LOIS, DECRETS, ORDONNANCES ET REGLEMENTS
WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN

SERVICE PUBLIC FEDERAL FINANCES

[C − 2019/40243]

25 JANVIER 2019. — Arrêté royal portant approbation du règlement de la Banque nationale de Belgique du 20 novembre 2018 précisant les modalités de certaines obligations de la loi du 24 mars 2017 relative à la surveillance des processeurs d'opérations de paiement

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique, l'article 8, § 2 ;

Vu la loi du 24 mars 2017 relative à la surveillance des processeurs d'opérations de paiement, les articles 8, alinéa 2, 11, § 5, 12, § 6 et 13, § 3 et § 4 ;

Sur la proposition du Ministre des Finances,

Nous avons arrêté et arrêtons :

Article 1er. Le règlement de la Banque nationale de Belgique du 20 novembre 2018 précisant les modalités de certaines obligations de la loi du 24 mars 2017 relative à la surveillance des processeurs d'opérations de paiement, annexé au présent arrêté, est approuvé.

Art. 2. Le présent arrêté entre en vigueur le jour de sa publication au *Moniteur belge*.

Art. 3. Le ministre qui a les Finances dans ses attributions est chargé de l'exécution du présent arrêté.

Donné à Bruxelles, le 25 janvier 2019.

PHILIPPE

Par le Roi :

Le Vice-Premier Ministre et Ministre des Finances,
A. DE CROO

Annexe à l'arrêté royal du 25 janvier 2019 portant approbation du règlement de la Banque nationale de Belgique du 20 novembre 2018 précisant les modalités de certaines obligations de la loi du 24 mars 2017 relative à la surveillance des processeurs d'opérations de paiement

La Banque nationale de Belgique,

Vu la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique, l'article 8 ;

FEDERALE OVERHEIDSDIENST FINANCIEN

[C − 2019/40243]

25 JANUARI 2019. — Koninklijk besluit tot goedkeuring van het reglement van de Nationale Bank van België van 20 november 2018 tot vaststelling van de modaliteiten van bepaalde verplichtingen van de wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, artikel 8, § 2;

Gelet op de wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties, de artikelen 8, tweede lid, 11, § 5, 12, § 6 en 13, § 3 en § 4;

Op de voordracht van de Minister van Financiën,

Hebben Wij besloten en besluiten Wij :

Artikel 1. Het bij dit besluit gevoegde reglement van de Nationale Bank van België van 20 november 2018 tot vaststelling van de modaliteiten van bepaalde verplichtingen van de wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties wordt goedgekeurd.

Art. 2. Dit besluit treedt in werking op de dag dat het in het *Belgisch Staatsblad* wordt bekendgemaakt.

Art. 3. De minister bevoegd voor Financiën is belast met de uitvoering van dit besluit.

Gegeven te Brussel 25 januari 2019.

FILIP

Van Koningswege :

De Vice-Eerste Minister en Minister van Financiën,
A. DE CROO

Bijlage bij het koninklijk besluit van 25 januari 2019 tot goedkeuring van het reglement van de Nationale Bank van België van 20 november 2018 tot vaststelling van de modaliteiten van bepaalde verplichtingen van de wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties

De Nationale Bank van België,

Gelet op de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, artikel 8;

Vu la loi du 24 mars 2017 relative à la surveillance des processeurs d'opérations de paiement, les articles 8, alinéa 2, 11, § 5, 12, § 6 et 13, §§ 3 et 4,

Arrête :

CHAPITRE 1er. — *Définitions*

Article 1er. Pour l'application du présent règlement, il y a lieu d'entendre par :

1° ″la loi″ : la loi du 24 mars 2017 relative à la surveillance des processeurs d'opérations de paiement ;

2° ″processeur″ : tout processeur d'importance systémique tel que visé par la loi.

Pour le reste, les définitions de l'article 3 de la loi sont applicables pour l'application du présent règlement.

CHAPITRE 2. — *Obligations de l'exploitant d'un schéma de paiement*

Art. 2. Les dispositions de ce Chapitre précisent les modalités des obligations visées à l'article 8 de la loi.

Art. 3. § 1er. Lorsqu'il existe une relation contractuelle entre l'exploitant d'un schéma de paiement et un processeur ou que l'exploitant d'un schéma de paiement impose au processeur d'obtenir son agrément (licence ou équivalent) pour traiter ses opérations, l'exploitant du schéma de paiement devra disposer d'une procédure visant à s'assurer de la capacité du processeur de se conformer aux dispositions du Chapitre 3 de la loi, et prend spécifiquement en compte la capacité du processeur à implémenter les développements et les adaptations qu'il doit apporter à ses systèmes afin de traiter les opérations du schéma de paiement.

§ 2. La diligence requise de l'exploitant du schéma de paiement s'exerce :

1° lorsqu'un processeur non-systémique utilisé par le schéma devient systémique et que notification en est faite par la Banque au processeur ;

2° préalablement à l'établissement de la relation entre l'exploitant du schéma de paiement et le processeur. L'exploitant du schéma de paiement s'abstient d'entrer en relation contractuelle avec un processeur qu'il estime, après analyse, incapable de se conformer au Chapitre 3 de la loi ;

3° durant la relation entre l'exploitant du schéma de paiement et le processeur. A cette fin l'exploitant du schéma de paiement obtient annuellement du processeur la confirmation qu'il est toujours en conformité avec le Chapitre 3 de la loi. Cette confirmation est réalisée ou validée par un auditeur interne du processeur ou externe.

§ 3. L'exploitant du schéma de paiement tient à la disposition de la Banque la documentation de la procédure visée au paragraphe premier, ainsi que les analyses qu'il a effectuées ou fait effectuer en vertu de cette procédure et les attestations annuelles obtenues des processeurs avec lesquels l'exploitant du schéma travaille sur une base contractuelle.

CHAPITRE 3. — *Identification et gestion des risques*

Section 1re. — Conception des systèmes

Art. 4. Les dispositions de cette Section précisent les modalités des obligations visées à l'article 11, § 2 de la loi.

Art. 5. Tout processeur met en place, préventivement, toute mesure raisonnable de réduction des risques opérationnels et de sécurité qu'il a identifiés.

Art. 6. Tout processeur prend les dispositions nécessaires en matière de cybersécurité et assure la confidentialité, l'intégrité et la disponibilité de l'ensemble de ses ressources physiques et logiques, ainsi que celles des données de paiement sensibles qu'elles soient stockées, en transit ou en cours de traitement. Le processeur met notamment, mais pas exclusivement, en œuvre les principes suivants :

1° une approche de type ″défense en profondeur″ (defence in depth), impliquant des contrôles en couches multiples et successives qui couvrent tant le personnel, les processus et la technologie utilisée ;

2° l'application de la ségrégation tant au niveau des environnements IT (développement, intégration, production) qu'au niveau des tâches à effectuer par le personnel. Le personnel est dûment formé et surveillé et dispose des accès aux fonctionnalités et aux données sur une base ″besoin d'en connaître″ (need-to-know). En outre, les membres du personnel se voient accorder les accès aux seules ressources indispensables à l'exercice de leurs tâches et responsabilités (principe du ″moindre privilège″ (least privilege)). L'allocation des privilèges d'accès fait l'objet d'une révision à intervalles réguliers, au minimum

Gelet op de wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties, de artikelen 8, tweede lid, 11, § 5, 12, § 6 en 13, §§ 3 en 4,

Besluit :

HOOFDSTUK 1. — *Definities*

Artikel 1. Voor de toepassing van dit reglement wordt verstaan onder:

1° ″de wet″: de wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties;

2° ″verwerker″: iedere systeemrelevante verwerker als bedoeld in de wet.

Voor het overige gelden de definities van artikel 3 van de wet voor de toepassing van dit reglement.

HOOFDSTUK 2. — *Verplichtingen van de uitbater van een betalingsschema*

Art. 2. Dit hoofdstuk legt de modaliteiten vast van de in artikel 8 van de wet bedoelde verplichtingen.

Art. 3. § 1. Wanneer er een contractuele relatie bestaat tussen de uitbater van een betalingsschema en een verwerker, of wanneer de uitbater van een betalingsschema de verwerker verplicht een vergunning (een licentie of een gelijkwaardig document) te verkrijgen voor de verwerking van zijn transacties, moet de uitbater van het betalingsschema over een procedure beschikken om zich ervan te vergewissen dat de verwerker kan voldoen aan de bepalingen van Hoofdstuk 3 van de wet, waarbij in het bijzonder rekening wordt gehouden met het vermogen van de verwerker om de wijzigingen en aanpassingen die hij in zijn systemen moet aanbrengen om de via het betalingsschema uit te voeren transacties te verwerken, te implementeren.

§ 2. De zorgvuldigheid die van de uitbater van het betalingsschema wordt vereist, dient in acht te worden genomen:

1° wanneer een niet-systeemrelevante verwerker waarop een beroep wordt gedaan door het schema, systeemrelevant wordt en de verwerker daarvan in kennis wordt gesteld door de Bank;

2° vóór de relatie met de verwerker wordt aangegaan. De uitbater van het betalingsschema gaat geen contractuele relatie aan met een verwerker die hij na analyse niet in staat acht te voldoen aan Hoofdstuk 3 van de wet;

3° tijdens de relatie met de verwerker. De uitbater van het betalingsschema dient van de verwerker jaarlijks bevestiging te krijgen dat hij nog steeds voldoet aan Hoofdstuk 3 van de wet. Die bevestiging wordt door een interne auditor van de verwerker of door een externe auditor gegeven of gevalideerd.

