d’exercice de l’activité. Les règles relatives au statut prudentiel de ces établissements, y compris les établissements de crédit, les sociétés de bourse, les entreprises d’assurance et les établissements de paiement, sont définies dans un cadre détaillé et juridiquement contraignant.

En outre, l’article 8 de la loi organique de la Banque prévoit que cette dernière veille également au bon fonctionnement des systèmes de compensation, de règlement et de paiement et qu’elle s’assure de leur efficacité et de leur solidité dans le respect des dispositions légales en vigueur. Cet *oversight* ne soumet pas les exploitants des systèmes concernés à une obligation d’agrément mais uniquement à des conditions bien définies d’exercice de leur activité. L’*oversight* repose en outre sur la coopération volontaire et sur les relations historiques avec les acteurs importants du marché financier, et il implique que la Banque engage un dialogue avec les entités exploitant des systèmes de compensation, de règlement et de paiement (ci-après, “les infrastructures de marchés financiers”) et, le cas échéant, sur la base de la force de persuasion morale, cherche à les persuader de respecter les normes qui doivent garantir le bon fonctionnement, l’efficacité et la solidité des systèmes en question. En effet, contrairement à ce que donnent à penser les dispositions du paragraphe 1er de l’article 8 de la loi organique, les normes à respecter par les exploitants d’infrastructures de marchés financiers en vertu de cet article ne sont généralement pas énoncées dans un cadre juridiquement contraignant et ne sont donc pas juridiquement exécutoires.

Aux niveaux international et global, les normes d’*oversight* des infrastructures de marchés financiers figurent principalement dans les Principes pour les infrastructures de marchés financiers (ci-après, “PIMF”), élaborés en 2012 dans le cadre d’une collaboration entre, d’une part, le Comité sur les paiements et les infrastructures de marché (ci-après, “CPIM”) constitué au sein de la Banque des règlements internationaux et, d’autre part, le Comité technique de l’Organisation internationale des commissions de valeurs (ci-après, “OICV”). Les PIMF sont consultables ici: *https://www.bis.org/cpmi/publ/d101a.pdf.*

Au niveau de l’Eurosystème, l’*oversight* des systèmes de paiement qui ne sont pas d’importance systémique est exercé sur la base des PIMF. Il en va de même,

het *oversight* betreft op centrale effectenbewaarinstellingen en centrale tegenpartijen. Het *oversight* op elektronische betaalinstrumenten, betaalschema's en betalingsregelingen wordt uitgeoefend conform het op de PFMI gebaseerde *Eurosystem Oversight Framework for Electronic Payment Instruments, Schemes and Arrangements* (het zogenaamde PISA Framework: *https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf).* Het Eurosysteem heeft eveneens *oversight*verwachtingen bekend gemaakt op het vlak van cyberweerbaarheid (*https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf*). Geen van deze *oversight*normen zijn neergelegd in een juridisch bindend kader. Een belangrijke uitzondering hierop betreft evenwel het *oversight* op systeemrelevante betalingssystemen (*Systemically Important Payment Systems of SIPS*), hetwelk zijn neerslag heeft gevonden in Verordening (EU) nr. 795/2014 van de Europese Centrale Bank van 3 juli 2014 (hierna: de SIPS-verordening).

De rol van de Bank in het oversight van kritieke dienstverleners

Zoals hierboven aangegeven heeft het *oversight* van de Bank, dat overwegend plaatsvindt binnen de context van het Eurosysteem, betrekking op exploitanten van financiële marktinfrastructuren of van daar nauw mee verbonden systemen zoals betaalschema's en betalingsregelingen. Aldus oefent de Bank vandaag de dag het *oversight* uit op onder meer het verrekeningssysteem UCV/CEC (*Centre for Exchange and Clearing*), de betaalschema's van Bancontact en Mastercard Europe, de verwerkers van betalingstransacties Worldline SA/NV en equensWorldline SE en het systeemrelevante betalingssysteem van Mastercard Europe. Meer toelichting bij het *oversight* door de Bank kan hier gevonden worden: *https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/latest/fmi_the_bank_role.pdf.*

Annex F van de PFMI bevat daarnaast ook specifieke *oversight*normen voor kritieke dienstverleners. Het betreft dienstverleners die als dusdanig zelf niet kwalificeren als financiële marktinfrastructuur maar wel diensten leveren die van kritiek belang zijn voor het functioneren van die marktinfrastructuren, zoals specifieke ICT-diensten en berichtendiensten. Toezichthouders mogen specifieke verwachtingen tot stand brengen ten aanzien van die kritieke dienstverleners om aldus de veiligheid en het deugdelijk functioneren van financiële marktinfrastructuren te ondersteunen. Op grond hiervan oefent de Bank sinds 1998 ook het *oversight* uit op de *Society*

entre autres, pour l'*oversight* des dépositaires centraux de titres et des contreparties centrales. L'*oversight* des instruments de paiement électronique, des schémas de paiement et des dispositifs de paiement est effectué conformément au cadre d'*oversight* de l'Eurosystème applicable aux instruments, schémas et dispositifs de paiement électronique (ci-après, "le cadre PISA": *https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf),* basé sur les PIMF. L'Eurosystème a également énoncé des attentes en matière d'*oversight* dans le domaine de la cyber-résilience (*https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf*). Aucune de ces normes d'*oversight* n'est inscrite dans un cadre juridiquement contraignant. Toutefois, une importante exception à cette règle réside dans l'*oversight* des systèmes de paiement d'importance systémique (*systemically important payment systems ou SIPS*), qui se reflète dans le règlement (UE) n° 795/2014 de la Banque centrale européenne du 3 juillet 2014 (ci-après, "le règlement SIPS").

Rôle de la Banque dans l'oversight des fournisseurs de services critiques

Comme indiqué ci-dessus, l'*oversight* de la Banque, qui s'exerce principalement dans le contexte de l'Eurosystème, concerne les exploitants d'infrastructures de marchés financiers ou de systèmes qui y sont étroitement liés, comme les schémas et les dispositifs de paiement. Ainsi, la Banque surveille aujourd'hui, entre autres, le système de compensation CEC/UCV (*Centre d'échange et de compensation*), les schémas de paiement de Bancontact et de Mastercard Europe, les processeurs d'opérations de paiement Worldline SA/NV et equensWorldline SE, ainsi que le système de paiement d'importance systémique de Mastercard Europe. De plus amples explications concernant l'*oversight* exercé par la Banque sont disponibles ici: *https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/latest/fmi_the_bank_role.pdf.*

L'annexe F aux PIMF contient en outre des normes d'*oversight* propres aux fournisseurs de services critiques. Il s'agit de prestataires de services qui, en tant que tels, ne sont pas considérés comme des infrastructures de marchés financiers mais qui fournissent des services d'importance critique pour le fonctionnement de ces infrastructures, tels des services TIC spécifiques et des services de messagerie. Les autorités de surveillance peuvent définir des attentes particulières à l'égard de ces fournisseurs de services critiques afin de favoriser la sécurité et la solidité des infrastructures de marchés financiers. Sur cette base, la Banque exerce également depuis

for Worldwide Interbank Financial Telecommunication (hierna: SWIFT).

Een groot aantal financiële instellingen en financiële marktinfrastructuren van systemisch belang zijn afhankelijk van SWIFT voor hun dagelijks berichtenverkeer. Als aanbieder van kritieke diensten voor deze systemen heeft SWIFT zelf ook een systemisch karakter. De Bank oefent het *oversight* op SWIFT, dat mondiaal actief is, uit samen met andere centrale banken. De Bank neemt de leiding en zorgt voor de coördinatie van dit coöperatief *oversight* omdat de maatschappelijke zetel van SWIFT gevestigd is in België. Meer informatie over het *oversight* op SWIFT kan gevonden worden op de website van de Bank (*https://www.nbb.be/nl/financieel-toezicht/oversight/andere-marktinfrastructuren-en-aanbieders-van-diensten)* en in haar jaarlijks verslag over financiële marktinfrastructuren en betaaldiensten (voor het verslag van 2024, zie *https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/2024/fmi-report2024.pdf*).

Van "soft law" naar een juridisch afdwingbaar kader

Zoals hierboven aangegeven, zijn de normen die financiële marktinfrastructuren en hun kritieke dienstverleners geacht worden na te leven doorgaans vervat in instrumenten die niet juridisch afdwingbaar zijn. Men stelt evenwel een tendens vast voor het beter wettelijk verankeren van het *oversight* gelet op de steeds verder geïntegreerde markt voor het uitvoeren van financiële transacties en de steeds complexere verhoudingen tussen de deelnemers aan die transacties.

Het op vrijwilligheid gebaseerde *oversight*systeem botste voor sommige marktinfrastructuren op zijn grenzen en kon niet altijd op efficiënte en solide wijze de naleving van de *oversight*normen verzekeren. Om die reden vaardigde de ECB op 3 juli 2014 de reeds vermelde SIPS-verordening uit met betrekking tot het *oversight* op systeemrelevante betalingssystemen of SIPS. De SIPS-verordening herneemt de *oversight*vereisten uit de PFMI die dienen nageleefd te worden door de SIPS en brengt ze daardoor onder in een juridisch afdwingbaar kader. De zesde considerans van de SIPS-verordening stelt dat ook autoriteiten in andere landen geacht worden op soortgelijke wijze de PFMI-beginselen te introduceren en toe te passen in hun respectievelijke wettelijke en regelgevende kaders, voor zover deze kaders dat toestaan.

Een Belgisch precedent is terug te vinden in de wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties. Deze wet onderwerpt

1998 l'*oversight* de la *Society for Worldwide Interbank Financial Telecommunication* (ci-après, "SWIFT").

Un grand nombre d'établissements financiers et d'infrastructures de marchés financiers d'importance systémique s'appuient sur SWIFT pour leurs messages quotidiens. En tant que fournisseur de services critiques pour ces systèmes, SWIFT présente elle-même un caractère systémique. La Banque exerce l'*oversight* de SWIFT, qui opère à l'échelle mondiale, en collaboration avec d'autres banques centrales. La Banque dirige cet *oversight* coopératif et en assure la coordination car le siège social de SWIFT est situé en Belgique. De plus amples informations concernant l'*oversight* de SWIFT sont disponibles sur le site internet de la Banque (*https://www.nbb.be/fr/supervision-financiere/oversight/autres-infrastructures-de-marche-et-fournisseurs-de-services)* et dans son Rapport annuel sur les infrastructures de marchés financiers et les services de paiement (pour le Rapport 2024, voir *https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/2024/fmi-report2024.pdf*).

De la "soft law" à un cadre juridiquement contraignant

Comme mentionné précédemment, les normes à respecter par les infrastructures de marchés financiers et leurs fournisseurs de services critiques sont en règle générale énoncées dans des instruments qui ne sont pas juridiquement contraignants. On constate cependant une tendance à un meilleur ancrage légal de l'*oversight*, compte tenu de l'intégration toujours croissante du marché de l'exécution des opérations financières et des relations de plus en plus complexes entre les participants à ces opérations.

Le système d'*oversight* basé sur la bonne volonté a atteint ses limites pour certaines infrastructures de marché et n'est pas toujours parvenu à assurer de façon efficace et robuste le respect des normes de surveillance. C'est la raison pour laquelle la BCE a adopté le 3 juillet 2014 le règlement SIPS susmentionné concernant les exigences de surveillance applicables aux systèmes de paiement d'importance systémique. Le règlement SIPS reprend les exigences d'*oversight* des PIMF que les SIPS doivent respecter et les intègre ainsi dans un cadre juridiquement contraignant. Dans son sixième considérant, le règlement SIPS indique que les autorités d'autres pays devraient elles aussi introduire et appliquer de façon similaire les principes des PIMF dans leurs cadres juridiques et réglementaires respectifs, dans toute la mesure autorisée par ces derniers.

On retrouve un précédent belge dans la loi du 24 mars 2017 relative à la surveillance des processeurs d'opérations de paiement. Cette loi soumet les processeurs

systeemrelevante verwerkers van betalingstransacties aan een select aantal *oversight*verwachtingen die gebaseerd zijn op de PFMI. Deze verwerkers worden niet aan prudentiële vereisten onderworpen, wat onder meer impliceert dat zij niet aan een vergunningsplicht onderworpen zijn. De wet leidt er wel toe dat de betrokken *oversight*verwachtingen juridisch afdwingbaar zijn.

De Bank en de deelnemers aan het coöperatief *oversight* op SWIFT beraden zich al enige tijd over een herziening van de op SWIFT toepasselijke *oversight*normen, die voor het laatst herzien werden in 2005. Sindsdien zijn de verwachtingen van toezichthouders op de financiële marktinfrastructuren geëvolueerd. Het CPMI en IOSCO vaardigden bijvoorbeeld richtsnoeren uit inzake de cyberweerbaarheid van financiële marktinfrastructuren, terwijl de verwachtingen van het Eurosysteem inzake het toezicht op de cyberweerbaarheid voor financiële marktdeelnemers en de Europese regelgeving over digitale operationele weerbaarheid (de zogenaamde DORA-verordening, waarover later meer) hebben geleid tot veranderingen in de verwachtingen met betrekking tot operationele risico's.

De toezichthouders van SWIFT zijn van mening dat een aantal van deze verwachtingen zouden moeten gecodificeerd worden om als juridisch vangnet te fungeren en om een gelijk speelveld met het toezicht op de financiële sector te garanderen. De voorgestelde herziening van het *oversight*kader richt zich op het belang van SWIFT als kritieke aanbieder van financiële berichtendiensten. Daarbij wordt aanbevolen om, rekening houdend met de specifieke aard van SWIFT en de diensten die het verleent, de nieuwe verwachtingen inzake bijvoorbeeld cyberweerbaarheid af te stemmen met de klassieke *oversight*verwachtingen die gelden voor de bredere financiële sector, en in het bijzonder met de PFMI. Het is niet de bedoeling om de inhoud of doelstellingen van het huidige *oversight*kader fundamenteel te veranderen, maar enkel om bepaalde aspecten van dit kader te codificeren zodat het als juridisch vangnet kan dienen. Men zou dan ook kunnen spreken van een "versterkt" *oversight*. De huidige organisatie en praktische aanpak van het *oversight* op SWIFT zou daarentegen ongewijzigd blijven. Aan de collaboratieve, consensusvormende interactie tussen de toezichthouders binnen het coöperatief *oversight*, zowel op technisch als senior niveau, zal dus niet geraakt worden.

De indieners ondersteunen ten volle de intenties van de toezichthouders van SWIFT en hebben daarom, met de technische ondersteuning van die toezichthouders, het voorliggend wetsvoorstel uitgewerkt. Er werd over gewaakt dat het wetsvoorstel een algemene draagwijdte heeft en potentieel van toepassing is op alle systeemrelevante aanbieders die in België gevestigd zijn. De

d'opérations de paiement d'importance systémique à un certain nombre d'exigences en matière d'*oversight* fondées sur les PIMF. Ces processeurs ne sont pas soumis à des exigences prudentielles, ce qui implique entre autres qu'ils ne sont pas soumis à une obligation d'agrément. En revanche, la loi rend ces exigences d'*oversight* juridiquement contraignantes.

La Banque et les participants à l'*oversight* coopératif de SWIFT envisagent depuis un certain temps déjà une révision des normes de surveillance applicables à SWIFT, qui ont été révisées pour la dernière fois en 2005. Depuis, les attentes des autorités de surveillance des infrastructures de marchés financiers ont évolué. Par exemple, le CPIM et l'OICV ont publié des orientations sur la cyber-résilience des infrastructures de marchés financiers, tandis que les exigences de l'Eurosystème en matière de surveillance de la cyber-résilience des acteurs des marchés financiers et le règlement européen sur la résilience opérationnelle numérique (*Digital Operational Resilience Act*, dit règlement DORA, voir *infra*) ont donné lieu à des changements dans les exigences relatives aux risques opérationnels.

Les autorités de surveillance de SWIFT estiment que certaines de ces exigences devraient être codifiées pour servir de filet de sécurité juridique et garantir des conditions équivalentes à celles qui régissent la surveillance du secteur financier. La proposition de révision du cadre de surveillance met l'accent sur l'importance de SWIFT en tant que fournisseur critique de services de messagerie financière. À cet égard, il est recommandé, compte tenu de la nature spécifique de SWIFT et des services qu'elle fournit, d'aligner les nouvelles exigences concernant, par exemple, la cyber-résilience sur les exigences classiques en matière d'*oversight* applicables au secteur financier au sens large, et en particulier sur les PIMF. L'intention n'est pas de modifier fondamentalement la teneur ou les objectifs du cadre d'*oversight* actuel, mais seulement d'en codifier certains aspects afin qu'il puisse servir de filet de sécurité juridique. On peut donc parler d'un *oversight* "renforcé". L'organisation et l'approche pratique actuelles de l'*oversight* de SWIFT demeureraient par contre inchangées. L'interaction consensuelle collaborative entre les autorités de surveillance dans le cadre de l'*oversight* coopératif, tant au niveau technique qu'au niveau supérieur, ne sera donc pas affectée.

Les déposants soutiennent pleinement les intentions des autorités de surveillance de SWIFT et ont donc rédigé la présente proposition de loi, avec le soutien technique de ces autorités de surveillance. On a veillé à ce que la proposition de loi ait une portée générale et à ce qu'elle s'applique potentiellement à tous les fournisseurs d'importance systémique établis en Belgique. À cet égard, les

indieners drukken daarbij de verwachting uit dat het voorliggend wetsvoorstel kan fungeren als blauwdruk voor eventuele toekomstige initiatieven waarbij *oversight*verwachtingen in een juridisch afdwingbaar kader worden ondergebracht.

Krachtlijnen van het wetsvoorstel

Het voorliggend wetsvoorstel is erop gericht de hierboven geschetste doelstellingen met betrekking tot een versterkt *oversight* in de praktijk te brengen, waarbij de krachtlijnen van het wetsvoorstel in een aantal grote blokken kunnen samengebracht worden.

De hoofdstukken 1 en 2 bepalen in essentie dat systeemrelevante aanbieders van financiële berichtendiensten geacht worden de bepalingen van het wetsvoorstel na te leven en dat zij onderworpen zijn aan het *oversight* door de Bank.

De hoofdstukken 3 tot 7 vormen de kern van het wetsvoorstel en bevatten de bedrijfsuitoefeningsvoorwaarden die systeemrelevante aanbieders moeten naleven. De keuze voor de opdeling in deze hoofdstukken verdient enige nadere toelichting.

Zoals hierboven reeds aangegeven, steunt het *oversight* op kritieke dienstverleners, waaronder SWIFT, in de eerste plaats op Annex F van de PFMI. Het is evenwel aangewezen om kritieke dienstverleners, met name wanneer zij van systemisch belang zijn, te onderwerpen aan alle PFMI die voor hen relevant geacht worden. Na grondige reflectie werden de volgende PFMI-principes geïdentificeerd als relevant voor systeemrelevante aanbieders: PFMI-principes 1 (juridische risico's), 2 (governance), 3 (integraal risicobeheerskader), 15 (algemeen bedrijfsrisico), 16 (beleggingsrisico), 17 (operationeel risico), 18 (toegang en deelnemingsvereisten), 22 (communicatieprocedures en normen) en 23 (openbaarmaking van regels, procedures en data). Elk PFMI-principe is verder onderverdeeld in een aantal kernbepalingen, waarvan sommige wel en andere niet overgenomen zijn in het voorliggend wetsvoorstel. Bij de artikelsgewijze bespreking wordt hierna in de mate van het mogelijke aangegeven van welk PFMI-principe en van welke kernbepalingen elk artikel de juridische vertaling vormt. De andere PFMI-principes zijn niet geïntegreerd in het wetsvoorstel om de evidente reden dat zij specifiek betrekking hebben op activiteiten die niet worden uitgeoefend door systeemrelevante aanbieders of op risico's die zich in principe niet of slechts in beperkte mate voordoen bij systeemrelevante aanbieders.

De juridische vertaling van de PFMI is voornamelijk terug te vinden in de hoofdstukken 3 en 7; de hoofdstukken

déposants espèrent que la présente proposition de loi pourra servir de modèle pour toute éventuelle initiative future visant à placer les attentes en matière d'*oversight* dans un cadre juridiquement contraignant.

Lignes de force de la proposition de loi

La présente proposition de loi vise à mettre en œuvre les objectifs décrits ci-dessus en ce qui concerne le renforcement de l'*oversight*, les lignes de force de la proposition de loi pouvant être regroupées en un certain nombre d'éléments majeurs.

Les chapitres 1 et 2 disposent essentiellement que les fournisseurs de services de messagerie financière d'importance systémique sont tenus de se conformer aux dispositions de la proposition de loi et qu'ils sont soumis à l'*oversight* de la Banque.

Les chapitres 3 à 7 constituent le cœur de la proposition de loi et définissent les conditions d'exercice de l'activité que les fournisseurs d'importance systémique doivent respecter. Le choix de cette division en chapitres mérite quelques explications.

Comme indiqué ci-dessus, l'*oversight* des fournisseurs de services critiques, dont SWIFT, repose principalement sur l'annexe F aux PIMF. Il convient toutefois de soumettre les fournisseurs de services critiques, en particulier lorsqu'ils sont d'importance systémique, à tous les PIMF jugés pertinents pour eux. Au terme d'une réflexion approfondie, les principes suivants des PIMF ont été jugés pertinents pour les fournisseurs d'importance systémique: les principes des PIMF 1 (base juridique), 2 (gouvernance), 3 (cadre de gestion intégrée des risques), 15 (risque d'activité), 16 (risque d'investissement), 17 (risque opérationnel), 18 (conditions d'accès et de participation), 22 (procédures et normes de communication) et 23 (communication des règles, procédures clés et données de marché). Chaque principe des PIMF est subdivisé en un certain nombre de dispositions essentielles, dont certaines ont ou non été reprises dans la présente proposition de loi. Le commentaire des articles ci-après précise dans la mesure du possible de quel principe des PIMF et de quelles dispositions essentielles chaque article est la traduction juridique. Les autres principes des PIMF n'ont pas été intégrés à la proposition de loi pour la raison évidente qu'ils se rapportent spécifiquement à des activités qui ne sont pas exercées par des fournisseurs d'importance systémique ou à des risques qui, en principe, ne concernent pas ou à peine les fournisseurs d'importance systémique.

La traduction juridique des PIMF se trouve principalement aux chapitres 3 et 7; les chapitres 4, 5 et 6

4, 5 en 6 bevatten een beperkt aantal bepalingen die weliswaar aansluiten bij de PFMI maar er niet rechtstreeks van afgeleid zijn.

Het is passend om er hier al op te wijzen dat de vertaling van twee PFMI-principes op een veel uitgebreidere wijze is uitgewerkt in het wetsvoorstel dan wat in de PFMI zelf het geval is. PFMI-principe 2 (governance) bevat belangrijke standaarden inzake governance en bestuur van financiële marktinfrastructuren, maar verwijst er in zijn toelichting naar dat de concrete invulling van deze standaarden in belangrijke mate geconditioneerd wordt door de toepasselijke nationale regels. Zie in die zin paragraaf 3.2.4 van de PFMI: "*No single set of governance arrangements is appropriate for all FMIs and all market jurisdictions. Arrangements may differ significantly because of national law, ownership structure, or organisational form*". Er werd dan ook voor geopteerd om de bepalingen van PFMI-principe 2 in detail uit te werken in het wetsvoorstel, naar analogie van de regels die al gelden voor andere instellingen die onder het toezicht van de Bank staan. Ook PFMI-principe 17 (operationeel risico) is in merkelijk meer detail uitgewerkt in het wetsvoorstel. De reden hiervoor is dat de beheersing van het cyberrisico, als onderdeel van het operationeel risico, afgedekt wordt door de richtsnoeren van CPMI en IOSCO inzake cyberweerbaarheid voor financiële marktinfrastructuren (*Guidance on Cyber Resilience for Financial Market Infrastructures*). Er werd voor geopteerd om die richtsnoeren, die een aanvulling vormen op de PFMI, eveneens te integreren in het wetsvoorstel, zij het dat voor de concrete juridische formulering daarvan gesteund werd op de bepalingen van de DORA-verordening (hierover later meer).

De hoofdstukken 8, 9 en 10, tot slot, zorgen voor de juridische afdwingbaarheid van de bepalingen van de voorgaande hoofdstukken. Zij regelen het toezicht door de Bank op systeemrelevante aanbieders en bepalen de maatregelen die kunnen opgelegd worden met het oog op de naleving van die bepalingen.

Bronnen voor de redactie van het wetsvoorstel

De PFMI-principes en hun kernbepalingen nemen de vorm aan van beginselen die een verwachting uitdrukken ten aanzien van financiële marktinfrastructuren, maar die zonder verder wetgevend of regelgevend ingrijpen niet juridisch bindend noch juridisch afdwingbaar zijn (zie in die zin ook paragraaf 1.30 van de PFMI). Zoals hierboven reeds aangegeven, wordt het toezicht of *oversight* op financiële marktinfrastructuren vaak op juridisch niet-bindende wijze uitgeoefend aan de hand

contiennent un nombre limité de dispositions qui, tout en étant cohérentes avec les PIMF, n'en découlent pas directement.

Il convient d'ores et déjà de souligner que la traduction de deux principes des PIMF a été élaborée de manière beaucoup plus complète dans la proposition de loi que dans les PIMF eux-mêmes. Le principe 2 des PIMF (gouvernance) contient des normes importantes en matière de gouvernance et d'administration des infrastructures de marchés financiers, mais le commentaire de ce principe mentionne que la mise en œuvre concrète de ces normes est dans une large mesure conditionnée par les règles nationales applicables. Voir à ce propos la section 3.2.4 des PIMF: "Aucun ensemble unique de dispositions relatives à la gouvernance ne saurait s'appliquer à toutes les IMF et à toutes les juridictions. Les dispositions peuvent différer nettement les unes des autres en fonction du droit national, du régime de propriété ou de la structure organisationnelle.". Il a donc été décidé de détailler les dispositions du principe 2 des PIMF dans la proposition de loi, par analogie avec les règles déjà en vigueur pour les autres établissements supervisés par la Banque. Le principe 17 des PIMF (risque opérationnel) a lui aussi été développé de manière beaucoup plus détaillée dans la proposition de loi. En effet, la maîtrise du cyber-risque, en tant qu'aspect du risque opérationnel, est couverte par les orientations du CPIM et de l'OICV relatives à la cyber-résilience des infrastructures de marchés financiers (*Guidance on Cyber Resilience for Financial Market Infrastructures*). Il a été décidé d'également intégrer ces orientations, qui complètent les PIMF, dans la proposition de loi, en s'appuyant toutefois sur les dispositions du règlement DORA pour leur formulation juridique concrète (plus d'informations à ce sujet suivront).

Enfin, les chapitres 8, 9 et 10 garantissent l'aspect juridiquement contraignant des dispositions énoncées aux chapitres précédents. Ils régissent la surveillance par la Banque des fournisseurs d'importance systémique et définissent les mesures qui peuvent être imposées en vue du respect de ces dispositions.

Sources ayant inspiré l'élaboration de la proposition de loi

Les principes des PIMF et leurs dispositions essentielles prennent la forme de principes qui expriment une attente à l'égard des infrastructures de marchés financiers mais qui, sans autre intervention législative ou réglementaire, ne sont ni juridiquement contraignants ni juridiquement exécutoires (à ce propos, voir également le paragraphe 1.30 des PIMF). Comme indiqué ci-dessus, la surveillance ou l'*oversight* des infrastructures de marchés financiers est souvent exercé de manière

van *moral suasion* en met rechtstreekse verwijzing naar de PFMI zelf.

Een aantal regelgevende teksten hebben onderdelen van de PFMI evenwel omgezet naar een juridisch bindend en afdwingbaar kader. Op Europees vlak dient in de eerste plaats verwezen te worden naar de reeds vermelde SIPS-verordening, die het *oversight* regelt op systeemrelevante betalingssystemen. Deze verordening herneemt op bijna letterlijke wijze de PFMI-principes en hun kernbepalingen, en is dan ook een belangrijke inspiratiebron geweest voor de concrete formulering van de bepalingen van hoofdstuk 7. Voor een beperkt aantal artikels werd ook inspiratie gevonden in Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie en betreffende centrale effectenbewaarinstellingen (hierna: de CSD-verordening), die voor centrale effectenbewaarinstellingen een aantal van de PFMI nader gepreciseerd heeft.

Zoals hierboven al aangegeven, is ervoor geopteerd om een meer concrete invulling te gegeven aan PFMI-principe 17 (operationeel risico) en aan de richtsnoeren van CPMI en IOSCO inzake cyberweerbaarheid voor financiële marktinfrastructuren door relevante bepalingen van Verordening (EU) 2022/2554 van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector (hierna: de DORA-verordening) te hernemen.

Wat de concrete vertaling van PFMI-principe 2 (governance) betreft, heeft vooral de prudentiële regelgeving voor instellingen die onder het toezicht van de Bank staan als model gediend. De wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen (hierna: de bankwet) werd hierbij als uitgangspunt genomen, maar er is telkens nagegaan of andere prudentiële regelgeving op dit punt beter tegemoet komt aan de doelstellingen die worden nagestreefd met het *oversight* op systeemrelevante aanbieders, dan wel geschikter is rekening houdend met het specifiek statuut en de specifieke activiteiten van systeemrelevante aanbieders. Aldus sluit de formulering van sommige artikelen nauwer aan bij gelijkaardige artikelen in de wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld (hierna: de wet van 11 maart 2018) of de wet van 20 juli 2022 op het statuut van en het toezicht op beursvennootschappen (hierna: de wet van 20 juli 2022). In elk geval werd iedere bepaling die als inspiratie heeft gediend aandachtig geanalyseerd en waar nodig aangepast om rekening te houden met het specifiek statuut en de specifieke activiteiten van systeemrelevante aanbieders. De bepalingen van hoofdstuk 2 wijken

juridiquement non contraignante, en recourant à la force de persuasion morale et en se référant directement aux PIMF eux-mêmes.

Un certain nombre de textes réglementaires ont toutefois converti certaines parties des PIMF en un cadre juridiquement contraignant et exécutoire. Au niveau européen, il convient tout d'abord de se référer au règlement SIPS susmentionné, qui régit l'*oversight* des systèmes de paiement d'importance systémique. Ce règlement reprend presque mot pour mot les principes des PIMF et leurs dispositions essentielles, et a donc été une source d'inspiration importante pour la formulation concrète des dispositions du chapitre 7. Pour un nombre limité d'articles, l'inspiration a également été puisée dans le règlement (UE) n° 909/2014 du Parlement européen et du Conseil du 23 juillet 2014 concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres (ci-après, "le règlement CSD"), qui a précisé certains des PIMF pour les dépositaires centraux de titres.

Comme indiqué ci-dessus, il a été choisi de donner une interprétation plus concrète au principe 17 des PIMF (risque opérationnel) et aux orientations du CPIM et de l'OICV relatives à la cyber-résilience des infrastructures de marchés financiers en reprenant des dispositions pertinentes du règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (ci-après, "le règlement DORA").

En ce qui concerne la traduction concrète du principe 2 des PIMF (gouvernance), la réglementation prudentielle applicable aux établissements supervisés par la Banque a principalement servi de modèle. La loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit (ci-après, "la loi bancaire") a servi de point de départ mais, dans chaque cas, il a été examiné si une autre réglementation prudentielle relative à ce point ne répondrait pas mieux aux objectifs poursuivis par l'*oversight* des fournisseurs d'importance systémique, ou ne serait pas plus appropriée compte tenu du statut spécifique et des activités particulières des fournisseurs d'importance systémique. Ainsi, la formulation de certains articles est proche de celle d'articles similaires de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique (ci-après, "la loi du 11 mars 2018") ou de la loi du 20 juillet 2022 relative au statut et au contrôle des sociétés de bourse (ci-après, "la loi du 20 juillet 2022"). En tout état de cause, chaque disposition ayant servi d'inspiration a été soigneusement analysée et, le cas échéant, adaptée pour tenir compte du statut spécifique et des activités particulières des fournisseurs d'importance systémique. Les dispositions du chapitre 2

op belangrijke punten dan ook af van de vereisten die doorgaans gelden voor andere instellingen onder het toezicht van de Bank.

