EBA/GL/2017/05

11/09/2017

Richtsnoeren

Richtsnoeren inzake de beoordeling van het ICT-risico in het kader van het proces van toetsing en evaluatie door de toezichthouder (SREP)

1. Nalevings- en rapportageverplichtingen

Status van deze richtsnoeren

1. Dit document bevat richtsnoeren die zijn uitgebracht op grond van artikel 16 van Verordening (EU) nr. 1093/2010[1]. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 moeten bevoegde autoriteiten en financiële instellingen zich tot het uiterste inspannen om aan die richtsnoeren te voldoen.

2. Richtsnoeren geven weer wat in de opvatting van de EBA passende toezichtpraktijken binnen het Europees Systeem voor financieel toezicht zijn en hoe het recht van de Unie op een specifiek gebied dient te worden toegepast. Bevoegde autoriteiten als bedoeld in artikel 4, lid 2, van Verordening (EU) nr. 1093/2010 voor wie richtsnoeren gelden, dienen hieraan te voldoen door deze op passende wijze in hun praktijken te integreren (bijvoorbeeld door hun wettelijk kader of hun toezichtprocessen aan te passen), ook wanneer richtsnoeren primair tot instellingen zijn gericht.

Kennisgevingsverplichtingen

3. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 stellen bevoegde autoriteiten EBA vóór 13.11.2017 ervan in kennis of zij aan deze richtsnoeren voldoen of voornemens zijn deze op te volgen, of, indien dit niet het geval is, wat de redenen van de niet-naleving zijn. Bevoegde autoriteiten die bij het verstrijken van de termijn niet hebben gereageerd, worden geacht niet te hebben voldaan aan de richtsnoeren. Kennisgevingen worden ingediend door het formulier op de EBA-website te versturen naar compliance@eba.europa.eu onder vermelding van "EBA/GL/2017/05". Kennisgevingen worden ingediend door personen die bevoegd zijn om namens hun bevoegde autoriteiten te melden of zij aan de richtsnoeren voldoen. Elke verandering in de status van de naleving dient eveneens aan EBA te worden gemeld.

4. Kennisgevingen worden overeenkomstig artikel 16, lid 3, van de EBA-verordening op haarwebsite bekendgemaakt.

1 Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12).

2. Onderwerp, toepassingsgebied en definities

Onderwerp en toepassingsgebied

5. Deze richtsnoeren, die zijn opgesteld op grond van artikel 107, lid 3, van Richtlijn 2013/36/EU[2] hebben tot doel te zorgen voor convergentie van toezichtpraktijken tijdens de beoordeling van het risico van de informatie- en communicatietechnologie (ICT) in het kader van het proces van toezicht en evaluatie door de toezichthouder (SREP) als bedoeld in artikel 97 van Richtlijn 2013/36/EU en nader gespecificeerd in de EBA-richtsnoeren inzake gemeenschappelijke procedures en methoden voor het proces van toetsing en evaluatie door de toezichthouder (SREP)[3]. In het bijzonder worden in deze richtsnoeren de beoordelingscriteria gespecificeerd die bevoegde autoriteiten tijdens de beoordeling door de toezichthouder van de governance en strategie inzake ICT van instellingen en tijdens de beoordeling door de toezichthouder van de risicoblootstellingen en risicobeheersing op ICT-gebied van instellingen, dienen toe te passen. Deze richtsnoeren vormen een integraal onderdeel van de SREP-richtsnoeren van EBA.

6. Bevoegde autoriteiten passen deze richtsnoeren toe overeenkomstig het toepassingsniveau dat is vastgesteld in de SREP-richtsnoeren van EBA en volgens het model van minimale toezichtsinspanning en de evenredigheidsvereisten die daarin worden vermeld.

Adressaten

7. Deze richtsnoeren zijn gericht tot bevoegde autoriteiten als bedoeld in artikel 4, lid 2, punt i), van Verordening (EU) nr. 1093/2010.

Definities

8. Tenzij anders aangegeven hebben de termen die in Richtlijn 2013/36/EU en in Verordening (EU) nr. 575/2013 worden gebruikt en gedefinieerd en de definities in de SREP-richtsnoeren van EBA in deze richtsnoeren dezelfde betekenis. In deze richtsnoeren gelden bovendien de volgende definities:

ICT-systemen	ICT-uitrusting als onderdeel van een mechanisme of een verbindend netwerk dat de werkzaamheden van een instelling

[2] Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen en beleggingsondernemingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van de Richtlijnen 2006/48/EG en 2006/49/EG (1) - PB L 176 van 27.6.2013.