§ 3. De uitbater van het betalingsschema houdt de documentatie van de in de eerste paragraaf bedoelde procedure, evenals de analyses die hij op grond van die procedure heeft uitgevoerd of laat uitvoeren en de jaarlijkse attesten van de verwerkers met wie hij op contractuele basis samenwerkt, ter beschikking van de Bank.

HOOFDSTUK 3. — *Risico-identificatie en -beheer*

Afdeling 1. — Ontwerp van de systemen

Art. 4. Deze afdeling legt de modaliteiten vast van de in artikel 11, § 2, van de wet bedoelde verplichtingen.

Art. 5. Elke verwerker neemt preventief alle redelijke maatregelen om de door hem geïdentificeerde operationele en veiligheidsrisico's te beperken.

Art. 6. Elke verwerker neemt de nodige cyberveiligheidsmaatregelen en waarborgt de vertrouwelijkheid, integriteit en beschikbaarheid van al zijn fysieke en logische middelen en van gevoelige betalingsgegevens, ongeacht of deze zijn opgeslagen of worden verstuurd of verwerkt. De verwerker past met name, maar niet uitsluitend, de volgende principes toe:

1° een benadering van het type ″verdediging in de diepte″ (defence in depth), waarbij gelaagde en opeenvolgende controles van het personeel, de processen en de gebruikte technologie worden uitgevoerd;

2° segregatie in de IT-omgevingen (ontwikkeling, integratie, productie) en in de door het personeel uit te voeren taken. Het personeel wordt terdege opgeleid en gecontroleerd en heeft toegang tot de functies en de gegevens op ″need-to-know″-basis. Voorts krijgen de personeelsleden enkel toegang tot de middelen die noodzakelijk zijn om hun taken uit te voeren en hun verantwoordelijkheden uit te oefenen (″least privilege″-beginsel). De toewijzing van toegangsprivileges wordt regelmatig en minstens eenmaal per jaar herzien en in elk geval (a) bij een overplaatsing binnen de onderneming, (b) bij de lancering van nieuwe

une fois par an, et dans tous les cas (a) lors d'un changement d'affectation à l'intérieur de l'entreprise, (b) lors de la mise en production de nouveaux services, (c) lors de toute modification affectant une prestation de service et (d) à la suite de tout incident trouvant sa cause, même partiellement, dans un accès inadéquat à une ou plusieurs ressources. Des "journaux/historiques d'événements" (loggings) relatifs aux accès sont réalisés et conservés pendant une période corrélée à la criticité de la fonctionnalité, du processus ou de "l'actif du système d'information" (information asset). Ces "journaux/historiques d'événements" sont notamment utilisés afin de faciliter l'identification et l'examen de toute activité anormale détectée dans l'exercice de la fourniture de services.

Art. 7. Tout processeur dispose de mesures de sécurité physique adéquates afin de protéger notamment l'ensemble des données qui font l'objet des services de traitement, ainsi que les systèmes ICT utilisés pour prester ces services.

Art. 8. Tout processeur dispose d'un processus formel de gestion des changements, assurant que ceux-ci soient correctement planifiés, testés, documentés et autorisés. En fonction des menaces observées en matière de sécurité ainsi que des modifications envisagées, lesdits tests incorporent des scénarios impliquant notamment des attaques déjà connues ou vraisemblables. Le processeur détermine si les changements apportés à son environnement opérationnel affectent d'une manière ou d'une autre les mesures de sécurité en place, ou requièrent l'adoption de mesures supplémentaires de réduction des risques.

Art. 9. Tout processeur s'assure de manière régulière que l'ensemble des programmes utilisés pour la prestation de ses services soient en permanence mis à jour, et que les patches et correctifs critiques, et singulièrement ceux relatifs à la sécurité, soient déployés sans retard. Des mécanismes de contrôle d'intégrité vérifient en permanence l'intégrité des applications, des "microprogrammes/micrologiciels" (firmware) ainsi que des données utilisées dans la prestation des services de traitement.

Art. 10. Tout processeur contrôle en permanence le degré d'utilisation des ressources informatiques mises en œuvre, et veille à disposer à tout moment des réserves de capacités adéquates pour faire face à des variations imprévues d'activités. Ce contrôle s'effectue également sur longues périodes afin de détecter les évolutions à l'œuvre et afin de pouvoir prévoir, le cas échéant, suffisamment à l'avance les adaptations majeures d'infrastructure à réaliser.

La Banque peut émettre des directives pour déterminer quelles adaptations sont majeures. Le processeur consulte la Banque en cas de doute sur l'importance de l'adaptation.

Art. 11. Tout processeur choisit son infrastructure et les technologies utilisées en tenant compte de l'évolution probable de ses activités.

Art. 12. Tout processeur évalue et implémente les mesures complémentaires à celles visées aux articles 5 à 11, qu'il convient de mettre en place pour atteindre les objectifs repris à l'article 11, § 2, de la loi.

Section 2. — Continuité des activités

Art. 13. Les dispositions de cette Section précisent les modalités des obligations visées à l'article 11, § 3, de la loi.

Art. 14. § 1er. La gestion efficace de la continuité des activités telle que mise en place doit avoir pour objectif de permettre au processeur d'être en toute circonstance et à tout moment capable de prester les services de traitement qui lui incombent et à limiter au maximum la durée des interruptions. Cette disposition n'exclut toutefois pas pour le processeur la possibilité de planifier des interruptions de services pour réaliser la maintenance de ses systèmes.

§ 2. Le processeur priorise les actions à entreprendre en matière de continuité des opérations, en analysant notamment les fonctions, processus, systèmes et transactions identifiés et classifiés comme critiques, et en adoptant une approche qui est notamment, mais pas exclusivement, basée sur les risques. Cette analyse permet au processeur de développer et d'activer à tout moment des procédures de continuité des activités afin de réagir de façon appropriée aux urgences, tout en continuant à prester ses activités critiques.

Art. 15. § 1er. Le processeur dispose d'un plan de continuité visant à :

1° limiter au maximum la durée des interruptions d'activités et

2° protéger et, si besoin, rétablir l'intégrité et la disponibilité des opérations et de la confidentialité des données.

diensten, (c) bij elke wijziging die invloed heeft op een dienstverlening en (d) bij incidenten die, zelfs gedeeltelijk, worden veroorzaakt door ongepaste toegang tot een of meerdere middelen. Over de toegangen worden er logs gecreëerd, die bewaard worden gedurende een periode die gecorreleerd is aan de kritikaliteit van de functie, het proces of de informatiemiddelen (information asset). Die logs worden met name gebruikt om de identificatie en het onderzoek van bij het verlenen van diensten vastgestelde abnormale activiteiten te vergemakkelijken.

Art. 7. Elke verwerker beschikt over passende fysieke veiligheidsmaatregelen om met name alle gegevens die door hem worden verwerkt, en de voor die diensten gebruikte ICT-systemen te beveiligen.

Art. 8. Elke verwerker beschikt over een formeel proces voor het beheer van de wijzigingen, dat ervoor zorgt dat deze wijzigingen naar behoren gepland, getest, gedocumenteerd en goedgekeurd worden. Afhankelijk van de vastgestelde veiligheidsdreigingen en van de geplande wijzigingen omvatten die tests scenario's waarin met name wordt uitgegaan van bekende of plausibele aanvallen. De verwerker bepaalt of de wijzigingen in zijn operationele omgeving op enigerlei wijze gevolgen hebben voor de bestaande veiligheidsmaatregelen, dan wel de invoering van bijkomende risicobeperkende maatregelen vereisen.

Art. 9. Elke verwerker controleert regelmatig of alle programma's die hij voor zijn dienstverlening gebruikt, permanent worden bijgewerkt en dat de kritieke patches (correcties) en in het bijzonder die welke verband houden met de beveiliging, onverwijld worden toegepast. Mechanismen voor integriteitscontrole verifiëren voortdurend de integriteit van de toepassingen, van de "microprogramma's/microsoftware" (firmware), en van de gegevens die bij het verrichten van de verwerkingsdiensten worden gebruikt.

Art. 10. Elke verwerker controleert voortdurend het niveau van benutting van de gebruikte informaticamiddelen en zorgt ervoor dat hij te allen tijde over voldoende reservecapaciteit beschikt om onverwachte schommelingen in de activiteiten te kunnen opvangen. Die controle wordt ook over lange periodes uitgevoerd om ontwikkelingen te kunnen opsporen en, in voorkomend geval, belangrijke infrastructuuraanpassingen voldoende van tevoren te kunnen plannen.

De Bank kan richtlijnen uitvaardigen om te bepalen welke aanpassingen belangrijk zijn. In geval van twijfel over het belang van de aanpassingen raadpleegt de verwerker de Bank.

Art. 11. Elke verwerker houdt rekening met het waarschijnlijke verloop van zijn activiteiten bij de keuze van de door hem gebruikte infrastructuur en technologieën.

Art. 12. Elke verwerker evalueert en implementeert maatregelen ter aanvulling van de in de artikelen 5 tot 11 bedoelde maatregelen, die moeten worden genomen om de in artikel 11, § 2, van de wet vermelde doelstellingen te bereiken.