Wat de redactie van de hoofdstukken 8, 9 en 10 betreft, werd eveneens inspiratie gevonden in de wetten die vermeld worden in de voorgaande alinea. De toezichtsbevoegdheden van de Bank en de maatregelen tot afdwinging van de naleving van het wetsvoorstel sluiten dus perfect aan bij wat vandaag de dag reeds geldt ten aanzien van andere instellingen onder het toezicht van de Bank.

Wat tot slot de redactie van hoofdstuk 2 betreft, inzake de kwalificatie van aanbieders als systeemrelevante aanbieders, werd inspiratie gevonden in de wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties.

Waar mogelijk verwijst de hiernavolgende artikelsgewijze bespreking naar de bronnen die als inspiratie gediend hebben voor de redactie van elk van de betrokken artikels.

Klassiek oversight

De Bank kan naast het toezicht op grond van het voorliggend wetsvoorstel ook nog het klassiek *oversight* op grond van *moral suasion* uitoefenen ten aanzien van systeemrelevante aanbieders. De Bank kan immers steeds bijkomende *oversight*verwachtingen uitdrukken ten aanzien van systeemrelevante aanbieders.

Voor alle onderwerpen en domeinen die niet expliciet het voorwerp uitmaken van dit wetsvoorstel gelden de klassieke *oversight*verwachtingen. Die klassieke *oversight*verwachtingen gelden bovendien ook ook voor alles wat te maken heeft met het functioneren en het op consensus gesteunde besluitvormingsproces tussen de Bank en andere autoriteiten waarmee een samenwerkingsregeling is gesloten ter ondersteuning van een coöperatief toezicht, zoals bijvoorbeeld het geval is voor het coöperatief toezicht op SWIFT door de Bank en de andere centrale banken van de G10.

diffèrent donc, sur des points importants, des exigences généralement applicables aux autres établissements supervisés par la Banque.

En ce qui concerne la rédaction des chapitres 8, 9 et 10, l'inspiration a également été puisée dans les lois mentionnées à l'alinéa précédent. Les compétences en matière de surveillance de la Banque et les mesures visant à faire respecter la proposition de loi sont donc parfaitement conformes à celles qui s'appliquent déjà aujourd'hui à d'autres établissements qu'elle supervise.

Enfin, en ce qui concerne le libellé du chapitre 2 relatif à la qualification des fournisseurs en tant que fournisseurs d'importance systémique, l'inspiration a été trouvée dans la loi du 24 mars 2017 relative à la surveillance des processeurs d'opérations de paiement.

Dans la mesure du possible, le commentaire des articles ci-dessous renvoie aux sources qui ont inspiré la rédaction de chacun des articles concernés.

Oversight classique

Outre la surveillance prévue par la présente proposition de loi, la Banque peut également exercer un *oversight* classique des fournisseurs d'importance systémique basé sur la force de persuasion morale. La Banque peut en effet toujours exprimer des attentes supplémentaires en matière d'*oversight* des fournisseurs d'importance systémique.

Les attentes classiques en matière d'*oversight* s'appliquent à tous les sujets et domaines qui ne font pas explicitement l'objet de la présente proposition de loi. En outre, ces attentes classiques en matière d'*oversight* s'appliquent également à tout ce qui a trait au fonctionnement et au processus décisionnel consensuel entre la Banque et les autres autorités avec lesquelles il existe un accord de coopération visant à soutenir la surveillance coopérative, comme c'est par exemple le cas pour la surveillance coopérative de SWIFT par la Banque et les autres banques centrales du G10.

TOELICHTING BIJ DE ARTIKELEN

HOOFDSTUK 1

Doel – definities – toepassingsgebied

Artikel 1

Overeenkomstig artikel 83 van de Grondwet, bepaalt dit artikel dat de wet een door artikel 74 van de Grondwet beoogde aangelegenheid regelt.

Art. 2

Dit artikel preciseert de reikwijdte en het doel van het wetsvoorstel: het regelt de activiteiten van en het toezicht door de Bank op de in België gevestigde systeemrelevante aanbieders van financiële berichtendiensten. Dit toezicht beoogt de bescherming van de goede werking, de soliditeit en de doelmatigheid van de verrekenings-, vereffenings- en betalingssystemen. Er wordt verduidelijkt dat het toezicht ook strekt tot het beschermen van de soliditeit van het financieel stelsel in het algemeen. Het betreft een opdracht die deel uitmaakt van de *oversight*taken die aan de Bank worden toevertrouwd door artikel 8 van haar organieke wet. Het artikel definieert aldus de finaliteit waarvoor de Bank haar bevoegdheden kan uitoefenen ten aanzien van systeemrelevante aanbieders en legt aldus de grenzen van die bevoegdheden vast.

Overeenkomstig artikel 8, § 2 van de organieke wet kan de Bank reglementen vaststellen ter aanvulling van het wetsvoorstel wat technische punten betreft. Deze reglementen hebben een algemeen bindend karakter en hebben uitwerking na goedkeuring door de Koning en bekendmaking in het *Belgisch Staatsblad*. De Bank kan de verwachtingen inzake naleving van de wet evenwel ook verduidelijken aan de hand van mededelingen, richtsnoeren en circulaires die, hoewel ze niet bindend zijn, een belangrijke indicatie geven van hoe de Bank de bepalingen van het wetsvoorstel en hun concrete invulling interpreteert. Zoals hierboven uitgelegd, verhindert dit niet dat de Bank ten aanzien van systeemrelevante aanbieders ook nog het klassiek *oversight* kan uitoefenen op grond van *moral suasion*.

Art. 3

Dit artikel bevat een aantal definities die, waar mogelijk, zijn overgenomen uit bestaande Europese of nationale regelgeving. Het artikel bevat onder meer definities die verband houden met de bestuurlijke organisatie

COMMENTAIRE DES ARTICLES

CHAPITRE 1ER

Objet – définitions – champ d'application

Article 1er

Conformément à l'article 83 de la Constitution, cet article précise que la loi règle une matière visée à l'article 74 de la Constitution.

Art. 2

Cet article précise la portée et l'objet de la proposition de loi: réglementer les activités de la Banque et la surveillance par celle-ci des fournisseurs de services de messagerie financière d'importance systémique établis en Belgique. Cette surveillance a pour objet de protéger le bon fonctionnement, la solidité et l'efficacité des systèmes de compensation, de règlement et de paiement. Il est précisé que la surveillance vise également à protéger la solidité du système financier en général. Cette tâche fait partie des missions d'*oversight* confiées à la Banque par l'article 8 de sa loi organique. L'article définit ainsi la finalité des compétences que la Banque peut exercer à l'égard des fournisseurs d'importance systémique et fixe donc les limites de ces compétences.

Conformément à l'article 8, § 2, de sa loi organique, la Banque peut adopter des règlements visant à compléter la proposition de loi concernant des points techniques. Ces règlements ont un caractère généralement contraignant et sortissent leurs effets après leur approbation par le Roi et leur publication au *Moniteur belge*. Toutefois, la Banque peut également clarifier les attentes en matière de respect de la loi par le biais de communications, de recommandations et de circulaires qui, bien que non contraignants, donnent une indication importante sur la manière dont la Banque interprète les dispositions de la proposition de loi et leur mise en œuvre concrète. Comme expliqué ci-dessus, cela n'empêche pas la Banque d'exercer également un *oversight* classique des fournisseurs d'importance systémique sur la base de la force de persuasion morale.

Art. 3

Cet article contient une série de définitions qui, dans la mesure du possible, sont calquées sur celles de réglementations européennes ou nationales. L'article contient notamment des définitions relatives à l'organisation

van systeemrelevante aanbieders en met hun digitale operationele weerbaarheid. Waar nodig worden die definities hierna nader toegelicht bij de bespreking van de artikelen waarvoor zij relevant zijn.

Art. 4

Dit artikel verduidelijkt dat het wetsvoorstel van toepassing is op aanbieders van financiële berichtendiensten die in België gevestigd zijn. Aanbieders die vanuit een andere lidstaat of een derde land in België financiële berichtendiensten verlenen, vallen dus niet onder het toepassingsgebied van dit wetsvoorstel.

Onder financiële berichtendiensten verstaat men diensten die financiële entiteiten en overheden toelaten om berichten met informatie betreffende financiële transacties, zoals betalings- en effectentransacties, te verzenden en ontvangen (zie artikel 3, 4°). Om alle relevante diensten te capteren, wordt verduidelijkt dat dit ook operationele diensten en nevendiensten betreft die daar nauw mee samenhangen, in het verlengde ervan liggen of er een aanvulling op vormen. Aldus wordt verzekerd dat het *oversight* door de Bank betrekking heeft op alle relevante diensten van systeemrelevante aanbieders van financiële berichtendiensten.

HOOFDSTUK 2

Drempel en kennisgevingsverplichtingen

Art. 5

De bepalingen van dit hoofdstuk zijn geïnspireerd op de artikelen 5, 6 en 7 van de wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties.

Artikel 5 legt de drempel vast die bepalend is voor de kwalificatie van een aanbieder van financiële berichtendiensten als een systeemrelevante aanbieder. De bepaling van deze drempel steunt op een analyse van de activiteiten van aanbieders van financiële berichtendiensten waarbij slechts die aanbieders die systemisch relevant zijn onder het toepassingsgebied van het wetsvoorstel vallen, met name wanneer een aanbieder minstens 1 miljard financiële berichten per jaar heeft verwerkt, gemeten als het gemiddelde over de drie voorgaande kalenderjaren. Dit bedrag is merkelijk lager dan het laatst gerapporteerde aantal verwerkte berichten door SWIFT (11,2 miljard per jaar, als gemiddelde van de

administrative des fournisseurs d'importance systémique et à leur résilience opérationnelle numérique. Le cas échéant, ces définitions sont expliquées plus en détail ci-dessous dans le commentaire des articles auxquels elles se rapportent.

Art. 4

Cet article précise que la proposition de loi s'applique aux fournisseurs de services de messagerie financière établis en Belgique. Les fournisseurs proposant des services de messagerie financière en Belgique depuis un autre État membre ou un pays tiers ne tombent donc pas dans le champ d'application de la présente proposition de loi.

Par services de messagerie financière, on entend les 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 (voir l'article 3, 4°). Afin d'englober tous les services pertinents, il est précisé que les services opérationnels et les services auxiliaires qui y sont étroitement liés, qui se situent dans leur prolongement direct ou qui en constituent le complément sont également concernés. Cela garantit que l'*oversight* exercé par la Banque couvre tous les services pertinents des fournisseurs de services de messagerie financière d'importance systémique.

CHAPITRE 2

Seuil et obligations de notification

Art. 5

Les dispositions du présent chapitre s'inspirent des articles 5, 6 et 7 de la loi du 24 mars 2017 relative à la surveillance des processeurs d'opérations de paiement.

L'article 5 fixe le seuil qui détermine si un fournisseur de services de messagerie financière peut être considéré comme un fournisseur d'importance systémique. La détermination de ce seuil repose sur une analyse des activités des fournisseurs de services de messagerie financière dans le cadre de laquelle seuls les fournisseurs d'importance systémique tombent dans le champ d'application de la proposition de loi, à savoir lorsque ces fournisseurs ont traité au minimum 1 milliard de messages financiers par an, un nombre calculé comme la moyenne des trois années civiles antérieures. Ce nombre est sensiblement inférieur au dernier nombre déclaré de messages traités par SWIFT (11,2 milliards

kalenderjaren 2021 tot 2023) maar voldoende hoog om niet-systeemrelevante aanbieders van het toepassingsgebied van de wet uit te sluiten. Een aanbieder wordt in principe beschouwd als een systeemrelevante aanbieder louter door het overschrijden van de drempel, met dien verstande dat het ogenblik van effectieve toepassing van de bepalingen van hoofdstuk 3 en volgende afhangt van de kennisgeving van de Bank bedoeld in artikel 7. De kwalificatie als systeemrelevante aanbieder met alle daaraan verbonden gevolgen geldt dus pas vanaf het ogenblik waarop de kennisgeving vanwege de Bank uitwerking heeft.

De Koning wordt de bevoegdheid verleend om, op advies van de Bank, het bedrag van de drempel te wijzigen en om nadere regels vast te leggen voor het berekenen van de drempel.

Art. 6

Dit artikel legt aan alle aanbieders van financiële berichtendiensten de verplichting op tot het meedelen van de informatie die de Bank nodig acht om haar toe te laten te oordelen of de in artikel 5 bedoelde drempel overschreden is. De Bank kan haar verwachtingen op dit punt nader preciseren bij reglement, mededeling, richtsnoer or circulaire. Daarnaast is iedere aanbieder ertoe gehouden de Bank in te lichten wanneer hij de in artikel 5 bedoelde drempel overschrijdt.

Art. 7

Dit artikel bepaalt dat de Bank een beslissing dient te nemen over de kwalificatie van een aanbieder van financiële berichtendiensten als een systeemrelevante aanbieder, en haar gemotiveerde beslissing ter kennis moet brengen van de betrokken aanbieder. De Bank kan haar beslissing baseren op de informatie die gerapporteerd werd in toepassing van artikel 6, maar ook op alle andere informatie waarover zij beschikt in de uitoefening van haar taken.

De kennisgeving heeft uitwerking vanaf de datum bepaald door de Bank, die ten vroegste zes maanden na de datum van de kennisgeving ligt. Dit moet de systeemrelevante aanbieder toelaten om zich binnen die termijn te schikken naar de bepalingen van het wetsvoorstel.

Paragraaf 2 bepaalt dat de kwalificatie als systeemrelevante aanbieder van toepassing is tot de systeemrelevante aanbieder niet langer de drempel overschrijdt, de Bank hierover een beslissing heeft genomen en de Bank de aanbieder daarvan in kennis heeft gesteld.

par an en moyenne sur les années civiles 2021 à 2023) mais est suffisamment élevé pour exclure les fournisseurs ne revêtant pas une importance systémique du champ d'application de la loi. Un fournisseur est en principe considéré comme un fournisseur d'importance systémique dès lors qu'il dépasse le seuil, étant entendu que le moment de l'application effective des dispositions des chapitres 3 et suivants est déterminé par la notification de la Banque visée à l'article 7. La qualification en tant que fournisseur d'importance systémique, avec toutes les conséquences que cela implique, ne s'applique donc qu'à partir du moment où la notification de la Banque prend effet.

Sur avis de la Banque, le Roi est habilité à modifier le montant du seuil et à fixer des règles plus précises pour le calcul du seuil.

Art. 6

Cet article impose à tous les fournisseurs de services de messagerie financière l'obligation de communiquer les informations que la Banque juge nécessaires pour lui permettre d'évaluer si le seuil visé à l'article 5 a été dépassé. La Banque peut préciser ses attentes à cet égard par voie de règlement, de communication, de recommandation ou de circulaire. En outre, tout fournisseur est tenu d'informer la Banque en cas de dépassement du seuil visé à l'article 5.

Art. 7

Cet article dispose que la Banque doit prendre une décision sur la qualification d'un fournisseur de services de messagerie financière en tant que fournisseur d'importance systémique et qu'elle doit porter sa décision motivée à la connaissance du fournisseur concerné. La Banque peut fonder sa décision sur toute information déclarée en application de l'article 6, mais aussi sur toute autre information dont elle dispose dans le cadre de l'exercice de ses missions.

La notification prend effet à compter de la date arrêtée par la Banque, au plus tôt six mois après la date de la notification. Ce délai doit permettre au fournisseur d'importance systémique de se conformer aux dispositions de la proposition de loi.

Aux termes du paragraphe 2, la qualification en tant que fournisseur d'importance systémique est d'application jusqu'à ce que celui-ci ne dépasse plus le seuil fixé, que la Banque ait pris une décision à ce sujet et que la Banque l'en ait notifié. La Banque prend cette

De Bank neemt die beslissing op eigen initiatief dan wel op gemotiveerd verzoek van de betrokken systeemrelevante aanbieder.

Art. 8

Dit artikel verplicht de Bank om een openbaar consulteerbaar register bij te houden dat alle systeemrelevante aanbieders oplijst. Dit vereiste wordt ingevoegd om transparantieredenen, met name om ervoor te zorgen dat alle betrokken marktspelers daadwerkelijk kennis hebben van de kwalificatie van de betrokken aanbieder als systeemrelevante aanbieder. De Bank moet dit register regelmatig actualiseren.

HOOFDSTUK 3

Organisatie en bestuur

Dit hoofdstuk geeft een concrete invulling aan PFMI-principe 2 en zijn kernbepalingen. Zoals hierboven reeds aangegeven, is dit principe in aanzienlijk meer detail uitgewerkt dan wat in de PFMI zelf is voorzien. PFMI-principe 2 bepaalt onder meer dat (i) financiële marktinfrastructuren gedocumenteerde bestuurs- en governanceregelingen moeten hebben met duidelijke lijnen van verantwoordelijkheid en rekenschap, (ii) de taken en verantwoordelijkheden van de leiding duidelijk beschreven moeten zijn, (iii) de leden die deel uitmaken van de leiding over de nodige vaardigheden moeten beschikken, (iv) interne controlefuncties onafhankelijk zijn en over voldoende autoriteit en middelen moeten beschikken, en (v) het bestuur instaat voor het bepalen van een duidelijk en gedocumenteerd risicobeheerskader.

Afdeling I

Vennootschapsvorm

Art. 9

Dit artikel bepaalt dat iedere systeemrelevante aanbieder moet opgericht worden in de vorm van een coöperatieve vennootschap of een naamloze vennootschap naar Belgisch recht. Deze vennootschapsvormen zijn het meest geschikt met het oog op de implementatie van de vereisten van het wetsvoorstel op het vlak van organisatie en bestuur.

décision de sa propre initiative ou à la demande motivée du fournisseur d'importance systémique concerné.

Art. 8

Aux termes de cet article, la Banque a l'obligation de tenir un registre public reprenant l'ensemble des fournisseurs d'importance systémique. Cette exigence a été introduite pour des questions de transparence, notamment pour s'assurer que tous les intervenants de marché concernés ont effectivement connaissance de la qualification du fournisseur concerné en tant que fournisseur d'importance systémique. La Banque doit régulièrement mettre ce registre à jour.

CHAPITRE 3

Organisation et administration

Ce chapitre donne une interprétation concrète au principe 2 des PIMF et à ses principales dispositions. Comme indiqué ci-dessus, ce principe a été élaboré de manière beaucoup plus détaillée que dans les PIMF eux-mêmes. Le principe 2 des PIMF dispose, entre autres, que (a) les infrastructures de marchés financiers devraient avoir des dispositions relatives à son administration et à sa gouvernance qui soient documentées et qui définissent des niveaux de responsabilité clairs et directs, (b) les rôles et responsabilités de la direction devraient être clairement énoncés, (c) les membres qui composent la direction devraient disposer des compétences nécessaires, (d) les fonctions de contrôle interne devraient avoir un pouvoir, une indépendance et des ressources suffisants, et (e) l'administration devrait définir un cadre de gestion des risques clair et documenté.

Section Ire

Forme de société

Art. 9

Le présent article dispose que chaque fournisseur d'importance systémique doit être constitué sous la forme d'une société coopérative ou d'une société anonyme de droit belge. Ces formes de société sont les plus appropriées pour mettre en œuvre les exigences de la proposition de loi sur les plans de l'organisation et de l'administration.

Afdeling II

Vennootschapsorganen

Art. 10

Dit artikel bepaalt dat het bestuur van een systeemrelevante aanbieder moet waargenomen worden door een raad van toezicht en een directieraad, ongeacht of de aanbieder is opgericht in de vorm van een naamloze vennootschap dan wel als een coöperatieve vennootschap. De bepalingen die het duaal bestuur bij naamloze vennootschap regelen, zoals bedoeld in afdeling 3 van boek 7, titel 4, hoofdstuk 1, van het Wetboek van Vennootschappen en Verenigingen (WVV), zijn van toepassing; dezelfde bepalingen zijn van overeenkomstige toepassing voor systeemrelevante aanbieders die zijn opgericht in de vorm van een coöperatieve vennootschap.

Er wordt aan herinnerd dat een vennootschap onder een monistisch bestuursmodel bestuurd wordt door één (collegiaal) bestuursorgaan. Het bestuursorgaan heeft in principe alle bevoegdheden die niet aan de algemene vergadering zijn voorbehouden: het bepaalt de algemene strategie van de vennootschap maar is eveneens bevoegd voor het management. Het bestuursorgaan bevat doorgaans dus zowel uitvoerende bestuurders (die het management voor hun rekening nemen) als niet-uitvoerende bestuurders, zonder dat er echter van een (duidelijke of institutionele) scheiding sprake is.

Het duaal bestuursmodel gaat wél uit van een duidelijke, institutionele scheiding tussen uitvoerende en niet-uitvoerende bestuurders. Daartoe dienen twee organen opgericht te worden. Het toezichtorgaan, of de raad van toezicht, is belast met (i) het bepalen van het algemeen beleid en de strategie van de vennootschap, en (ii) het toezicht op het managementorgaan. Het managementorgaan, of de directieraad, voert het algemeen beleid en de strategie uit in de praktijk en legt verantwoording af aan het toezichtorgaan. Het managementorgaan bestaat doorgaans uitsluitend uit uitvoerende bestuurders, terwijl het toezichtorgaan uitsluitend uit niet-uitvoerende bestuurders bestaat.

Het WVV voorziet standaard in een monistisch bestuur voor zowel de naamloze vennootschap als de coöperatieve vennootschap. Artikel 7:104 WVV bepaalt evenwel dat de statuten van een naamloze vennootschap kunnen voorzien dat, in afwijking op het monistisch bestuur, het bestuur wordt waargenomen door enerzijds de raad van toezicht en anderzijds de directieraad.

Krachtens artikel 7:105 WVV is de raad van toezicht steeds een collegiaal orgaan dat minstens drie leden telt. Zij kunnen niet tegelijk ook lid zijn van de directieraad. Er

Section II

Organes sociétaires

Art. 10

Le présent article dispose que l'administration d'un fournisseur d'importance systémique doit être assurée par un conseil de surveillance et un conseil de direction, que le fournisseur soit constitué sous la forme d'une société anonyme ou d'une société coopérative. Les dispositions relatives à l'administration duale des sociétés anonymes, visées à la section 3 du livre 7, titre 4, chapitre 1er, du Code des sociétés et des associations (CSA), sont d'application; ces mêmes dispositions s'appliquent par analogie aux fournisseurs d'importance systémique constitués sous la forme d'une société coopérative.

Il est rappelé qu'une société régie par un modèle d'administration moniste est dirigée par un organe d'administration unique (collégial). L'organe d'administration dispose en principe de tous les pouvoirs qui ne sont pas réservés à l'assemblée générale: il détermine la stratégie globale de la société mais est également responsable de sa gestion. Ainsi, l'organe d'administration se compose généralement à la fois d'administrateurs exécutifs (qui prennent en charge la gestion) et d'administrateurs non exécutifs, sans qu'il n'y ait toutefois de distinction (claire ou institutionnelle) entre les deux groupes.

Le modèle d'administration dual suppose néanmoins une distinction institutionnelle claire entre les administrateurs exécutifs et les administrateurs non exécutifs. À cette fin, deux organes doivent être mis en place. L'organe de surveillance, soit le conseil de surveillance, est chargé (a) de déterminer la politique générale et la stratégie de la société, et (b) de surveiller l'organe de gestion. L'organe de gestion, soit le conseil de direction, met en œuvre la politique globale et la stratégie et rend compte à l'organe de surveillance. L'organe de gestion se compose généralement exclusivement d'administrateurs exécutifs, tandis que l'organe de surveillance se compose uniquement d'administrateurs non exécutifs.

Par défaut, le CSA prévoit une administration moniste tant pour les sociétés anonymes que pour les sociétés coopératives. Toutefois, l'article 7:104 CSA dispose que les statuts d'une société anonyme peuvent prévoir que, par dérogation à l'administration moniste, l'administration est assurée par le conseil de surveillance, d'une part, et le conseil de direction, d'autre part.

En vertu de l'article 7:105 CSA, le conseil de surveillance est toujours un organe collégial qui compte au moins trois membres. Les membres du conseil de

is dus een strikte scheiding. De leden worden aangesteld en ontslagen door de algemene vergadering. De raad van toezicht is bevoegd voor (i) het algemeen beleid van de vennootschap, (ii) de strategie van de vennootschap, (iii) alle handelingen waarvan het WVV bepaalt dat zij aan de raad van bestuur zijn voorbehouden (zoals de samenroeping en voorbereiding van de algemene vergadering en de redactie van de bestuursverslagen), en (iv) het toezicht op de directieraad en het verlenen van kwijting aan de leden van de directieraad. Leden van de raad van toezicht zijn steeds niet-uitvoerende bestuurders.

Krachtens artikel 7:107 WVV is de directieraad steeds een collegiaal orgaan dat minstens drie leden telt. Zij kunnen niet tegelijk ook lid zijn van de raad van toezicht. Zij worden aangesteld en ontslagen door de raad van toezicht. De directieraad oefent alle (residuaire) bestuursbevoegdheden uit die niet aan de raad van toezicht zijn voorbehouden. De directieraad is dus bevoegd voor het operationeel beleid van de vennootschap en de operationele directiefuncties. De bevoegdheden van de directieraad en de raad van toezicht mogen en kunnen elkaar niet overlappen. Leden van de directieraad zijn steeds uitvoerende bestuurders. De directieraad kan het dagelijks bestuur opdragen aan één of meer personen die elk alleen, gezamenlijk of als college optreden. Bestuurders aan wie het dagelijks bestuur is opgedragen, moeten eveneens beschouwd worden als uitvoerend bestuurders. Paragraaf 3 van artikel 10 bepaalt dan ook dat het dagelijks bestuur niet mag worden opgedragen aan leden van de raad van toezicht. Artikel 3, 7°, van het wetsvoorstel, tot slot, definieert de effectieve leiding als de personen die lid zijn van de directieraad en de personen die belast zijn met het dagelijks bestuur; de leden van de raad van toezicht worden dus niet beschouwd als de effectieve leiding in de zin van dit wetsvoorstel.

Artikel 10 maakt de bovenstaande regeling aldus verplicht van toepassing op alle systeemrelevante aanbieders. Het duaal bestuursmodel biedt immers meer mogelijkheden voor extra *checks and balances*, aangepast aan de concrete situatie en rekening houdend met de nadere bepalingen van het wetsvoorstel op dit punt.

De keuze voor een duaal bestuursmodel strookt met de benadering gevolgd in PFMI-principe 2, dat de mogelijkheid van dit bestuursmodel erkent maar het niet verplicht oplegt gelet op de belangrijke verschillen

surveillance ne peuvent être en même temps membres du conseil de direction. Il y a donc une distinction stricte entre les deux. Les membres sont désignés et démis par l'assemblée générale. Le conseil de surveillance est chargé (a) de la politique générale de la société, (b) de la stratégie de la société, (c) de tous les actes qui, selon le CSA, sont réservés au conseil d'administration (tels que la convocation et la préparation de l'assemblée générale et la rédaction des rapports d'administration), et (d) de la surveillance du conseil de direction et du vote de la décharge des membres du conseil de direction. Les membres du conseil de surveillance sont toujours des administrateurs non exécutifs.

En vertu de l'article 7:107 CSA, le conseil de direction est toujours un organe collégial composé d'au moins trois membres. Ceux-ci ne peuvent pas être en même temps membres du conseil de surveillance. Ils sont nommés et révoqués par le conseil de surveillance. Le conseil de direction exerce tous les pouvoirs de gestion (résiduaires) qui ne sont pas réservés au conseil de surveillance. Le conseil de direction est donc compétent pour les politiques opérationnelles de la société et pour les fonctions de direction opérationnelles. Les pouvoirs du conseil de direction et du conseil de surveillance ne doivent ni ne peuvent se chevaucher. Les membres du conseil de direction sont toujours des administrateurs exécutifs. Le conseil de direction peut charger une ou plusieurs personnes, qui agissent chacune individuellement, conjointement ou collégialement, de la gestion journalière. Les administrateurs chargés de la gestion journalière doivent également être considérés comme des administrateurs exécutifs. Le paragraphe 3 de l'article 10 dispose donc que la gestion journalière ne peut être confiée aux membres du conseil de surveillance. Enfin, l'article 3, 7°, de la proposition de loi définit la direction effective comme les personnes qui sont membres du conseil de direction et les personnes auxquelles la gestion journalière est déléguée; les membres du conseil de surveillance ne sont donc pas considérés comme la direction effective au sens de la présente proposition de loi.

L'article 10 rend ainsi les règles précitées obligatoirement applicables à tous les fournisseurs d'importance systémique. En effet, le modèle d'administration duale offre davantage de possibilités de mettre en place des contrepouvoirs ("*checks and balances*") supplémentaires, en fonction de la situation concrète et compte tenu des dispositions plus précises de la proposition de loi sur ce point.

Le choix d'un modèle d'administration duale est cohérent avec l'approche suivie dans le principe 2 des PIMF, qui reconnaît la possibilité de mettre en place ce modèle d'administration mais ne le rend pas obligatoire,

op dit vlak tussen de nationale rechtsstelsels (zie paragraaf 3.2.4 van de PFMI).

Art. 11

Paragraaf 1 van dit artikel bepaalt dat minstens één derde maar niet minder dan drie leden van de raad van toezicht, waaronder in elk geval de voorzitter, onafhankelijke bestuurders moeten zijn. PFMI-principe 2 benadrukt het belang van de vaardigheid van bestuursleden om op onafhankelijke wijze te oordelen en beslissingen te nemen (zie paragraaf 3.2.10 van de PFMI). Waar de nationale toezichtswetten doorgaans niet precies bepalen hoeveel leden van het bestuursorgaan onafhankelijk dienen te zijn, achten de indieners het aangewezen om een meer concreet vereiste op te leggen wat systeemrelevante aanbieders betreft. De minimale aanwezigheid van één derde onafhankelijke bestuurders in de raad van toezicht is geënt op een gelijkaardig vereiste voor centrale effectenbewaarinstellingen (zie artikel 27 van de CSD-verordening).

Paragraaf 2 bevat de criteria waaraan de onafhankelijkheid van de leden van de raad van toezicht getoetst wordt. De punten 1° en 2° betreffen de zogenaamde onafhankelijkheid van geest en vergen dat elke onafhankelijke bestuurder verwacht wordt plichtsbewust, objectief en onafhankelijk te kunnen oordelen in het belang van de systeemrelevante aanbieder en zijn stakeholders, na zorgvuldige afweging van alle beschikbare informatie en meningen en los van allerlei externe invloeden. De Bank kan haar verwachtingen op dit vlak nader verduidelijken, in het bijzonder rekening houdend met bestaande richtlijnen zoals vervat in het handboek inzake de geschiktheidsbeoordeling (hierna: het "*fit & proper*" handboek), zie *https://www.nbb.be/nl/financieel-toezicht/prudentieel-toezicht/handboek-inzake-de-geschiktheidsbeoordeling-fit-proper.*

De punten 3° tot 7° betreffen de zogenaamde formele onafhankelijkheidscriteria. Zij zijn deels ontleend aan de definitie bedoeld in artikel 3, 83°, van de bankwet en waar nodig aangepast om rekening te houden met de specifieke situatie van systeemrelevante aanbieders. Het betreft criteria die op gelijkaardige wijze gelden voor een groot aantal andere financiële instellingen die aan het toezicht van de Bank onderworpen zijn. Deze criteria zijn in hun huidige bewoordingen op hun beurt geïnspireerd op de richtsnoeren van de Europese Bankautoriteit voor het beoordelen van de geschiktheid van leden van het leidinggevend orgaan en medewerkers met een sleutelfunctie (EBA/GL/2021/06 van 2 juli 2021). Ook hier kan de Bank haar verwachtingen nader verduidelijken, in het

compte tenu des différences importantes qui existent à cet égard entre les systèmes juridiques nationaux (cf. paragraphe 3.2.4 des PIMF).

Art. 11

Le paragraphe 1er de cet article dispose qu'au moins un tiers mais pas moins de trois des membres du conseil de surveillance, y compris au moins le président, doivent être des administrateurs indépendants. Le principe 2 des PIMF souligne l'importance de la capacité des administrateurs d'exercer un jugement et de prendre des décisions de manière indépendante (cf. paragraphe 3.2.10 des PIMF). Si les lois nationales de contrôle ne précisent généralement pas combien de membres de l'organe d'administration doivent être indépendants, les déposants considèrent qu'il s'indique d'imposer une exigence plus concrète en ce qui concerne les fournisseurs d'importance systémique. La présence minimale d'un tiers d'administrateurs indépendants au sein du conseil de surveillance s'inspire d'une exigence similaire imposée aux dépositaires centraux de titres (cf. article 27 du règlement CSD).