[3] EBA/GL/2014/13

	ondersteunt.
ICT-diensten	Diensten die door ICT-systemen aan een of meer interne of externe gebruikers worden verleend. Voorbeelden zijn diensten op het gebied van het invoeren, opslaan, verwerken en rapporteren van gegevens, maar ook diensten ter ondersteuning van toezicht, bedrijfsactiviteiten en de besluitvorming.
ICT-beschikbaarheids- en continuïteitsrisico	Het risico dat de prestaties en beschikbaarheid van ICT-systemen en -gegevens negatief worden beïnvloed, waaronder onvermogen om diensten van de instelling tijdig te herstellen bij een storing in ICT-hardware of -software; zwakke plekken in het ICT-systeembeheer; of enige andere gebeurtenis zoals in de bijlage nader wordt beschreven.
ICT-beveiligingsrisico	Het risico van ongeoorloofde toegang tot ICT-systemen en -gegevens van binnen of buiten de instelling (bijv. cyberaanvallen), zoals in de bijlage nader wordt beschreven.
ICT-wijzigingsrisico	Het risico dat voortvloeit uit het onvermogen van de instelling om wijzigingen in de ICT-systemen tijdig en op gecontroleerde wijze uit te voeren, met name in omvangrijke en ingewikkelde wijzigingsprogramma's, zoals in de bijlage nader wordt beschreven.
ICT-data-integriteitsrisico	Het risico dat gegevens die door ICT-systemen zijn opgeslagen en verwerkt, onvolledig, onnauwkeurig en/of inconsistent zijn tussen verschillende ICT-systemen, bijvoorbeeld als gevolg van gebrekkige of ontbrekende ICT-controles gedurende de verschillende fasen van de levenscyclus van ICT-gegevens (d.w.z. ontwerpen van de dataarchitectuur, het bouwen van gegevensmodellen en/of data dictionaries, controle van invoer, extractie van data, overdracht en verwerking van gegevens, inclusief gegevensuitvoer), waardoor een instelling minder goed in staat is correct en tijdig diensten te verlenen en informatie op het gebied van (risico)beheer en financiën te genereren, zoals in de bijlage nader wordt beschreven.
ICT-uitbestedingsrisico	Het risico dat de inschakeling van een derde of een andere groepsentiteit (uitbesteding binnen de groep) om ICT-diensten of daarmee verband houdende diensten te verlenen, een negatieve uitwerking heeft op de prestaties en het risicobeheer van de instelling, zoals in de bijlage nader wordt beschreven.

3. Tenuitvoerlegging

Toepassingsdatum

9. Deze richtsnoeren zijn van toepassing met ingang van 1 januari 2018.

4. Vereisten voor de beoordeling van het ICT-risico

Titel 1 - Algemene bepalingen

10. Bevoegde autoriteiten voeren de beoordeling van het ICT-risico en de governanceregeling en ICT-strategie als onderdeel van het SREP-proces uit volgens het model van minimale toezichtinspanning en de evenredigheidscriteria die in titel 2 van de SREP-richtsnoeren van EBA worden vermeld. Dit betekent in het bijzonder dat:

    a. de frequentie van de beoordeling van het ICT-risico afhangt van het model van minimale toezichtinspanning dat gehanteerd wordt op basis van de SREP-categorie waarin een instelling is ingedeeld, en het voor de instelling specifieke toezichtsprogramma van de toezichthouder; en,

    b. dat de diepte, gedetailleerdheid en intensiteit van de ICT-beoordeling evenredig dienen te zijn met de omvang, structuur en operationele omgeving van de instelling, evenals met de aard, schaal en complexiteit van haar activiteiten.

11. Het evenredigheidsbeginsel is in deze richtsnoeren geheel van toepassing ten aanzien van de omvang, de frequentie en de intensiteit van de toezichtsinspanning, de dialoog met de instelling, en de verwachtingen van de toezichthouder met betrekking tot de normen waaraan de instelling dient te voldoen.

12. Om tot een actueel beeld te komen, mogen bevoegde autoriteiten vertrouwen op, en rekening houden met werkzaamheden die de instelling of de bevoegde autoriteit reeds in het kader van de beoordelingen van andere risico's of SREP-elementen heeft verricht. Bevoegde autoriteiten kiezen bij het verrichten van de in deze richtsnoeren vermelde beoordelingen de aanpak en de methode die het meest geschikt en het meest evenredig is ten aanzien van de instelling, en maken gebruik van bestaande en beschikbare documentatie (bijvoorbeeld relevante verslagen en andere documenten, vergaderingen met het (risico)management, inspecties ter plaatse) als input voor de beoordeling.