Afdeling 2. — Bedrijfscontinuïteit

Art. 13. Deze afdeling legt de modaliteiten vast van de in artikel 11, § 3, van de wet bedoelde verplichtingen.

Art. 14. § 1. Het doeltreffend bedrijfscontinuïteitsmanagement dat door de verwerker wordt toegepast, moet tot doel hebben hem in staat te stellen te allen tijde en onder alle omstandigheden de van hem verwachte verwerkingsdiensten te leveren en de duur van de onderbrekingen zoveel mogelijk te beperken. Dit sluit niet uit dat de verwerker onderbrekingen van de dienstverlening kan plannen om zijn systemen te onderhouden.

§ 2. De verwerker prioriteert de maatregelen die moeten worden genomen op het gebied van bedrijfscontinuïteit door met name de als kritiek aangemerkte functies, processen, systemen en transacties te analyseren en een benadering te hanteren die met name, maar niet uitsluitend, risicogebaseerd is. Op grond van die analyse kan de verwerker op elk ogenblik bedrijfscontinuïteitsprocedures ontwikkelen en activeren om passend te reageren op noodgevallen, zonder zijn kritieke activiteiten stop te zetten.

Art. 15. § 1. De verwerker beschikt over een bedrijfscontinuïteitsplan dat ertoe strekt:

1° de duur van de onderbrekingen van de bedrijfsactiviteiten zoveel mogelijk te beperken en

2° de integriteit en de beschikbaarheid van de verrichtingen en de vertrouwelijkheid van de gegevens te beschermen en, zo nodig, te herstellen.

Le plan de continuité est bien documenté, disponible et directement accessible au personnel des services opérationnels et de support. Ce plan se focalise sur le rétablissement rapide de l'exercice et du traitement des fonctions, processus, systèmes et transactions critiques.

§ 2. Le plan de continuité est testé au moins annuellement. Les tests considèrent un ensemble adéquat de scénarios plausibles, et incluent des procédures pour vérifier la capacité du personnel (y compris en matière de prise de décision) et des processus de faire face adéquatement aux scénarios proposés. Les plans sont tenus à jour :

1° régulièrement pour tenir compte des résultats des tests, des menaces nouvellement identifiées et des leçons tirées des incidents antérieurs et des objectifs adaptés de rétablissement des activités ;

2° après tout changement apporté aux systèmes et processus.

Art. 16. En situation d'urgence ou d'interruption des activités, le processeur dispose de et utilise des procédures de communication de crise afin d'informer rapidement et de manière appropriée toutes les parties prenantes qu'elles soient internes (direction, équipes techniques, etc.) ou externes (schémas de paiement, marchands, détenteurs de cartes, régulateurs, etc.).

Section 3. — Politique de gestion des risques opérationnels et de sécurité

Art. 17. Les dispositions de cette Section précisent les modalités des obligations visées à l'article 11, §§ 1er et 4 de la loi.

Art. 18. § 1er. Tout processeur conçoit, développe et met en œuvre sur une base permanente un cadre global de gestion des risques opérationnels. Ce cadre est présenté par la direction au conseil d'administration qui :

1° l'approuve formellement ;

2° veille à soutenir effectivement sa mise en œuvre et son évolution, en prenant les décisions adéquates en termes de moyens tant humains que techniques à y consacrer ;

3° est impliqué de façon active, notamment au moyen de rapports qui lui sont fournis par la direction, dans la définition du niveau de tolérance aux risques de l'entreprise, ainsi que dans la validation des orientations à suivre dans la mise en œuvre effective des mesures de réduction de risques.

§ 2. Le cadre global de gestion des risques opérationnels est documenté en détails et doit notamment, mais pas exclusivement :

1° détailler la politique globale de gestion des risques opérationnels pour l'ensemble de l'entreprise. A cette fin le processeur établit un inventaire complet, ainsi qu'une classification selon leur criticité respective (a) des fonctions opérationnelles, rôles clés et processus sous-jacents, ainsi que leurs interdépendances éventuelles et (b) des "actifs du système d'information", tels que les systèmes ICT, leurs configurations et leurs interconnexions avec d'autres systèmes internes et externes ;

2° prévoir la mise en œuvre de politiques spécifiques visant à disposer à tout moment des ressources humaines expérimentées, ainsi que des procédures et systèmes indispensables afin d'identifier, mesurer et gérer l'ensemble des risques opérationnels liés à la prestation de services de processing. À cet effet, le processeur veille à définir clairement les responsabilités incombant à chaque membre du personnel en matière de gestion des risques opérationnels, avec une attention particulière pour l'existence d'un processus clair et efficace de prise de décision en situation d'urgence et/ou période de crise.

§ 3. Le cadre global de gestion des risques opérationnels est revu selon une fréquence adéquate, au minimum une fois par an, de sorte que ses mises à jour intègrent les leçons tirées de sa mise en œuvre quotidienne. Une mise à jour est également effectuée :

1° à l'issue de chaque incident majeur, de nature opérationnelle ou relatif à la sécurité des services presté ;

2° préalablement à la mise en production de changements majeurs relatifs à l'infrastructure, aux processus et procédures.

La Banque peut émettre des directives pour déterminer quels incidents ou changements sont majeurs. Le processeur consulte la Banque en cas de doute sur l'importance de l'incident ou du changement.

Het bedrijfscontinuïteitsplan is goed gedocumenteerd, beschikbaar en rechtstreeks toegankelijk voor het personeel van de operationele en ondersteunende diensten. Dit plan spitst zich toe op het snelle herstel van de bedrijfsactiviteiten en van de verwerking van de kritieke functies, processen, systemen en transacties.

§ 2. Het bedrijfscontinuïteitsplan wordt minstens jaarlijks getest. De tests gaan uit van een adequate reeks plausibele scenario's en omvatten procedures om te controleren of het personeel (ook op het gebied van besluitvorming) en de processen passend kunnen reageren op de voorgestelde scenario's. De plannen worden als volgt bijgewerkt:

1° regelmatig, om rekening te houden met de resultaten van de tests, de nieuw vastgestelde dreigingen en de uit eerdere incidenten getrokken lessen en de aangepaste doelstellingen inzake het herstel van de bedrijfsactiviteiten;

2° na elke wijziging in de systemen en processen.

Art. 16. In noodsituaties of bij onderbreking van de bedrijfsactiviteiten beschikt de verwerker over procedures voor crisiscommunicatie waarvan hij gebruikmaakt om alle betrokkenen, ongeacht of ze intern (directie, technische teams, enz.) of extern (betalingsschema's, handelaars, kaarthouders, regulatoren, enz.) zijn, snel en op passende wijze in te lichten.

Afdeling 3. — Beleid inzake het beheer van operationele en veiligheidsrisico's

Art. 17. Deze afdeling legt de modaliteiten vast van de in artikel 11, §§ 1 en 4, van de wet bedoelde verplichtingen.

Art. 18. § 1. Elke verwerker ontwerpt, ontwikkelt en implementeert voortdurend een algemeen kader voor het beheer van operationele risico's. De directie legt dit kader voor aan de raad van bestuur die:

1° het formeel goedkeurt;

2° zorgt voor een doeltreffende ondersteuning bij de uitvoering en de ontwikkeling van het kader, door passende beslissingen te nemen met betrekking tot de personele en technische middelen die hiervoor moeten worden ingezet;

3° actief betrokken is, met name via de door de directie geleverde verslagen, bij de vaststelling van het risicotolerantieniveau van de onderneming, en bij de validatie van de richtsnoeren die moeten worden gevolgd bij de effectieve tenuitvoerlegging van de risicobeperkende maatregelen.

§ 2. Het algemeen kader voor het beheer van de operationele risico's wordt uitvoerig gedocumenteerd en moet in het bijzonder, maar niet uitsluitend:

1° het algemeen beleid inzake het beheer van operationele risico's op het niveau van de onderneming uitvoerig beschrijven. Met het oog hierop stelt de verwerker een volledige inventaris op, en maakt hij een indeling op basis van de respectieve kritikaliteit (a) van de operationele functies, sleutelrollen en onderliggende processen, alsook van hun eventuele interdependenties en (b) van de informatiemiddelen, zoals de ICT-systemen, hun configuratie en hun interconnecties met andere interne en externe systemen;

2° voorzien in de uitvoering van specifieke beleidslijnen om te allen tijde over ervaren personeel te beschikken, en over de procedures en systemen die nodig zijn om alle operationele risico's in verband met het verlenen van de verwerkingsdiensten te identificeren, meten en beheren. Daartoe geeft de verwerker een duidelijke omschrijving van de verantwoordelijkheden van elk personeelslid op het vlak van het beheer van de operationele risico's, met bijzondere aandacht voor het bestaan van een duidelijk en doeltreffend besluitvormingsproces in noodsituaties en/of crisisperiodes.

§ 3. Het algemeen kader voor het beheer van de operationele risico's wordt met een passende frequentie en minstens eenmaal per jaar herzien, zodat bij de bijwerking ervan rekening gehouden kan worden met de lessen die uit de dagelijkse uitvoering ervan zijn getrokken. Voorts wordt het kader ook bijgewerkt:

1° na elk ernstig incident dat van operationele aard is of betrekking heeft op de veiligheid van de geleverde diensten;

2° vóór de invoering van belangrijke wijzigingen in de infrastructuur, de processen en procedures.