Le paragraphe 2 énumère les critères permettant d'évaluer l'indépendance des membres du conseil de surveillance. Les points 1° et 2° concernent ce que l'on appelle l'indépendance d'esprit et requièrent que tout administrateur indépendant puisse décider en conscience, en toute objectivité et de manière indépendante, dans l'intérêt du fournisseur d'importance systémique et de ses parties prenantes, après avoir soigneusement soupesé toutes les informations et opinions disponibles, et indépendamment de toute influence extérieure. La Banque peut préciser ses attentes en la matière, notamment compte tenu des directives existantes énoncées dans le manuel relatif à l'évaluation de l'aptitude (ci-après: le manuel "*fit & proper*"), cf. *https://www.nbb.be/fr/supervision-financiere/controle-prudentiel/manuel-relatif-levaluation-de-laptitude-fit-proper.*

Les points 3° à 7° concernent les critères dits d'indépendance formelle. Ils sont en partie empruntés à la définition visée à l'article 3, 83°, de la loi bancaire et adaptés, le cas échéant, pour tenir compte de la situation spécifique des fournisseurs d'importance systémique. Ces critères s'appliquent de manière similaire à un grand nombre d'autres établissements financiers soumis au contrôle de la Banque. La formulation actuelle de ces critères s'inspire à son tour des orientations de l'Autorité bancaire européenne en matière d'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés (EBA/GL/2021/06 du 2 juillet 2021). Ici aussi, la Banque peut préciser ses attentes, notamment compte tenu de ces orientations. Ainsi, les

bijzonder rekening houdend met die richtsnoeren. Aldus mogen onafhankelijke leden van de raad van toezicht:

1° gedurende vijf jaar voorafgaand aan de benoeming, bij de systeemrelevante aanbieder geen mandaat hebben uitgeoefend van persoon belast met de effectieve leiding, en bij een verbonden vennootschap of persoon geen mandaat hebben uitgeoefend van lid van het bestuursorgaan, noch belast geweest zijn met de effectieve leiding;

2° gedurende een tijdvak van drie jaar voorafgaand aan de benoeming, geen deel hebben uitgemaakt van het personeel van de systeemrelevante aanbieder;

3° met de systeemrelevante aanbieder of met een verbonden vennootschap geen significante zakelijke relatie hebben of gehad hebben gedurende een tijdvak van een jaar voorafgaand aan de benoeming;

4° gedurende een tijdvak van drie jaar voorafgaand aan de benoeming, geen vennoot of lid van het auditteam geweest zijn van de huidige of vorige revisor van de systeemrelevante aanbieder of van een verbonden vennootschap;

5° geen echtgenoot, wettelijk samenwonende partner of bloed- of aanverwanten tot de tweede graad hebben die bij de systeemrelevante aanbieder of een verbonden vennootschap een mandaat uitoefent van lid van het bestuursorgaan, belast is met de effectieve leiding of deel uitmaakt van het leidinggevend personeel, of die zich in één van de andere in de punten 1° tot 4° beschreven gevallen bevinden.

Paragraaf 4 bepaalt dat een systeemrelevante aanbieder kan afwijken van de criteria bedoeld in paragraaf 2, mits hiervoor een terdege onderbouwde rechtvaardiging wordt verstrekt en op voorwaarde dat de Bank niet anders oordeelt. Het betreft een mogelijkheid die bijv. ook geldt bij de beoordeling van de onafhankelijkheid van bestuurders bij kredietinstellingen (zie artikel 3, 83°, laatste alinea, van de bankwet). Niet-naleving van één van de onafhankelijkheidscriteria heeft dus niet automatisch tot gevolg dat de betrokkene niet langer als onafhankelijk kan worden beschouwd. De aanbieder heeft immers de mogelijkheid om tegenover de Bank aan te tonen dat, hoewel niet alle criteria vervuld zijn, de onafhankelijkheid van de betrokkene niet in het gedrang komt (toepassing van het "*comply or explain*"-beginsel).

Paragraaf 3 bepaalt verder dat onafhankelijke leden van de raad van toezicht geen deel mogen uitmaken van het personeel van een systeemrelevante aanbieder, maar dat zij wel deel mogen uitmaken van het personeel van een verbonden vennootschap, mits de systeemrelevante

membres indépendants du conseil de surveillance ne peuvent pas:

1° durant les cinq années précédant leur nomination, avoir exercé auprès du fournisseur d'importance systémique un mandat de personne chargée de la direction effective, ni avoir exercé auprès d'une société ou personne liée un mandat de membre de l'organe d'administration ou un mandat de personne chargée de la direction effective;

2° durant une période de trois années précédant leur nomination, avoir fait partie du personnel du fournisseur d'importance systémique;

3° entretenir, ni avoir entretenu durant une période d'un an précédant leur nomination, une relation d'affaires significative avec le fournisseur d'importance systémique ou avec une société liée;

4° durant une période de trois années précédant leur nomination, avoir été associés ou membres de l'équipe d'audit du commissaire, actuel ou précédent, du fournisseur d'importance systémique ou d'une société liée;

5° avoir au sein du fournisseur d'importance systémique ou au sein d'une société liée un conjoint, un cohabitant légal, un parent ou allié jusqu'au deuxième degré exerçant un mandat de membre de l'organe d'administration ou de personne chargée de la direction effective, ou faisant partie du personnel de direction, ou se trouvant dans un des autres cas définis aux points 1° à 4°.

Le paragraphe 4 dispose que, moyennant justification dûment motivée et sous réserve d'une appréciation contraire de la Banque, un fournisseur d'importance systémique peut déroger aux critères visés au paragraphe 2. Cette possibilité existe par exemple également pour l'évaluation de l'indépendance des administrateurs des établissements de crédit (cf. article 3, 83°, dernier alinéa, de la loi bancaire). Le non-respect de l'un des critères d'indépendance n'implique donc pas automatiquement que l'intéressé ne puisse plus être considéré comme indépendant. En effet, le fournisseur a la possibilité de démontrer à la Banque que, même si tous les critères ne sont pas remplis, l'indépendance de l'intéressé n'est pas compromise (application du principe dit "*comply or explain*").

Le paragraphe 3 dispose en outre que les membres indépendants du conseil de surveillance ne peuvent pas faire partie du personnel d'un fournisseur d'importance systémique, mais qu'ils peuvent faire partie du personnel d'une société liée, à condition que le fournisseur

aanbieder afdoende garanties kan bieden dat de onafhankelijke uitoefening van het bestuursmandaat hierdoor niet in het gedrang komt. Die onafhankelijkheid wordt geacht niet in het gedrang te komen wanneer de betrokkene of diens directe verantwoordelijke bij de verbonden vennootschap niet betrokken is bij strategische beslissingen inzake de systeemrelevante aanbieder, de betrokkene geen commerciële functie uitoefent bij de verbonden vennootschap of de systeemrelevante aanbieder enige andere, gefundeerde garantie kan bieden die de Bank gunstig beoordeelt. Het betreft een specifieke regeling voor onafhankelijke bestuurders bij systeemrelevante aanbieders, teneinde te verzekeren dat een voldoende aantal personen met een geschikt profiel, die in de praktijk deel kunnen uitmaken van het personeel van een verbonden vennootschap, in aanmerking komen om als onafhankelijke bestuurder benoemd te worden.

Bij het voorgaande dient opgemerkt te worden dat de definitie van “verbonden vennootschap”, zoals bedoeld in artikel 3, 9°, verwijst naar de betekenis die aan dit begrip toekomt volgens artikel 1:20 WVV. Het betreft aldus de vennootschappen waarover een systeemrelevante aanbieder een controlebevoegdheid uitoefent, de vennootschappen die een controlebevoegdheid over de aanbieder uitoefenen, de vennootschappen waarmee de aanbieder een consortium vormt (in de zin van artikel 1:19 WVV), en de andere vennootschappen die, bij weten van de raad van toezicht van de aanbieder, onder de controle staan van de voornoemde vennootschappen.

Paragraaf 5 vergt geen nadere toelichting.

Art. 12

Dit artikel bepaalt dat leden van de raad van toezicht hun mandaat in totaal (en dus niet noodzakelijk gedurende één onafgebroken periode) maximaal gedurende twaalf jaar mogen uitoefenen. Dit vereiste is gebaseerd op de Belgische Corporate Governance Code 2020, en is bijvoorbeeld ook terug te vinden in artikel 3, 83°, b), van de bankwet. De statuten kunnen strengere termijnen voorzien.

Afdeling III

Oprichting van comités

Art. 13

Paragraaf 1 van dit artikel bepaalt dat systeemrelevante aanbieders binnen hun raad van toezicht minstens drie comités moeten oprichten: een auditcomité, een

d’importance systémique puisse fournir des garanties suffisantes que cela ne compromet pas l’exercice indépendant du mandat d’administrateur. Cette indépendance est réputée non compromise lorsque ni la personne concernée, ni son supérieur direct au sein de la société liée ne sont impliqués dans les décisions stratégiques relatives au fournisseur d’importance systémique, lorsque la personne concernée n’exerce pas de fonction commerciale au sein de la société liée, ou lorsque que le fournisseur d’importance systémique peut offrir toute autre garantie fondée et jugée favorablement par la Banque. Ces règles spécifiques applicables aux administrateurs indépendants des fournisseurs d’importance systémique ont pour objet de garantir qu’un nombre suffisant de personnes ayant un profil approprié, pouvant en pratique faire partie du personnel d’une société liée, entrent en ligne de compte pour être désignées administrateurs indépendants.

En ce qui concerne ce qui précède, il convient de noter que la définition de “société liée”, telle que visée dans l’article 3, 9°, renvoie au sens attribué à ce terme dans l’article 1:20 CSA. Il s’agit donc des sociétés qu’un fournisseur d’importance systémique contrôle, des sociétés qui contrôlent le fournisseur, des sociétés avec lesquelles le fournisseur forme un consortium (au sens de l’article 1:19 CSA), et des autres sociétés qui, à la connaissance du conseil de surveillance du fournisseur, sont contrôlées par les sociétés susvisées.

Le paragraphe 5 n’appelle pas de commentaires.

Art. 12

Cet article dispose que les membres du conseil de surveillance peuvent exercer leur mandat pour une durée maximale de douze ans au total (et donc pas nécessairement durant une période ininterrompue). Cette exigence se fonde sur le Code belge de gouvernance d’entreprise 2020 et figure également, par exemple, à l’article 3, 83°, b), de la loi bancaire. Les statuts peuvent prévoir des délais plus stricts.

Section III

Mise en place de comités

Art. 13

Le paragraphe 1er de cet article prévoit que les fournisseurs d’importance systémique doivent constituer au moins trois comités au sein de leur conseil de surveillance:

risicocomité en een bestuurs- en benoemingscomité. PFMI-principe 2 stelt wat dat betreft dat bestuursregelingen en een goede werking van het bestuursorgaan hand in hand gaan met de oprichting van (advies)comités (zie paragraaf 3.2.9 van de PFMI). Waar het WVV enkel voorziet in de verplichte oprichting van een audit-, remuneratie- en benoemingscomité voor genoteerde vennootschappen, voorziet de bankwet daarenboven in de verplichte oprichting door kredietinstellingen van een risicocomité. De indieners oordelen dat systeemrelevante aanbieders minstens een auditcomité en een risicocomité dienen op te richten, evenals een bestuurs- en benoemingscomité. Rekening houdend met de bestaande praktijk in de Belgische financiële sector, worden bestuurs- en benoemingscomité samengebracht in één enkel comité aangezien de opdrachten in verband met bestuur en benoeming nauw bij elkaar aansluiten. Deze comités zijn belast met het voorbereiden van de beslissingen van de raad van toezicht in hun respectieve domeinen. Nadere toelichting bij de taken van deze comités volgt hierna.

In lijn met de strikte scheiding, onder het duaal bestuursmodel, tussen de raad van toezicht en de directieraad, bepaalt het artikel dat deze comités uitsluitend mogen samengesteld zijn uit leden van de raad van toezicht. Om voldoende onafhankelijkheid te verzekeren, mag eenzelfde lid van de raad van toezicht bovendien hoogstens in twee van deze comités zetelen.

Paragraaf 2 van het artikel bepaalt dat de voorzitter van ieder comité onafhankelijk moet zijn en slechts van één enkel comité de voorzitter mag zijn. Ieder comité wordt dus voorgezeten door een ander lid van de raad van toezicht. Paragraaf 3 verduidelijkt dat de onafhankelijkheid van de voorzitter wordt beoordeeld in het licht van dezelfde criteria die gelden voor de onafhankelijke leden van de raad van toezicht. De regeling voor de voorzitters van de comités verschilt evenwel op twee punten.

Ten eerste kunnen systeemrelevante aanbieders niet afwijken van de criteria bedoeld in artikel 11, § 2. Het bepaalde in artikel 11, § 4, waarbij systeemrelevante aanbieders kunnen afwijken van de onafhankelijkheidscriteria op basis van het *comply or explain*-beginsel, is niet van toepassing. De onafhankelijkheidscriteria voor de voorzitters van comités dienen strikt toegepast te worden.

Ten tweede is het bepaalde in artikel 11, § 3, evenmin van toepassing. Paragraaf 4 van artikel 13 bepaalt immers dat de voorzitter van een comité onder geen beding deel mag uitmaken van het personeel van de systeemrelevante aanbieder, noch van een vennootschap waarmee de systeemrelevante aanbieder een deelnemingsverhouding

un comité d'audit, un comité des risques et un comité de gouvernance et de nomination. À cet égard, le principe 2 des PIMF indique que les dispositions relatives à la gouvernance et le bon fonctionnement de l'organe d'administration vont de pair avec l'établissement de comités (consultatifs) (cf. paragraphe 3.2.9 des PIMF). Si le CSA prévoit uniquement l'obligation de constituer un comité d'audit, de rémunération et de nomination pour les sociétés cotées, la loi bancaire impose en outre la création d'un comité des risques par les établissements de crédit. Les déposants estiment que les fournisseurs d'importance systémique doivent mettre en place au moins un comité d'audit et un comité des risques, ainsi qu'un comité de gouvernance et de nomination. Eu égard à la pratique en place dans le secteur financier belge, les comités de gouvernance et de nomination sont réunis en un seul comité, étant donné la proximité des missions liées à la gouvernance et à la nomination. Ces comités sont chargés de préparer les décisions du conseil de surveillance dans leurs matières respectives. Les missions de ces comités sont précisées ci-après.

Conformément à la stricte séparation du conseil de surveillance et du conseil de direction dans le modèle d'administration duale, l'article dispose que ces comités peuvent exclusivement être composés de membres du conseil de surveillance. En outre, afin de garantir une indépendance suffisante, un même membre du conseil de surveillance ne peut pas siéger dans plus de deux de ces comités.

Le paragraphe 2 de l'article dispose que le président de chaque comité doit être indépendant et ne peut être le président que d'un seul comité. Chaque comité est donc présidé par un membre différent du conseil de surveillance. Le paragraphe 3 précise que l'indépendance du président est évaluée à l'aune des mêmes critères que ceux qui s'appliquent aux membres indépendants du conseil de surveillance. Cependant, les règles prévues pour les présidents des comités diffèrent à deux égards.

Premièrement, les fournisseurs d'importance systémique ne peuvent déroger aux critères visés à l'article 11, § 2. Les dispositions de l'article 11, § 4, qui permettent aux fournisseurs d'importance systémique de déroger aux critères d'indépendance en vertu du principe "comply or explain", ne s'appliquent pas. Les critères d'indépendance doivent être strictement appliqués pour les présidents des comités.

Deuxièmement, les dispositions de l'article 11, § 3, ne s'appliquent pas non plus. En effet, le paragraphe 4 de l'article 13 dispose que le président d'un comité ne peut en aucun cas faire partie du personnel du fournisseur d'importance systémique ou d'une société avec laquelle le fournisseur d'importance systémique a un

heeft in de zin van artikel 1:23 WVV. Het betreft (a) vennootschappen waarin de systeemrelevante aanbieder of zijn dochters een deelneming aanhouden, (b) vennootschappen die rechtstreeks of via hun dochters een deelneming aanhouden in het kapitaal van de systeemrelevante aanbieder, en (c) vennootschappen die, bij weten van de raad van toezicht van de systeemrelevante aanbieder, dochters zijn van de vennootschappen bedoeld in (b). Ook hier dienen de onafhankelijkheidscriteria dus strikt toegepast te worden. Immers, wanneer een systeemrelevante aanbieder is opgericht in de vorm van een coöperatieve vennootschap zijn de dienstafnemers van die aanbieder tevens ook coöperanten of aandeelhouders van die aanbieder. Zonder een strikte toepassing van de onafhankelijkheidscriteria zouden de voorzitters van de comités gewoon personeelsleden van de coöperanten of aandeelhouders kunnen zijn, wat niet wenselijk wordt geacht met het oog op de onafhankelijke werking van de comités.

Paragraaf 5 vergt geen nadere toelichting.

Art. 14

Dit artikel bevat nadere bepalingen inzake de werking van het auditcomité.

De raad van toezicht benoemt de voorzitter van het auditcomité, op aanbeveling van het bestuurs- en benoemingscomité.

Naar analogie van artikel 28, § 1, van de bankwet dienen de leden van het auditcomité te beschikken over een collectieve deskundigheid wat de activiteiten van de systeemrelevante aanbieder betreft; minstens één lid is deskundig op het gebied van boekhouding en audit. De deskundigheid voor de uitoefening van deze functie worden beoordeeld in het licht van de kennis, vaardigheden ("*skills*") en ervaring die nodig zijn voor de uitoefening van deze functie.

Het auditcomité oefent minstens de in artikel 7:99, § 4 WVV bepaalde taken uit. Het betreft onder meer het in kennis stellen van de raad van toezicht van het resultaat van de controle op de jaarrekening, het monitoren van het financiële verslaggevingsproces en het monitoren van de doeltreffendheid van de systemen voor interne controle en risicobeheer. Het auditcomité dient geregeld verslag uit de brengen bij de raad van toezicht over de uitoefening van zijn taken.

lien de participation au sens de l'article 1:23 CSA. Il s'agit (a) des sociétés dans lesquelles le fournisseur d'importance systémique ou ses filiales détiennent une participation; (b) des sociétés qui détiennent directement ou par le biais de leurs filiales une participation dans le capital du fournisseur d'importance systémique; et (c) des sociétés qui, à la connaissance du conseil de surveillance du fournisseur d'importance systémique, sont filiales des sociétés visées en (b). Ici aussi, les critères d'indépendance doivent donc être strictement appliqués. En effet, lorsqu'un fournisseur d'importance systémique est établi sous la forme d'une société coopérative, les acheteurs de services de ce fournisseur sont également coopérateurs ou actionnaires de ce fournisseur. Faute d'application stricte des critères d'indépendance, les présidents des comités pourraient simplement être des membres du personnel des coopérateurs ou des actionnaires, ce qui n'est pas jugé souhaitable aux fins du fonctionnement indépendant des comités.

Le paragraphe 5 n'appelle pas de commentaires.

Art. 14

Cet article contient des dispositions plus précises sur le fonctionnement du comité d'audit.

Le conseil de surveillance désigne le président du comité d'audit, sur recommandation du comité de gouvernance et de nomination.

Par analogie avec l'article 28, § 1er, de la loi bancaire, les membres du comité d'audit doivent disposer d'une compétence collective en ce qui concerne les activités du fournisseur d'importance systémique; au moins un membre est compétent en matière de comptabilité et d'audit. L'expertise requise pour exercer cette fonction est évaluée à la lumière des connaissances, des compétences ("*skills*") et de l'expérience nécessaires à l'exercice de cette fonction.

Le comité d'audit exerce au moins les missions prévues par l'article 7:99, § 4 CSA. Il s'agit notamment de communiquer au conseil de surveillance les résultats du contrôle des comptes annuels, de suivre le processus d'élaboration de l'information financière et de suivre l'efficacité des systèmes de contrôle interne et de gestion des risques. Le comité d'audit doit régulièrement faire rapport au conseil de surveillance sur l'exercice de ses missions.

Art. 15

Dit artikel bevat nadere bepalingen inzake de werking van het risicocomité.

De raad van toezicht benoemt de voorzitter van het risicocomité, op aanbeveling van het bestuurs- en benoemingscomité.

Naar analogie van artikel 29, § 1, van de bankwet dienen de leden van het risicocomité individueel de kennis, deskundigheid, ervaring en vaardigheden te bezitten die nodig zijn om de strategie en de risicotolerantie van de systeemrelevante aanbieder te begrijpen. Het is immers van essentieel belang dat ieder afzonderlijk lid van het risicocomité beschikt over een perfect inzicht in de relevante materies, die soms uitermate complex kunnen zijn. Deze vereiste leidt niet tot de uitsluiting van bepaalde opleidingen maar betekent dat de leden over de nodige professionele of academische bagage moeten beschikken om de onderwerpen die door het genoemde comité worden behandeld, met een kritische geest te kunnen benaderen. Het is met kennis van zaken dat de raad van toezicht dan de risico- en risicotolerantiestrategie van de aanbieder zal kunnen bepalen, en nauwgezet toezicht zal kunnen uitoefenen op de tenuitvoerlegging en naleving ervan door de effectieve leiding van de aanbieder.

Om zijn taken naar behoren te kunnen uitoefenen, bepaalt het risicocomité de aard, omvang, vorm en frequentie van de informatie over de risico's die aan het comité moet worden overgemaakt. Het comité heeft daarenboven rechtstreeks toegang tot de operationele onafhankelijke risicobeheerfunctie van de systeemrelevante aanbieder en tot het advies van externe deskundigen.

Art. 16

Dit artikel bevat nadere bepalingen inzake de werking van het bestuurs- en benoemingscomité. De vereisten inzake dit comité zijn geïnspireerd op de bepalingen van artikel 31 van de bankwet maar zij worden aangevuld met een aantal specifieke vereisten inzake bestuur en governance, zoals die in de praktijk reeds toegepast worden bij bepaalde aanbieders van financiële berichtendiensten. De indieners achten het immers wenselijk om die aanvullende vereisten van toepassing te verklaren op alle systeemrelevante aanbieders.

De raad van toezicht benoemt de voorzitter van het bestuurs- en benoemingscomité, op aanbeveling van dat comité.

Art. 15

Cet article contient des dispositions plus précises sur le fonctionnement du comité des risques.

Le conseil de surveillance désigne le président du comité des risques, sur recommandation du comité de gouvernance et de nomination.

Par analogie avec l'article 29, § 1er, de la loi bancaire, les membres du comité des risques doivent disposer individuellement des connaissances, des compétences, de l'expérience et des aptitudes nécessaires pour leur permettre de comprendre la stratégie et le niveau de tolérance au risque du fournisseur d'importance systémique. Il s'impose en effet que chacun des membres du comité des risques dispose individuellement d'une parfaite compréhension des matières pertinentes qui peuvent s'avérer particulièrement complexes. Cette exigence ne conduit pas à une exclusivité en termes de formation mais signifie que les membres doivent disposer du bagage professionnel ou académique leur permettant d'exercer un esprit critique adéquat eu égard aux matières traitées par ledit comité. C'est en connaissance de cause que le conseil de surveillance pourra alors fixer la stratégie en matière de risque et le niveau de tolérance au risque du fournisseur, et en superviser étroitement la mise en œuvre et le respect par la direction effective du fournisseur.

Afin d'exercer correctement ses missions, le comité des risques détermine la nature, le volume, la forme et la fréquence des informations concernant les risques à lui transmettre. Il dispose en outre d'un accès direct à la fonction de gestion des risques indépendante opérationnelle du fournisseur d'importance systémique et aux conseils d'experts extérieurs.

Art. 16

Cet article contient des dispositions plus précises sur le fonctionnement du comité de gouvernance et de nomination. Les exigences liées à ce comité s'inspirent des dispositions de l'article 31 de la loi bancaire, mais elles sont complétées par des exigences spécifiques en matière d'administration et de gouvernance, telles qu'elles sont déjà appliquées dans la pratique par certains fournisseurs de services de messagerie financière. Les déposants considèrent en effet qu'il est souhaitable de rendre ces exigences supplémentaires applicables à tous les fournisseurs d'importance systémique.

Le conseil de surveillance désigne le président du comité de gouvernance et de nomination, sur recommandation de ce comité.

Het bestuurs- en benoemingscomité moet zodanig samengesteld zijn 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. Afhankelijk van de ontwikkeling van de aanbieder en zijn omgeving, dient het bestuurs- en benoemingscomité de noden van de raad van toezicht te identificeren en het passende profiel te bepalen dat moet worden gezocht om daaraan tegemoet te komen.

Het bestuurs- en benoemingscomité is belast met dezelfde taken als degene waarmee het benoemingscomité bij kredietinstellingen belast is op grond van artikel 31, § 2, van de bankwet. Daarnaast moet dit comité zorgen voor het ontwikkelen van statuten, bedrijfsregels en gedragscodes, het voorbereiden en toetsen van procedures met betrekking tot belangenconflicten, het promoten van een cultuur van permanente opleiding van de leden van de raad van toezicht, het identificeren van hiaten in de bestuursprocessen en het voorstellen van veranderingen op basis van best practices.

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. Het comité kan gebruikmaken van alle vormen van hulpmiddelen die het geschikt acht voor de uitvoering van zijn opdracht.

Art. 17

Overeenkomstig dit artikel kan de Bank reglementen vaststellen tot nadere precisering en aanvulling van de bepalingen inzake het auditcomité, het risicocomité en het bestuurs- en benoemingscomité.

Afdeling IV

Operationele onafhankelijke controlefuncties

Art. 18

Kernbepaling 6 van PFMI-principe 2 bepaalt onder meer dat de bestuursregelingen van een financiële marktinfrastructuur interne controlefuncties moeten voorzien. De regelgeving die van toepassing is op financiële

Le comité de gouvernance et de nomination doit être composé de manière à lui permettre d'exercer un jugement pertinent et indépendant sur la gouvernance d'entreprise et sur 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. En fonction de l'évolution du fournisseur et de son environnement, le comité de gouvernance et de nomination doit identifier les besoins du conseil de surveillance et définir le profil adéquat recherché pour y répondre.

Le comité de gouvernance et de nomination est chargé des mêmes missions que celles confiées au comité de nomination des établissements de crédit en vertu de l'article 31, § 2, de la loi bancaire. Il doit en outre élaborer les statuts, les règles d'entreprise et les codes de conduite, préparer et examiner les procédures relatives aux conflits d'intérêts, promouvoir une culture de formation continue des membres du conseil de surveillance, identifier les lacunes dans les processus de gouvernance et proposer des changements basés sur les meilleures pratiques.

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. Le comité peut recourir à tout type de ressource qu'il considère comme étant appropriée à l'exercice de sa mission.

Art. 17

Conformément à cet article, la Banque peut adopter des règlements qui précisent et complètent les dispositions relatives au comité d'audit, au comité des risques et au comité de gouvernance et de nomination.

Section IV

Fonctions de contrôle indépendantes opérationnelles

Art. 18

La considération essentielle 6 du principe 2 des PIMF indique, entre autres, que les dispositions relatives à la gouvernance d'une infrastructure de marché financier doivent prévoir des fonctions de contrôle interne. La

instellingen onder het toezicht van de Bank schrijft eveneens vaak voor dat deze instellingen bepaalde interne controlefuncties moeten organiseren. Aldus moeten kredietinstellingen, verzekeringsondernemingen, beursvennootschappen en betalingsinstellingen de volgende onafhankelijke controlefuncties organiseren: *compliance*, risicobeheer en interne audit. Het wordt wenselijk geacht om, naar analogie van artikel 35 van de bankwet, een gelijkaardige verplichting op te leggen aan systeemrelevante aanbieders. Het is immers nodig dat het toezicht dat de systeemrelevante aanbieder op zichzelf uitoefent onder meer op de drie voornoemde onafhankelijke controlefuncties kan steunen.

Artikel 18 bepaalt dat de voornoemde drie functies onafhankelijk moeten zijn, wat minstens tot uiting moet komen in het statuut van de betrokken functie bij de aanbieder (hiërarchische en organisatorische scheiding), de prerogatieven van deze functie (middelen en toegang binnen de aanbieder) en de regeling voor de beloning van de verantwoordelijke voor deze functie en van het personeel dat voor de uitoefening ervan beschikbaar is gesteld (waarbij met andere dan commerciële doeleinden rekening wordt gehouden en die noodzakelijkerwijs losstaat van de resultaten van de werkzaamheden waarop toezicht wordt gehouden). Gezien het belang van de onafhankelijke controlefuncties voor de goede werking van de systeemrelevante aanbieder, worden de verantwoordelijken voor deze functies beschouwd als sleutelpersonen die moeten voldoen aan de voorwaarden inzake professionele betrouwbaarheid en deskundigheid die opgenomen zijn in artikel 25.

Art. 19

De compliancefunctie is verantwoordelijk voor het toezicht op de naleving van de wettelijke en/of reglementaire regels inzake integriteit en gedrag voor systeemrelevante aanbieders. De compliancefunctie moet aldus beletten dat de systeemrelevante aanbieder de gevolgen moet dragen — met name een verlies van reputatie of geloofwaardigheid dat een ernstig financieel nadeel kan berokkenen — van de niet-naleving van de wettelijke en reglementaire bepalingen of van de deontologische bepalingen die in voorkomend geval gelden voor het aanbieden van financiële berichtendiensten (*compliancerisico*).

Naar analogie van artikel 36 van de bankwet bepaalt paragraaf 2 dat de personen die belast zijn met de compliancefunctie minstens jaarlijks verslag uitbrengen aan de raad van toezicht, die op zijn beurt verslag uitbrengt aan de Bank.

réglementation applicable aux établissements financiers soumis au contrôle de la Banque impose également souvent à ces établissements d'organiser certaines fonctions de contrôle interne. Ainsi, les établissements de crédit, les entreprises d'assurance, les sociétés de bourse et les établissements de paiement doivent organiser les fonctions de contrôle indépendantes suivantes: conformité ("*compliance*"), gestion des risques et audit interne. Par analogie avec l'article 35 de la loi bancaire, il est jugé souhaitable d'imposer une obligation similaire aux fournisseurs d'importance systémique. Il est en effet nécessaire que le contrôle du fournisseur d'importance systémique par lui-même puisse, notamment, s'appuyer sur les trois fonctions de contrôle indépendantes précitées.

L'article 18 précise la nécessaire indépendance des trois fonctions précitées, qui doit à tout le moins se matérialiser dans le statut de la fonction concernée au sein du fournisseur (séparation hiérarchique et organisationnelle), dans les prérogatives qui lui sont attribuées (moyens et accès au sein du fournisseur) et dans les modalités de rémunération de son responsable et du personnel qui est affecté à son exercice (répondant à des objectifs autres que commerciaux et déterminées, nécessairement, de manière indépendante des performances relatives aux domaines d'activité contrôlés). Compte tenu de l'importance des fonctions de contrôle indépendantes pour le bon fonctionnement du fournisseur d'importance systémique, les responsables de ces fonctions sont considérés comme des personnes clés devant répondre aux conditions d'honorabilité professionnelle et d'expertise prévues à l'article 25.

Art. 19

La fonction de conformité, communément désignée par le mot "*compliance*", est chargée de veiller au respect des règles légales et/ou réglementaires d'intégrité et de conduite qui s'appliquent aux fournisseurs d'importance systémique. La fonction de conformité ("*compliance*") a ainsi pour objectif d'éviter que le fournisseur d'importance systémique ne subisse les conséquences – en termes de perte de réputation ou de crédibilité susceptible de causer un grave préjudice financier – du non-respect des dispositions légales et réglementaires ou tenant à la déontologie applicables, le cas échéant, à la fourniture de services de messagerie financière (risque de conformité ou de "*compliance*").

Par analogie avec l'article 36 de la loi bancaire, le paragraphe 2 dispose que les personnes qui assurent la fonction de conformité ("*compliance*") font rapport au moins une fois par an au conseil de surveillance, qui, à son tour, fait rapport à la Banque.