13. Bevoegde autoriteiten maken een samenvatting van bevindingen ten aanzien van de in deze richtsnoeren vermelde criteria, en gebruiken deze als basis om conclusies te trekken ten aanzien van de SREP-elementen zoals genoemd in de in de SREP-richtsnoeren van EBA.

14. In het bijzonder dient de beoordeling van de governance en ICT-strategie die in overeenstemming met titel 2 van deze richtsnoeren wordt verricht, te leiden tot bevindingen die als input dienen voor de samenvatting van de bevindingen van de beoordeling van de internegovernance- en instellingsbrede risicobeheersingselementen van SREP als beschreven in titel 5 van de SREP-richtsnoeren van EBA, en in

de desbetreffende score van dat SREP-element worden weerspiegeld. Verder nemen bevoegde autoriteiten in overweging dat een aanzienlijke nadelige uitwerking van de beoordeling van de ICT-strategie op de bedrijfsstrategie van de instelling of eventuele zorgen dat de instelling niet voldoende ICT-middelen en ICT-capaciteit heeft om belangrijke geplande strategische wijzigingen aan te brengen en te ondersteunen, als input dient voor de analyse van het bedrijfsmodel die in overeenstemming met titel 4 van de SREP-richtsnoeren van EBA wordt verricht.

15. De uitkomsten van de beoordeling van de in titel 3 van deze richtsnoeren vermelde ICT-risico's dienen als input voor de bevindingen van de beoordeling van het operationele risico en worden geacht als input te dienen voor de relevante score als bedoeld in titel 6.4 van de SREP-richtsnoeren van EBA.

16. Doorgaans beoordelen bevoegde autoriteiten subcategorieën als onderdeel van de hoofdcategorieën (d.w.z. ICT-risico's worden beoordeeld als onderdeel van het operationele risico), maar wanneer bevoegde autoriteiten bepaalde subcategorieën wezenlijk achten, mogen zij die subcategorieën afzonderlijk beoordelen. Met het oog hierop bevatten deze richtsnoeren ook een scoretabel (tabel 1), voor het geval dat de bevoegde autoriteit het ICT-risico als wezenlijk aanmerkt. Die tabel moet in dat geval worden gebruikt om een zelfstandige subcategoriescore voor ICT-risico's vast te stellen volgens de algehele aanpak voor het toekennen van scores aan kapitaalrisico's in de SREP-richtsnoeren van EBA.

17. Om te bepalen of ICT-risico's als wezenlijk dienen te worden beschouwd en het dus mogelijk dient te zijn om ICT-risico's als een afzonderlijke subcategorie van het operationele risico te beoordelen en daaraan scores toe te kennen, mogen bevoegde autoriteiten de in paragraaf 6.1 van de SREP-richtsnoeren van EBA vermelde criteria hanteren.

18. Bij de toepassing van deze richtsnoeren kijken bevoegde autoriteiten, waar relevant, naar de niet-volledige lijst van ICT-risicosubcategorieën en risicoscenario's die in de bijlage worden beschreven; hierbij dient in het achterhoofd te worden gehouden dat het in deze bijlage gaat om ICT-risico's die tot verliezen met een grote impact kunnen leiden. Bevoegde autoriteiten mogen sommige in de taxonomie opgenomen ICT-risico's uitsluiten als deze voor hun beoordeling niet relevant zijn. Van instellingen wordt verwacht dat zij hun eigen risicotaxonomieën handhaven en niet de in de bijlage beschreven risicotaxonomie gebruiken.

19. Wanneer deze richtsnoeren worden toegepast op grensoverschrijdende bankgroepen, en de entiteiten ervan en er een college van toezichthouders is ingesteld, stemmen betrokken bevoegde autoriteiten in het kader van hun samenwerking met het oog op de beoordeling van het SREP overeenkomstig paragraaf 11.1 van de SREP-richtsnoeren van EBA de exacte en gedetailleerde reikwijdte van elk informatieonderdeel zo veel mogelijk consequent voor alle groepsentiteiten op elkaar af.

Titel 2 - Beoordeling van governance en strategie van instellingen inzake ICT

2.1 Algemene beginselen

20. Bevoegde autoriteiten beoordelen of in het algemene kader voor governance en interne risicobeheersing van de instelling de ICT-systemen en de bijbehorende risico's naar behoren zijn opgenomen, en of het leidinggevende orgaan voldoende naar deze aspecten kijkt en er adequaat mee omgaat. ICT is immers essentieel voor het juist functioneren van een instelling.