De Bank kan richtlijnen uitvaardigen om te bepalen welke incidenten ernstig of welke wijzigingen belangrijk zijn. In geval van twijfel over de ernst van het incident of het belang van de wijzigingen raadpleegt de verwerker de Bank.

Art. 19. § 1er. Le processeur s'organise de manière telle qu'il surveille de près, sur une base permanente, les menaces et vulnérabilités. Il adapte régulièrement les scénarios de risques susceptibles d'impacter ses fonctions opérationnelles, processus et "actifs du système d'information" critiques.

§ 2. Pour atteindre l'objectif visé au paragraphe premier, le processeur effectue et documente des études et évaluations de risques, à une fréquence annuelle ou plus courte si la Banque l'exige, pour chaque fonction opérationnelle, processus et "actif du système d'information" tel qu'identifié et classé par niveau de criticité, ainsi que préalablement à toute modification majeure apportée à son infrastructure, ses processus et ses procédures. Les conclusions des études et évaluations de risques sont également utilisées afin de déterminer dans quelle mesure des adaptations doivent être apportées aux technologies utilisées, aux mesures de sécurité et aux procédures en place, ainsi qu'aux prestations offertes. Les études et évaluations de risques, ainsi que leurs conclusions sont tenues à la disposition de la Banque.

La Banque peut émettre des directives pour déterminer quels changements sont majeurs. Le processeur consulte la Banque en cas de doute sur l'importance du changement.

§ 3. L'identification et la gestion sur le terrain des risques opérationnels et de sécurité s'opère à l'aide d'un modèle interne de contrôle et de gestion des risques, tel que celui des trois lignes de défense. Ce modèle interne dispose de l'autorité, de l'indépendance et des ressources requises, ainsi que d'un canal de rapportage direct vers la direction et le conseil d'administration.

Les mesures mises en place pour gérer les risques opérationnels et de sécurité font l'objet d'un audit régulier, selon une fréquence adéquate mené par des auditeurs spécialisés en matière IT et de sécurité IT. L'audit est mené par des auditeurs internes mais indépendants des fonctions business, ou par des auditeurs externes du processeur.

CHAPITRE 4. — *Continuité des services de traitement des opérations de paiement*

Section 1re. — Conformité de l'organisation du processeur

Art. 20. Les dispositions de cette Section précisent les modalités des obligations visées à l'article 12, §§ 1er et 2 de la loi.

Art. 21. § 1er. Le processeur fait évaluer par un auditeur interne ou externe la conformité de son organisation avec les dispositions de l'article 12, §§ 1er et 2 de la loi. La Banque peut si elle l'estime nécessaire demander expressément que le processeur fasse réaliser cette évaluation par un organisme indépendant (c'est-à-dire qui ne fait pas partie de la même entité juridique que le processeur, ni du groupe auquel le processeur appartient) L'organisme indépendant devra jouir d'un degré élevé d'expertise et de compétence dans le domaine concerné et est reconnu comme tel par l'industrie concernée.

§ 2. Le rapport de conformité est actualisé au minimum tous les trois ans, ou après chaque adaptation majeure des infrastructures et/ou des processus du processeur.

La Banque peut émettre des directives pour déterminer quelles adaptations sont majeures. Le processeur consulte la Banque en cas de doute sur l'importance de l'adaptation.

Section 2. — Communication

Art. 22. Les dispositions de cette Section précisent les modalités des obligations visées à l'article 12, § 5, de la loi.

Art. 23. § 1er. Le processeur met en place un canal de communication permettant d'informer les prestataires de services de paiement, les schémas de paiement et les utilisateurs des services de paiement concernés des indisponibilités de service de traitement des opérations de paiement visées par la loi. Ce canal de communication peut notamment comprendre une page sur le site internet du processeur indiquant entre autres l'état du réseau.

Les informations transmises peuvent être différenciées en fonction de leurs destinataires et des besoins de ceux-ci en la matière :

1° pour les prestataires de services de paiement et pour les schémas de paiement il s'agira notamment des causes et conséquences, ainsi que la durée prévue de la perturbation et le délai de rétablissement total estimé ;

2° pour les utilisateurs des services de paiement, ces informations pourront se limiter à une estimation de la durée prévue de la perturbation et du délai de rétablissement total.

Ces informations seront communiquées sans délai dès qu'elles seront connues du processeur et seront mises à jour régulièrement.

Art. 19. § 1. De verwerker organiseert zich op een zodanige wijze dat hij de dreigingen en kwetsbaarheden voortdurend nauwgezet kan opvolgen. Hij past de scenario's met risico's die een impact kunnen hebben op zijn kritieke operationele functies, processen en informatiemiddelen, regelmatig aan.

§ 2. Om de in de paragraaf 1 bedoelde doelstelling te bereiken, voert de verwerker jaarlijks of vaker indien de Bank dat eist, risicostudies en -beoordelingen uit voor elke operationele functie, elk proces en elk informatiemiddel, zoals vastgesteld en ingedeeld per niveau van kritikaliteit, en vóór elke belangrijke wijziging in zijn infrastructuur, processen en procedures en documenteert hij die studies en beoordelingen. De conclusies van die risicostudies en -beoordelingen dienen ook gebruikt te worden om te bepalen in welke mate de gebruikte technologieën, de veiligheidsmaatregelen, de bestaande procedures, en de aangeboden prestaties moeten worden aangepast. De risicostudies en -beoordelingen en de conclusies ervan worden ter beschikking van de Bank gehouden.

De Bank kan richtlijnen uitvaardigen om te bepalen welke wijzigingen belangrijk zijn. In geval van twijfel over het belang van de wijzigingen raadpleegt de verwerker de Bank.

§ 3. Voor de identificatie en het beheer van de operationele risico's wordt in de praktijk gebruikgemaakt van een intern model voor de bewaking en het beheer van de risico's, zoals dat van de drie verdedigingslinies. Dit intern model beschikt over de vereiste autoriteit, onafhankelijkheid en middelen, evenals over een kanaal voor de rechtstreekse rapportering aan de directie en de raad van bestuur.

De maatregelen voor het beheer van de operationele en veiligheidsrisico's worden regelmatig onderworpen aan audits, die met een passende frequentie worden uitgevoerd door in IT en IT-veiligheid gespecialiseerde auditoren, die hetzij interne auditoren van de verwerker zijn die onafhankelijk zijn van de bedrijfsfuncties, hetzij externe auditoren.

HOOFDSTUK 4. — *Continuïteit van de diensten met betrekking tot de verwerking van betalingstransacties*

Afdeling 1. — Conformiteit van de organisatie van de verwerker

Art. 20. Deze afdeling legt de modaliteiten vast van de in artikel 12, §§ 1 en 2, van de wet bedoelde verplichtingen.

Art. 21. § 1. De verwerker moet door een interne of externe auditor laten beoordelen of zijn organisatie in overeenstemming is met de bepalingen van artikel 12, §§ 1 en 2, van de wet. Indien zij dit nodig acht kan de Bank uitdrukkelijk verlangen dat de verwerker deze beoordeling laat uitvoeren door een onafhankelijke instelling (d.w.z. een instelling die geen deel uitmaakt van dezelfde juridische entiteit als de verwerker, noch van de groep waartoe de verwerker behoort). De onafhankelijke instelling dient op het betrokken gebied over een hoog niveau van deskundigheid en bekwaamheid te beschikken en wordt als zodanig erkend door de betrokken sector.

§ 2. Het conformiteitsverslag wordt minstens om de drie jaar bijgewerkt, of na elke belangrijke aanpassing in de infrastructuren en/of processen van de verwerker.

De Bank kan richtlijnen uitvaardigen om te bepalen welke aanpassingen belangrijk zijn. In geval van twijfel over het belang van de aanpassingen raadpleegt de verwerker de Bank.

Afdeling 2. — Communicatie

Art. 22. Deze afdeling legt de modaliteiten vast van de in artikel 12, § 5, van de wet bedoelde verplichtingen.

Art. 23. § 1. De verwerker dient een communicatiekanaal op te zetten waarmee de betrokken betalingsdienstaanbieders, betalingsschema's en betalingsdienstgebruikers kunnen worden ingelicht wanneer de diensten met betrekking tot de verwerking van betalingstransacties niet beschikbaar zijn in de zin van de wet. Dit kan met name een pagina op de website van de verwerker zijn, waarop onder andere de staat van het netwerk wordt vermeld.

De informatie die wordt meegedeeld kan variëren naar gelang van de ontvanger ervan en diens behoeften ter zake:

1° voor betalingsdienstaanbieders en betalingsschema's is dit met name informatie over de oorzaken en gevolgen, de verwachte duur van de verstoring evenals de geschatte totale hersteltijd;

2° voor betalingsdienstgebruikers kan deze informatie zich beperken tot een schatting van de verwachte duur van de verstoring en van de totale hersteltijd.

Deze informatie wordt zo spoedig mogelijk meegedeeld zodra de verwerker erover beschikt en wordt regelmatig bijgewerkt.