Art. 20

Naar analogie van artikel 37 van de bankwet voorziet dit artikel in de organisatie van een onafhankelijke risicobeheerfunctie. Het regelt de nodige onafhankelijkheid van de risicobeheerfunctie ten opzichte van de commerciële en risiconemende functies en de rol van deze functie. Het artikel voorziet ook in een rechtstreekse toegang tot de raad van toezicht, in voorkomend geval via het risicocomité, dat aldus volledige informatie kan verkrijgen over alle risico's waaraan de aanbieder blootstaat.

Art. 21

Dit artikel voorziet, naar analogie van artikel 38 van de bankwet, in de mogelijkheid voor de compliance- en de risicobeheerfunctie om rechtstreeks te rapporteren aan de raad van toezicht. Deze rechtstreekse toegang, die dus inhoudt dat niet eerst via de directieraad moet worden gepasseerd, is nodig om de raad van toezicht in staat te stellen zijn toezichtsfunctie wat betreft de uitvoering van de uitgestippelde strategie en de werking van de aanbieder, strenger uit te oefenen, met inachtneming van het vastgestelde kader (risicotolerantie), ook voor wat betreft het reputatierisico.

Art. 22

De interne auditfunctie heeft, naar analogie van artikel 39 van de bankwet, tot doel aan de raad van toezicht en aan de effectieve leiders een onafhankelijke garantie te verschaffen met betrekking tot de kwaliteit en de doeltreffendheid van de interne controlesystemen van de systeemrelevante aanbieder.

Daarom moet de interne auditfunctie onbeperkt toegang hebben tot alle werkzaamheden van de aanbieder, ongeacht of ze rechtstreeks worden uitgeoefend of worden uitbesteed, tot het volledige netwerk van de aanbieder en tot de entiteiten in zijn bezit, inclusief de werkzaamheden van de risicobeheerfunctie en van de compliancefunctie.

Deze bevoegdheden moeten geformaliseerd worden in een auditcharter, dat het interne document is waarmee de aanbieder aan de hand van een aantal maatregelen met betrekking tot de doelstellingen, de positie en het gezag van de interne auditfunctie garandeert dat deze functie onafhankelijk is en doeltreffend werkt, zodat zij haar taken in alle objectiviteit kan uitoefenen.

Art. 20

Par analogie avec l'article 37 de la loi bancaire, cet article prévoit l'organisation d'une fonction de gestion des risques indépendante. Il règle la nécessaire indépendance de la fonction de gestion des risques par rapport aux fonctions commerciales et de prise de risques, ainsi que son rôle. L'article prévoit, en outre, un accès direct au conseil de surveillance, le cas échéant par l'intermédiaire du comité des risques, qui peut ainsi recevoir une information complète concernant tous les risques auxquels le fournisseur se voit exposé.

Art. 21

Par analogie avec l'article 38 de la loi bancaire, cet article prévoit la possibilité pour les fonctions de conformité ("compliance") et de gestion des risques de rendre compte directement au conseil de surveillance. Cet accès direct, à savoir sans le passage préalable par le conseil de direction, est nécessaire pour permettre au conseil de surveillance d'exercer plus étroitement sa fonction de surveillance en ce qui concerne la mise en œuvre de la stratégie qui a été définie et le fonctionnement du fournisseur dans le respect du cadre fixé (niveau de tolérance au risque), y compris pour ce qui concerne le risque de réputation.

Art. 22

Par analogie avec l'article 39 de la loi bancaire, la fonction d'audit interne a pour objet de fournir au conseil de surveillance et aux dirigeants effectifs une assurance indépendante quant à la qualité et à l'efficience des systèmes de contrôle interne du fournisseur d'importance systémique.

C'est pourquoi la fonction d'audit interne doit avoir accès sans restriction à toutes les activités du fournisseur, qu'elles soient exercées directement ou sous-traitées, à l'intégralité de son réseau et aux entités détenues, y compris aux activités de la fonction de gestion des risques et de la fonction de conformité ("*compliance*").

Ces prérogatives doivent être formalisées dans une charte d'audit qui constitue le document interne par lequel le fournisseur garantit, par un ensemble de mesures concernant les objectifs, la position, et l'autorité de la fonction d'audit interne, son indépendance et son efficacité de façon à ce qu'elle puisse exercer ses missions en toute objectivité.

Paragraaf 3 bepaalt voor het overige dat de interne auditfunctie onder de verantwoordelijkheid valt van de raad van toezicht, in voorkomend geval via het auditcomité.

Art. 23

Om het statuut te versterken van de verantwoordelijken voor de onafhankelijke controlefuncties, bepaalt dit artikel, naar analogie van artikel 61 van de bankwet, dat deze personen enkel door de raad van toezicht uit hun functie kunnen worden verwijderd. Het is immers noodzakelijk dat de raad van toezicht het enige orgaan is dat gemachtigd is om een dergelijke verantwoordelijke uit zijn functie te verwijderen, aangezien die functie inhoudt dat toezicht wordt gehouden op de wijze waarop de directieraad zijn taken uitvoert.

Indien er overwogen zou worden een verantwoordelijke voor een onafhankelijke controlefunctie uit zijn functie te verwijderen, moet de systeemrelevante aanbieder de Bank daar voorafgaandelijk van in kennis stellen, zodat deze kan nagaan of de redenen voor het ontslag gegrond zijn, en, in voorkomend geval, kan onderzoeken of er op grond van de corporate governance van de aanbieder geen bijzondere maatregelen moeten worden genomen.

Art. 24

Dit artikel machtigt de Bank om bij reglement nadere regels vast te leggen voor verschillende aspecten van de operationele onafhankelijke controlefuncties.

Afdeling V

Leiding, professionele betrouwbaarheid en passende deskundigheid

Art. 25

Naar analogie van artikel 19 van de bankwet bepaalt dit artikel dat de leiding van systeemrelevante aanbieders, met het oog op de goede werking en de integriteit van die aanbieders, moet beschikken over de vereiste professionele betrouwbaarheid en de passende deskundigheid voor de uitoefening van hun functie. Met andere woorden, zij dienen grondig gescreend te worden op hun zogenaamde "*fit & proper*" karakter.

De beoordeling van het "*fit & proper*" karakter van de leden van de raad van toezicht vergt een verhoogde aandacht om na te gaan of de noodzakelijke deskundigheid aanwezig is, individueel en collectief, om de opdrachten

Le paragraphe 3 prévoit, pour le surplus, que la fonction d'audit interne relève du conseil de surveillance, le cas échéant par l'intermédiaire du comité d'audit.

Art. 23

Afin de renforcer le statut des personnes qui sont responsables des fonctions de contrôle indépendantes, cet article dispose, par analogie avec l'article 61 de la loi bancaire, qu'elles ne peuvent être démises de leurs fonctions que par le conseil de surveillance. Il est, en effet, essentiel que le conseil de surveillance soit le seul organe habilité à démettre un tel responsable dès lors que ses fonctions impliquent un contrôle de la manière dont le conseil de direction s'acquitte de ses missions.

Dans le cas où il serait envisagé de démettre un responsable d'une fonction de contrôle indépendante, le fournisseur d'importance systémique doit en informer préalablement la Banque afin de permettre à celle-ci de vérifier le bien-fondé des motifs justifiant la révocation et le cas échant, d'examiner si la gouvernance du fournisseur ne requiert pas l'adoption de mesures particulières.

Art. 24

Cet article habilite la Banque à définir, par voie de règlement, des règles plus précises concernant divers aspects des fonctions de contrôle indépendantes opérationnelles.

Section V

Dirigeants, honorabilité professionnelle et expertise adéquate

Art. 25

Par analogie avec l'article 19 de la loi bancaire, cet article dispose que les dirigeants des fournisseurs d'importance systémique doivent disposer de l'honorabilité professionnelle nécessaire et de l'expertise adéquate à l'exercice de leur fonction, aux fins du bon fonctionnement et de l'intégrité de ces fournisseurs. En d'autres termes, il y a lieu de procéder à une évaluation approfondie de leur caractère "*fit & proper*".

L'évaluation du caractère "*fit & proper*" des membres du conseil de surveillance requiert une attention accrue pour vérifier la présence de l'expertise nécessaire – sur les plans tant individuel que collectif – pour mener à bien

van de raad van toezicht te kunnen vervullen, met name het vastleggen van de strategische oriëntaties en het controleren van de uitvoering van het beleid door de directieraad. Er dient met andere woorden voor te worden gezorgd dat de leden van de raad van toezicht over de nodige deskundigheid beschikken om de voorstellen van de directieraad kritisch in vraag te stellen ("*challengen*"), zodat het beleid oordeelkundig wordt vastgesteld. In dezelfde optiek is ook de deskundigheid van de effectieve leiding en van de verantwoordelijken voor de onafhankelijke controlefuncties van groot belang. Artikel 3, 7°, definieert de effectieve leiding als de personen die lid zijn van de directieraad en de personen die belast zijn met het dagelijks bestuur. De effectieve leiding refereert aldus aan de groep van personen waarvan de functie binnen de systeemrelevante aanbieder impliceert dat ze op het hoogste niveau een rechtstreekse en beslissende invloed uitoefenen op het beheer van de bedrijfsactiviteit.

Paragraaf 1 van het artikel verduidelijkt vooreerst dat alleen natuurlijke personen een mandaat mogen opnemen als lid van de raad van toezicht, persoon belast met de effectieve leiding of verantwoordelijke voor een onafhankelijke controlefunctie.

De ontwikkelingen inzake corporate governance van financiële instellingen, als gevolg van de recentste financiële crisissen, leggen het accent op de persoonlijkheid en de eigenschappen van ieder bestuurslid als individu, in plaats van een louter functionele visie op de rol van de bestuurder te huldigen. Hetzelfde geldt voor de effectieve leiding en de verantwoordelijken voor de onafhankelijke controlefuncties.

Paragraaf 2 van het artikel bepaalt vervolgens dat van de betrokken personen verwacht wordt dat zij permanent over de voor de uitoefening van hun functie vereiste professionele betrouwbaarheid en passende deskundigheid beschikken.

Betrouwbaarheid houdt in dat de leider eerlijk en integer is. Deze betrouwbaarheid vereist van hem of haar een onberispelijke beroepsethiek, die garant staat voor de naleving door de systeemrelevante aanbieder van de in de wet vermelde verplichtingen en verbodsbepalingen, en van de andere gedragsregels die van toepassing zijn in de sector. De voorwaarde inzake professionele betrouwbaarheid is geen formele voorwaarde die kan worden teruggevoerd op het ontbreken van een strafrechtelijke veroordeling. Op grond van haar eigen analyse van de feiten in het dossier, kan de Bank oordelen dat sommige handelingen of gedragingen van de leiders een aantasting vormen van de professionele betrouwbaarheid van deze personen, wat losstaat van

les missions du conseil de surveillance que sont, notamment, la détermination des orientations stratégiques et le suivi de leur mise en œuvre par le conseil de direction. Autrement dit, il faut veiller à ce que les membres du conseil de surveillance disposent de l'expertise nécessaire pour examiner d'un œil critique les propositions du conseil de direction ("*challenging*"), de telle sorte que la définition de la politique à suivre soit judicieuse. C'est dans ce même ordre d'idées que l'expertise de la direction effective et des responsables des fonctions de contrôle indépendantes revêt également une grande importance. L'article 3, 7°, définit la direction effective comme les personnes qui sont membres du conseil de direction et les personnes auxquelles la gestion journalière est déléguée. Il y a ainsi lieu d'entendre par la direction effective le groupe de personnes dont la fonction au sein du fournisseur d'importance systémique implique qu'elles exercent au plus haut niveau une influence directe et décisive sur la direction de l'activité de l'entreprise.

Le paragraphe 1er de l'article précise tout d'abord que seules des personnes physiques peuvent exercer un mandat de membre du conseil de surveillance, de personne chargée de la direction effective ou de responsable d'une fonction de contrôle indépendante.

Les évolutions en matière de gouvernance des établissements financiers, à la suite des dernières crises financières, mettent l'accent sur la personnalité ainsi que sur les qualités de chaque administrateur en tant qu'individu, plutôt que sur une vision purement fonctionnelle de son rôle. Il en va de même pour la direction effective et pour les responsables des fonctions de contrôle indépendantes.

Le paragraphe 2 de l'article prévoit en outre que les personnes concernées doivent disposer en permanence de l'honorabilité professionnelle nécessaire et de l'expertise adéquate à l'exercice de leur fonction.

L'honorabilité vise l'honnêteté et l'intégrité du dirigeant. Elle implique une éthique professionnelle irréprochable de sa part, éthique garante du respect par le fournisseur d'importance systémique des obligations et interdictions prévues par la loi ainsi que des autres règles de conduite applicables dans le secteur. Il ne s'agit pas d'une condition formelle se résumant à une absence de condamnation pénale. Sur la base de sa propre analyse des faits du dossier, la Banque peut considérer que certains comportements ou agissements des dirigeants sont constitutifs d'une atteinte à l'honorabilité professionnelle que doivent présenter ces personnes, indépendamment de toute qualification pénale desdits comportements ou agissements ou de l'issue d'une

de strafrechtelijke kwalificatie van deze gedragingen of handelingen of van de afloop van een strafrechtelijke procedure die in voorkomend geval zou zijn ingesteld tegen deze personen.

De passende deskundigheid voor de uitoefening van een specifieke functie omvat de nodige kennis, vaardigheden ("*skills*") en ervaring voor de uitoefening van deze functie. Met de term "deskundigheid" beoogt men de drie voornoemde eigenschappen te omvatten. Deze eigenschappen worden beoordeeld op grond van de kenmerken van de systeemrelevante aanbieder waar de betrokken personen hun functies uitoefenen (aard van de werkzaamheden, complexiteit, risicoprofiel, etc.), maar ook van de inhoud van de functie. Er wordt van hen dan ook verwacht dat zij een passende professionele houding aannemen.

Art. 26

Dit artikel bepaalt dat leden van de raad van toezicht, personen belast met de effectieve leiding en verantwoordelijken voor een onafhankelijke controlefunctie niet veroordeeld mogen zijn tot een straf bedoeld in artikel 20, § 1, van de bankwet. Zij zijn aldus aan een stelsel van een beroepsverbod onderworpen. Het beroepsverbod geldt voor een termijn van twintig of van tien jaar, naar gelang van de zwaarte van de straf. Voor nadere toelichting zij verwezen naar de parlementaire voorbereiding van de bankwet (*Parl.St.* Kamer 2013-2014, DOC 53 3406/001, blz. 40-42).

Art. 27

Systeemrelevante aanbieders dienen er in de eerste plaats zelf op toe te zien dat hun leden van de raad van toezicht, personen belast met de effectieve leiding en verantwoordelijken voor een onafhankelijke controlefunctie over de vereiste betrouwbaarheid en de passende deskundigheid beschikken om hun functie uit te oefenen.

Artikel 27 versterkt het toezicht op de naleving van deze verplichting. Deze versterking houdt in dat de Bank voorafgaandelijk wordt ingelicht (paragraaf 1) en dat de te verrichten benoemingen voorafgaandelijk door haar worden goedgekeurd (paragraaf 2), met name wat de benoeming betreft van de voorzitter van de raad van toezicht, de voorzitter van de directieraad, de voorzitter van ieder comité bedoeld in artikel 13, en de verantwoordelijken voor de risicobeheerfunctie en de interne auditfunctie. Een voorafgaande goedkeuring door de Bank is daarentegen niet vereist voor de andere functies die aan het vereiste van professionele betrouwbaarheid

procédure pénale qui aurait, le cas échéant, été initiée à l'encontre de ces personnes.

L'expertise adéquate à l'exercice d'une fonction spécifique recouvre les connaissances, les compétences ("*skills*") et l'expérience nécessaires à l'exercice de cette fonction. On entend par le terme "expertise" englober les trois qualités précitées. Celles-ci sont appréciées eu égard aux caractéristiques du fournisseur d'importance systémique au sein duquel les personnes concernées sont appelées à exercer leurs fonctions (nature des activités, complexité, profil de risque, etc.), mais également sur la base du contenu de la fonction. Il est dès lors attendu d'elles qu'elles fassent preuve d'un comportement professionnel adéquat.

Art. 26

Cet article prévoit que les membres du conseil de surveillance, les personnes chargées de la direction effective et les responsables d'une fonction de contrôle indépendante ne peuvent avoir été condamnés à une peine visée à l'article 20, § 1er, de la loi bancaire. Ils sont ainsi soumis à un régime d'interdictions professionnelles. L'interdiction professionnelle s'applique pour une durée de vingt ou de dix ans, en fonction de la gravité de la peine. Pour plus de précisions, il est renvoyé aux travaux parlementaires préparatoires de la loi bancaire *(Doc. Parl.*, Chambre, 2013-2014, DOC 53 3406/001, pp. 40-42).

Art. 27

Il incombe au premier chef aux fournisseurs d'importance systémique eux-mêmes de veiller à ce que les membres de leur conseil de surveillance, les personnes chargées de la direction effective et les responsables d'une fonction de contrôle indépendante présentent l'honorabilité nécessaire et l'expertise adéquate à l'exercice de leur fonction.

L'article 27 vient renforcer le contrôle exercé sur le respect de cette obligation. Ce renforcement repose sur une information préalable de la Banque (paragraphe 1er) assortie d'une approbation préalable par celle-ci des nominations à effectuer (paragraphe 2), notamment en ce qui concerne la nomination du président du conseil de surveillance, du président du conseil de direction, du président de chaque comité visé à l'article 13 et des responsables de la fonction de gestion des risques et de la fonction d'audit interne. En revanche, l'approbation préalable par la Banque n'est pas requise pour les autres fonctions soumises à l'exigence d'honorabilité

en passende deskundigheid onderworpen zijn; dit belet evenwel niet dat die vereisten wel degelijk van toepassing blijven op de betrokken functies en dat de Bank op doorlopende basis toeziet op de naleving daarvan.

Het past hier te verduidelijken dat de functie van voorzitter van de directieraad in een internationale (doorgaans Angelsaksisch geïnspireerde) context vaak samenvalt met de functie van *Chief Executive Officer* of CEO. Wanneer de CEO zijn of haar functie uitoefent in de hoedanigheid van voorzitter van de directieraad, zal diens benoeming aldus voorafgaand moeten goedgekeurd worden door de Bank. In de context van een duale bestuursstructuur hanteert de Belgische *Corporate Governance Code* 2020 de term “CEO” in elk geval alleen om te verwijzen naar de persoon die de directieraad leidt.

De verplichting om de Bank in te lichten en haar goedkeuring te verkrijgen geldt eveneens voor voorstellen tot hernieuwing van de functies bedoeld in paragraaf 1 van het artikel, voor de niet-hernieuwing van die benoemingen en voor de afzetting of het ontslag van de betrokken personen.

De termijn waarbinnen een beslissing moet worden genomen, leent zich niet tot een formalisering aangezien die termijn uiteraard kan variëren naargelang van de complexiteit van het voorgelegde dossier en met name van het vereiste overleg (met gerechtelijke overheden, buitenlandse autoriteiten, etc.). Het spreekt voor zich dat de Bank erop moet toezien dat zij haar beslissing neemt binnen een redelijke termijn na de ontvangst van een volledig dossier, met inachtneming van het beginsel van goed bestuur.

Overeenkomstig paragraaf 3 van dit artikel dient in dit verband nog opgemerkt te worden dat een verandering van functie, bijvoorbeeld een nieuwe taakverdeling binnen de raad van toezicht of de directieraad, beschouwd moet worden als een nieuwe benoeming voor de betrokken leiders, die in voorkomend geval (met name wanneer zij betrekking heeft op een persoon bedoeld in artikel 27, § 1) voorafgaandelijk aan de Bank moet worden gemeld en waarvoor zij voorafgaandelijk haar goedkeuring moet verlenen.

De professionele betrouwbaarheid en de passende deskundigheid worden beoordeeld bij de infunctietreding, maar ook in de loop van de uitoefening van de functie. De vereisten inzake betrouwbaarheid en deskundigheid moeten met andere woorden noodzakelijkerwijs vervuld zijn tijdens de volledige duur van de uitoefening van de functie en niet alleen bij de infunctietreding. Bijgevolg bepaalt paragraaf 4 van artikel 27 dat de systeemrelevante aanbieder evenals de betrokken personen zelf de Bank onverwijld in kennis moeten stellen van elk nieuw

professionnelle et d’expertise adéquate; cela n’empêche toutefois pas que ces exigences continuent de s’appliquer aux fonctions concernées et que la Banque en contrôle le respect de manière continue.

Il convient de préciser ici que la fonction de président du conseil de direction coïncide souvent, dans un contexte international (généralement d’inspiration anglo-saxonne), avec celle de *Chief Executive Officer* ou CEO. Lorsque le CEO exerce sa fonction en qualité de président du conseil de direction, sa nomination devra donc être préalablement approuvée par la Banque. En tout état de cause, dans le cadre d’une structure d’administration duale, le Code belge de gouvernance d’entreprise 2020 n’utilise le terme “CEO” que pour désigner la personne qui dirige le conseil de direction.

L’obligation d’informer la Banque et d’obtenir son approbation s’applique également aux propositions de renouvellement des fonctions visées au paragraphe 1er de l’article, au non-renouvellement de ces nominations, ainsi qu’à la révocation ou à la démission des personnes concernées.

S’agissant du délai dans lequel une décision doit être rendue, celui-ci ne se prête pas à une formalisation dès lors qu’il peut, bien évidemment, varier selon la complexité du dossier soumis et notamment des consultations (avec les autorités judiciaires, les autorités étrangères, etc.) requises. Dans le respect du principe de bonne administration, il est évident que la Banque veillera à rendre sa décision dans un délai raisonnable à partir de la réception d’un dossier complet.

Conformément au paragraphe 3 de l’article, il est encore à noter qu’un changement de fonction, par exemple une nouvelle répartition des tâches au sein du conseil de surveillance ou du conseil de direction, est à considérer comme une nouvelle nomination pour les dirigeants concernés, nécessitant le cas échéant (notamment lorsqu’elle porte sur une personne visée à larticle 27, § 1er) une information préalable de la Banque et l’approbation préalable de celle-ci.

Les qualités d’honorabilité professionnelle et d’expertise adéquate s’apprécient lors de l’entrée en fonction mais également en cours d’exercice de celle-ci. En d’autres termes, les exigences d’honorabilité et d’expertise doivent nécessairement être satisfaites pendant toute la durée de l’exercice des fonctions et non pas seulement au moment de l’entrée en fonction. Le paragraphe 4 de l’article 27 dispose dès lors que le fournisseur d’importance systémique et les personnes concernées doivent informer la Banque sans délai de tout fait nouveau ou

feit dat of elke nieuwe omstandigheid die twijfel kan doen rijzen over de professionele betrouwbaarheid of de deskundigheid die verlangd wordt van de personen bedoeld in paragraaf 1. De Bank kan de naleving van de betrokken vereisten overigens ook opnieuw beoordelen wanneer zij anderszins tijdens de uitoefening van haar toezichtsopdracht op de hoogte is van een dergelijk feit of een dergelijke omstandigheid.

Art. 28

Dit artikel bevat, naar analogie van artikel 61, § 1, en artikel 62, § 1, van de bankwet, de uitdrukkelijke verplichting voor alle leden van de raad van toezicht, de personen belast met de effectieve leiding en de verantwoordelijken voor de onafhankelijke controlefuncties om de nodige tijd te besteden aan hun functie bij de systeemrelevante aanbieder.

Art. 29

Dit artikel behoeft geen nadere toelichting.

Afdeling VI

Bedrijfsorganisatie

Art. 30

In zijn inleidend gedeelte formuleert dit artikel in de vorm van een algemeen beginsel de vereiste om te beschikken over een solide bedrijfsorganisatie. Dit beginsel, dat geïnspireerd is op het bepaalde in artikel 21 van de bankwet, wordt toegelicht aan de hand van een thematische lijst die dit algemeen beginsel van goed bestuur beoogt te concretiseren door een niet-limitatieve opsomming te geven van de verschillende behandelde aspecten. Die aspecten worden nader bepaald in verschillende daaropvolgende afdelingen, evenals in bepaalde andere hoofdstukken van het wetsvoorstel.

Van de aspecten die in artikel 30 concreter worden opgesomd, formuleert de bepaling als eerste beginsel de basisregel dat de bedrijfsorganisatie moet berusten op schriftelijk vastgelegde doelstellingen waarin een hoge prioriteit wordt gegeven aan de veiligheid en de efficiëntie van het verlenen van financiële berichtendiensten, en die expliciet financiële stabiliteit en andere relevante overwegingen van publiek belang, in het bijzonder open en efficiënte markten, bevorderen. Het betreft de vertaling van de verwachtingen uitgedrukt in kernbepaling 1 van PFMI-principe 2.

de toute circonstance nouvelle susceptible de mettre en doute l'honorabilité professionnelle ou l'expertise requises des personnes visées au paragraphe 1er. Par ailleurs, la Banque peut également réévaluer le respect des exigences concernées lorsqu'elle a connaissance autrement, au cours de l'exercice de sa mission de contrôle, d'un tel fait ou d'une telle circonstance.

Art. 28

Cet article contient, par analogie avec l'article 61, § 1er, et l'article 62, § 1er, de la loi bancaire, l'obligation explicite pour tous les membres du conseil de surveillance, les personnes chargées de la direction effective et les responsables des fonctions de contrôle indépendantes de consacrer le temps nécessaire à leurs fonctions auprès du fournisseur d'importance systémique.

Art. 29

Cet article n'appelle pas de commentaires.

Section VI

Organisation d'entreprise

Art. 30

Dans sa partie introductive, cet article énonce, sous la forme d'un principe général, l'exigence de disposer d'un dispositif solide et adéquat d'organisation d'entreprise. Ce principe, qui s'inspire des dispositions de l'article 21 de la loi bancaire, se voit explicité par une liste thématique qui a pour objet de concrétiser ce principe général de bonne administration, en énonçant, de manière non limitative, les divers aspects qu'il recouvre. Ces aspects sont précisés dans différentes sections ultérieures, ainsi que dans certains autres chapitres de la proposition de loi.

Parmi les aspects que l'article 30 énumère de manière plus concrète, la disposition énonce comme premier principe la règle de base selon laquelle l'organisation d'entreprise doit être fondée sur des objectifs consignés par écrit axés sur la sécurité et l'efficacité de la fourniture de services de messagerie financière, et qui soutiennent explicitement la stabilité du système financier et d'autres considérations d'intérêt public, en particulier des marchés financiers ouverts et efficaces. Il s'agit de la traduction des attentes exprimées dans la considération essentielle 1 du principe 2 des PIMF.

Vervolgens bevat het artikel de basisregel van de verdeling, op het hoogste niveau, tussen de functies die toezicht houden op de leiding en de functies die verantwoordelijk zijn voor de effectieve leiding.

De regeling omvat verder een aantal specifieke aspecten, zoals de verplichting om te beschikken over een intern waarschuwingssysteem (*whistleblowing*) in overeenstemming 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, de verplichting om te beschikken over passende onafhankelijke controlefuncties, of nog de noodzaak om de continuïteit van de diensten en werkzaamheden te garanderen en om een regeling uit te werken ter beheersing van belangenconflicten. Bijzondere aandacht gaat naar het uitwerken van de nodige regelingen op het vlak van risicobeheer (in overeenstemming met het bepaalde in artikel 47) en van digitale operationele weerbaarheid (onder meer in overeenstemming met het bepaalde in artikel 52).

Er zij op gewezen dat de wet van 28 november 2022 op grond van zijn artikel 2 van toepassing is op de bescherming van melders van inbreuken die onder meer betrekking hebben op financiële diensten, producten en markten, waaronder dus ook financiële berichtendiensten moeten begrepen worden. Artikel 6, § 1, van die wet bepaalt verder dat zij van toepassing is op in de private sector werkzame melders die informatie over inbreuken hebben verkregen in een werkgerelateerde context, waaronder ook werknemers en personen die behoren tot het bestuurlijke, leidinggevend of toezichthoudend orgaan van een onderneming. De door die wet geboden bescherming geldt dus bijvoorbeeld ook voor de leden van de raad van toezicht of van de directieraad van systeemrelevante aanbieders.

Paragraaf 2 van het artikel bepaalt opnieuw dat de Bank bij reglement kan preciseren en aanvullen wat dient verstaan te worden onder de vereisten bedoeld in paragraaf 1.

Art. 31

Enerzijds bekrachtigt dit artikel een verplichting tot uitputtende uitwerking van de organisatieregeling en het passende karakter, dit wil zeggen een organisatie die rekening houdt met de specifieke kenmerken van de systeemrelevante aanbieder en derhalve met al zijn werkzaamheden, en anderzijds het evenredigheidsbeginsel, dat in voorkomend geval kan leiden tot een verlichting van de vereisten voor kleinere structuren of, omgekeerd, tot een verzwaring voor zeer belangrijke, mondiaal actieve structuren. De organisatieregeling

L'article comporte ensuite la règle de base de la répartition, au plus haut niveau, entre les fonctions de supervision de la direction et celles responsables de la direction effective.

Il comprend également un certain nombre d'aspects spécifiques, tels que l'obligation de disposer d'un système d'alerte interne (*whistleblowing*) conformément 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, l'obligation de disposer de fonctions de contrôle indépendantes adéquates, ou encore la nécessité d'assurer la continuité des services et des activités et d'élaborer un dispositif visant à gérer les conflits d'intérêts. Une attention particulière est accordée à l'élaboration des dispositions nécessaires en matière de gestion des risques (conformément aux dispositions de l'article 47) ainsi que de résilience opérationnelle numérique (conformément, entre autres, aux dispositions de l'article 52).

Il convient de noter que la loi du 28 novembre 2022, en vertu de son article 2, s'applique à la protection des personnes signalant des violations qui concernent notamment les services, produits et marchés financiers, dans lesquels il faut donc également inclure les services de messagerie financière. L'article 6, § 1er de cette loi dispose en outre qu'elle s'applique aux auteurs de signalement travaillant dans le secteur privé qui ont obtenu des informations sur des violations dans un contexte professionnel, y compris les travailleurs et les membres de l'organe d'administration, de direction ou de surveillance d'une entreprise. Ainsi, la protection prévue par cette loi s'applique également, par exemple, aux membres du conseil de surveillance ou du conseil de direction des fournisseurs d'importance systémique.

Le paragraphe 2 de l'article dispose à nouveau que la Banque peut, par voie de règlement, préciser et compléter ce qu'il y a lieu d'entendre par les exigences visées au paragraphe 1er.

Art. 31

Cet article consacre, d'une part, une obligation d'exhaustivité du dispositif organisationnel, c'est-à-dire son caractère approprié au regard des spécificités du fournisseur d'importance systémique et dès lors de l'ensemble ses activités et, d'autre part, le principe de proportionnalité qui peut conduire, le cas échéant, à un allègement des exigences à l'égard des plus petites structures et inversement à leur durcissement à l'égard des structures très importantes opérant au niveau international. Les dispositifs organisationnels doivent en

moet in het bijzonder, doch niet uitsluitend, rekening houden met de verplichtingen inzake bedrijfsvoering en risicobeheer zoals bedoeld in hoofdstuk 7 van het wetsvoorstel.

Art. 32

Dit artikel bepaalt, naar analogie van artikel 22 van de bankwet, dat nauwe banden tussen de systeemrelevante aanbieder en andere natuurlijke of rechtspersonen, evenals voor die personen geldende wettelijke en bestuursrechtelijke bepalingen of de tenuitvoerlegging ervan, geen belemmering mogen vormen voor het toezicht op de aanbieder door de Bank. De Bank zou moeten optreden indien de nauwe banden die tussen de aanbieder en andere natuurlijke of rechtspersonen bestaan, van dien aard zijn dat zij een belemmering vormen voor de juiste uitoefening van haar toezichtstaken.

Afdeling VII

Toezicht en leiding

Art. 33

Het toezicht op de werkzaamheden en de regelmatige beoordeling van de beleidsstructuur, de organisatie en de interne controlemechanismen van de systeemrelevante aanbieder vormen een belangrijke pijler van de verantwoordelijkheden die het wetsvoorstel toekent aan de raad van toezicht. Artikel 33 bepaalt, naar analogie van artikel 56 van de bankwet, dat dit toezicht betrekking moet hebben op de effectieve leiding en diens beslissingen. De raad van toezicht moet ook de goede werking van de onafhankelijke controlefuncties beoordelen en erop toezien dat de aanbieder voldoende middelen wijdt aan de permanente opleiding van de leden van de raad van toezicht. In een jaarlijks verslag moet de raad van toezicht ook de individuele en collectieve deskundigheid rechtvaardigen van de leden van de comités bedoeld in artikel 13.

