de Berlaimontlaan 14 – BE-1000 Brussel
tel. +32 2 221 48 66
ondernemingsnummer: 0203.201.340
RPR Brussel
www.nbb.be

BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

# Circulaire

Brussel, 23 november 2021

Kenmerk: NBB_2021_26

uw correspondent:
Thomas Plomteux
tel. +32 2 221 21 97
thomas.plomteux@nbb.be

**Rapportering inzake operationele en veiligheidsrisico's van betalingsdiensten voor betalingsinstellingen en instellingen voor elektronisch geld**

## Toepassingsveld

*Betalingsinstellingen naar Belgisch recht, geregistreerde betalingsinstellingen naar Belgisch recht die rekeningaggregatiediensten aanbieden, beperkte betalingsinstellingen naar Belgisch recht, instellingen voor elektronisch geld naar Belgisch recht, beperkte instellingen voor elektronisch geld naar Belgisch recht.*

## Samenvatting/Doelstelling

*Deze circulaire bepaalt hoe de betalingsinstellingen en instellingen voor elektronisch geld de rapporteringsverplichting opgelegd in artikel 50, § 2 van de Wet van 11 maart 2018[1] dienen in te vullen. Deze circulaire is van toepassing vanaf 1 januari 2022 en vervangt circulaire NBB_2020_24, die vanaf deze datum niet langer van toepassing is.*

[1] De wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen, B.S. 26 maart 2018 (hierna: 'de wet van 11 maart 2018').

Geachte mevrouw
Geachte heer

Met deze circulaire wenst de Nationale Bank van Belgie (hierna, de "Bank") de rapporteringsverplichting opgelegd in artikel 50, § 2 van de wet van 11 maart 2018 te verduidelijken.

Artikel 50 § 2 van de wet van 11 maart 2018 vereist een rapportering aan de toezichthouder van "een geactualiseerde en uitgebreide beoordeling van zowel de operationele en veiligheidsrisico's die aan de door de instelling aangeboden betalingsdiensten zijn verbonden, als van de toereikendheid van de in reactie op deze risico's getroffen risicobeperkende maatregelen en ingevoerde controlemechanismen.

Door middel van deze circulaire wenst de Bank haar verwachtingen inzake het jaarlijks over te maken verslag te verduidelijken aan de betalingsinstellingen naar Belgisch recht, de geregistreerde betalingsinstellingen naar Belgisch recht die rekeningaggregatiediensten aanbieden, de beperkte betalingsinstellingen naar Belgisch recht, de instellingen voor elektronisch geld naar Belgisch recht en de beperkte instellingen voor elektronisch geld naar Belgisch recht.

Deze instellingen dienen een gedetailleerde en onderbouwde beoordeling van de operationele en beveiligingsrisico's over te maken van zowel de reeds bestaande betalingsdiensten als die betalingsdiensten waarvan verwacht wordt dat deze binnen het komend jaar aangeboden zullen worden. Dit houdt in dat:

1. de beoordeling voor elk geïdentificeerd risico de volgende elementen dient te omvatten:

    - een beschrijving van het geïdentificeerd risico, met inbegrip van de gevolgen ervan voor de instelling en haar cliënten indien het risico zich zou materialiseren;
    - de inherente risiconiveau's, met een inschatting van de waarschijnlijkheid en de impact ervan voor de instelling;
    - de reeds bestaande mitigerende controles voor het geïdentificeerde risico, met inbegrip van een beschrijving van het effect ervan op het risiconiveau van de instelling;
    - het niveau van het residueel risico dat overblijft na de implementatie van de risicobeperkende maatregelen;
    - de nog uit te voeren acties die geïdentificeerd werden om de doeltreffendheid van de controles te verbeteren, indien deze er zijn, en de voorziene planning van de implementatie hiervan.

2. de instellingen een beoordeling geven van hun naleving van de EBA-richtsnoeren inzake risicobeheer op het gebied van ICT en veiligheid die zijn ingevoerd via circulaire NBB_2020_23[2]. Deze beoordeling dient een beschrijving te geven van de bepalingen uit deze Richtsnoeren waar de instelling niet in conformiteit mee is en een beoordeling te omvatten van het effect van deze niet-conformiteit op het risiconiveau van de instelling.
3. de instellingen ook de ontwikkelingen omschrijven die plaatsvonden sinds de vorige indiening van het rapport (of sinds de vergunningverlening door de Bank).

[2] De EBA-richtsnoeren naar de welke deze circulaire verwijst, verduidelijken overigens dat operationele risico's in de context van betalingsdiensten mogen geïnterpreteerd worden als zijnde hoofdzakelijk ICT- en veiligheidsrisico's gezien het veelal elektronische karakter van deze betalingsdiensten.

Teneinde een voldoende hoge kwaliteit van deze rapportering na te streven en instellingen optimaal te ondersteunen bij het vervullen van hun rapporteringsverplichting, zal de Bank jaarlijks gestandaardiseerde IT-risicovragenlijsten en een praktische instructie ter beschikking stellen aan de instellingen die onder het toepassingsgebied van deze circulaire vallen. De vragenlijsten zullen meer bepaald peilen naar de inherente blootstelling van deze instellingen aan een aantal ICT-risicocategorieën[3] en de overeenkomstige mitigerende maatregelen en controles in een aantal ICT-risicocontroledomeinen[4]. Bovendien kunnen deze vragenlijsten, rekening houdend met het principe van proportionaliteit, tussen instellingen onderling verschillen, bijvoorbeeld in functie van de omvang en interne organisatie van de instelling, alsook de aard, omvang, complexiteit en het risicogehalte van de diensten en producten die de financiële instellingen verstrekken of van plan zijn te verstrekken.

Instellingen worden verwacht deze vragenlijsten jaarlijks op een voldoende allesomvattende en kritische wijze in te vullen. In dat geval, en indien de instellingen op adequate wijze gevolg geven aan eventuele vragen voor bijkomende informatie en/of documentatie, zal de Bank het invullen van deze vragenlijst beschouwen als voldoende om in overeenstemming te zijn met de wettelijke rapporteringsverplichting.

Deze circulaire wordt van toepassing op 1 januari 2022.

Een kopie van deze circulaire wordt naar de commissaris(sen), erkend revisor(en) van uw instelling verstuurd.

Hoogachtend

p.p. Pierre Wunsch
Gouverneur

**Steven Vanackere**
**Vicegouverneur**

[3] Dit kan de volgende categorieën omvatten: ICT-beschikbaarheids- en -continuïteitsrisico, ICT-veiligheidsrisico, ICT-wijzigingsrisico, ICT-data-integriteitsrisico en ICT-uitbestedingsrisico.

[4] Dit kan de volgende domeinen omvatten: ICT-bestuur, ICT-organisatie en ICT-uitbesteding, ICT-risicobeheer, ICT-veiligheidsbeheer, beheer van ICT-activiteiten, acquisitie en ontwikkeling van software en projectbeheer, beheer van datakwaliteit, ICT-continuïteitsbeheer, ICT-rapportering en interne ICT-audit.