Si le processeur est dans l'impossibilité de communiquer ces informations, l'exploitant du schéma de paiement visé à l'article 5 de la loi se chargera de communiquer aux prestataires de services de paiement et aux utilisateurs finaux les informations dont il dispose concernant notamment la durée prévue de la perturbation dans le traitement de ses opérations et le délai de rétablissement total estimé.

§ 2. Le processeur informe au préalable les prestataires de services de paiement, les schémas de paiement et les utilisateurs de services de paiement, du canal de communication qui sera utilisé en priorité aux fins visées au paragraphe premier, ainsi que d'un éventuel canal de réserve ou de secours.

CHAPITRE 5. — *Notification des incidents et communication de l'analyse approfondie*

Section 1re. — Modalités de notification des incidents et informations à fournir

Art. 24. Les dispositions de cette Section précisent les modalités des obligations visées à l'article 13, §§ 1er et 2, de la loi.

Art. 25. § 1er. Le processeur notifie la Banque de toute indisponibilité (au sens de la loi) des services de traitement des opérations de paiement. Cette notification peut être communiquée par téléphone ou par courrier électronique dans les délais prévus à l'article 13, § 1er, de la loi, et est en tout cas suivie par une deuxième notification par courrier électronique pour confirmation dans les 24 heures ouvrables après la première notification. Une liste de personnes de contact est convenue avec la Banque et fait l'objet d'une mise à jour à chaque changement de personne de contact.

§ 2. Les informations à transmettre lors des notifications de l'indisponibilité visées au paragraphe premier, comprennent au minimum :

1° la date et l'heure de détection et de début de l'indisponibilité ;

2° la description de l'incident ayant conduit à l'indisponibilité ;

3° le ou les schéma(s) de paiement concerné(s) ;

4° le volume de transactions concerné ;

5° la durée estimée ou mesurée, si l'indisponibilité a pris fin avant sa notification.

Si certaines de ces informations ne sont pas disponibles au moment de la notification, elles sont transmises dès qu'elles seront connues du processeur.

Section 2. — Communication de l'analyse approfondie d'un incident

Art. 26. Les dispositions de cette Section précisent les modalités des obligations visées à l'article 13, § 4, de la loi.

Art. 27. § 1er. L'analyse approfondie d'un incident qui constitue une infraction aux dispositions des articles 11 et 12 de la loi, est transmise à la Banque dès qu'elle est réalisée et validée par le processeur et au plus tard dans les deux semaines après la résolution de l'incident.

Si la nature et la complexité de l'incident ne permettent pas d'en réaliser une analyse suffisamment détaillée dans le délai visé à l'alinéa précédent, la Banque et le processeur peuvent convenir d'un délai supplémentaire, après communication d'une analyse intermédiaire.

§ 2. L'analyse approfondie indique également les mesures que le processeur envisage de prendre pour éviter que l'incident ne se reproduise et le délai endéans lequel elles seront mises en place.

§ 3. Le rapportage de l'analyse approfondie peut, le cas échéant et après accord de la Banque, être aligné avec d'autres rapportages d'incidents qui s'imposent au processeur en vertu d'autres législations.

CHAPITRE 6. — *Dispositions diverses*

Art. 28. Tout processeur examine et répond aux questions reprises dans l'annexe, pour valider sa conformité avec les Chapitres 3 et 4 de ce règlement. Ces questions sont fournies à titre de guidance.

Art. 29. Le présent règlement entre en vigueur à la date d'entrée en vigueur de l'arrêté royal qui l'approuve.

Bruxelles, le 20 novembre 2018.

Le Gouverneur,
J. SMETS

Indien de verwerker deze informatie niet kan meedelen, deelt de in artikel 5 van de wet bedoelde uitbater van het betalingsschema aan de betalingsdienstgebruikers en aan de eindgebruikers de informatie mee waarover hij beschikt, over met name de verwachte duur van de verstoring in de verwerking van de transacties en de geschatte totale hersteltijd.

§ 2. De verwerker licht de betalingsdienstaanbieders, de betalingsschema's en de betalingsdienstgebruikers vooraf in over het communicatiekanaal dat prioritair zal worden gebruikt voor de in paragraaf 1 bedoelde doelstellingen, en over het eventuele reserve- of noodkanaal.

HOOFDSTUK 5. — *Kennisgeving van incidenten en mededeling van de grondige analyse*

Afdeling 1. — Modaliteiten voor de kennisgeving van incidenten en te verstrekken informatie

Art. 24. Deze afdeling legt de modaliteiten vast van de in artikel 13, §§ 1 en 2, van de wet bedoelde verplichtingen.

Art. 25. § 1. De verwerker stelt de Bank in kennis wanneer de diensten met betrekking tot de verwerking van betalingstransacties niet beschikbaar zijn (in de zin van de wet). Die kennisgeving kan telefonisch of per e-mail worden meegedeeld binnen de in artikel 13, § 1, van de wet bepaalde termijnen en wordt in elk geval binnen 24 werkuren na de eerste kennisgeving gevolgd door een tweede kennisgeving per e-mail waarin de niet-beschikbaarheid wordt bevestigd. Er wordt een lijst met contactpersonen opgesteld in overleg met de Bank, die bij elke verandering van contactpersoon wordt bijgewerkt.

§ 2. De informatie die moet worden meegedeeld in de in paragraaf 1 bedoelde kennisgevingen van de niet-beschikbaarheid, bevat minstens:

1° de datum en het uur van de vaststelling en van het begin van de niet-beschikbaarheid;

2° de beschrijving van het incident dat aanleiding heeft gegeven tot de niet-beschikbaarheid;

3° het of de betrokken betalingsschema('s);

4° het betrokken transactievolume;

5° de vermoedelijke of gemeten duur indien de diensten opnieuw beschikbaar zijn vóór de kennisgeving van de niet-beschikbaarheid ervan.

Indien niet alle informatie beschikbaar is op het moment van de kennisgeving, deelt de verwerker de ontbrekende informatie mee zodra hij die heeft.

Afdeling 2. — Mededeling van de grondige analyse van een incident

Art. 26. In deze afdeling worden de modaliteiten van de in artikel 13, § 4, van de wet bedoelde verplichtingen vastgesteld.

Art. 27. § 1. De grondige analyse van een incident dat een inbreuk uitmaakt op de bepalingen van de artikelen 11 en 12 van de wet, wordt meegedeeld aan de Bank zodra ze is uitgevoerd en gevalideerd door de verwerker en uiterlijk twee weken nadat het incident is opgelost.

Indien het door de aard en de complexiteit van het incident niet mogelijk is om een voldoende gedetailleerde analyse uit te voeren binnen de in het vorige lid bedoelde termijn, kunnen de Bank en de verwerker in onderling overleg een bijkomende termijn vaststellen nadat de verwerker aan de Bank een tussentijdse analyse heeft bezorgd.

§ 2. In de grondige analyse worden eveneens de maatregelen vermeld die de verwerker voornemens is te treffen om te voorkomen dat het incident zich opnieuw voordoet, evenals de termijn waarbinnen deze maatregelen zullen worden genomen.

§ 3. De rapportering van de grondige analyse kan, in voorkomend geval en met instemming van de Bank, worden afgestemd op andere incidentrapporteringen die de verwerker krachtens andere wetgeving moet verrichten.

HOOFDSTUK 6. — *Diverse bepalingen*

Art. 28. Elke verwerker bestudeert en beantwoordt de in de bijlage opgenomen vragen om te bevestigen dat hij voldoet aan de hoofdstukken 3 en 4 van dit reglement. Deze vragen dienen als richtsnoer.

Art. 29. Dit reglement treedt in werking op de datum van inwerkingtreding van het koninklijk besluit tot goedkeuring ervan.

Brussel, 20 november 2018.

De Gouverneur,
J. SMETS

Annexe

Afin d'évaluer sa conformité aux Chapitres 3 et 4 de ce règlement, le processeur examine et répond aux questions suivantes :

1. DETECTION ET GESTION DES RISQUES

Cadre de gestion des risques à l'échelle de l'entreprise

- Quels sont les processus et les systèmes du processeur pour recenser et documenter ses risques, y compris les risques opérationnels, financiers et de ressources humaines pertinents ? Quels risques le processeur a-t-il recensés et documentés à l'aide de ses processus et de ses systèmes ?

- Quels sont les processus et les systèmes du processeur pour gérer ces risques ? Comment le processeur décide-t-il d'accepter les risques résiduels ?

- Comment le processeur réévalue-t-il ses risques et le caractère adéquat de son cadre de gestion des risques pour faire face aux risques recensés ? À quelle fréquence cette réévaluation est-elle effectuée ?

- Comment le processeur répond-il aux exigences légales ou réglementaires ou aux changements d'exigences ?

- Comment le processeur évalue-t-il les risques liés à ses relations avec les utilisateurs ?

- Comment le processeur intègre-t-il la gestion des risques dans son processus décisionnel stratégique, y compris l'évaluation des risques commerciaux généraux et de la situation financière ?

Dépendances à l'égard des tiers

- Comment le processeur recense-t-il et surveille-t-il les risques que les dépendances à l'égard de fournisseurs tiers pourraient poser pour ses activités ?

- Comment le processeur évalue-t-il que la sécurité, la fiabilité et la résilience de ses activités ne sont pas réduites par les dépendances à l'égard de tiers ?

- Comment le processeur gère-t-il et traite-t-il toute réduction non acceptée en matière de sécurité, de fiabilité et de résilience de ses activités découlant de ses dépendances à l'égard de tiers ?