Art. 34

Dit artikel bepaalt dat de leden van de raad van toezicht passende toegang moeten hebben tot alle informatie en documenten die nodig zijn om de opdrachten uit te voeren waarmee ze belast zijn met toepassing van de bepalingen van het wetsvoorstel en zijn uitvoeringsbesluiten.

particulier, mais pas exclusivement, tenir compte des obligations de conduite des activités et de gestion de risque visées au chapitre 7 de la proposition de loi.

Art. 32

Cet article prévoit, par analogie avec l'article 22 de la loi bancaire, que les liens étroits entre le fournisseur d'importance systémique et d'autres personnes physiques ou morales, ainsi que les dispositions légales, réglementaires et administratives applicables à ces personnes ou leur mise en œuvre, ne peuvent entraver l'exercice du contrôle du fournisseur par la Banque. La Banque devrait intervenir si les liens étroits qui unissent le fournisseur à d'autres personnes physiques ou morales sont de nature à entraver le bon exercice de sa mission de surveillance.

Section VII

Contrôle et direction

Art. 33

La surveillance des activités et l'évaluation régulière de la structure de gestion, de l'organisation et des mécanismes de contrôle interne du fournisseur d'importance systémique constituent un axe important des responsabilités que la proposition de loi attribue au conseil de surveillance. L'article 33 prévoit, par analogie avec l'article 56 de la loi bancaire, que cette surveillance doit porter sur la direction effective et sur les décisions prises par celle-ci. Le conseil de surveillance doit également évaluer le bon fonctionnement des fonctions de contrôle indépendantes et s'assurer que le fournisseur consacre des ressources adéquates à la formation continue des membres du conseil de surveillance. Le conseil de surveillance doit également justifier, dans le rapport annuel, la compétence individuelle et collective des membres des comités visés à l'article 13.

Art. 34

Cet article dispose que les membres du conseil de surveillance doivent disposer d'un accès adéquat à l'ensemble des informations et des documents nécessaires pour assurer les missions dont ils sont chargés en application des dispositions de la proposition de loi et des arrêtés pris pour son exécution.

Art. 35

Buiten de bepalingen betreffende de effectieve leiders van de systeemrelevante aanbieder als personen, bevat het wetsvoorstel weinig specifieke bepalingen over de directieraad als orgaan of de effectieve leiders als dusdanig. Op twee punten verduidelijkt artikel 35, naar analogie van artikel 59 van de bankwet, welke taken in elk geval door de directieraad moeten uitgeoefend worden.

In de eerste plaats dient de directieraad de nodige maatregelen te nemen voor de naleving en de tenuitvoerlegging van de regeling voor de bedrijfsorganisatie als bedoeld in artikel 30.

Vervolgens bepaalt het artikel dat de directieraad minstens jaarlijks een verslag moet opstellen over de beoordeling van de doeltreffendheid van de regeling voor de bedrijfsorganisatie, evenals over de maatregelen die in voorkomend geval moeten worden genomen om eventuele tekortkomingen aan te pakken. De directieraad maakt dit verslag over aan de raad van toezicht en aan de Bank. Op basis van dit verslag moet kunnen nagegaan worden of voldaan is aan de vereisten.

Art. 36

Dit artikel behoeft geen nadere toelichting.

HOOFDSTUK 4

Kapitaalvereisten

Art. 37

De indieners achten het wenselijk om systeemrelevante aanbieders verplichtingen op te leggen inzake het aanhouden van kapitaal, samen met het overgedragen resultaat en reserves. Die kapitaalvereisten moeten evenredig zijn met de risico's die uit de activiteiten van de aanbieder voortkomen en moeten steeds voldoende zijn om te waarborgen dat de aanbieder (a) wordt beschermd tegen risico's zodat hij zijn diensten kan blijven verrichten als *going concern*, en (b) in geval van stressscenario's uitvoering kan geven aan het herstel- of ordelijke liquidatieplan dat krachtens artikel 48 moet opgesteld worden.

PFMI-principe 15 erkent het belang voor financiële marktinfrastructuren om voldoende kapitaal aan te houden tot dekking van het algemeen bedrijfsrisico (zie met

Art. 35

En dehors des dispositions concernant les dirigeants effectifs du fournisseur d'importance systémique en tant que personnes, la proposition de loi comprend peu de dispositions spécifiques concernant le conseil de direction en tant qu'organe ou les dirigeants effectifs en tant que tels. Sur deux points, l'article 35 précise, par analogie avec l'article 59 de la loi bancaire, quelles missions doivent en tout cas être exercées par le conseil de direction.

Tout d'abord, le conseil de direction doit prendre les mesures nécessaires pour assurer le respect et la mise en œuvre du dispositif d'organisation d'entreprise tel que visé à l'article 30.

Ensuite, l'article prévoit que le conseil de direction doit établir au moins une fois par an un rapport concernant l'évaluation de l'efficacité des dispositifs d'organisation, ainsi que sur les mesures à prendre, le cas échéant, pour remédier à d'éventuelles déficiences. Le conseil de direction soumet ce rapport au conseil de surveillance et à la Banque. Le rapport doit permettre de vérifier que les exigences sont respectées.

Art. 36

Cet article n'appelle pas de commentaires.

CHAPITRE 4

Exigences de capital

Art. 37

Les déposants estiment qu'il est souhaitable d'imposer aux fournisseurs d'importance systémique des obligations concernant la détention de fonds propres complétés par des résultats reportés et des réserves. Ces exigences de fonds propres doivent être proportionnelles au risque découlant des activités du fournisseur et doivent être suffisantes, à tout moment, pour garantir a) que le fournisseur bénéficie d'une protection adéquate à l'égard des risques, de telle manière qu'il puisse assurer la continuité de l'exploitation et b) qu'il puisse exécuter, dans le cadre de scénarios de crise, le plan de redressement ou de liquidation ordonnée qui doit être élaboré en vertu de l'article 48.

Le principe 15 des PIMF reconnaît l'importance pour les infrastructures de marchés financiers de détenir des fonds propres suffisants pour couvrir le risque général

name paragraaf 3.15.9 van de PFMI). Dit principe werd voor bepaalde marktinfrastructuren, en in het bijzonder voor centrale effectenbewaarinstellingen, neergelegd in een juridisch bindend kader. Artikel 37 sluit dan ook aan bij wat artikel 47 van de CSD-verordening op dit vlak voorschrijft voor centrale effectenbewaarinstellingen.

Paragraaf 2 bepaalt opnieuw dat de Bank bij reglement nadere regels kan vastleggen tot bepaling van de vereisten inzake het kapitaal, de ingehouden winst en de reserves van een systeemrelevante aanbieder.

Art. 38

Dit artikel bepaalt dat systeemrelevante aanbieders een plan moeten aanhouden voor het aantrekken van extra kapitaal ingeval het aandelenkapitaal het vereiste bedoeld in artikel 37 nadert of daaronder daalt. De aanbieder moet ook een plan aanhouden om het herstel of de ordelijke liquidatie te kunnen verzekeren indien geen extra kapitaal kan aangetrokken worden. Dat plan moet door de raad van toezicht of door een bevoegd comité goedgekeurd worden en minstens jaarlijks geactualiseerd. De Bank moet van elke actualisering op de hoogte gebracht worden en zij kan de systeemrelevante aanbieder aanvullende maatregelen opleggen indien zij het plan ontoereikend acht.

HOOFDSTUK 5

Strategische beslissingen

Art. 39

Krachtens dit artikel is, naar analogie van artikel 77 van de bankwet, de voorafgaande toestemming van de Bank vereist wanneer een systeemrelevante aanbieder strategische beslissingen neemt.

Artikel 3, 11° definieert een strategische beslissing als een beslissing genomen door de systeemrelevante aanbieder die een significante impact kan hebben op het risicoprofiel van de aanbieder, of die gelijkaardige gevolgen heeft voor de aanbieder maar die genomen wordt door een aandeelhouder die controle uitoefent over de aanbieder. In tegenstelling tot de bankwet bevat het wetsvoorstel geen opsomming van beslissingen die als strategisch beschouwd kunnen worden. Paragraaf 3 van artikel 39 laat het uitsluitend aan de Bank over om bij reglement te bepalen welke beslissingen als strategisch moeten worden beschouwd, rekening houdend met het risicoprofiel en de aard van de werkzaamheden van

d'entreprise (cf. notamment le paragraphe 3.15.9 des PIMF). Ce principe a été inscrit dans un cadre juridiquement contraignant pour certaines infrastructures de marché, et en particulier pour les dépositaires centraux de titres. L'article 37 est donc conforme à ce que l'article 47 du règlement CSD exige à cet égard pour les dépositaires centraux de titres.

Le paragraphe 2 dispose de nouveau que la Banque peut fixer, par voie de règlement, des règles supplémentaires pour déterminer les exigences en matière de fonds propres, de bénéfices non redistribués et de réserves d'un fournisseur d'importance systémique.

Art. 38

Cet article prévoit que chaque fournisseur d'importance systémique doit tenir à jour un plan pour lever des capitaux supplémentaires, pour le cas où son capital approcherait du seuil visé à l'article 37 ou tomberait sous ce seuil. Le fournisseur doit également tenir à jour un plan 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. Ce plan doit être approuvé par le conseil de surveillance ou un comité approprié et être mis à jour au moins une fois par an. Toute mise à jour doit être notifiée à la Banque; elle peut imposer des mesures supplémentaires au fournisseur d'importance systémique si elle estime le plan insuffisant.

CHAPITRE 5

Décisions stratégiques

Art. 39

En vertu de cet article, l'autorisation préalable de la Banque est requise, par analogie avec l'article 77 de la loi bancaire, lorsqu'un fournisseur d'importance systémique prend des décisions stratégiques.

L'article 3, 11° définit une décision stratégique comme une décision prise par le fournisseur d'importance systémique qui peut avoir une incidence significative sur le profil de risque du fournisseur, ou qui produit des effets similaires dans le chef du fournisseur mais qui est prise par un actionnaire qui exerce le contrôle sur le fournisseur. Contrairement à la loi bancaire, la proposition de loi n'énumère pas les décisions qui peuvent être considérées comme stratégiques. Le paragraphe 3 de l'article 39 laisse à la Banque seule le soin de déterminer, par voie de règlement, quelles décisions doivent être considérées comme stratégiques, compte tenu du profil de risque et de la nature des activités des fournisseurs

systeemrelevante aanbieders. Zouden onder meer als strategische beslissingen kunnen beschouwd worden: fusies van een systeemrelevante aanbieder met bepaalde andere instellingen, de volledige of gedeeltelijke overdracht van werkzaamheden van de aanbieder, of de splitsing van diens activiteiten.

De Bank dient te beslissen binnen twee maanden na ontvangst van een volledig dossier van de voorgenomen strategische beslissing, en mag haar toestemming enkel weigeren om redenen die verband houden met het vermogen van de aanbieder om te voldoen aan de bepalingen die door of krachtens het wetsvoorstel 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 de Bank niet binnen de voornoemde termijn optreedt, wordt de toestemming geacht te zijn verkregen. De Bank kan haar toestemming tevens aan voorwaarden onderwerpen wanneer dat nodig is om de hiervoor vermelde doelstellingen te verzekeren.

HOOFDSTUK 6

Uitbesteding

Art. 40

Dit artikel bepaalt, naar analogie van artikel 30 van de CSD-verordening, dat systeemrelevante aanbieders verantwoordelijk blijven voor het vervullen van hun verplichtingen uit hoofde van het wetsvoorstel wanneer zij activiteiten aan derden uitbesteden. Artikel 3, 12°, omschrijft wat moet verstaan worden onder het begrip “uitbesteding”, met name een overeenkomst van om het even welke vorm tussen een systeemrelevante aanbieder en een dienstverrichter 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. Deze omschrijving is geïnspireerd op de gelijkluidende definitie in de richtsnoeren van de EBA inzake uitbesteding (EBA/GL/2019/02, 25 februari 2019).

Systeemrelevante aanbieders moeten de mogelijkheid hebben de exploitatie van hun diensten uit te besteden mits de risico’s die voortvloeien uit de uitbestedingsregelingen beheerd worden. De uitbesteding mag daarom de relatie en verplichtingen van de aanbieder ten opzichte van zijn klanten niet wijzigen, de naleving van de wettelijke vereisten niet ondermijnen en geen

d’importance systémique. Pourraient être considérées comme des décisions stratégiques, entre autres, les fusions d’un fournisseur d’importance systémique avec certaines autres institutions, le transfert total ou partiel d’activités du fournisseur, ou la scission de ses activités.

La Banque doit se prononcer 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 de satisfaire aux dispositions prévues par ou en vertu de la proposition de 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 la Banque n’intervient pas dans le délai fixé ci-dessus, l’autorisation est réputée acquise. La Banque peut également soumettre son autorisation à des conditions lorsque cela s’avère nécessaire pour garantir les objectifs susmentionnés.

CHAPITRE 6

Externalisation

Art. 40

Cet article prévoit, par analogie avec l’article 30 du règlement CSD, que les fournisseurs d’importance systémique restent pleinement responsables du respect des obligations qui leur incombent en vertu de la proposition de loi lorsqu’ils externalisent des activités à des tiers. L’article 3, 12°, définit ce qu’il faut entendre par le terme “externalisation”, à savoir un accord, de quelque forme que ce soit, conclu entre un fournisseur d’importance systémique et un prestataire de services, en vertu duquel ce prestataire de services prend en charge un processus, ou exécute un service ou une activité aux fins de permettre au fournisseur d’importance systémique la fourniture de services de messagerie financière, et qui autrement serait exécuté par ce fournisseur lui-même Cette description s’inspire de la définition similaire figurant dans les orientations de l’ABE relatives à l’externalisation (EBA/GL/2019/02, 25 février 2019).

Les fournisseurs d’importance systémique doivent avoir la possibilité d’externaliser l’exploitation de leurs services, à condition que les risques découlant des accords d’externalisation soient gérés. L’externalisation ne peut donc pas modifier la relation et les obligations du fournisseur vis-à-vis de ses clients, ni altérer le respect des exigences réglementaires; elle ne peut

wezenlijke afbreuk doen aan de interne controle van de aanbieder en het externe toezicht door de Bank. De aanbieder moet directe toegang hebben tot de relevante informatie over de uitbestede diensten en ervoor zorgen dat de derde-dienstverrichter met de Bank samenwerkt wat het toezicht op de uitbestede activiteiten betreft. De systeemrelevante aanbieder moet in een schriftelijke overeenkomst zijn rechten en verplichtingen bepalen en die van de derde-dienstverrichter.

Art. 41

Dit artikel bepaalt, naar analogie van artikel 10 van de wet van 24 maart 2017, dat systeemrelevante aanbieders kritieke of belangrijke functies enkel kunnen uitbesteden na voorafgaande toestemming van de Bank. Artikel 3, 13°, definieert het begrip “kritieke of belangrijke functie”. Het betreft iedere 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 financiële transacties, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door een systeemrelevante aanbieder van de verplichtingen uit hoofde van het wetsvoorstel.

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 daarenboven aan bijkomende voorwaarden onderwerpen. Het betreft hier geen algemeen regelgevend optreden vanwege de Bank doch wel een ad hoc beslissing in een specifiek uitbestedingsdossier.

Art. 42

Dit artikel bepaalt dat de Bank bij reglement de elementen bedoeld in de artikelen 40 en 41 kan preciseren en aanvullen.

nuire sérieusement à la qualité du contrôle interne du fournisseur, ni à la surveillance externe exercée par la Banque. Le fournisseur doit avoir un accès direct aux informations pertinentes concernant les services externalisés et s’assurer que le prestataire de services tiers coopère avec la Banque en ce qui concerne la surveillance des activités externalisées. Le fournisseur d’importance systémique doit définir par un accord écrit ses droits et obligations et ceux du prestataire de services tiers.

Art. 41

Cet article prévoit, par analogie avec l’article 10 de la loi du 24 mars 2017, que les fournisseurs d’importance systémique ne peuvent externaliser des tâches opérationnelles importantes relatives aux services de messagerie financière à un prestataire de services qu’avec l’autorisation préalable de la Banque. L’article 3, 13°, définit la notion de “fonction critique ou importante”. Il s’agit de toute fonction dont la perturbation est susceptible de nuire sérieusement aux performances financières 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 nationales ou internationales, ou dont une interruption, une anomalie ou une 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 proposition de loi.

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 tâches opérationnelles importantes à des conditions additionnelles. Il ne s’agit pas ici d’une intervention réglementaire générale de la part de la Banque, mais d’une décision *ad hoc* dans un dossier d’externalisation spécifique.

Art. 42

Cet article prévoit que la Banque peut, par voie de règlement, préciser et compléter les éléments visés aux articles 40 et 41.

HOOFDSTUK 7

Bedrijfsvoering en risicobeheersing

Hoofdstuk 7 bevat belangrijke verwachtingen ten aanzien van systeemrelevante aanbieders op het vlak van bedrijfsvoering en risicobeheersing. De formulering van deze verwachtingen is, in tegenstelling tot de meeste bepalingen van de voorgaande hoofdstukken, rechtstreeks ontleend aan de PFMI.

Zoals nader uitgelegd in de algemene toelichting, hebben de indieners alle PFMI-principes die relevant zijn voor systeemrelevante aanbieders geïdentificeerd en geconsolideerd in het juridisch bindend kader van het voorliggend wetsvoorstel. PFMI-principes die niet relevant geacht worden gelet op de aard van de activiteiten of risico's van aanbieders van financiële berichtendiensten, werden uiteraard niet opgenomen in hoofdstuk 7. Het betreft onder meer de PFMI-principes die betrekking hebben op onderpand (principe 5, collateral), het definitieve karakter van de afwikkeling van transacties (principe 8, *settlement finality*), levering van fysieke instrumenten (principe 10, *physical deliveries*) en de werking van centrale effectenbewaarinstellingen en waarde-uitwisselingssystemen (principes 11 en 12). Waar het *oversight* op systeemrelevante aanbieders traditioneel enkel berust op een toetsing van de werking van die aanbieders aan de *oversight*verwachtingen zoals neergelegd in Annex F bij de PFMI, strekt hoofdstuk 7 van het wetsvoorstel er aldus toe om alle voor systeemrelevante aanbieders relevant geachte PFMI als dusdanig van toepassing te verklaren op die aanbieders.

De PFMI zijn de uitdrukking van bepaalde verwachtingen ten aanzien van financiële marktinfrastructuren die als dusdanig en bij gebreke van een specifieke wettelijke basis niet juridisch afdwingbaar zijn. De overgang naar een juridisch afdwingbaar kader vergt een aantal aanpassingen in de formulering van deze verwachtingen. Bij de redactie van hoofdstuk 7 van het wetsvoorstel hebben de indieners dan ook in belangrijke mate gesteund op de bewoordingen van de SIPS-verordening. Voor de implementatie van een beperkt aantal PFMI werd evenwel steun gevonden in andere wetgevende teksten, in het bijzonder de CSD-verordening. Tot slot bevat hoofdstuk 7 zeer specifieke vereisten op het vlak van digitale operationele weerbaarheid, die rechtstreeks ontleend zijn aan de bepalingen van de DORA-verordening.

CHAPITRE 7

Conduite des activités et gestion des risques

Le chapitre 7 contient des attentes essentielles vis-à-vis des fournisseurs d'importance systémique sur le plan des activités et de la gestion des risques. Contrairement à la plupart des dispositions des chapitres précédents, la formulation de ces attentes est directement empruntée aux PIMF.

Comme expliqué dans l'exposé général, les déposants ont identifié et consolidé tous les PIMF pertinents pour les fournisseurs d'importance systémique dans le cadre juridiquement contraignant de la présente proposition de loi. Les PIMF qui ne sont pas considérés comme pertinents compte tenu de la nature des activités ou des risques des fournisseurs de services de messagerie financière n'ont bien entendu pas été inclus dans le chapitre 7. Il s'agit notamment des PIMF relatifs aux garanties (principe 5, garanties), au caractère définitif du règlement des transactions (principe 8, *settlement finality*), à la livraison d'instruments physiques (principe 10, livraisons physiques) et au fonctionnement des dépositaires centraux de titres et des systèmes d'échange de valeurs (principes 11 et 12). Alors que la surveillance des fournisseurs d'importance systémique ne repose traditionnellement que sur un examen du fonctionnement de ces fournisseurs au regard des attentes en matière de surveillance énoncées à l'annexe F des PIMF, le chapitre 7 de la proposition de loi vise à déclarer tous les PIMF jugés pertinents pour les fournisseurs d'importance systémique applicables à ces fournisseurs.

Les PIMF sont l'expression de certaines attentes à l'égard des infrastructures des marchés financiers qui, en tant que telles et en l'absence d'une base juridique spécifique, ne sont pas juridiquement exécutoires. Le passage à un cadre juridiquement contraignant nécessite quelques ajustements dans la formulation de ces attentes. Ainsi, en rédigeant l'article 7 de la proposition de loi, les déposants se sont largement appuyés sur la formulation du règlement SIPS. Toutefois, la mise en œuvre d'un nombre limité de PIMF s'est également appuyée sur d'autres textes législatifs, en particulier le règlement CSD. Enfin, le chapitre 7 contient des exigences très spécifiques en matière de résilience opérationnelle numérique, qui sont directement empruntées aux dispositions du règlement DORA.

Afdeling I

Algemene bepalingen

Art. 43

Artikel 43 bevat, samen met de artikelen 44 en 45, een aantal bepalingen die op algemene wijze betrekking hebben op de verwachtingen ten aanzien van systeemrelevante aanbieders op het vlak van bedrijfsvoering en risicobeheersing. Aldus bepaalt dit artikel, naar analogie van artikel 32 van de CSD-verordening, dat systeemrelevante aanbieders welomschreven doelstellingen moeten hebben die haalbaar zijn, onder meer op het gebied van minimumdienstniveaus, risicomanagementverwachtingen en zakelijke prioriteiten.

Art. 44

Dit artikel herneemt kernbepaling 1 van PFMI-principe 15. Het bepaalt op algemene wijze, en dit naar analogie van artikel 13, lid 1, van de SIPS-verordening, dat systeemrelevante aanbieders voor solide beheers- en controlesystemen moet zorgen voor het vaststellen, bewaken en beheren van algemene bedrijfsrisico's.

Art. 45

Dit artikel bevestigt dat de Bank bij reglement kan preciseren en aanvullen wat dient verstaan te worden onder elk van de vereisten van hoofdstuk 7, met inbegrip van de vereisten op het vlak van digitale operationele weerbaarheid. Er wordt voor geopteerd om deze mogelijkheid één enkele keer te vermelden voor het gehele hoofdstuk 7, in plaats van voor elk artikel afzonderlijk. Het is immers van belang dat de Bank haar verwachtingen inzake de toepassing van hoofdstuk 7 nader kan preciseren, aangezien sommige bepalingen eerder algemeen geformuleerd zijn en andere baat kunnen hebben bij nadere technische preciseringen.

Afdeling II

Juridische risico's

Art. 46

Dit artikel herneemt de kernbepalingen 2, 4 en 5, van PFMI-principe 1, wat de beheersing van juridische risico's betreft (zie ook artikel 3, leden 2, 4 en 5 van de SIPS-verordening). Voor een algemene toelichting bij het

Section Ire

Dispositions générales

Art. 43

L'article 43, ainsi que les articles 44 et 45, contiennent un certain nombre de dispositions qui se rapportent de manière générale aux attentes à l'égard des fournisseurs d'importance systémique sur le plan des activités et de la gestion des risques. Ainsi, par analogie avec l'article 32 du règlement CSD, cet article dispose que les fournisseurs d'importance systémique doivent avoir 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

Cet article reprend la considération essentielle 1 du principe 15 des PIMF. Par analogie avec l'article 13, paragraphe 1, du règlement SIPS, il prévoit de manière générale que les fournisseurs d'importance systémique doivent établir des systèmes de gestion et de contrôle solides afin d'identifier, de surveiller et de gérer les risques d'activité.

Art. 45

Cet article confirme que la Banque peut, par voie de règlement, préciser et compléter ce qu'il y a lieu d'entendre par chacune des exigences du chapitre 7, y compris celles relatives à la résilience opérationnelle numérique. L'option retenue est de mentionner cette possibilité une seule fois pour l'ensemble du chapitre 7, plutôt que pour chaque article séparément. En effet, il est important que la Banque puisse préciser plus avant ses attentes concernant l'application du chapitre 7, étant donné que certaines dispositions sont formulées de manière plutôt générale et que d'autres pourraient bénéficier de clarifications techniques supplémentaires.

Section II

Risque juridique

Art. 46

Cet article reprend les considérations essentielles 2, 4 et 5 du principe 1 des PIMF, concernant la maîtrise des risques juridiques (cf. également l'article 3, paragraphes 2, 4 et 5, du règlement SIPS). Pour un commentaire général

belang van een robuuste juridische basis in het kader van risicobeheer, zij verwezen naar paragraaf 3.1.1 van de PFMI.

Afdeling III

Integraal risicobeheerskader

Art. 47

Dit artikel herneemt alle kernbepalingen van PFMI-principe 3, wat het opzetten van een integraal risicobeheerskader betreft (zie ook artikel 5 van de SIPS-verordening). Het risicobeheerskader is gericht op het identificeren, meten, opvolgen en beheersen van de risico's die een systeemrelevante aanbieder kan lopen. Dit strekt zich ook uit tot het stimuleren van diens klanten om de risico's die zij vormen voor de verlening van financiële berichtendiensten te beheersen en beperken, evenals tot het toetsen van de risico's die de systeemrelevante aanbieder op zijn beurt mogelijks genereert voor andere entiteiten. Van belang daarbij is het identificeren van de kritieke bedrijfsactiviteiten en -diensten van de aanbieder en de mogelijkheden tot herstel of liquidatie ingeval die activiteiten of diensten niet kunnen geleverd worden. Voor een algemene toelichting bij het belang van een integraal risicobeheerskader zij verwezen naar paragraaf 3.3.1 van de PFMI.

Afdeling IV

Herstel en ordelijke liquidatie

Art. 48

Paragraaf 1 van dit artikel herneemt een deel van PFMI-principe 3, met name wat de verplichting betreft om een uitvoerbaar herstelplan of een ordelijke liquidatieplan op te stellen (zie ook een deel van artikel 5, lid 4, van de SIPS-verordening). Het werd logischer geacht om deze bepaling onder te brengen in afdeling IV aangezien die afdeling integraal betrekking heeft op de verwachtingen inzake herstel en ordelijke liquidatie van systeemrelevante aanbieders.

De overige paragrafen van dit artikel hernemen de kernbepalingen 2, 3 en 4 van PFMI-principe 15 (zie ook artikel 13, leden 3, 4 en 5, van de SIPS-verordening). Systeemrelevante aanbieders moeten voldoende activa (minstens het equivalent van de exploitatiekosten over zes maanden) aanhouden om in voorkomend geval een herstel of ordelijke liquidatie tot stand te kunnen brengen van hun kritieke activiteiten en diensten. Dit bedrag

concernant l'importance d'une base juridique solide dans le cadre de la gestion des risques, l'on se référera au paragraphe 3.1.1 des PIFM.

Section III

Cadre de gestion global des risques

Art. 47

Cet article reprend toutes les considérations essentielles du principe 3 des PIMF, concernant la mise en place d'un cadre de gestion global des risques (cf. également l'article 5 du règlement SIPS). Le cadre de gestion des risques vise à identifier, mesurer, suivre et maîtriser les risques auxquels un fournisseur d'importance systémique est susceptible d'être exposé. Il vise également à encourager les clients de ce dernier à gérer et à contenir les risques qu'ils font courir à la fourniture de services de messagerie financière, ainsi qu'à examiner les risques que le fournisseur d'importance systémique peut à son tour éventuellement générer pour d'autres entités. Il importe dans ce cadre d'identifier les opérations et services critiques du fournisseur et les possibilités de redressement ou de liquidation au cas où ces activités ou ces services ne pourraient pas être fournis. Pour un commentaire général concernant l'importance d'un cadre de gestion global des risques, l'on se référera à la section 3.3.1 des PIFM.

Section IV

Redressement et liquidation ordonnée

Art. 48

Le paragraphe 1er de cet article reprend une partie du principe 3 des PIFM, en particulier en ce qui concerne l'obligation d'élaborer un plan viable de redressement ou de liquidation ordonnée (cf. également une partie de l'article 5, paragraphe 4, du règlement SIPS). Il a été jugé plus logique d'intégrer cette disposition à la section IV, étant donné que cette section porte intégralement sur les attentes en matière de redressement et de liquidation ordonnée de fournisseurs d'importance systémique.

Les autres paragraphes de cet article reprennent les dispositions essentielles 2, 3 et 4 du principe 15 des PIMF (cf. également l'article 13, paragraphes 3, 4 et 5, du règlement SIPS). Les fournisseurs d'importance systémique doivent détenir suffisamment d'actifs (cela doit représenter au moins six mois de charges d'exploitation courantes) pour pouvoir, le cas échéant, procéder à un redressement ou une liquidation ordonnée de leurs

moet afgedekt worden door liquide, tijdig beschikbare en kwalitatieve netto-activa zoals aandelen, reserves en ingehouden winsten. De paragrafen 3.15.5 tot 3.15.8 van de PFMI verstrekken nadere toelichting bij het vereiste om voldoende liquide netto-activa aan te houden.

Afdeling V

Beleggingsrisico's

Art. 49

Dit artikel herneemt kernbepaling 4 van PFMI-principe 16, inzake de beheersing van beleggingsrisico's van systeemrelevante aanbieders (zie ook artikel 14, leden 4 en 5, van de SIPS-verordening). De investeringsstrategie van systeemrelevante aanbieders moet consistent zijn met hun algemene risicobeheerstrategie en gedekt door debiteuren van hoge kwaliteit of vorderingen op hen.

Afdeling VI

Operationeel risico

Art. 50

Dit artikel herneemt de kernbepalingen 1, 2, 3, 5 en 7 van PFMI-principe 17, inzake de beheersing van operationele risico's van systeemrelevante aanbieders (zie ook artikel 15, leden 1, 1 *bis*, 2, 4, 6 en 7, van de SIPS-verordening). Systeemrelevante aanbieders dienen een solide kader op te zetten met toepasselijke systemen, beleidslijnen, procedures en controles voor het vaststellen, bewaken en beheren van hun exploitatierisico's, en identificeren wie hun kritieke dienstafnemers zijn. Zij dienen eveneens een beleid op te zetten met betrekking tot de fysieke veiligheid en beveiliging, beschikbaarheid, confidentialiteit, authenticiteit en integriteit van informatie. Dit artikel behoeft voor het overige geen nadere toelichting.

activités et services critiques. Ce montant doit être couvert par des actifs nets liquides, de qualité et disponibles en temps utile, tels que des actions, des réserves et des bénéfices non distribués. Les paragraphes 3.15.5 à 3.15.8 des PIFM fournissent de plus amples explications sur l'obligation de détenir suffisamment d'actifs nets liquides.

Section V

Risques d'investissement

Art. 49

Cet article reprend la considération essentielle 4 du principe 16 des PIMF, concernant la maîtrise des risques d'investissement des fournisseurs d'importance systémique (cf. également l'article 14, paragraphes 4 et 5, du règlement SIPS). La stratégie d'investissement des fournisseurs d'importance systémique doit être compatible avec leur stratégie globale de gestion du risque et les placements qu'ils effectuent doivent être garantis par, ou être des créances sur, des débiteurs de haute qualité.

Section VI

Risque opérationnel

Art. 50

Cet article reprend les considérations essentielles 1, 2, 3, 5 et 7 du principe 17 des PIMF, concernant la maîtrise des risques opérationnels des fournisseurs d'importance systémique (cf. également l'article 15, paragraphes 1, 1 *bis*, 2, 4, 6 et 7, du règlement SIPS). Les fournisseurs d'importance systémique doivent mettre en place un cadre solide, doté de systèmes, de politiques, de procédures et de contrôles appropriés pour identifier, surveiller et gérer les risques opérationnels, et identifier leurs acheteurs de services critiques. Ils doivent également disposer de politiques en termes de sécurité physique et de sécurité, disponibilité, confidentialité, authenticité et intégrité de l'information. Pour le reste, cet article n'appelle pas de commentaires.