Gouvernance du cadre de gestion des risques à l'échelle de l'entreprise

- Quelles sont les modalités de gouvernance du processeur pour le recensement et la gestion des risques ? Quelles sont les chaînes de responsabilité au sein du processeur en matière de gestion des risques ? À quelle fréquence l'efficacité de la fonction d'audit interne fait - elle l'objet d'un examen ?

- Comment le conseil d'administration du processeur examine-t-il et approuve-t-il explicitement le cadre de gestion des risques à l'échelle de l'entreprise ?

Fonction d'audit interne

- Comment le processeur assure-t-il l'indépendance et le professionnalisme de la fonction d'audit ? À quelles pratiques acceptées à l'échelle internationale qui régissent la profession d'auditeur la fonction d'audit interne adhère-t-elle ?

- Quels sont les mécanismes de reporting permettant à la fonction d'audit interne de communiquer ses constatations au conseil d'administration et, le cas échéant, à son autorité de contrôle ou d'oversight ?

2. SECURITE DE L'INFORMATION

Cadre de sécurité de l'information

- Quel est le cadre de sécurité de l'information du processeur à l'échelle de l'entreprise permettant de fournir une orientation générale et globale sur les solutions et les pratiques destinées à faire face aux risques de sécurité physique et de cybersécurité ? Comment ce cadre englobe-t-il les politiques et les procédures destinées à :

1° la catégorisation des actifs (systèmes et services) selon la confidentialité, l'intégrité et la disponibilité ;

2° le recensement continu des menaces internes et externes ;

3° la sélection, la mise en œuvre et la documentation des contrôles de sécurité afin d'atténuer les risques et les vulnérabilités recensés ; et

4° la gouvernance adéquate de toutes les activités de gestion des risques en matière de sécurité ?

- Comment le processeur intègre-t-il les normes internationales, nationales et sectorielles pertinentes dans ses politiques et ses procédures ?

Bijlage

Om te beoordelen of hij voldoet aan de hoofdstukken 3 en 4 van dit reglement bestudeert en beantwoordt de verwerker de volgende vragen:

1. RISICO-IDENTIFICATIE EN -BEHEER

Risicobeheerkader op het niveau van de onderneming

- Over welke processen en systemen beschikt de verwerker om de door hem gelopen risico's, met inbegrip van relevante operationele, financiële en personeelsrisico's, te identificeren en te documenteren? Welke risico's heeft de verwerker aan de hand van zijn processen en systemen geïdentificeerd en gedocumenteerd?

- Over welke processen en systemen beschikt de verwerker om deze risico's te beheren? Hoe beslist de verwerker of hij restrisico's aanvaardt?

- Hoe herbeoordeelt de verwerker zijn risico's en de geschiktheid van zijn risicobeheerkader om de geïdentificeerde risico's aan te pakken? Hoe vaak wordt deze herbeoordeling uitgevoerd?

- Hoe komt de verwerker tegemoet aan de wettelijke of reglementaire vereisten of aan veranderde vereisten?

- Hoe beoordeelt de verwerker de risico's die verbonden zijn aan zijn relaties met gebruikers?

- Hoe integreert de verwerker het risicobeheer, met inbegrip van de beoordeling van het algemeen bedrijfsrisico en de financiële toestand, in zijn strategisch besluitvormingsproces?

Afhankelijkheid van derden

- Hoe identificeert en bewaakt de verwerker de risico's die de afhankelijkheid van derde leveranciers kan inhouden voor zijn activiteiten?

- Hoe beoordeelt de verwerker of de veiligheid, betrouwbaarheid en veerkracht van zijn activiteiten niet worden verminderd door zijn afhankelijkheid van derden?

- Hoe beheert de verwerker een eventuele niet-aanvaarde vermindering van de veiligheid, betrouwbaarheid en veerkracht van zijn activiteiten als gevolg van zijn afhankelijkheid van derden en hoe pakt hij dit probleem aan?

Governance van het risicobeheerkader op het niveau van de onderneming

- Over welke governanceregelingen beschikt de verwerker voor het identificeren en beheren van risico's? Welke zijn de lijnen van verantwoordelijkheid en verantwoording bij de verwerker op het gebied van risicobeheer? Hoe vaak wordt de doeltreffendheid van de interne auditfunctie beoordeeld?

- Hoe wordt het risicobeheerkader op het niveau van de onderneming formeel onderzocht en goedgekeurd door de raad van bestuur?

Interne auditfunctie

- Hoe garandeert de verwerker de onafhankelijkheid en het professionalisme van de auditfunctie? Welke internationaal aanvaarde praktijken past de interneauditfunctie toe met betrekking tot het auditberoep?

- Van welke rapporteringsmechanismen maakt de interneauditfunctie gebruik om haar bevindingen aan de raad van bestuur en, in voorkomend geval, aan haar toezichthouder of overseer mee te delen?

2. INFORMATIEBEVEILIGING

Informatiebeveiligingskader

- Over welk informatiebeveiligingskader beschikt de verwerker op het niveau van de onderneming om algemene, overkoepelende richtlijnen te geven met betrekking tot oplossingen en methodes voor het aanpakken van risico's met betrekking tot de fysieke veiligheid en cyberveiligheidsrisico's? Welke beleidslijnen en procedures omvat dit kader voor:

1° de indeling van de activa (systemen en diensten) op grond van vertrouwelijkheid, integriteit en beschikbaarheid;

2° de voortdurende opsporing van interne en externe bedreigingen;

3° het selecteren, implementeren en documenteren van veiligheidscontroles om de vastgestelde risico's en kwetsbaarheden te verhelpen; en

4° het adequate beheer van alle activiteiten die verband houden met het beheer van het veiligheidsrisico?

- Hoe integreert de verwerker relevante internationale, nationale en sectorale normen in zijn beleidslijnen en procedures?

- Quelles sources de risques liés à la sécurité de l'information le processeur a-t-il recensées en ce qui concerne ses services critiques ? Comment le processeur a-t-il traité ces risques ?

- Quel est le rôle joué par le conseil d'administration dans le cadre de sécurité de l'information du processeur ? Le conseil d'administration examine-t-il et approuve-t-il explicitement ce cadre ? À quelle fréquence le conseil d'administration révise-t-il ce cadre ?

- Comment le conseil d'administration du processeur a-t-il approuvé les rôles et les responsabilités clés de la haute direction en matière de sécurité de l'information ?

Politiques et procédures de sécurité de l'information

- Quelles sont les politiques et procédures utilisées pour prévenir l'accès non autorisé et la divulgation non autorisée de l'information ? En particulier, quelles sont les politiques et les procédures concernant les aspects suivants :

1° l'octroi et la suppression d'autorisations aux utilisateurs, y compris l'accès logique et l'accès physique ;

2° la recertification périodique des privilèges d'utilisateur ;

3° l'octroi, l'utilisation et le contrôle des comptes administrateurs (ou hautement privilégiés) ;

4° la prévention des atteintes à la confidentialité des données ;

5° la protection de l'intégrité des systèmes contre les attaques logiques ou physiques ; et

6° l'intégration de contrôles dans des applications fournies au schéma de paiement pour prévenir les erreurs, la perte, la modification non autorisée ou l'utilisation abusive de l'information ?

- Comment le processeur s'assure-t-il que tous les employés et toutes les tierces parties concernées sont informés de leurs responsabilités, ainsi que des menaces à la sécurité, telles que définies dans le cadre de sécurité de l'information ?

- Quelles sont les politiques et procédures utilisées pour assurer la confidentialité, l'intégrité et la non-répudiation des données, y compris lorsqu'elles sont en transit sur les réseaux et stockées chez le processeur ?

- Quelles sont les politiques et procédures utilisées pour détecter les incidents liés à la sécurité de l'information, y réagir et rétablir la situation ?

Suivi de la conformité à la sécurité

- Comment le processeur vérifie-t-il la conformité à son cadre de sécurité de l'information et surveille-t-il l'efficacité des contrôles de sécurité ? Plus précisément, ces politiques et procédures comprennent-elles une analyse de vulnérabilité et des tests de pénétration au niveau de l'infrastructure et des applications ?

- Dans quelle mesure le cadre de sécurité de l'information du processeur est-il assujetti à un audit interne et externe ?

- Comment et à quelle fréquence le conseil d'administration du processeur est-il informé des principales constatations des activités de suivi de la conformité en matière de sécurité ?

Planification des capacités

- Quelles sont les politiques du processeur en matière de planification des capacités ? Comment le processeur surveille-t-il et ajuste-t-il l'utilisation des ressources pour répondre aux besoins du schéma de paiement et, le cas échéant, de ses participants, même au cours de périodes de tensions sur les marchés ? Comment le processeur aborde-t-il les situations où les besoins du schéma de paiement ou des participants dépassent la capacité opérationnelle ?

- Comment le processeur examine-t-il, audite-t-il et teste-t-il l'évolutivité et l'adéquation de sa capacité à gérer, à tout le moins, les volumes de tension projetés qui sont recensés par un schéma de paiement donnée et, le cas échéant, les volumes de tension projetés concomitants lorsqu'il agit pour plusieurs schémas de paiement ? À quelle fréquence le processeur effectue-t-il ces examens, audits et tests ?

Gestion du changement

- Comment les politiques et procédures du processeur en matière de gestion du changement et de gestion de projet atténuent-elles les risques que des changements nuisent fortuitement à la sécurité et à la fiabilité des activités du processeur ?

- Comment les politiques de gestion du changement élaborées par le processeur définissent-elles les responsabilités et procédures officielles de gestion pour la planification et les tests des changements, y compris en matière de tests de régression, de performance et de sécurité ?

- Welke bronnen van informatiebeveiligingsrisico's heeft de verwerker vastgesteld met betrekking tot zijn kritieke diensten? Hoe heeft de verwerker deze risico's aangepakt?

- Wat is de rol van de raad van bestuur van de verwerker met betrekking tot het informatiebeveiligingskader van de verwerker? Wordt dit kader formeel onderzocht en goedgekeurd door de raad van bestuur? Hoe vaak beoordeelt de raad van bestuur het kader?

- Hoe heeft de raad van bestuur van de verwerker de belangrijkste taken en verantwoordelijkheden van de effectieve leiding op het gebied van informatiebeveiliging goedgekeurd?

Beleidslijnen en procedures op het gebied van informatiebeveiliging

- Over welke beleidslijnen en procedures beschikt de verwerker om ongeoorloofde toegang tot en ongeoorloofde bekendmaking van informatie te voorkomen? Welke beleidslijnen en procedures worden er meer in het bijzonder gevolgd voor:

1° het verlenen en intrekken van toegangsrechten voor gebruikers, met inbegrip van logische en fysieke toegang;

2° de periodieke hercertificering van gebruikersprivileges;

3° het toekennen, gebruiken en beheren van beheerdersaccounts (of accounts met uitgebreide toegangsprivileges);

4° het voorkomen van inbreuken op de vertrouwelijkheid van gegevens;

5° de bescherming van de integriteit van de systemen tegen logische of fysieke aanvallen; en

6° het integreren van controles in toepassingen die aan het betalingsschema worden verstrekt om fouten, verlies, ongeoorloofde wijzigingen in of misbruik van informatie te voorkomen?

- Hoe zorgt de verwerker ervoor dat alle werknemers en betrokken externe partijen bewust worden gemaakt van hun verantwoordelijkheden en aansprakelijkheden en van veiligheidsbedreigingen, zoals gedefinieerd in het informatiebeveiligingskader?

- Welke beleidslijnen en procedures worden er gevolgd om de vertrouwelijkheid, integriteit en onweerlegbaarheid van gegevens te waarborgen, ook wanneer ze in transit zijn op de netwerken en wanneer ze bij de verwerker zijn opgeslagen?

- Welke beleidslijnen en procedures worden er gevolgd om informatieveiligheidsincidenten op te sporen, erop te reageren en de situatie te herstellen?

Monitoring van de naleving van het informatiebeveiligingskader

- Hoe gaat de verwerker na of zijn informatiebeveiligingskader wordt nageleefd en hoe houdt hij toezicht op de doeltreffendheid van de bestaande veiligheidscontroles? Meer in het bijzonder, voorzien deze beleidslijnen en procedures in de uitvoering van kwetsbaarheidsanalyses en penetratietests op het niveau van de infrastructuur en de toepassingen?

- In hoeverre is het informatiebeveiligingskader van de verwerker onderworpen aan interne en externe audits?

- Hoe en met welke frequentie wordt de raad van bestuur van de verwerker op de hoogte gebracht van de voornaamste bevindingen van de monitoring van de naleving van het informatiebeveiligingskader?

Capaciteitsplanning

- Wat zijn de beleidslijnen van de verwerker op het gebied van capaciteitsplanning? Hoe houdt de verwerker toezicht op het gebruik van de middelen en hoe past hij dit aan om te voldoen aan de behoeften van het betalingsschema en, in voorkomend geval, van haar deelnemers, zelfs onder gespannen marktomstandigheden? Hoe reageert de verwerker wanneer de behoeften van de betalingsschema's of van zijn deelnemers de operationele capaciteit overschrijden?

- Hoe onderzoekt, controleert en test de verwerker de opschaalbaarheid en toereikendheid van zijn capaciteit om minstens de door een bepaald betalingsschema vastgestelde geprojecteerde stressvolumes, en, in voorkomend geval, gelijktijdige geprojecteerde stressvolumes te beheren wanneer er meerdere betalingsschema's zijn? Hoe vaak voert de verwerker deze onderzoeken, audits en tests uit?

Veranderingsbeheer

- Hoe beperken de beleidslijnen en procedures voor veranderingsbeheer en projectbeheer van de verwerker de risico's dat wijzigingen een ongewilde invloed hebben op de veiligheid en betrouwbaarheid van de activiteiten van de verwerker?

- Hoe bepalen de beleidslijnen inzake veranderingsbeheer van de verwerker de formele bestuurlijke verantwoordelijkheden en procedures voor het plannen en testen van veranderingen, met inbegrip van regressie-, prestatie- en veiligheidstests?

- Dans quelle mesure les changements ayant une incidence sur les utilisateurs sont-ils soumis à la consultation du schéma de paiement et testés avec la participation de ce dernier et, le cas échéant, de ses participants ?

3. FIABILITE ET RESILIENCE

Des activités disponibles, fiables et résilientes

- Quels sont les objectifs de disponibilité, de fiabilité et de résilience opérationnelles du processeur et comment sont-ils documentés ? Comment ces objectifs répondent-ils aux besoins du schéma de paiement et, le cas échéant, de ses participants ou les dépassent-ils ?

- Comment les politiques et les procédures du processeur étayent-elles ses objectifs de disponibilité, de fiabilité et de résilience ?

- Comment le processeur s'assure-t-il qu'il fournit des activités fiables et résilientes au schéma de paiement et, le cas échéant, à ses participants ? En particulier, comment s'assure-t-il que ses différents sites d'exploitation présentent des profils de risque suffisamment différents ? Comment s'assure-t-il que ses sites d'exploitation sont adéquatement protégés contre les catastrophes naturelles, les pannes d'électricité et les actions humaines préjudiciables ? Comment s'assure-t-il que ses sites de sauvegarde disposent d'une capacité suffisante pour traiter les services critiques pendant une période prolongée ?

Suivi des activités et gestion des incidents

- Comment le processeur surveille-t-il ses activités ? Comment vérifie-t-il s'il atteint les objectifs de fiabilité et de résilience du schéma de paiement ? Comment ce processus est-il documenté et comment le maintien de sa mise en œuvre est-il assuré ?

- Comment le processeur recense-t-il, enregistre-t-il, catégorise-t-il, analyse-t-il et gère-t-il les incidents opérationnels ? Comment ces incidents sont-ils signalés à la haute direction ? Comment le processeur informe-t-il le schéma de paiement et, le cas échéant, les autorités compétentes de ces incidents ? Quel est le processus permettant de faire passer un incident au statut de crise ?

- Quel est le processus d'analyse post mortem des incidents et comment ce processus est-il conçu pour assurer la détermination de la cause profonde des incidents et pour éviter qu'ils ne se reproduisent ? Quelle est la contribution du schéma de paiement à cette analyse post mortem ?

Continuité des activités

- Quels sont les objectifs du processeur en matière de continuité des activités et de reprise après sinistre ? Comment ces objectifs sont-ils fixés par le conseil d'administration et la haute direction ? À quelle fréquence ces objectifs sont-ils réexaminés par le conseil d'administration et la haute direction ?

- Comment les plans de continuité des activités et de reprise après sinistre élaborés par le processeur garantissent-ils la reprise en temps opportun de ses services critiques en cas d'interruption de service, y compris en cas de perturbation à grande échelle ? Que prévoient ces plans en matière de perte potentielle de données à la suite d'une interruption de service ?

- Comment le processeur détermine-t-il les scénarios de perturbation potentielle du service et comment le schéma de paiement participe-t-il à ce processus ?

- Que prévoient les plans du processeur en matière de continuité des activités et de reprise après sinistre pour ce qui concerne les cyberattaques ? Comment ces plans garantissent-ils que le processeur aura la capacité de déterminer et de gérer l'incidence d'une cyberattaque, y compris en matière de rétablissement des systèmes après un compromis ?

- Quel est le plan de communication de crise du processeur pour faire face aux interruptions de service ? En particulier, comment le plan aborde-t-il les communications et l'échange d'informations avec le schéma de paiement et les autorités compétentes ?

- Comment les plans de continuité des activités et de reprise après sinistre sont-ils testés et à quelle fréquence ? Quels sont les scénarios testés, et incluent-ils des cyberattaques ? Comment les résultats de ces tests sont-ils évalués et audités ? Comment le schéma de paiement et, le cas échéant, ses participants, contribuent-ils aux tests de simulation de continuité des activités ?

- Qu'est-il prévu pour l'évaluation régulière, en fonction des attentes du schéma de paiement, des plans du processeur en matière de continuité des activités et de reprise après sinistre ?

- In hoeverre wordt er over veranderingen die van invloed zijn op de gebruikers overlegd met het betalingsschema en worden deze veranderingen getest in samenwerking met het betalingsschema en, in voorkomend geval, met zijn deelnemers?