Afdeling VII

Bedrijfscontinuïteit en beschikbaarheid van de dienstverlening

Art. 51

Dit artikel herneemt de kernbepalingen 4 en 6 van PFMI-principe 17 (zie ook artikel 15, leden 4 en 6 van de SIPS-verordening). Gelet op hun belang werd ervoor geopteerd om de bepalingen inzake bedrijfscontinuïteit en beschikbaarheid van de dienstverlening onder te brengen in een afzonderlijke afdeling van hoofdstuk 7, ook al sluiten zij aan bij de beheersing van operationele risico's zoals geregeld in de voorgaande afdeling.

Systeemrelevante aanbieders dienen een bedrijfscontinuïteitsplan op te stellen dat streeft naar een snel en zo spoedig mogelijk herstel van de activiteiten in geval van een verstoring in het verstrekken van financiële berichtendiensten. Het plan moet ten minste jaarlijks getest worden, in voorkomend geval samen met dienstafnemers en aanbieders van kritieke ICT-diensten. Systeemrelevante aanbieders moeten hun capaciteit voor het verlenen van financiële berichtendiensten steeds kunnen uitbreiden in geval van toename van de te behandelen volumes ingevolge stress-evenementen.

Kernbepaling 6 van PFMI-principe 17 vermeldt dat het bedrijfscontinuïteitsplan zodanig moet opgesteld zijn dat kritieke activiteiten kunnen hervat worden binnen een periode van twee uur nadat een incident zich heeft voorgedaan (het zogenaamde *2 hours recovery time objective* of 2hRTO). Er wordt voor geopteerd om deze doelstelling als dusdanig niet te vermelden in het wetsvoorstel en om het aan de Bank over te laten om het *recovery time objective* voor systeemrelevante aanbieders nader te bepalen bij reglement. Dat laat de Bank toe om een meer granulaire benadering te volgen en om in voorkomend geval verschillende RTO's voor te schrijven, bijv. in functie van de aard van de geïmpacteerde dienstverlening en de ernst van het incident. Dit belet echter niet dat systeemrelevante aanbieders de 2hRTO als maatstaf kunnen hanteren bij het opstellen van hun bedrijfscontinuïteitsplan.

Section VII

Continuité d'activité et disponibilité des services

Art. 51

Cet article reprend les considérations essentielles 4 et 6 du principe 17 des PIMF (cf. également l'article 15, paragraphes 4 et 6, du règlement SIPS). Compte tenu de leur importance, il a été décidé de regrouper les dispositions relatives à la continuité des activités et à la disponibilité des services dans une section distincte du chapitre 7, même si elles se rattachent à la maîtrise des risques opérationnels telle qu'elle est traitée dans la section précédente.

Les fournisseurs d'importance systémique doivent établir un plan de continuité des activités qui tend vers une reprise la plus rapide possible des activités en cas de perturbation de la fourniture de services de messagerie financière. Le plan doit être testé au moins une fois par an, avec, le cas échéant, la participation des acheteurs de services ainsi que des fournisseurs de services TIC critiques. Les fournisseurs d'importance systémique doivent à tout moment être en mesure d'étendre leur capacité à fournir des services de messagerie financière en cas d'augmentation des volumes à traiter en raison d'événements de crise.

La considération essentielle 6 du principe 17 des PIMF mentionne que le plan de continuité des activités doit être établi de telle sorte que les activités critiques peuvent être redémarrées dans une période de deux heures après qu'un incident s'est produit (ce que l'on appelle le "*2 hours recovery time objective*" ou 2hRTO). L'option retenue est de ne pas mentionner cet objectif en tant que tel dans la proposition de loi et de laisser à la Banque le soin de définir, par voie de règlement, l'objectif de temps de redémarrage (*recovery time objective* ou RTO) pour les fournisseurs d'importance systémique. Cela permet à la Banque d'adopter une approche plus granulaire et d'imposer, le cas échéant, différents RTO, par exemple en fonction de la nature de la prestation de service touchée et de la gravité de l'incident. Cela n'empêche toutefois pas les fournisseurs d'importance systémique de pouvoir utiliser le 2hRTO comme norme lors de la préparation de leur plan de continuité des activités.

Afdeling VIII

Digitale operationele weerbaarheid

De PFMI bevatten oorspronkelijk een beperkt aantal bepalingen die specifiek betrekking hebben op het beheersen van cyberrisico's door financiële marktinfrastructuren. Gelet op de voortschrijdende digitalisering en de noodzaak om cyberrisico's beter te beheersen, vaardigden CPMI en IOSCO in juni 2016 nadere richtsnoeren uit inzake cyberweerbaarheid voor financiële marktinfrastructuren (*Guidance on Cyber Resilience for Financial Market Infrastructures*). Sindsdien maken die richtsnoeren een vast onderdeel uit van het arsenaal van bepalingen op basis waarvan de Bank haar *oversight* uitoefent, inclusief op aanbieders van financiële berichtendiensten.

De indieners wensen de essentiële elementen van de CPMI-IOSCO *Cyber Guidance* eveneens binnen het bestek van het voorliggend wetsvoorstel te brengen, maar stellen vast dat een één-op-één vertaling van die richtsnoeren naar een juridisch bindende context niet evident is gelet op de techniek van de *moral suasion* die aan de grondslag ligt van de betrokken richtsnoeren. Er bestaat evenwel een recent precedent dat de principes van de *Cyber Guidence* vertaalt naar een juridisch bindende context, met name de hierboven reeds vermelde DORA-verordening. Die verordening bevat een uitgebreid en gedetailleerd kader dat erop gericht is de digitale operationele weerbaarheid van financiële entiteiten te versterken. Systeemrelevante aanbieders vallen in principe niet binnen het toepassingsgebied van de DORA-verordening, met name omdat zij geen financiële entiteiten zijn in de zin van die verordening of er anderszins van uitgesloten zijn. Er werd geanalyseerd welke van de vele bepalingen van de DORA-verordening relevant zijn voor systeemrelevante aanbieders, in het bijzonder rekening houdend met de CPMI-IOSCO *Cyber Guidance*. Het resultaat van die oefening vindt zijn weerslag in afdeling VIII van hoofdstuk 7 van het voorliggend wetsvoorstel.

Er zij voor het overige op gewezen dat diverse bepalingen van de DORA-verordening nader uitgewerkt zijn in gedelegeerde handelingen en technische uitvoeringsnormen van de Commissie die gebaseerd zijn op door de Europese Toezichthoudende Autoriteiten ontwikkelde technische reguleringsnormen. Het spreekt voor zich dat de Bank zich in voorkomend geval kan inspireren op die uitvoeringshandelingen wanneer zij haar verwachtingen inzake de naleving van afdeling VIII nader verduidelijkt.

Section VIII

Résilience opérationnelle numérique

Les PIMF comportent à l'origine un nombre limité de dispositions traitant spécifiquement de la gestion des cyber-risques par les infrastructures de marchés financiers. Compte tenu de la numérisation croissante et de la nécessité de mieux gérer les cyber-risques, le CPIM et l'OICV ont publié en juin 2016 des orientations supplémentaires relatives à la cyber-résilience des infrastructures de marchés financiers (*Guidance on Cyber Resilience for Financial Market Infrastructures*). Depuis lors, ces orientations font partie intégrante de l'arsenal de dispositions en vertu desquelles la Banque exerce sa surveillance, y compris sur les fournisseurs de services de messagerie financière.

Les déposants souhaitent également intégrer les éléments essentiels des orientations relatives à la cyber-résilience CPIM-OICV dans le champ d'application de la présente proposition de loi, mais notent qu'une traduction article par article de ces orientations dans un contexte juridiquement contraignant n'est pas évidente étant donné la technique du principe de la force de persuasion morale (*moral suasion*) qui sous-tend les orientations en question. Il existe toutefois un précédent récent qui traduit les principes de la cyber-résilience dans un contexte juridiquement contraignant, à savoir le règlement DORA susmentionné. Ce règlement comporte un cadre complet et détaillé visant à renforcer la résilience opérationnelle numérique des entités financières. Les fournisseurs d'importance systémique ne relèvent en principe pas du champ d'application du règlement DORA, notamment parce qu'ils ne sont pas des entités financières au sens de ce règlement ou qu'ils en sont exclus d'une autre manière. Dans les nombreuses dispositions du règlement DORA, on a analysé lesquelles sont pertinentes pour les fournisseurs d'importance systémique, en tenant compte en particulier des orientations relatives à la cyber-résilience CIPM-OICV. Le résultat de cet exercice se reflète dans la section VIII du chapitre 7 de cette proposition de loi.

Il convient également de noter que plusieurs dispositions du règlement DORA sont détaillées dans des actes délégués et des normes techniques d'exécution de la Commission, qui sont basés sur des normes techniques réglementaires élaborées par les Autorités européennes de surveillance. Il va sans dire que la Banque peut, le cas échéant, s'inspirer de ces actes d'exécution pour préciser ses attentes en matière de respect de la section VIII.

Art. 52

Dit artikel bepaalt op algemene wijze en naar analogie van artikel 5 van de DORA-verordening (en tevens rekening houdend met het bepaalde in artikel 15, lid 4 *bis* van de SIPS-verordening) dat systeemrelevante aanbieders een effectief kader moeten opzetten voor het beheer van het ICT-risico met passende governancemaatregelen teneinde een hoog niveau van digitale operationele weerbaarheid te verkrijgen. Zij moeten alle activiteiten en onderliggende activa identificeren en passende maatregelen treffen om ze te beschermen tegen cyberaanvallen, deze op te sporen, erop te reageren en ervan te herstellen. Paragraaf 2 van het artikel beschrijft wat de verantwoordelijkheden van de raad van toezicht zijn op dit vlak, vaak met verwijzing naar de nadere bepalingen van afdeling VIII. Van de leden van de raad van toezicht wordt dan ook verwacht dat zij actief voldoende kennis en vaardigheden onderhouden om het ICT-risico en de gevolgen daarvan voor de verrichtingen van de systeemrelevante aanbieder te begrijpen en te beoordelen.

Art. 53

Dit artikel schrijft voor dat systeemrelevante aanbieders moeten beschikken over een passende functie van beveiliging van de netwerk- en informatiesystemen. Deze zogenaamde CISO-functie (*Chief Information Security Officer*) zorgt voor de ontwikkeling, implementatie en controle door de aanbieder van een beleid en procedures die een passende beveiliging bieden van de netwerk- en informatiesystemen en een passend beheer van de daaraan verbonden ICT-risico's.

De DORA-verordening schrijft momenteel niet voor dat financiële entiteiten een CISO-functie dienen in te voeren. De indieners achten het echter wenselijk om voor systeemrelevante aanbieders wel in die verplichting te voorzien. Die functie kan evenwel niet beschouwd worden als een onafhankelijke controlefunctie zoals de compliance-, interne audit- en risicobeheerfunctie (zie artikel 18). De Belgische en internationale financiële sector hanteren sinds lang het principe van de drie verdedigingslinies (*three lines of defence*) als referentie voor goed bestuur en risicobeheersing. De interne controlefuncties bevinden zich in de tweede (compliance en risicobeheer) en derde (interne audit) verdedigingslinie. De CISO-functie bevindt zich daarentegen op de grens tussen de eerste en tweede lijn, omdat diens taken activiteiten omvatten die zowel tot de eerste lijn (operationeel bedrijfsbeheer) als tot de tweede lijn kunnen behoren. De betrokken bepalingen worden daarom ook

Art. 52

Cet article prévoit, de manière générale et par analogie avec l'article 5 du règlement DORA (compte tenu également des dispositions de l'article 15, paragraphe 4 *bis*, du règlement SIPS), que les fournisseurs d'importance systémique doivent établir 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. Ils doivent identifier toutes les opérations et les actifs sous-jacents et instaurer des mesures adéquates afin de les protéger des cyberattaques, de réagir à celles-ci et de les surmonter. Le paragraphe 2 de l'article décrit les responsabilités du conseil de surveillance à cet égard, en renvoyant souvent aux dispositions détaillées de la section VIII. Les membres du conseil de surveillance sont donc censés maintenir 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.

Art. 53

Cet article exige que les fournisseurs d'importance systémique disposent d'une fonction de sécurité des réseaux et systèmes d'information adéquate. Cette fonction dite CISO (*Chief Information Security Officer*) assure le développement, la mise en œuvre et le contrôle, par le fournisseur, 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.

Le règlement DORA n'exige actuellement pas des entités financières qu'elles mettent en place une fonction de CISO. Les déposants estiment toutefois qu'il est souhaitable de prévoir une telle obligation pour les fournisseurs d'importance systémique. Cette fonction ne peut néanmoins pas être considérée comme une fonction de contrôle indépendante comme les fonctions de conformité (*compliance*), d'audit interne et de gestion des risques (cf. l'article 18). Les secteurs financiers belge et international utilisent depuis longtemps le principe des trois lignes de défense (*three lines of defence*) comme référence pour la bonne gouvernance et la gestion des risques. Les fonctions de contrôle interne se situent dans les deuxième (conformité et gestion des risques) et troisième (audit interne) lignes de défense. En revanche, la fonction de CISO se situe à la frontière entre la première et la deuxième ligne, car ses tâches comprennent des activités qui peuvent appartenir à la

opgenomen in afdeling VIII van hoofdstuk 7 en niet in afdeling IV van hoofdstuk 3.

Paragraaf 2 van het artikel bevat de nodige waarborgen om te verzekeren dat de CISO-functie zijn taken op voldoende onafhankelijke wijze kan uitoefenen. Aldus moet de CISO onafhankelijk zijn van de operationele functies, in het bijzonder van de diensten die verantwoordelijk zijn voor de exploitatie en de ontwikkeling van ICT-systemen, en mag deze niet betrokken zijn bij interne auditactiviteiten. Hij of zij moet voldoende gezag, status en middelen hebben en een gedegen kennis van logische en fysieke beveiligingsoplossingen in de context van de systeemrelevante aanbieder. Tot slot heeft de CISO rechtstreeks toegang tot de raad van toezicht en de directieraad. Zij brengen minstens tweemaal per jaar verslag uit aan de directieraad.

Art. 54

Dit artikel bepaalt, naar analogie van artikel 6, leden 1, 2, 5 en 8, van de DORA-verordening, dat systeemrelevante aanbieders een solide, alomvattend en goed gedocumenteerd kader voor ICT-risicobeheer moeten opstellen, als onderdeel van het integraal risicobeheerskader bedoeld in artikel 47. Paragraaf 2 beschrijft de inhoud die het kader voor ICT-risicobeheer minstens moet omvatten, terwijl paragraaf 3 voorschriften bevat inzake de documentatie en regelmatige evaluatie van dit kader. Het artikel behoeft voor het overige geen nadere toelichting.

Art. 55

Dit artikel bepaalt, naar analogie van artikel 7 van de DORA-verordening, dat systeemrelevante aanbieders geactualiseerde ICT-systemen, -protocollen en -instrumenten moeten gebruiken en onderhouden. Paragraaf 2 voegt hier, naar analogie van artikel 12, § 4, van de wet van 24 maart 2017, aan toe dat systeemrelevante aanbieders moeten beschikken over robuuste methodologieën teneinde te kunnen plannen voor de gehele levensloop van de gebruikte technologieën en de selectie van technologische standaarden.

Art. 56

Dit artikel bevat, naar analogie van artikel 8 van de DORA-verordening, voorschriften inzake de identificatie, classificatie en documentatie van alle door ICT ondersteunde bedrijfsfuncties, taken en verantwoordelijkheden,

fois à la première ligne (gestion opérationnelle) et à la deuxième ligne. Les dispositions en question sont donc également incluses dans la section VIII du chapitre 7 et non dans la section IV du chapitre 3.

Le paragraphe 2 de l'article contient les garanties nécessaires pour que le CISO puisse exercer ses missions de manière suffisamment indépendante. Ainsi, le CISO doit être indépendant des fonctions opérationnelles, notamment des services responsables de l'exploitation et du développement des systèmes ICT, et ne doit pas être impliqué dans les activités d'audit interne. Il doit disposer d'une autorité, d'un statut et de ressources suffisants et posséder une solide connaissance des solutions de sécurité logique et physique dans le contexte du fournisseur d'importance systémique. Enfin, le CISO a un accès direct au conseil de surveillance et au conseil de direction. Il fait rapport au conseil de direction au moins deux fois par an.

Art. 54

Par analogie avec l'article 6, paragraphes 1, 2, 5 et 8, du règlement DORA, cet article dispose que les fournisseurs d'importance systémique doivent établir un cadre de gestion du risque lié aux TIC solide, complet et bien documenté, dans le contexte de son cadre de gestion global des risques visé à l'article 47. Le paragraphe 2 décrit le contenu que le cadre de gestion du risque lié aux TIC doit au moins englober, tandis que le paragraphe 3 contient des règles relatives à la documentation et à l'examen régulier de ce cadre. Pour le reste, l'article n'appelle pas de commentaires.

Art. 55

Cet article dispose, par analogie avec l'article 7 du règlement DORA, que les fournisseurs d'importance systémique doivent utiliser et maintenir à jour les systèmes, protocoles et outils de TIC. Le paragraphe 2 ajoute, par analogie avec l'article 12, § 4, de la loi du 24 mars 2017, que les fournisseurs d'importance systémique doivent disposer de méthodologies robustes afin de pouvoir planifier l'ensemble de la durée de vie des technologies utilisées et la sélection de normes technologiques.

Art. 56

Cet article comporte, par analogie avec l'article 8 du règlement DORA, des exigences relatives à l'identification, à la classification et à la documentation de toutes les fonctions "métiers", tous les rôles et toutes

de informatie- en ICT-activa die deze functies ondersteunen, en hun taken en afhankelijkheden met betrekking tot ICT-risico's. Systeemrelevante aanbieders moeten de bronnen van ICT-risico, cyberdreigingen en ICT-kwetsbaarheden permanent identificeren en beoordelen. Zij moeten daarbij ook alle processen identificeren die afhankelijk zijn van derde aanbieders van ICT-diensten.

Art. 57

Dit artikel bevat de verplichting voor systeemrelevante aanbieders, naar analogie van artikel 9 van de DORA-verordening, om maatregelen te nemen ter bescherming van de ICT-systemen en -instrumenten. Zij moeten daartoe passende ICT-beveiligingsinstrumenten, -beleidslijnen en -procedures inzetten. Zij moeten onder meer ook een beleid ontwikkelen en documenteren 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. Het artikel behoeft voor het overige geen nadere toelichting.

Art. 58

Dit artikel bepaalt, naar analogie van artikel 10 van de DORA-verordening, dat systeemrelevante aanbieders moeten beschikken over mechanismen om afwijkende activiteiten zo spoedig mogelijk te detecteren. Die detectie dient rekening te houden met het bepaalde in artikel 65 inzake de detectie van incidenten. De detectiemechanismen moeten regelmatig getest worden.

Art. 59

Dit schrijft voor, naar analogie van artikel 11 van de DORA-verordening, dat systeemrelevante aanbieders een alomvattend maar specifiek ICT-bedrijfscontinuïteitsbeleid moeten voeren. Dit beleid maakt onderdeel uit van het ruimere beleid inzake bedrijfscontinuïteit als bedoeld in artikel 51 Het is onder meer gericht op het verzekeren van de continuïteit van de kritieke of belangrijke functies van de systeemrelevante aanbieder en op het bieden van een snelle, passende en doeltreffende respons en oplossing voor alle ICT-gerelateerde incidenten. Systeemrelevante aanbieders dienen daarom ook bijhorende ICT-respons- en herstelplannen in te voeren en een bedrijfsimpactanalyse uit te voeren van hun blootstelling

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. Les fournisseurs d'importance systémique doivent identifier et évaluer, de manière continue, toutes les sources de risque lié aux TIC, les cybermenaces et les vulnérabilités des TIC. Dans ce cadre, ils doivent également identifier tous les processus qui dépendent de prestataires tiers de services TIC.

Art. 57

Cet article contient, par analogie avec l'article 9 du règlement DORA, l'obligation pour les fournisseurs d'importance systémique de prendre des mesures pour protéger les systèmes et outils de TIC. Ils doivent à cette fin déployer des outils, des stratégies et des procédures appropriés en matière de sécurité des TIC. Ils doivent notamment élaborer et documenter 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. Pour le reste, l'article n'appelle pas de commentaires.

Art. 58

Cet article prévoit, par analogie avec l'article 10 du règlement DORA, que les fournisseurs d'importance systémique doivent disposer de mécanismes permettant de détecter rapidement les activités anormales. Cette détection doit tenir compte des dispositions de l'article 65 sur la détection des incidents. Les mécanismes de détection doivent être testés régulièrement.

Art. 59

Cet article exige, par analogie avec l'article 11 du règlement DORA, que les fournisseurs d'importance systémique se dotent d'une politique de continuité des activités de TIC complète mais spécifique. Cette politique s'inscrit dans le cadre plus large de la politique de continuité d'activité visée à l'article 51. Elle a notamment pour objectif de garantir la continuité des fonctions critiques ou importantes du fournisseur d'importance systémique, ainsi que de répondre aux incidents liés aux TIC et de les résoudre rapidement, dûment et efficacement. Les fournisseurs d'importance systémique doivent dès lors également mettre en œuvre des plans de réponse et de rétablissement des TIC et procéder à une analyse

aan ernstige verstoringen van de bedrijfsactiviteiten. Het artikel behoeft voor het overige geen nadere toelichting.

Art. 60

Dit artikel bevat de verplichting, naar analogie van artikel 12 van de DORA-verordening, om een back-upbeleid en back-upprocedures te ontwikkelen evenals procedures en methoden voor terugzetting en herstel. Dat beleid en die procedures zijn erop gericht het terugzetten van ICT-systemen en gegevens te verzekeren met een minimale uitval en een beperkte verstoring en beperkt verlies. Systeemrelevante aanbieders moeten in het licht daarvan minstens één secundaire verwerkingslocatie handhaven. Het artikel behoeft voor het overige geen nadere toelichting.

Art. 61

Dit artikel bepaalt, naar analogie van artikel 13 van de DORA-verordening, dat systeemrelevante aanbieders moeten beschikken over capaciteiten en personele middelen om informatie te verzamelen over kwetsbaarheden en cyberdreigingen, ICT-gerelateerde incidenten en om de waarschijnlijke gevolgen ervan voor hun digitale operationele weerbaarheid te analyseren. Zij verrichten ICT-gerelateerde post-incidentevaluaties na verstoringen van hun kernactiviteiten ten gevolge van een ICT-gerelateerd incident. Systeemrelevante aanbieders moeten ook bewustmakingsprogramma's ontwikkelen op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele weerbaarheid als verplichte modules in de opleidingsprogramma's voor het personeel, en moeten op de hoogte blijven van relevante technologische ontwikkelingen.

Art. 62

Dit artikel bevat, naar analogie van artikel 14 van de DORA-verordening, voorschriften inzake de communicatie in geval van ICT-gerelateerde incidenten of kwetsbaarheden en inzake een communicatiebeleid naar het personeel en externe partijen toe.

Art. 63

Dit artikel bevat, naar analogie van artikel 24 van de DORA-verordening, algemene vereisten voor de uitvoering van tests van de digitale operationele weerbaarheid van systeemrelevante aanbieders. Het testprogramma

des incidences sur les activités de leurs expositions à de graves perturbations de leurs activités. Pour le reste, l'article n'appelle pas de commentaires.

Art. 60

Cet article contient, par analogie avec l'article 12 du règlement DORA, l'obligation de définir des politiques et procédures de sauvegarde ainsi que des procédures et méthodes de restauration et de rétablissement. Ces politiques et procédures visent à garantir la restauration des systèmes et des données TIC en limitant au maximum la durée d'indisponibilité, les perturbations et les pertes. Les fournisseurs d'importance systémique doivent donc maintenir au moins un site de traitement secondaire. Pour le reste, l'article n'appelle pas de commentaires.

Art. 61

Cet article prévoit, par analogie avec l'article 13 du règlement DORA, que les fournisseurs d'importance systémique doivent disposer 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. Ils réalisent des examens post-incident lié aux TIC après qu'un incident majeur lié aux TIC a perturbé leurs activités principales. Les fournisseurs d'importance systémique doivent également élaborer des programmes de sensibilisation à la sécurité des TIC et des formations à la résilience opérationnelle numérique qu'ils intègrent à leurs programmes de formation du personnel sous la forme de modules obligatoires. Ils doivent se tenir informés des évolutions technologiques pertinentes.

Art. 62

Par analogie avec l'article 14 du règlement DORA, cet article contient des prescriptions relatives à la communication en cas d'incidents liés aux TIC ou de vulnérabilités ainsi que concernant une politique de communication à l'intention des membres du personnel et des parties prenantes externes.

Art. 63

Par analogie avec l'article 24 du règlement DORA, cet article définit les exigences générales pour la réalisation de tests de résilience opérationnelle numérique des fournisseurs d'importance systémique. Le programme

van systeemrelevante aanbieders moet gericht zijn op 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. Het artikel behoeft voor het overige geen nadere toelichting.

Art. 64

Dit artikel concretiseert, naar analogie van artikel 25, lid 1 van de DORA-verordening, de vereisten van artikel 63. Het schrijft voor dat het testprogramma voor digitale operationele weerbaarheid moet voorzien 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

Dit artikel bepaalt, naar analogie van artikel 26 van de DORA-verordening, dat systeemrelevante aanbieders ten minste om de drie jaar geavanceerde tests moeten uitvoeren door middel van TLPT. Onder TLPT (*threat led penetration testing* of dreigingsgestuurde penetratietests) verstaat men het geheel van technieken en procedures waarbij levensechte, als een reële cyberdreiging ervaren dreigingsactoren worden nagebootst en waarin een gecontroleerde test wordt uitgevoerd van de kritieke reëel bestaande productiesystemen van een systeemrelevante aanbieder (zie definitie in artikel 3, 25°). TLPT heeft betrekking op kritieke of belangrijke functies. Derde aanbieders van ICT-diensten dienen in voorkomend geval deel te nemen aan de TLPT.

De Bank is als Belgische autoriteit verantwoordelijk voor TLPT-gerelateerde aangelegenheden in de financiële sector en zal in principe dus ook betrokken zijn bij de uitvoering van TLPT ten aanzien van systeemrelevante aanbieders. Die tests zijn momenteel gebaseerd op het TIBER-EU-kader dat de Europese Centrale Bank heeft goedgekeurd, maar kunnen in de toekomst eventueel ook gebaseerd zijn op de technische reguleringsnorm die de Europese Toezichthoudende Autoriteiten dienen uit te werken op grond van artikel 26, lid 11, van de DORA-verordening. Meer toelichting over TLPT tests is

de test des fournisseurs d'importance systémique doit porter sur l'évaluation de l'état de préparation en ce qui concerne la gestion d'incidents liés aux TIC, sur l'identification de faiblesses, de déficiences et de lacunes au niveau de la résilience opérationnelle numérique, et sur la mise en œuvre rapide de mesures correctives. L'article n'appelle pas de commentaires.

Art. 64

Par analogie avec l'article 25, paragraphe 1, du règlement DORA, cet article concrétise les exigences de l'article 63. Il dispose que le programme de tests de résilience opérationnelle numérique doit prévoir 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

Par analogie avec l'article 26 du règlement DORA, cet article stipule que les fournisseurs d'importance systémique doivent effectuer au moins tous les trois ans des tests avancés au moyen d'un test de pénétration fondé sur la menace (TLPT, ou *threat-led penetration testing*). TLPT désigne l'ensemble des techniques et procédures imitant des acteurs de la menace réels perçus comme représentant une véritable cybermenace, qui permettent de tester de manière contrôlée les systèmes critiques en environnement de production du fournisseur d'importance systémique (cf. la définition de l'article 3, 25°). TLPT se rapporte à des fonctions critiques ou importantes. Les fournisseurs tiers de services TIC doivent prendre part au TLPT le cas échéant.

En qualité d'autorité belge, la Banque est responsable des matières liées au TLPT dans le secteur financier et sera donc, en principe, également impliquée dans la mise en œuvre du TLPT portant sur les fournisseurs d'importance systémique. Ces tests sont actuellement fondés sur le cadre TIBER-UE adopté par la Banque centrale européenne, mais pourraient à l'avenir reposer également sur la norme technique réglementaire qui doit être élaborée par les autorités européennes de surveillance en vertu de l'article 26, paragraphe 11, du règlement DORA. De plus amples explications sur les

terug te vinden op de website van de Bank (*https://www.nbb.be/nl/betalingen-en-effecten/tiber-be-framework).*

Afdeling IX

Beheer, classificatie en melding van incidenten

Art. 66

Dit artikel verplicht systeemrelevante aanbieders tot het vastleggen en tenuitvoerleggen van een incidentbeheerproces dat gericht is op het detecteren, beheren en melden van incidenten. Zij dienen daartoe alle incidenten en ernstige cyberdreigingen te monitoren en registreren en ervoor te zorgen dat onderliggende oorzaken worden opgespoord, gedocumenteerd en weggenomen om dergelijke incidenten te voorkomen.

Het artikel is gebaseerd op artikel 17, leden 1 en 2, van de DORA-verordening maar wordt van toepassing verklaard op het beheer, de classificatie en de rapportage van alle incident en dus niet alleen op ICT-gerelateerde incidenten. Om die reden worden de artikelen 66 tot 70 niet opgenomen in afdeling VIII inzake digitale operationele weerbaarheid, maar wel in een afzonderlijke afdeling die specifiek betrekking heeft op dit onderwerp.

Art. 67

Dit artikel bepaalt, naar analogie van artikel 18 van de DORA-verordening, dat systeemrelevante aanbieders alle incidenten en ernstige cyberdreigingen moeten classificeren en de effecten daarvan bepalen op basis van de in het partikel vermelde criteria.

Art. 68

Dit artikel bepaalt op algemene wijze dat systeemrelevante aanbieders alle incidenten moeten melden aan de Bank; cyberdreigingen die geen ernstig karakter hebben, hoeven niet gemeld te worden. Het artikel legt geen nadere vereisten vast en laat het aan de Bank over om haar verwachtingen ter zake te verduidelijken aan de hand van mededelingen, richtsnoeren, circulaires of reglementen.

Art. 69

Dit artikel vult artikel 68 aan door striktere rapportagevereisten op te leggen wat ernstige incidenten maar ook ernstige cyberdreigingen betreft. Systeemrelevante

TLPT sont disponibles sur le site internet de la Banque (*https://www.nbb.be/fr/paiements-et-titres/tiber-be-framework).*

Section IX

Gestion, classification et notification des incidents

Art. 66

Cet article requiert des fournisseurs d'importance systémique qu'ils établissent et mettent en œuvre un processus de gestion des incidents dans le but de déceler, de gérer et de signaler les incidents. À cette fin, ils sont tenus de surveiller et de consigner tous les incidents et cybermenaces majeures et de veiller à ce que les causes sous-jacentes en soient identifiées, documentées et éliminées afin de prévenir de tels incidents.

L'article est fondé sur l'article 17, paragraphes 1 et 2, du règlement DORA, mais il s'applique à la gestion, à la classification et au *reporting* de tous les incidents, et pas seulement aux incidents liés aux TIC. Pour ces motifs, les articles 66 à 70 sont inclus non pas dans la section VIII sur la résilience opérationnelle numérique, mais dans une section distincte consacrée spécifiquement à ce sujet.

Art. 67

Par analogie avec l'article 18 du règlement DORA, cet article prévoit que les fournisseurs d'importance systémique sont tenus de classer tous les incidents et les cybermenaces majeures et de déterminer leurs retombées sur la base des critères énoncés dans l'article.

Art. 68

Cet article prévoit de manière générale que les fournisseurs d'importance systémique doivent notifier tous les incidents à la Banque; les cybermenaces qui ne sont pas de nature majeure ne doivent pas être signalées. L'article ne fixe pas d'exigences supplémentaires et laisse à la Banque le soin de préciser ses attentes à cet égard par la voie de communications, de recommandations, de circulaires ou de règlements.

Art. 69

Cet article complète l'article 68 en imposant des exigences de déclaration plus strictes concernant les incidents graves ainsi que les cybermenaces majeures.

aanbieders moeten die incidenten en cyberdreigingen onverwijld melden aan de Bank en in geen geval later dan op de dag waarop het incident of de dreiging zich voordoet. Zij moeten de Bank na de initiële kennisgeving op de hoogte houden van nieuwe informatie over het ernstig incident of de ernstige dreiging en over de vooruitgang in de implementatie van respons-, herstel- en corrigerende maatregelen. Tot slot moet een eindverslag opgesteld worden en overgemaakt aan de Bank. Ook hier kan de Bank haar verwachtingen nader verduidelijken aan de hand van mededelingen, richtsnoeren, circulaires of reglementen.

Art. 70

Dit artikel bepaalt, naar analogie van artikel 19, lid 3, van de DORA-verordening, dat systeemrelevante aanbieders hun cliënten onverwijld op de hoogte moeten brengen wanneer een ernstig incident optreedt en gevolgen heeft voor de financiële belangen van die cliënten. In het geval van een ernstige cyberdreiging moeten zij hun mogelijk getroffen cliënten in kennis stellen van de passende beschermingsmaatregelen die zij kunnen nemen.

Afdeling X

Dienstverleningscriteria

Art. 71

Dit artikel herneemt de kernbepalingen van PFMI-principe 18, wat de criteria voor het aanbieden van financiële berichtendiensten aan alle dienstafnemers van de systeemrelevante aanbieder betreft (zie ook artikel 16 van de SIPS-verordening). Objectieve, op risico's gebaseerde en openbaar gemaakte criteria, die een correcte en een (aan acceptabele risicobeheersingnormen onderworpen) vrije toegang tot de diensten van een systeemrelevante aanbieder mogelijk maken, bevorderen de veiligheid en de efficientie van een systeemrelevante aanbieder en de markten die erdoor worden bediend, zonder disproportionele belemmering van de vrijheid van dienstverlening.

Afdeling XI

Communicatieprocedures en normen

Art. 72

Dit artikel herneemt kernbepaling 1 van PFMI-principe 22, wat het gebruik van internationaal

Les fournisseurs d'importance systémique sont tenus de notifier à la Banque les incidents majeurs et les cybermenaces importantes sans délai et au plus tard le jour où l'incident ou la menace se produit. Après la notification initiale, ils doivent tenir la Banque informée des nouvelles informations sur l'incident majeur ou la menace grave et du progrès réalisé dans la mise en œuvre des mesures de réponse, de rétablissement et de correction. Enfin, un rapport final doit être préparé et soumis à la Banque. À cet égard également, la Banque peut préciser ses attentes par la voie de communications, de recommandations, de circulaires ou de règlements.

Art. 70

Par analogie avec l'article 19, paragraphe 3, du règlement DORA, cet article dispose que les fournisseurs d'importance systémique doivent informer leurs clients sans délai lorsqu'un incident grave survient et a une incidence sur les intérêts financiers desdits clients. En cas de cybermenace majeure, ils sont tenus d'informer leurs clients 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

Cet article reprend les considérations essentielles du principe 18 des PIMF, concernant les critères d'offre de services de messagerie financière à tous les destinataires de services du fournisseur d'importance systémique (cf. également l'article 16 du règlement SPIS). Des critères objectifs, fondés sur le risque et rendus publics, qui permettent un accès correct et libre (sous réserve de normes acceptables de gestion des risques) aux services d'un fournisseur d'importance systémique, favorisent la sécurité et l'efficacité d'un fournisseur d'importance systémique et des marchés qu'il dessert, sans entraver de manière disproportionnée la liberté de la fourniture de services.

Section XI

Procédures et normes de communication

Art. 72

Cet article reprend la considération essentielle 1 du principe 22 des PIMF, concernant l'utilisation de

geaccepteerde communicatieprocedures en -normen betreft (zie ook artikel 19 van de CSD-verordening). Om een efficiënte dienstverlening te vergemakkelijken, moeten systeemrelevante aanbieders in hun procedures voor communicatie met hun dienstafnemers plaats inruimen voor de op hun vakgebied bestaande internationale open communicatieprocedures en normen voor het versturen van berichten en referentiegegevens.

Afdeling XII

Openbaarmaking van regels, cruciale procedures en marktgegevens

Art. 73

Dit artikel herneemt kernbepalingen 1 tot 4 van PFMI-principe 23, wat de openbaarmaking van regels, cruciale procedures en marktgegevens betreft (zie ook artikel 20, leden 1 tot 4 van de SIPS-verordening). Systeemrelevante aanbieders moeten ook hun tarieven en het beleid inzake kortingen bekend maken. Het artikel behoeft voor het overige geen nadere toelichting.

HOOFDSTUK 8

Toezicht op aanbieders van financiële berichtendiensten

Afdeling I

Toezicht door de Bank

Art. 74

Dit artikel bepaalt dat aanbieders van financiële berichtendiensten onderworpen zijn aan het toezicht van de Bank. Zoals toegelicht bij artikel 2 betreft het hier een *oversight*opdracht van de Bank zoals bedoeld in artikel 8 van haar organieke wet.

Paragraaf 2 bepaalt dat de Bank erop toeziet dat iedere aanbieder doorlopend functioneert met inachtneming van de bepalingen van het wetsvoorstel die op hem van toepassing zijn. Ten aanzien van alle aanbieders heeft het toezicht van de Bank aldus voornamelijk betrekking op de naleving van de artikelen 5 en 6, en ten aanzien van systeemrelevante aanbieders betreft het toezicht de naleving van het bepaalde in de artikelen 9 tot 73. 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 systeemrelevante aanbieders verrichte activiteiten, en de eraan verbonden risico's.

procédures et de normes de communication internationalement acceptées (cf. également l'article 19 du règlement CSD). Pour faciliter une fourniture de services efficace, les fournisseurs d'importance systémique doivent adapter, dans leurs procédures de communication avec leurs clients, les procédures et normes de communication internationales pour les données de messagerie et de référence en vigueur dans leur domaine.

Section XII

Communication de règles, procédures clés et données de marché

Art. 73

Cet article reprend les considérations essentielles 1 à 4 du principe 23 des PIMF, concernant la publicité des règles, des procédures cruciales et des données de marché (cf. également l'article 20, paragraphes 1 à 4, du règlement SIPS). Les fournisseurs d'importance systémique sont également tenus de communiquer leurs commissions et leurs politiques de remises. Pour le reste, l'article n'appelle pas de commentaires.

CHAPITRE 8

Surveillance des fournisseurs de services de messagerie financière

Section Ire

Surveillance par la Banque

Art. 74

Cet article stipule que les fournisseurs de services de messagerie financière sont soumis à la surveillance de la Banque. Comme expliqué à l'article 2, il s'agit d'une mission de surveillance de la Banque telle que visée à l'article 8 de sa loi organique.

Le paragraphe 2 dispose que la Banque veille à ce que chaque fournisseur opère en permanence dans le respect des dispositions de la proposition de loi qui lui sont applicables. S'agissant de l'ensemble des fournisseurs, la surveillance de la Banque porte donc principalement sur le respect des articles 5 et 6, tandis que pour les fournisseurs d'importance systémique, la surveillance porte sur le respect des dispositions des articles 9 à 73. La surveillance de la Banque doit être proportionnée et appropriée, à la lumière de la nature, de l'ampleur et de la complexité des activités exercées par les fournisseurs d'importance systémique, ainsi

Dit mag niet aldus worden geïnterpreteerd dat daarbij andere controle- en toezichtsbevoegdheden worden verleend dan die welke bij artikel 74 en volgende worden toegekend aan de Bank.

Art. 75

De Bank kan zich, in het kader van haar toezichtsopdracht, door iedere aanbieder alle inlichtingen doen verstrekken die zij nodig acht volgens de modaliteiten die zij bepaalt.

De Bank kan die informatie opvragen in de mate zij nodig of nuttig is voor het bereiken van de doelstellingen die met het *oversight* op aanbieders worden nagestreefd, met name om na te gaan of de voorschriften van het wetsvoorstel of de ter uitvoering ervan genomen besluiten en reglementen zijn nageleefd, evenals om bij te dragen tot de doelstellingen bedoeld in artikel 2, § 1, dit is met inbegrip van het verzekeren van de soliditeit van het financieel stelsel in het algemeen. Aldus is het niet uitgesloten dat de Bank ook transactiegegevens kan opvragen bij systeemrelevante aanbieders (waaronder verstaan wordt, geïndividualiseerde of individualiseerbare informatie over financiële transacties met betrekking waartoe een systeemrelevante aanbieder financiële berichtendiensten verstrekt), mits dit strookt met het hiervoor tot uitdrukking gebrachte finaliteitsbeginsel.

De Bank kan zich ook inlichtingen doen verstrekken door agenten van aanbieders of door entiteiten waaraan een systeemrelevante aanbieder activiteiten heeft uitbesteed. Het betreft een bevoegdheid die de Bank ook heeft ten aanzien van andere financiële instellingen waarop zij toezicht houdt, zoals bijvoorbeeld voorzien in artikel 102 van de wet van 11 maart 2018.

Art. 76

Dit artikel bepaalt dat de Bank bij iedere aanbieder ter plaatse inspecties kan verrichten en ter plaatse kennis kan nemen en een kopie maken van elk gegeven in het bezit van de aanbieder. Ook hier dient de Bank het hierboven toegelichte finaliteitsbeginsel te respecteren. Zie in die zin bijv. ook artikel 15 van de wet van 24 maart 2017. De inspecties kunnen uitgevoerd worden in de Belgische en de buitenlandse kantoren van een aanbieder.

Paragraaf 2 verduidelijkt, naar analogie van artikel 103 van de wet van 11 maart 2018, dat de prerogatieven van de Bank met betrekking tot de toegang

que des risques qui y sont associés. Il n'y a pas lieu d'interpréter ce qui précède comme dotant la Banque de pouvoirs de surveillance et de contrôle autres que ceux qui lui sont conférés par les articles 74 et suivants.

Art. 75

La Banque peut, dans le cadre de sa mission de surveillance, se faire transmettre par chaque fournisseur tous les renseignements qu'elle juge nécessaires selon les modalités qu'elle détermine.

La Banque est habilitée à demander ces informations pour autant qu'elles soient nécessaires ou utiles afin d'atteindre les objectifs fixés dans le cadre de *l'oversight* des fournisseurs, à savoir pour vérifier si les prescriptions de la proposition de loi ou celles des arrêtés ou règlements pris en exécution de celui-ci sont respectées, de même que pour contribuer aux objectifs visés par l'article 2, § 1er, en ce compris la préservation de la solidité du système financier dans son ensemble. Aussi n'est-il pas exclu que la Banque puisse également demander des données de transaction aux fournisseurs d'importance systémique (autrement dit des informations individualisées ou individualisables sur les transactions financières pour lesquelles un fournisseur d'importance systémique fournit des services de messagerie financière), à condition que cette requête soit compatible avec le principe de finalité susvisé.

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. Il s'agit d'une compétence dont la Banque dispose également à l'égard d'autres établissements financiers qu'elle supervise, comme le prévoit par exemple l'article 102 de la loi du 11 mars 2018.

Art. 76

Cet article dispose que la Banque peut procéder auprès de chaque fournisseur à des inspections sur place et prendre connaissance et copie, sans déplacement, de toute information détenue par le fournisseur. La Banque se doit ici encore de respecter le principe de finalité expliqué ci-avant. Cf. notamment à cet effet l'article 15 de la loi du 24 mars 2017. Les inspections peuvent être effectuées dans les bureaux belges et étrangers du fournisseur.

Par analogie avec l'article 103 de la loi du 11 mars 2018, le paragraphe 2 précise que les prérogatives de la Banque en matière d'accès à l'information couvrent

tot informatie uiteraard ook slaan op de toegang tot de agenda's en de notulen van de vergaderingen van de verschillende organen van aanbieders en van hun interne comités, evenals tot de bijbehorende documenten (agenda's van de vergaderingen, en bijlagen bij die documenten, presentaties, etc.) en tot de resultaten van de interne of externe beoordeling van de werking van die organen.

Paragraaf 3 preciseert dat de Bank ook inspecties ter plaatse kan verrichten bij agenten van aanbieders of bij entiteiten waaraan een systeemrelevante aanbieder taken heeft uitbesteed, en ter plaatse kennis kan nemen en een kopie kan maken van alle gegevens waarover zij beschikken (zie in die zin bijv. ook artikel 103 van de wet van 11 maart 2018). Hiermee worden de inspecties bij in België of in het buitenland gevestigde agenten of onderaannemers bedoeld.

Er zij tot slot nog verduidelijkt dat artikel 76 de Bank niet toelaat om huiszoekingen met een louter repressief doel uit te voeren, maar uitsluitend verwijst naar onderzoeken en controles die doelstellingen en oogmerken nastreven die verband houden met opdrachten van de Bank en dus verschillen van de doelstellingen die met een huiszoeking worden nagestreefd. Onderzoeken en controles ter plaatse kunnen niet worden uitgevoerd tegen de wil van de betrokken aanbieder. De Bank kan onderzoeken en controles ter plaatse dus niet met geweld uitvoeren. Indien de aanbieder zich zou verzetten tegen een onderzoek, zou het aan de Bank toekomen om te beoordelen of, in het licht van de feiten, de weigering van de aanbieder zou kunnen worden beschouwd als een belemmering en de toepassing zou rechtvaardigen van, onder meer, de maatregelen bedoeld in de artikelen 88 en 89, of in artikel 36/20, § 1, van de organieke wet van de Bank. Het gebruik van dwang, en in het bijzonder fysieke dwang, is bijgevolg uitgesloten. Onderzoeken en controles ter plaatse hebben *a priori* geen betrekking op privéwoningen, tenzij er een beroepsactiviteit wordt uitgeoefend die door het wetsvoorstel wordt gedekt.

Art. 77

Dit artikel versterkt, naar analogie van artikel 136 van de bankwet, de doeltreffendheid van het toezicht en in het bijzonder van de inspecties ter plaatse, door te bepalen dat de personen die belast zijn met het toezicht, en met name met de inspecties ter plaatse, gemachtigd zijn om alle inlichtingen en uitleg te verkrijgen die zij nodig achten voor de uitvoering van hun opdracht en dat zij in dit verband de leiders of personeelsleden van de aanbieder (of hun agenten) die zij aanduiden mogen uitnodigen voor een (in voorkomend geval individueel)

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 (ordres du jour des réunions et annexes à ces documents, présentations, etc.) et aux résultats de l'évaluation interne ou externe du fonctionnement desdits organes.

Le paragraphe 3 précise que la Banque est également habilitée à effectuer des contrôles sur place auprès des agents des fournisseurs ou des entités auxquelles un fournisseur d'importance systémique sous-traite l'exécution de tâches, et peut prendre connaissance et copie, sans déplacement, de toutes informations détenues par ces derniers (cf. notamment à cet effet l'article 103 de la loi du 11 mars 2018). Sont visées ici les inspections menées auprès d'agents ou de sous-traitants établis en Belgique ou à l'étranger.

Enfin, il y a lieu de préciser que l'article 76 ne permet pas à la Banque d'effectuer des perquisitions à finalité exclusivement répressive. Il vise uniquement les inspections et les contrôles qui poursuivent des objectifs et finalités liés aux missions de la Banque et donc différents de ceux poursuivis par une perquisition. Les inspections et contrôles sur place ne peuvent être effectués contre la volonté du fournisseur concerné. La Banque ne peut donc pas procéder de force à une inspection ou à un contrôle sur place. Dans l'hypothèse où le fournisseur venait à s'opposer à une inspection, il reviendrait à la Banque d'apprécier si, au regard des éléments de fait, le refus du fournisseur peut s'analyser comme une obstruction au contrôle et justifie l'application notamment des mesures visées aux articles 88 et 89 ou à l'article 36/20, § 1er, de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique. L'utilisation de la contrainte, et en particulier de la contrainte physique, est donc exclue. Les inspections et contrôles sur place ne concernent *a priori* pas les domiciles privés, à moins qu'une activité professionnelle visée par la proposition de loi n'y soit exercée.

Art. 77

Par analogie avec l'article 136 de la loi bancaire, cet article renforce l'efficacité du contrôle et, en particulier, celle des inspections sur place, en prévoyant que les personnes chargées du contrôle, spécialement des inspections sur place, sont habilitées à obtenir toutes les informations et explications qu'elles jugent nécessaires à l'accomplissement de leur mission et peuvent, à cet égard, inviter les dirigeants ou les membres du personnel du fournisseur (ou leurs mandataires) qu'elles désignent à un entretien (individuel, le cas échéant). On

gesprek. In dit verband zij opgemerkt dat het voeren van gesprekken met sleutelpersonen integraal deel uitmaakt van de tests en werkzaamheden die worden uitgevoerd in het kader van de analyses die in de loop van een inspectieopdracht worden verricht.

Art. 78

Dit artikel preciseert, naar analogie van artikel 140, tweede lid, van de bankwet, dat de Bank voor de uitvoering van haar toezichtsopdracht een beroep mag doen op deskundigen die zij aanstelt. De Bank kan de kost van deze deskundigen aanrekenen aan de betrokken aanbieders.

Art. 79

Dit artikel verleent, naar analogie van artikel 136/2 van de bankwet, het niveau van bescherming dat inherent is aan de vertrouwelijkheid van de inspectieverslagen van de Bank aan alle documenten die zij naar de aanbieders verstuurt en waarvan zij aangeeft dat ze vertrouwelijk zijn. Die documenten mogen door de aanbieders niet aan derden worden bekendgemaakt zonder uitdrukkelijke toestemming van de Bank. De effectiviteit van deze verplichting wordt verzekerd door een sanctie die bestaat in de straffen die in artikel 458 van het Strafwetboek worden opgelegd (pro memorie: conform deze bepaling wordt de niet-naleving van een geheimhoudingsplicht in het kader van een beroepsgeheimregeling als een inbreuk beschouwd).

Art. 80

Deze bepaling schrijft voor, naar analogie van artikel 29, lid 1, van de CSD-verordening, dat systeemrelevante aanbieders al hun vastleggingen over de verrichte diensten en activiteiten moeten bewaren voor zo lang als nodig is om de Bank toe te laten de naleving van het wetsvoorstel te controleren.

De Bank dient bij reglement te preciseren welke vastleggingen systeemrelevante aanbieders moeten bewaren evenals de bewaartermijnen, die 10 jaar niet mogen overschrijden. De Bank kan bij het vastleggen van deze nadere regels rekening houden met de bestaande praktijken bij systeemrelevante aanbieders, in het bijzonder wanneer het vastleggingen betreft van informatie die afkomstig is van cliënten (zoals bijvoorbeeld transactiegegevens, dit zijn de gegevens inzake financiële transacties met betrekking waartoe aanbieders financiële berichtendiensten verstrekken). De Bank

note, à cet égard, que la tenue d'entretiens avec des personnes clés fait partie intégrante des tests et travaux à mener dans le cadre des analyses conduites au cours d'une mission d'inspection.

Art. 78

Par analogie avec l'article 140, alinéa 2, de la loi bancaire, cet article précise que la Banque peut désigner un expert aux fins de l'exercice de sa mission de contrôle. La Banque peut répercuter le coût de ces experts sur le fournisseur concerné.

Art. 79

Par analogie avec l'article 136/2 de la loi bancaire, cet article confère le niveau de protection inhérent à la confidentialité des rapports d'inspection de la Banque à tous les documents qu'elle transmet aux fournisseurs et qu'elle indique comme étant confidentiels. Ces documents ne peuvent être divulgués par les fournisseurs à des tiers sans le consentement exprès de la Banque. L'efficacité de cette obligation est assurée par une sanction correspondant aux peines prévues à l'article 458 du Code pénal (pour mémoire: conformément à cette disposition, le non-respect d'une obligation de confidentialité dans le cadre d'un régime de secret professionnel est considéré comme une faute).

Art. 80

Par analogie avec l'article 29, paragraphe 1, du règlement CSD, cette disposition prévoit que les fournisseurs d'importance systémique doivent conserver 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 proposition de loi.

La Banque est réglementairement tenue de préciser les enregistrements que les fournisseurs d'importance systémique doivent conserver, de même que le délai de conservation, lequel ne peut excéder dix ans. En établissant ces règles supplémentaires, la Banque peut prendre en compte les pratiques existantes auprès des fournisseurs d'importance systémique, en particulier lorsqu'il s'agit d'enregistrer des informations provenant de clients (comme les données de transaction, autrement dit les données relatives aux transactions financières pour lesquelles les fournisseurs offrent des services de

dient ook hier rekening te houden met het hierboven al toegelichte finaliteitsbeginsel, wanneer zij verplichtingen oplegt tot het bewaren van bepaalde vastleggingen en de bijhorende bewaartermijnen vaststelt.

Afdeling II

Coöperatief toezicht

Art. 81

Dit artikel bevestigt dat de Bank op het vlak van het toezicht van systeemrelevante aanbieders niet-bindende samenwerkingsregelingen kan sluiten met andere centrale banken of monetaire autoriteiten, evenals met andere autoriteiten die gelijkwaardige opdrachten uitvoeren als deze bedoeld in artikel 8 van de organieke wet. Het artikel consolideert aldus de bestaande praktijk waarbij de Bank samenwerkingsregelingen treft met andere autoriteiten, in het bijzonder wanneer haar toezicht betrekking heeft op instellingen of financiële marktinfrastructuren die Europees of mondiaal actief zijn en de betrokken autoriteiten een uitgesproken belang hebben bij het goed functioneren van de instelling of marktinfrastructuur op hun grondgebied. Aan de hand van dergelijke samenwerkingsregelingen kan een coöperatief toezicht tot stand gebracht worden.

Wanneer het toezicht op een systeemrelevante aanbieder het voorwerp uitmaakt van een samenwerkingsregeling als bedoeld in dit artikel, oefent de Bank de haar door het wetsvoorstel toevertrouwde opdrachten uit ter ondersteuning van die samenwerking. Dit betekent evenwel niet dat de Bank in de uitoefening van haar toezicht kan beknot worden door het coöperatief toezicht; de bindende bepalingen van het wetsvoorstel hebben steeds voorrang op de niet-bindende bepalingen van de hier bedoelde samenwerkingsregelingen. De Bank kan steeds relevante informatie inzake het toezicht op systeemrelevante aanbieders delen met deelnemers aan het coöperatief toezicht, in voorkomend geval rekening houdend met haar beroepsgeheim en met de specifieke voorwaarden die gelden voor het delen van vertrouwelijke informatie (zie in het bijzonder artikel 35 van de organieke wet). Omgekeerd kan de Bank van andere deelnemers aan een coöperatief toezicht informatie ontvangen die nuttig is voor de uitoefening van haar bevoegdheden op grond van het voorliggend wetsvoorstel.

Paragraaf 3 van het artikel bepaalt dat de Bank de deelnemers aan de samenwerkingsregelingen raadpleegt wanneer zij overweegt een mededeling, richtsnoer of

messagerie financière). En l'occurrence également, la Banque doit tenir compte du principe de finalité déjà expliqué ci-avant lorsqu'elle impose l'obligation de conserver certains enregistrements et qu'elle fixe les délais de conservation correspondants.

Section II

Surveillance coopérative

Art. 81

Cet article confirme que, dans le domaine de la surveillance des fournisseurs d'importance systémique, la Banque est habilitée à conclure des arrangements de coopération non contraignants avec d'autres banques centrales ou autorités monétaires, ainsi qu'avec d'autres autorités exerçant des missions équivalentes à celles visées à l'article 8 de la loi organique. L'article consolide ainsi la pratique en place selon laquelle la Banque conclut des arrangements de coopération avec d'autres autorités, en particulier lorsque sa surveillance concerne des établissements ou des infrastructures de marchés financiers qui opèrent à l'échelle européenne ou mondiale et que les autorités concernées ont un intérêt marqué pour le bon fonctionnement de l'établissement ou de l'infrastructure de marché sur leur territoire. La surveillance coopérative peut être mise en place par le biais de ces arrangements de coopération.

Lorsque la surveillance d'un fournisseur d'importance systémique fait l'objet d'un arrangement de coopération visé au présent article, la Banque exerce les missions qui lui sont dévolues par la présente proposition de loi en soutien de cette coopération. Pour autant, cela ne signifie pas que la Banque peut être entravée dans l'exercice de sa surveillance par ladite surveillance coopérative; les dispositions contraignantes de la proposition de loi priment toujours sur les dispositions non contraignantes des arrangements de coopération visés ici. La Banque peut toujours partager les informations pertinentes concernant la surveillance des fournisseurs d'importance systémique avec les participants à la surveillance coopérative, compte tenu, le cas échéant, du secret professionnel auquel elle est tenue et des conditions spécifiques applicables au partage d'informations confidentielles (cf., en particulier, l'article 35 de la loi organique). Inversement, la Banque peut recevoir des autres participants à la surveillance coopérative des informations utiles à l'exercice des compétences qui lui sont conférées par la présente proposition de loi.

Le paragraphe 3 de l'article dispose que la Banque consulte les participants aux arrangements de coopération lorsqu'elle envisage de publier une communication,

circulaire uit te vaardigen of een reglement vast te stellen als bedoeld in artikel 8, § 2, van de organieke wet. Op die manier wordt verzekerd dat de Bank desgewenst rekening kan houden met opmerkingen van deelnemers aan een samenwerkingsregeling, zonder dat zij daar evenwel toe verplicht is of zonder haar uiteindelijke beslissing ten aanzien van die deelnemers te moeten motiveren.

Gelet op de bestaande positieve ervaringen met cooperatieve toezichtstructuren, beperkt het wetsvoorstel zich tot deze enkele bepalingen en wordt het voor het overige aan de deelnemers van de samenwerkingsregelingen overgelaten om één en ander in onderling overleg nader te regelen.

HOOFDSTUK 9

Dwingende maatregelen

Art. 82

Dit artikel vormt, naar analogie van artikel 234 van de bankwet, de wettelijke basis waarop de Bank zich kan beroepen om een systeemrelevante aanbieder te verzoeken maatregelen te nemen om inbreuken op de bepalingen van het wetsvoorstel of de uitvoeringsbesluiten en -reglementen ervan te verhelpen.

De Bank kan ook anticiperen op inbreuken door maatregelen op te leggen waarmee deze inbreuken kunnen worden voorkomen wanneer de Bank over gegevens beschikt waaruit blijkt dat het gevaar bestaat dat een systeemrelevante aanbieder in de komende twaalf maanden niet meer zal werken overeenkomstig de toepasselijke wetsbepalingen De Bank kan die gegevens hebben verkregen in het kader van al haar toezichtstaken. Zij kan bijvoorbeeld beschikken over inlichtingen waaruit blijkt dat het niveau van de kapitaalvereisten van een systeemrelevante aanbieder binnenkort niet langer voldoende zal zijn, gezien de verwachte verslechtering van zijn resultaten.

Tot slot kan de Bank ook optreden wanneer de uitoefening van het bedrijf van de systeemrelevante aanbieder een bedreiging vormt voor de stabiliteit en continuïteit van nationale en internationale financiële transacties of anderszins een bedreiging vormt voor het verzekeren van de doelstellingen die met het wetsvoorstel worden nagestreefd.

In al deze gevallen kan de Bank een termijn opleggen waarbinnen de situatie moet worden verholpen en kan zij aldus eisen dat er maatregelen worden genomen binnen de vastgestelde termijn. Zolang de systeemrelevante

une recommandation ou une circulaire ou d'adopter un règlement tel que visé à l'article 8, § 2, de la loi organique. Cela permettra à la Banque de prendre en compte les commentaires des participants à un arrangement de coopération si elle le souhaite, sans pour autant y être obligée, ou de justifier sa décision finale à l'égard de ces participants.

Au vu de l'expérience positive des structures de surveillance coopérative, la proposition de loi se limite à ces quelques dispositions et laisse aux participants aux arrangements de coopération le soin de prendre d'autres dispositions d'un commun accord.

CHAPITRE 9

Mesures contraignantes

Art. 82

Par analogie avec l'article 234 de la loi bancaire, cet article constitue la base légale sur laquelle peut s'appuyer la Banque pour requérir d'un fournisseur d'importance systémique qu'il prenne des mesures afin de remédier à des manquements aux dispositions de la proposition de loi ou des arrêtés et règlements pris pour son exécution.

La Banque peut également anticiper la survenance de manquements en imposant des mesures visant à prévenir cette survenance lorsqu'elle dispose d'éléments indiquant qu'un fournisseur d'importance systémique risque, au cours des douze mois suivants, de ne plus fonctionner en conformité avec les dispositions légales applicables. Ces éléments peuvent avoir été relevés par la Banque au cours de la procédure de contrôle prudentiel. La Banque peut, par exemple, disposer d'informations indiquant que le niveau des fonds propres réglementaires d'un fournisseur d'importance systémique ne sera bientôt plus suffisant, compte tenu d'une baisse prévisible de ses résultats.

Enfin, la Banque peut également intervenir lorsque l'activité du fournisseur d'importance systémique menace la stabilité et la continuité de transactions financières nationales et internationales ou présente une menace pour l'assurance des objectifs poursuivis par la proposition de loi.

Dans tous ces cas, la Banque peut imposer un délai dans lequel il doit être remédié à la situation observée et peut ainsi requérir l'adoption de mesures dans le délai fixé. Aussi longtemps que le fournisseur d'importance

aanbieder de vastgestelde toestand niet heeft verholpen, kan de Bank te allen tijde de maatregelen opleggen vermeld in paragraaf 2 van het artikel.

Wanneer de Bank van oordeel is dat de maatregelen die de systeemrelevante aanbieder binnen de opgelegde termijn heeft genomen om de vastgestelde situatie te verhelpen voldoende zijn, heft zij de maatregelen die zij heeft genomen geheel of gedeeltelijk op.

Art. 83

Dit artikel stelt, naar analogie van artikel 236 van de bankwet, vast welke maatregelen de Bank kan treffen wanneer een systeemrelevante aanbieder niet of niet langer voldoet aan de met toepassing van artikel 82 door de Bank opgelegde dwingende maatregelen of wanneer de aanbieder de vastgestelde inbreuken niet heeft verholpen binnen de met toepassing van artikel 82 door de Bank vastgestelde termijn.

Aldus kan de Bank een systeemrelevante aanbieder gelasten om de algemene vergadering bijeen te roepen. Deze maatregel heeft tot doel de aandeelhouders ertoe te brengen zich uit te spreken over een maatregel die een beslissing van de algemene vergadering vergt. In het verlengde van deze bepaling kunnen de voorlopige bestuurder(s) die werden aangewezen ter vervanging van een lid of meerdere leden van de raad van toezicht of van de effectieve leiding, eveneens een algemene vergadering van aandeelhouders bijeenroepen en de agenda ervan vaststellen, mits ze hiervoor de toestemming van de Bank hebben gekregen. De Bank kan daarnaast ook de maatregelen nemen die hierna onder de artikelen 84 en 85 nader worden toegelicht.

Zoals in paragraaf 2 wordt bepaald, kan de Bank die maatregelen in uiterst spoedeisende gevallen ook treffen zonder vooraf een termijn op te leggen en zonder dat niet of niet langer is voldaan aan de dwingende maatregelen van artikel 82. Dit is bijvoorbeeld mogelijk bij fraudegevallen die een snelle reactie vergen of waarbij er door de ernst van de feiten snel moet worden opgetreden door de Bank.

Er zij op gewezen dat de in de artikelen 82 en 83 omschreven administratieve maatregelen niet de aard van sancties hebben. Het betreft hier immers corrigerende maatregelen die noch tot doel noch tot gevolg hebben enige schuld vast te stellen of te straffen, maar die ernaar streven de stabiliteit van de financiële sector in stand te houden, en het vertrouwen van het publiek, inzonderheid van gebruikers van financiële berichtendiensten, in de financiële sector als geheel en in de operatoren van die sector te handhaven. Door hun preventieve aard

systémique n'a pas remédié à la situation constatée, la Banque peut imposer à tout moment les mesures visées au paragraphe 2 de l'article.

Lorsque la Banque estime que les mesures prises par le fournisseur d'importance systémique dans le délai fixé pour remédier à la situation constatée sont satisfaisantes, elle lève tout ou partie des mesures décidées.

Art. 83

Par analogie avec l'article 236 de la loi bancaire, cet article définit les mesures que la Banque peut prendre lorsqu'un fournisseur d'importance systémique ne respecte pas ou cesse de respecter les mesures contraignantes imposées par la Banque en application de l'article 82, ou lorsque le fournisseur ne remédie pas aux manquements observés dans le délai fixé par la Banque en vertu de l'article 82.