3. BETROUWBAARHEID EN VEERKRACHT

Beschikbare, betrouwbare en veerkrachtige activiteiten

- Wat zijn de operationele doelstellingen van de verwerker op het gebied van beschikbaarheid, betrouwbaarheid en veerkracht en hoe worden deze gedocumenteerd? Hoe voldoen deze doelstellingen aan of overtreffen ze de behoeften van het betalingsschema en, in voorkomend geval, van zijn deelnemers?

- Hoe ondersteunen de beleidslijnen en de procedures van de verwerker de doelstellingen inzake beschikbaarheid, betrouwbaarheid en veerkracht?

- Hoe zorgt de verwerker ervoor dat de activiteiten die hij voor het betalingsschema en, in voorkomend geval, voor zijn deelnemers verricht, betrouwbaar en veerkrachtig zijn? Hoe zorgt de verwerker er in het bijzonder voor dat zijn verschillende bedrijfsruimten voldoende verschillende risicoprofielen hebben? Hoe zorgt de verwerker ervoor dat zijn bedrijfsruimten adequaat worden beschermd tegen natuurrampen, stroomstoringen en schadelijke menselijke handelingen? Hoe zorgt de verwerker ervoor dat zijn vervangende locaties voldoende capaciteit hebben om de kritieke diensten gedurende een langere periode te leveren?

Monitoring van de activiteiten en incidentbeheer

- Hoe monitort de verwerker zijn activiteiten? Hoe controleert de verwerker of hij voldoet aan de doelstellingen van het betalingsschema inzake betrouwbaarheid en veerkracht? Hoe wordt dit proces gedocumenteerd en bijgewerkt?

- Hoe identificeert, registreert, categoriseert, analyseert en beheert de verwerker operationele incidenten? Hoe worden deze incidenten gemeld aan de effectieve leiding? Hoe licht de verwerker het betalingsschema en, in voorkomend geval, de bevoegde autoriteiten in over dergelijke incidenten? Welk proces wordt er gevolgd om een incident als crisis aan te merken?

- Welk proces wordt er gevolgd voor het uitvoeren van een post-mortemanalyse van incidenten en hoe is dit proces opgezet om ervoor te zorgen dat de hoofdoorzaak van de incidenten vastgesteld kan worden en dat vermeden kan worden dat er zich in de toekomst opnieuw incidenten voordoen? Welke rol vervult het betalingsschema bij deze post-mortemanalyse?

Bedrijfscontinuïteit

- Wat zijn de doelstellingen van de verwerker op het gebied van bedrijfscontinuïteit en rampherstel? Hoe worden deze doelstellingen bepaald door de raad van bestuur en de effectieve leiding? Hoe vaak worden deze doelstellingen herzien door de raad van bestuur en de effectieve leiding?

- Hoe zorgen de bedrijfscontinuïteits- en rampherstelplannen van de verwerker ervoor dat zijn kritieke diensten tijdig hervat kunnen worden in geval van een verstoring van de dienstverlening, onder meer in geval van een grootschalige verstoring? Wat bepalen deze plannen met betrekking tot een potentieel gegevensverlies als gevolg van een verstoring van de dienstverlening?

- Hoe stelt de verwerker scenario's van verstoring van de dienstverlening vast en hoe is het betalingsschema bij dit proces betrokken?

- Wat bepalen de bedrijfscontinuïteits- en rampherstelplannen van de verwerker met betrekking tot cyberaanvallen? Hoe zorgen deze plannen ervoor dat de verwerker in staat is om de gevolgen van een cyberaanval vast te stellen en te beheren, met inbegrip van systeemherstel wanneer het systeem is aangetast?

- Over welk crisiscommunicatieplan beschikt de verwerker om verstoringen van de dienstverlening aan te pakken? Wat bepaalt het plan in verband met de communicatie en informatie-uitwisseling met het betalingsschema en de bevoegde autoriteiten?

- Hoe worden de bedrijfscontinuïteits- en rampherstelplannen getest en hoe vaak gebeurt dit? Welke scenario's worden getest en omvatten die scenario's cyberaanvallen? Hoe worden de resultaten van deze tests beoordeeld en geauditeerd? Hoe zijn het betalingsschema en, in voorkomend geval, haar deelnemers, betrokken bij de bedrijfscontinuïteitssimulatietests?

- Worden de bedrijfscontinuïteits- en rampherstelplannen van de verwerker regelmatig getoetst aan de verwachtingen van het betalingsschema en zo ja, hoe?

4. PLANIFICATION TECHNOLOGIQUE

Politiques, procédures et modalités de gouvernance en matière de planification technologique

- Quelles sont les politiques, les procédures et les modalités de gouvernance du processeur en matière de planification technologique ? Que prévoient ces politiques, procédures et modalités de gouvernance concernant le cycle de vie en matière d'utilisation des technologies et de choix des normes technologiques ?

- À quelle fréquence le processeur évalue-t-il ses risques technologiques ? Comment ces évaluations tiennent-elles compte de la fiabilité et de la résilience, des risques d'obsolescence et des risques de sécurité de l'information liés à l'utilisation de sa technologie ? Comment ces évaluations tiennent-elles compte des risques technologiques susceptibles de nuire au schéma de paiement et, le cas échéant, à ses participants ?

Politiques, procédures et modalités de gouvernance en matière de gestion des changements technologiques

- Quelles sont les politiques, les procédures et les modalités de gouvernance du processeur en matière de mise en œuvre des changements à apporter aux technologies utilisées ? Comment ces politiques et ces procédures abordent-elles la gestion des versions, l'utilisation cohérente de la technologie et le maintien de la sécurité et de la stabilité de la technologie ?

- Comment ces politiques, ces procédures et ces modalités de gouvernance garantissent-elles que les risques liés aux changements technologiques sont recensés et atténués de façon adéquate, afin d'éviter que ces changements puissent nuire à la fiabilité et à la résilience des services critiques du fournisseur ? Comment et à quelle fréquence le processeur évalue-t-il et teste-t-il les processus utilisés pour mettre en œuvre les changements technologiques ?

- Comment le processeur consulte-t-il le schéma de paiement et, le cas échéant, ses participants, au sujet de toute proposition de changement important à apporter à sa technologie qui pourrait avoir une incidence importante sur le schéma de paiement ?

- Comment le service critique fait-il intervenir le schéma de paiement lorsque cela est opportun lors de la mise en œuvre d'un changement technologique ? Par exemple, le schéma de paiement participe-t-il aux tests des changements technologiques de façon appropriée ?

Vu pour être annexé à Notre arrêté du 25 janvier 2019 portant approbation du règlement de la Banque nationale de Belgique du 20 novembre 2018 précisant les modalités de certaines obligations de la loi du 24 mars 2017 relative à la surveillance des processeurs d'opérations de paiement.

PHILIPPE

Par le Roi :

Le Vice-Premier Ministre et Ministre des Finances,
A. DE CROO

4. TECHNOLOGIEPLANNING

Beleidslijnen, procedures en governanceregelingen voor technologieplanning

- Over welke beleidslijnen, procedures en governanceregelingen beschikt de verwerker op het gebied van technologieplanning? Wat bepalen deze beleidslijnen, procedures en governanceregelingen in verband met de levenscyclus voor het gebruik van technologie en de keuze van nieuwe technologische standaarden?

- Hoe vaak beoordeelt de verwerker de door hem gelopen technologische risico's? Hoe wordt er bij dergelijke beoordelingen rekening gehouden met de betrouwbaarheid en de veerkracht, evenals met de verouderingsrisico's en informatiebeveiligingsrisico's die verbonden zijn aan het gebruik van zijn technologie? Hoe wordt er bij deze beoordelingen rekening gehouden met de technologische risico's die schadelijk kunnen zijn voor het betalingsschema en, in voorkomend geval, voor haar deelnemers?

Beleidslijnen, procedures en governanceregelingen voor het beheer van technologische veranderingen

- Over welke beleidslijnen, procedures en governanceregelingen beschikt de verwerker voor de implementatie van de wijzigingen die in de gebruikte technologieën moeten worden aangebracht? Hoe behandelen deze beleidslijnen en procedures het releasebeheer, het consistent gebruik van technologie en het behoud van de veiligheid en stabiliteit van de technologie?

- Hoe zorgen deze beleidsregels, procedures en governanceregelingen ervoor dat de risico's die verbonden zijn aan technologische veranderingen worden opgespoord en adequaat worden beperkt, om te voorkomen dat deze wijzigingen afbreuk kunnen doen aan de betrouwbaarheid en veerkracht van de kritieke diensten van de leverancier? Hoe en hoe vaak beoordeelt en test de verwerker de processen die worden toegepast voor het implementeren van technologische veranderingen?

- Hoe verloopt het overleg tussen de verwerker en het betalingsschema en, in voorkomend geval, haar deelnemers, over voorstellen voor belangrijke veranderingen in zijn technologie die een wezenlijke invloed kunnen hebben op het betalingsschema?

- Hoe betrekt de kritieke dienst het betalingsschema in voorkomend geval bij het implementeren van een technologische verandering? Is het betalingsschema bijvoorbeeld betrokken bij het testen van technologische veranderingen?

Gezien om te worden gevoegd bij Ons besluit van 25 januari 2019 tot goedkeuring van het reglement van de Nationale Bank van België van 20 november 2018 tot vaststelling van de modaliteiten van bepaalde verplichtingen van de wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties.

FILIP

Van Koningswege :

De Vice-Eerste Minister en Minister van Financiën,
A. DE CROO