La Banque peut ainsi requérir d'un fournisseur d'importance systémique qu'il convoque l'assemblée générale. Cette mesure a pour objet de conduire les actionnaires à se prononcer sur une mesure nécessitant une décision de leur assemblée. Dans le prolongement de cette disposition, le ou les administrateurs provisoires désignés en remplacement d'un ou de plusieurs membres du conseil de surveillance ou de la direction effective, peuvent également convoquer une assemblée générale des actionnaires et en établir l'ordre du jour, à condition d'avoir obtenu l'autorisation de la Banque à cette fin. La Banque est par ailleurs aussi habilitée à prendre les mesures détaillées ci-dessous au titre des articles 84 et 85.

Ainsi que le précise le paragraphe 2, la Banque peut également adopter lesdites mesures en cas d'extrême urgence sans qu'un délai ne soit fixé au préalable et sans que les mesures contraignantes visées à l'article 82 ne soient pas ou plus respectées. Il s'agit par exemple de situations de fraude nécessitant une réaction prompte ou dont le degré de gravité requiert une action prompte de la Banque.

On rappelle que les mesures administratives prévues aux articles 82 et 83 n'ont pas la nature de sanctions. En effet, il s'agit ici de mesures correctrices qui n'ont ni pour but ni pour effet de constater une quelconque culpabilité ou de punir, mais qui tendent à préserver la stabilité du secteur financier, ainsi que la confiance du public, plus particulièrement celle des utilisateurs de services de messagerie financière, dans le secteur financier dans son ensemble et dans les opérateurs de ce secteur. Ces mesures administratives, de par

vallen die administratieve maatregelen aldus onder de taak van administratieve politie die inherent is aan het optreden van de Bank. De benaming administratieve maatregelen houdt niet in dat die maatregelen kunnen worden genomen zonder enige procedurele garantie voor de betrokkenen. Aangezien de genoemde maatregelen immers berusten op rechtshandelingen van de actieve administratie, moeten ze uiteraard voldoen aan de algemene beginselen van het administratief recht waaraan de Bank als administratieve autoriteit onderworpen is. Hierbij kan onder meer worden gedacht aan het debat op tegenspraak, het onpartijdigheidsbeginsel, het recht om te worden gehoord en de naleving van het evenredigheidsbeginsel (zie A. DIRKX, "*La CBFA, les infractions à la législation financière et la sanction par les amendes administratives*", in *Le droit pénal financier en marche* / Het financieel strafrecht in opmars, AEDBF, Anthemis, 2009, p. 273, nrs. 5 tot 7).

leur caractère préventif, relèvent ainsi de la mission de police administrative inhérente à l'action de la Banque. La qualification de mesures administratives ne conduit pas à ce que l'adoption de ces mesures puisse s'effectuer sans aucune garantie d'ordre procédural pour les personnes concernées. En effet, relevant d'actes de l'administration active, lesdites mesures doivent bien évidemment satisfaire aux principes généraux du droit administratif auxquelles la Banque est soumise en sa qualité d'autorité administrative. On pense ici notamment au débat contradictoire, au principe d'impartialité, au droit d'être entendu et au respect du principe de proportionnalité (cf. A. DIRKX, "La CBFA, les infractions à la législation financière et la sanction par les amendes administratives", dans Le droit pénal financier en marche / *Financial criminal law on the rise*, AEDBF, Anthemis, 2009, p. 273, n°s 5 à 7).

Art. 84

Dit artikel legt, naar analogie van artikel 236, § 1, 1°, van de bankwet, de regels vast inzake de aanstelling van een speciaal commissaris door de Bank. Het artikel bevat geen nieuwigheden ten aanzien van de bevoegdheden die de Bank op dit vlak reeds kan uitoefenen jegens andere financiële instellingen onder haar toezicht.

De aanstelling van een speciaal commissaris, wiens toelating vereist is voor de handelingen en beslissingen van de organen van de systeemrelevante aanbieder alsook van de personen die instaan voor het beleid, is een in beginsel bewarende, niet-publieke maatregel. In sommige gevallen heeft de speciaal commissaris als opdracht de algemene evolutie van de aanbieder te volgen en er toezicht op te houden. Daarom bepaalt het artikel dat, ingeval de speciaal commissaris geen toestemming heeft gegeven voor verrichtingen waarvoor dit vereist is, de leiders hoofdelijk aansprakelijk zijn voor het nadeel dat hieruit voor de aanbieder of voor derden voortvloeit. Bovendien mogen de aanstelling en de bevoegdheden van de speciaal commissaris in het *Belgisch Staatsblad* worden bekendgemaakt. In dat geval zijn de onregelmatige handelingen en beslissingen van rechtswege nietig. De nietigheid geldt ten aanzien van iedere derde.

De speciaal commissaris kan de handelingen en beslissingen bekrachtigen waarvoor zijn toestemming wel vereist maar niet verleend is. Dit betekent evenwel niet dat de speciaal commissaris op basis van een algemene bekrachtiging alle nietigverklaringen alsnog zou kunnen herstellen. De speciaal commissaris kan enkel bekrachtigen indien hij dat noodzakelijk acht voor de uitoefening van zijn opdracht.

Art. 84

Par analogie avec l'article 236, § 1er, 1°, de la loi bancaire, cet article fixe les règles relatives à la désignation par la Banque d'un commissaire spécial. L'article ne contient aucune nouveauté par rapport aux compétences que la Banque peut déjà exercer à cet égard vis-à-vis des autres établissements financiers soumis à son contrôle.

La désignation d'un commissaire spécial, dont l'autorisation est requise pour les actes et décisions des organes du fournisseur d'importance systémique ainsi que pour ceux des personnes chargées de la gestion, est une mesure essentiellement conservatoire et non publique. Dans certains cas, le commissaire spécial est chargé de suivre et de contrôler l'évolution globale du fournisseur. L'article prévoit par conséquent que, dans le cas où le commissaire spécial n'a pas ratifié les opérations pour lesquelles son autorisation est requise, les dirigeants sont conjointement et solidairement responsables de tout préjudice en résultant pour le fournisseur ou pour des tiers. En outre, la désignation et les pouvoirs du commissaire spécial peuvent être publiés au *Moniteur belge*. En pareil cas, les actes et décisions irréguliers sont nuls de plein droit. La nullité s'applique à l'égard de tout tiers.

Le commissaire spécial peut ratifier les actes et décisions pour lesquels son consentement est requis mais non accordé. Cela ne signifie toutefois pas que le commissaire spécial pourrait encore rétablir toutes les annulations sur la base d'une ratification générale. Le commissaire spécial ne peut procéder à une ratification que s'il l'estime nécessaire à l'exercice de ses fonctions.

Art. 85

Dit artikel regelt, naar analogie van artikel 236, § 1, 2°, van de bankwet, de vervanging door de Bank 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. Indien binnen de door de Bank opgelegde 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. In gerechtvaardigde gevallen 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.

Deze maatregel moet openbaar worden gemaakt en is onmisbaar om te kunnen optreden tegenover hetzij leiders die niet de nodige hoedanigheden bezitten voor het voeren van een beleid in overeenstemming met het bepaalde in het wetsvoorstel, hetzij wanneer het nodig blijkt de leiding te saneren of nog wanneer de leiding weigert de verslechtering van de toestand van de systeemrelevante aanbieder in te zien.

Art. 86

Dit artikel bevat, naar analogie van artikel 236/1 van de bankwet, nadere regels inzake het statuut van de in toepassing van de artikelen 84 en 85 aangestelde speciaal commissaris en voorlopige bestuurder(s). Er wordt verwezen naar de uitgebreide toelichting bij artikel 373 van de wet van 20 juli 2022 op het statuut van en het toezicht op beursvennootschappen en houdende diverse bepalingen (*Parl.St.* Kamer, 2021-2022, DOC 55 2763/001, blz. 135-139).

Art. 87

Dit artikel bepaalt, naar analogie van artikel 236, § 8, van de bankwet, dat de ondernemingsrechtbank op verzoek van elke belanghebbende de nietigverklaringen uitspreekt bedoeld in artikel 84. Het artikel regelt ook de procedure en de vervaltermijn van de nietigheidsvordering. De nietigheidsvordering kan door iedere belanghebbende worden ingesteld, dus ook door de speciaal commissaris en de Bank. Voor het overige wordt verwezen naar de memorie van toelichting bij de artikelen 10 en 11 van het wetsontwerp tot wijziging,

Art. 85

Par analogie avec l'article 236, § 1er, 2°, de la loi bancaire, cet article régit le remplacement par la Banque de tout ou partie des membres du conseil de surveillance et/ou des personnes chargées de la direction effective du fournisseur d'importance systémique. À défaut d'un tel remplacement dans le délai fixé par la Banque, celle-ci 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. Dans les cas où cela se justifie, la Banque peut procéder à la désignation d'un ou de plusieurs administrateurs provisoires sans procéder préalablement à l'injonction de remplacer tout ou partie des dirigeants du fournisseur d'importance systémique.

Cette mesure doit être rendue publique et est indispensable soit pour confronter les dirigeants qui ne possèdent pas les qualités requises pour mener une politique conforme aux dispositions de la proposition de loi, soit lorsqu'il s'avère nécessaire d'assainir la direction soit, plus encore, lorsque la direction refuse de reconnaître la détérioration de la situation du fournisseur d'importance systémique.

Art. 86

Par analogie avec l'article 236/1 de la loi bancaire, cet article contient des règles détaillées sur le statut du commissaire spécial et de l'administrateur provisoire ou des administrateurs provisoires désignés en application des articles 84 et 85. Il est fait référence au commentaire détaillé de l'article 373 de la loi du 20 juillet 2022 relative au statut et au contrôle des sociétés de bourse et portant dispositions diverses (*Parl.St.* Chambre, 2021-2022, DOC 55 2763/001, pp. 135-139).

Art. 87

Par analogie avec l'article 236, § 8, de la loi bancaire, cet article prévoit que le tribunal de l'entreprise prononce, à la requête de tout intéressé, les nullités prévues à l'article 84. L'article régit également la procédure et le délai d'expiration de l'action en nullité. L'action en nullité peut être intentée par tout intéressé, en ce compris le commissaire spécial et la Banque. Pour le surplus, il est renvoyé à l'exposé des motifs des articles 10 et 11 du projet de loi modifiant, en ce qui concerne les fusions et scissions de sociétés, les lois sur les sociétés

wat de fusies en splitsingen van vennootschappen betreft, van de wetten op de handelsvennootschappen, gecoördineerd op 30 november 1935 (*Parl.St.* Kamer, 1989-1990, nr. 1214/1, 32-35).

HOOFDSTUK 10

Dwangsommen, administratieve sancties en andere maatregelen

Art. 88

Dit artikel bepaalt, naar analogie van artikel 345 van de bankwet, dat de Bank kan 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

Dit artikel bepaalt, naar analogie van artikel 346 van de bankwet, dat de Bank een dwangsom kan opleggen wanneer een systeemrelevante aanbieder binnen een door de Bank opgelegde termijn geen gevolg heeft gegeven aan haar oproep om een onregelmatige toestand te verhelpen. De dwangsom mag per dag niet meer bedragen dan 50.000 euro, noch in het totaal 2.500.000 euro overschrijden.

Bij de vaststelling van het bedrag van de dwangsom dient de Bank onder meer rekening te houden met de ernst van de vastgestelde tekortkomingen en de impact op de financiële sector, evenals met de draagkracht van de systeemrelevante aanbieder.

Men dient op te merken dat de door de Bank opgelegde dwangsommen niet mogen beschouwd worden als sancties doch wel als administratieve maatregelen die erop gericht zijn de betrokken systeemrelevante aanbieders zo snel en efficiënt mogelijk te doen functioneren conform de bepalingen van het wetsvoorstel. Net zoals de dwangsommen in prudentiële aangelegenheden, worden zij opgelegd door het Directiecomité van de Bank.

Art. 90

Dit artikel bepaalt, naar analogie van artikel 347 van de bankwet, dat de Bank een administratieve geldboete kan opleggen indien zij een inbreuk vaststelt op de bepalingen van de wet of op de ter uitvoering ervan genomen besluiten en reglementen. De geldboete kan

commerciales, coordonnées le 30 novembre 1935 (*Parl. St.* Chambre, 1989-1990, n° 1214/1, 32-35).

CHAPITRE 10

Astreintes, sanctions administratives et autres mesures

Art. 88

Par analogie avec l'article 345 de la loi bancaire, cet article dispose que 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

Par analogie avec l'article 346 de la loi bancaire, cet article prévoit que la Banque peut infliger une astreinte lorsqu'un fournisseur d'importance systémique n'a pas donné suite à son invitation à remédier à une situation irrégulière dans un délai imposé par la Banque. L'astreinte ne pourra excéder 50.000 euros par jour, ni 2.500.000 euros au total.

Pour déterminer le montant de l'astreinte, la Banque doit tenir compte, notamment, de la gravité des manquements rencontrés et de l'impact sur le secteur financier, ainsi que de l'assise du fournisseur d'importance systémique.

Il convient de noter que les astreintes infligées par la Banque sont à considérer non pas comme des sanctions mais plutôt comme des mesures administratives visant à amener les fournisseurs d'importance systémique concernés à opérer aussi rapidement et efficacement que possible conformément aux dispositions de la proposition de loi. À l'instar des astreintes en matière prudentielle, elles sont imposées par le Comité de direction de la Banque.

Art. 90

Par analogie avec l'article 347 de la loi bancaire, cet article prévoit que la Banque peut infliger une amende administrative si elle constate une infraction aux dispositions de la loi ou des décrets et règlements pris en exécution de celle-ci. L'amende peut être imposée au

worden opgelegd aan de systeemrelevante aanbieder maar eveneens aan iedere verantwoordelijke natuurlijke persoon. De 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. Het artikel behoeft voor het overige geen nadere toelichting, aangezien het hier gaat om de toepassing van een bevoegdheid die de Bank reeds kan uitoefenen ten aanzien van andere instellingen onder haar toezicht.

De Bank dient bij het opleggen van de administratieve geldboetes rekening te houden met de duur en de ernst van de gepleegde inbreuk evenals met andere omstandigheden. Het artikel geeft de Bank aldus de mogelijkheid om, in voorkomend geval, met verzachtende en verzwarende omstandigheden rekening te houden bij het bepalen van de hoogte van de administratieve geldboete.

Administratieve geldboetes worden opgelegd door de in de schoot van de Bank opgerichte Sanctiecommissie. Tegen beslissingen waarbij een administratieve geldboete wordt opgelegd, kan krachtens artikel 36/21 van de organieke wet beroep worden aangetekend bij het hof van beroep te Brussel.

Art. 91 en 92

Deze artikelen behoeven geen nadere toelichting.

HOOFDSTUK 11

Wijzigingsbepalingen en inwerkingtreding

Art. 93

Dit artikel brengt een wijziging aan in artikel 8 van de organieke wet. De wijziging strekt ertoe de Bank de mogelijkheid te bieden de werkingskosten die betrekking hebben op haar *oversight*taken te verhalen op de instellingen die onder dat *oversight* staan.

De werkingskosten kunnen verhaald worden volgens de nadere regels vastgesteld door de Koning. Het is dus noodzakelijk dat het koninklijk besluit van 17 juli 2012 betreffende de dekking van de werkingskosten van de Bank gewijzigd wordt, of dat een afzonderlijk besluit in die zin wordt genomen, alvorens de Bank deze werkingskosten effectief kan verhalen op instellingen die onder haar *oversight* vallen.

Toezichtsactiviteiten brengen vaak aanzienlijke kosten met zich mee, waaronder deze voor personeel,

fournisseur d'importance systémique, mais aussi à toute personne physique responsable. Le montant de l'amende, 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. Pour le reste, l'article n'appelle pas de commentaires, puisqu'il porte sur l'application d'une compétence que la Banque peut déjà exercer à l'égard d'autres établissements placés sous sa surveillance.

Lorsqu'elle inflige des amendes administratives, la Banque doit tenir compte de la durée et de la gravité de l'infraction commise ainsi que d'autres circonstances. L'article permet donc à la Banque de prendre en compte, le cas échéant, les circonstances atténuantes et aggravantes lors de la détermination du montant de l'amende administrative.

Les amendes administratives sont infligées par la Commission des sanctions instituée dans le giron de la Banque. Les décisions infligeant une amende administrative peuvent faire l'objet d'un recours devant la Cour d'appel de Bruxelles en vertu de l'article 36/21 de la loi organique.

Art. 91 et 92

Ces articles n'appellent pas de commentaires.

CHAPITRE 11

Modifications et entrée en vigueur

Art. 93

Cet article modifie l'article 8 de la loi organique. La modification vise à permettre à la Banque de recouvrer les frais de fonctionnement liés à ses missions de surveillance auprès des établissements soumis à cet *oversight*.

Les frais de fonctionnement peuvent être récupérés selon les modalités détaillées fixées par le Roi. Il est dès lors nécessaire de modifier l'arrêté royal du 17 juillet 2012 relatif à la couverture des frais de fonctionnement de la Banque, ou d'adopter un arrêté distinct en ce sens, afin que la Banque puisse effectivement récupérer ces frais de fonctionnement auprès des établissements soumis à son *oversight*.

Les activités de surveillance impliquent souvent des coûts importants, notamment en matière de personnel,

technologie en administratie. Door deze kosten aan te rekenen aan de onder toezicht staande entiteiten, wordt ervoor gezorgd dat de kosten eerlijk worden verdeeld onder de entiteiten die onder toezicht staan in plaats van deze volledig te laten dragen door de belastingbetaler. Wanneer entiteiten moeten betalen voor hun toezicht, kunnen ze meer gemotiveerd zijn om te voldoen aan de regelgeving en om hoge normen te handhaven; niet-naleving of slechte prestaties kunnen immers leiden tot meer toezicht en daardoor hogere kosten. Door kosten te verhalen, kunnen toezichthouders meer middelen inzetten om de kwaliteit en effectiviteit van hun toezicht te verbeteren, bijvoorbeeld door meer gekwalificeerd personeel aan te werven, te investeren in geavanceerde technologieën of grondiger inspecties en audits uit te voeren. Die overwegingen rechtvaardigen de voorgestelde wijziging van artikel 8 van de organieke wet.

Art. 94

Dit artikel behoeft geen nadere toelichting.

Koen Van den Heuvel (cd&v)
Steven Matheï (cd&v)
Nathalie Muylle (cd&v)

de technologie et d'administration. L'imputation de ces coûts aux entités contrôlées garantit une répartition équitable des frais entre les entités contrôlées et veille à ce qu'ils ne soient pas entièrement assumés par les contribuables. L'imputation aux entités concernées des frais inhérents à leur contrôle peut les encourager à se conformer aux réglementations et à maintenir des normes élevées. Le non-respect des réglementations ou les mauvaises performances peuvent en effet conduire à un renforcement du contrôle et, partant, alourdir les coûts. La récupération des frais permet aux autorités prudentielles d'allouer davantage de ressources à l'amélioration de la qualité et de l'efficacité de leur surveillance, par exemple en recrutant du personnel plus qualifié, en investissant dans des technologies de pointe ou en menant des inspections et des audits plus poussés. Ces considérations justifient la modification proposée de l'article 8 de la loi organique.

Art. 94

Cet article n'appelle pas de commentaires.

WETSVOORSTEL

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 systeemrelevante 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.

§ 3. Onverminderd het bepaalde in artikel 8, § 2, van de wet van 22 februari 1998, 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 Nationale Bank van België: 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

PROPOSITION DE LOI

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 d’importance systémique 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.

§ 3. Sans préjudice des dispositions de l’article 8, § 2, de la loi du 22 février 1998, 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 nationale de Belgique: 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,

ontvangen, met inbegrip van operationele diensten en 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

telles que les paiements et les transactions sur titres, y 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

activiteiten of aan de uitvoering van nationale of internationale financiële transacties, of waarvan de beëindiging 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 een financiële berichtendienst kan verstoren of verstoort, waaronder, in voorkomend geval, een ICT-gerelateerd incident;

et activités ou à l'exécution de transactions financières nationales ou internationales, ou dont une interruption, une anomalie ou une 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 réévaluer 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° ICT-gerelateerd incident: één gebeurtenis of een reeks gekoppelde gebeurtenissen die niet door de systeemrelevante aanbieder zijn gepland en die de beveiliging van de 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 (*red team*) 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;

20° incident lié aux TIC: un événement ou une série d'événements liés entre eux que le fournisseur 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: 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 (*red team*) 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° werkdag: alle dagen met uitsluiting van de zondagen en wettelijke feestdagen.

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.

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 gemotiveerde 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.

28° jour ouvrable: tous les jours à l'exception des dimanches et jours fériés.

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 auquel 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

§ 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 motivée 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. 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 gemotiveerde 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 aanbieders aan wie zij krachtens artikel 7, § 1, een kennisgeving heeft bezorgd. 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 aanbieder.

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.

§ 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 motivée 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 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 à qui elle a adressé une notification en vertu de l'article 7, § 1er. La Banque publie cette liste sur son site internet et le met à jour si besoin en est.

La liste visée à l'alinéa 1er doit mentionner 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.

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.

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 afdeling 3 van boek 7, titel 4, hoofdstuk 1, van het Wetboek van Vennootschappen en Verenigingen van toepassing.

§ 2. De statuten van een systeemrelevante aanbieder die anders dan als naamloze 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 afdeling 3 van boek 7, titel 4, hoofdstuk 1, 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 in elk geval de voorzitter, zijn onafhankelijke bestuurders.

§ 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

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 à la section 3 du livre 7, titre 4, chapitre 1er, du Code des sociétés et associations sont d'application.

§ 2. Les statuts d'un fournisseur d'importance systémique constitué sous une autre forme que celle de société anonyme 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 à la section 3 du livre 7, titre 4, chapitre 1er, 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 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, y compris au moins le président, sont des administrateurs indépendants.

§ 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

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 punten 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.

De in het voorgaande 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 enige andere, gefundeerde en voor de Bank aanvaardbare garantie kan bieden.

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 au cours du dernier exercice social, 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, associé ou salarié du commissaire, 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 points 3° à 6°.

§ 3. Un administrateur indépendant ne peut 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.

L'indépendance visée à l'alinéa précédent 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. Een systeemrelevante aanbieder kan van de criteria bedoeld in paragraaf 2 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 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 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.

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.

§ 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.

§ 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 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 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.

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 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. 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 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.

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

§ 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 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

§ 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

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 comité.

§ 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 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 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

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.

§ 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 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

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 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;

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 sans 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 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° 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 aanbieder, de leden van zijn raad van toezicht, de personen belast met de effectieve leiding, de werknemers en gevolmachtigden te verzekeren van 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

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, les membres de son conseil de surveillance, les personnes chargées de la direction 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

beeld te geven van het hele scala van risico's die de 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.

§ 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.

et peuvent fournir une vue complète de toute la gamme des risques auxquels est exposé le fournisseur.

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. 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.

Afdeling V

Leiding, professionele betrouwbaarheid en passende deskundigheid

Art. 25

§ 1. De leden van de raad van toezicht van de systeemrelevant 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 het 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 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;

Section V

Dirigeants, 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 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° 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 niethernieuwing 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 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 opnieuw beoordelen 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, evenals de personen die verantwoordelijk zijn voor de onafhankelijke controlefuncties besteden de nodige tijd aan de uitoefening van hun functies bij de systeemrelevante aanbieder.

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 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

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 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, 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 aanbieder en, anderzijds, het toezicht op die leiding, en die binnen de 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

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, reposant notamment sur:

1° des objectifs consignés par écrit axés sur la sécurité et l'efficacité de la fourniture de services de messagerie financière, et qui soutiennent 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'une part, et le contrôle sur cette direction d'autre part, et prévoyant, au sein du fournisseur, 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

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 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.

Art. 31

De in artikel 30 bedoelde organisatieregeling is 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:

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.

§ 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

Les dispositifs organisationnels visés à l'article 30 sont 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 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° 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 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. 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.

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 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

Les membres du conseil de surveillance disposent d'un accès adéquat aux informations et 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 comité 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.

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

2° in een reeks stressscenario's het herstel of de ordelijke liquidatie te verzekeren overeenkomstig het plan bepaald in artikel 48.

§ 2. Bij reglement vastgesteld in toepassing van artikel 8, § 2, van de wet van 22 februari 1998 kan de Bank nadere regels vastleggen tot bepaling van de vereisten bedoeld in paragraaf 1.

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 vereisten 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.

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

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

§ 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 approprié 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.

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 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 aanbieder zijn verantwoordelijkheden voor het vervullen van zijn verplichtingen uit hoofde van deze wet delegeert;

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

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

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

CHAPITRE 6

Externalisation

Art. 40

§ 1er. Si le fournisseur d'importance systémique externalise des activités, 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 pour respecter les obligations qui lui incombent en vertu de la présente loi;

2° la relation et les obligations du fournisseur vis-à-vis de ses clients ne sont pas modifiées;

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

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

5° de 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 aanbieder de overeenkomst beëindigt.

Art. 41

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

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

5° le fournisseur 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'y mettre un terme.

Art. 41

§ 1er. Un fournisseur d'importance systémique ne peut externaliser des tâches opérationnelles importantes 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 tâches opérationnelles 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

Le fournisseur d'importance systémique a des objectifs clairement définis et réalisables, notamment en

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 toepassingsmodaliteiten van de vereisten van dit hoofdstuk preciseren en aanvullen.

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 contracten 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

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.

Section II

Risque juridique

Art. 46

§ 1er. Le 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. Le fournisseur d'importance systémique conçoit ses règles, procédures et contrats de telle manière qu'ils soient exécutoires dans tous les systèmes juridiques pertinents.

§ 3. Le 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

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 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 bedrijfsactiviteiten en -diensten. Hij identificeert specifieke scenario's waardoor hij deze kritieke bedrijfsactiviteiten en -diensten als going concern mogelijkerwijze niet zou kunnen leveren en beoordeelt de effectiviteit van alle herstelacties en een ordelijke liquidatie. Hij beoordeelt de kritieke bedrijfsactiviteiten en -diensten tenminste eenmaal per jaar.

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 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 opérations et services critiques. Il identifie les scénarios susceptibles de l'empêcher d'assurer sans interruption ces opérations et services critiques, et évalue l'efficacité d'un éventail complet de solutions permettant le redressement ou la cessation ordonnée de ses activités. Il réexamine les opérations et services critiques au moins une fois par an.

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 bevatten onder meer een inhoudelijke samenvatting van de cruciale herstel- of ordelijke liquidatiestrategieën, een herformulering van de kritieke activiteiten en -diensten 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 bedrijfsvoering en diensten. 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 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 algemeen 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.

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 opérations et services critiques 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 de son profil de risque d'activité et du temps nécessaire pour procéder, si besoin, à un redressement ou à la liquidation ordonnée de ses opérations et services essentiels. 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 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 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. 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, voert een systeemrelevante aanbieder een audit uit op systemen, operationeel beleid, procedures en controles, en toetst en test deze.

§ 2. Een systeemrelevante aanbieder stelt doelstellingen vast met betrekking tot het dienstverleningsniveau en de betrouwbaarheid van de exploitatie, evenals 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 toetst het plan 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 en bewaakt en beheert deze, die kritieke dienstafnemers, andere financiële marktinfrastructuren en

§ 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 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

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. Het 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 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 het bedrijfscontinuïteitsplan mogelijks geheel of gedeeltelijk wordt toegepast.

§ 3. Een systeemrelevante aanbieder verzekert dat hij de 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

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 supervision 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 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 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 lorsque le plan de continuité d'activité est potentiellement 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

niveau van digitale operationele weerbaarheid te verkrijgen. De aanbieder identificeert alle activiteiten en onderliggende activa, en treft 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 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 60, § 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 materiële 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;

d'atteindre un niveau élevé de résilience opérationnelle numérique. Après avoir identifié toutes ses opérations et les actifs sous-jacents, le fournisseur instaure des mesures afin de les protéger des cyber-attaques, 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 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 60, § 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 rétablissement 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° 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 materiële 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 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 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;

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 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, 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 ICT;

2° wordt niet betrokken bij interne auditactiviteiten;

3° heeft voldoende gezag, status en middelen;

4° heeft een gedegen kennis van logische en fysieke beveiligingsoplossingen evenals een grondig begrip van het bedrijfsmodel en de organisatiestructuur van de systeemrelevante aanbieder;

5° 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.

§ 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.

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

3° dispose d'une autorité, d'un statut et de ressources suffisants;

4° 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;

5° 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. 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 ICT, 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

§ 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 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

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 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

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 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

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 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

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 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.

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 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. 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;

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.

§ 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° 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. 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;

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.

§ 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° 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. 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.

§ 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 financiële entiteit haar 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.

§ 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. 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. 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 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

§ 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 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,

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 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 cliënten 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

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 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 clients 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

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.

§ 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,

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. 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

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.

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 Belgische autoriteit die verantwoordelijk is voor TLPT-gerelateerde aangelegenheden in de financiële sector.

§ 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.

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.

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 l'autorité belge chargée des questions liées aux tests de pénétration fondés sur la menace dans le secteur financier.

§ 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. 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.

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 cliënten;

2° de mate waarin cliënten 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.

§ 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

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 clients touchés;

2° la mesure dans laquelle les clients 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

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;

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 cliënten 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 cliënten die mogelijk getroffen kunnen worden in kennis van de passende beschermingsmaatregelen die zij kunnen nemen.

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 importantes 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.

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

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° 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 clients 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 clients susceptibles d'être affectés de toute mesure de protection appropriée que ces derniers pourraient envisager de prendre.

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 dienstverleningscriteria. Hij stelt non-discriminatoire procedures vast, en maakt deze openbaar, op basis waarvan het mogelijk is het beroep op de diensten van de aanbieder te schorsen of ordelijk te beëindigen wanneer de dienstafnemer niet voldoet aan de dienstverleningscriteria. De systeemrelevante aanbieder herziet de procedures tenminste eenmaal per jaar.

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.

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 de fourniture de services. 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 de fourniture de services. Il réexamine ces procédures au moins une fois par an.

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.

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 de individuele financiële berichtendiensten evenals het beleid inzake kortingen. De systeemrelevante aanbieder geeft heldere beschrijvingen van de betaalde diensten, zodat vergelijking mogelijk is.

HOOFDSTUK 8

Toezicht op aanbieders van financiële berichtendiensten

Afdeling I

Toezicht door de Bank

Art. 74

§ 1. Aanbieders van financiële berichtendiensten 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

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.

CHAPITRE 8

Surveillance des fournisseurs de services de messagerie financière

Section Ire

Surveillance par la Banque

Art. 74

§ 1er. Les fournisseurs de services de messagerie financière 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

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 modaliteiten 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.

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.

§ 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.

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.

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.

§ 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.

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 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.

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 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.

Afdeling II

Coöperatief toezicht

Art. 81

§ 1. In voorkomend geval kan de Bank niet-bindende samenwerkingsregelingen sluiten met autoriteiten van de 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 van financiële berichtendiensten 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 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 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 de aanbieder in de komende 12 maanden niet meer zal werken overeenkomstig deze bepalingen;

Section II

Surveillance coopérative

Art. 81

§ 1er. Le cas échéant, la Banque peut conclure des arrangements de coopération non contraignants avec 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 de services de messagerie financière 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 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 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° que le fournisseur risque de ne plus fonctionner en conformité avec ces dispositions au cours des douze prochains mois;

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

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

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 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.

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

4 que l'exercice de l'activité du fournisseur présente une menace pour l'assurance des objectifs visés à l'article 2, § 1er,

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 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

§ 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:

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

2° 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 bestuurder, 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.

§ 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 of de vervulling van de formaliteiten overeenkomstig de voorschriften van paragraaf 1.

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.

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

2° suspendre 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.

§ 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 ou formalités accomplies conformément aux dispositions du paragraphe 1er.

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 aanbieder voorleggen, inclusief de algemene vergadering.

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

§ 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 l'établissement 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 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.

§ 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 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 als bedoeld 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 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 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 de betaling van 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. 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

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

vermijden, mag dit maximum worden verhoogd tot het drievoud van deze winst of dit verlies.

§ 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.

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

maximum peut être porté au triple du montant de ce profit ou de cette perte.

§ 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.

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, modifié

België, voor het laatst gewijzigd bij de wet van 20 juli 2022, 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.

11 december 2024

Koen Van den Heuvel (cd&v)
Steven Matheï (cd&v)
Nathalie Muylle (cd&v)

en dernier lieu par la loi du 20 juillet 2022, 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.

11 décembre 2024

Centrale drukkerij - Imprimerie centrale