21. Tijdens deze beoordeling maken bevoegde autoriteiten gebruik van de vereisten en normen voor ten aanzien van goede interne governance en risicobeheersing, zoals vermeld in de EBA-richtsnoeren inzake interne governance (GL 44)[4] en internationale richtsnoeren op dit terrein voor zover deze van toepassing zijn gezien het specifieke karakter van ICT-systemen en risico's.

22. De in deze titel beschreven beoordeling heeft geen betrekking op de specifieke onderdelen van de governance, het risicobeheer en de risicobeheersing in verband met ICT-systemen die gericht zijn op het beheren van specifieke ICT-risico's die in titel 3 van deze richtsnoeren aan de orde komen, maar richt zich op de volgende gebieden:

    a. ICT-strategie: - of de instelling een ICT-strategie heeft die adequaat wordt beheerd en in lijn is met de bedrijfsstrategie van de instelling;

    b. algehele interne governance: - of de regelingen voor de algehele interne governance van de instelling toereikend zijn voor de ICT-systemen van de instelling; en

    c. ICT-risico als onderdeel van het risicobeheer raamwerk van de instelling: of het risico management en de interne beheersing van de instelling de ICT-systemen van de instelling voldoende beschermt.

23. Werkzaamheden volgend uit punt a) onder paragraaf 22leiden tot informatie over onderdelen van de governance van de instelling. Echter, deze informatie dient voornamelijk te worden toegepast bij de beoordeling van het bedrijfsmodel zoals besproken in titel 4 van de EBA SREP-richtsnoeren. De punten b) en c) bieden een verdere aanvulling ten behoeve van de beoordeling van onderwerpen die behandeld worden in titel 5 van de EBA SREP-richtsnoeren. De in deze richtsnoeren beschreven beoordeling dient als input voor de desbetreffende beoordeling op grond van titel 5 van de SREP-richtsnoeren van EBA.

24. De uitkomsten van deze beoordeling worden, waar relevant, meegenomen in de beoordeling van het risicobeheer en de risicobeheersing die in titel 3 van deze richtsnoeren aan de orde komt.

[4] EBA-richtsnoeren inzake interne governance, GL 44, 27 september 2011.

2.2 ICT-strategie

25. Op basis van deze paragraaf beoordelen bevoegde autoriteiten of de instelling een ICT-strategie heeft waarop het leidinggevend orgaan van de instelling adequaat toezicht houdt, dat strookt met de bedrijfsstrategie, vooral om haar ICT actueel te houden en met het oog op de planning of uitvoering van belangrijke en complexe ICT-wijzigingen, en die het bedrijfsmodel van de instelling ondersteunt.

2.2.1 Ontwikkeling en toereikendheid van de ICT-strategie

26. Bevoegde autoriteiten beoordelen of de instelling een kader heeft dat evenredig is met de aard, schaal en complexiteit van haar ICT-activiteiten, met het oog op het voorbereiden en ontwikkelen van de ICT-strategie van de instelling. Hierbij houden zij rekening met de vraag of:

    a. de directie[5] van het/de bedrijfsonderde(e)l(en) naar behoren betrokken is bij het vaststellen van de strategische ICT-prioriteiten van de instelling en of de directie van de ICT-functie zich ervan bewust is dat er belangrijke bedrijfsstrategieën en -initiatieven worden ontwikkeld, ontworpen en opgestart om ervoor te zorgen dat enerzijds de ICT-systemen, ICT-diensten en de ICT-functie (d.w.z. degenen die verantwoordelijk zijn voor het beheer en de uitrol van deze systemen en diensten) en anderzijds de bedrijfsstrategie van de instelling voortdurend op elkaar afgestemd blijven, en of de ICT doeltreffend wordt geactualiseerd;

    b. de ICT-strategie gedocumenteerd is, en de uitvoering daarvan gerealiseerd wordt aan de hand van concrete op de strategie gebaseerde uitvoeringsplannen. Deze zijn realistisch, en bevatten ten minste belangrijke mijlpalen en een concrete resource planning (inclusief financiële middelen en personeel);

    c. de instelling haar ICT-strategie periodiek actualiseert, vooral bij een wijziging van de bedrijfsstrategie, om ervoor te zorgen dat de ICT- en bedrijfsmatige doelstellingen voor de middellange tot lange termijn, plannen en activiteiten voortdurend op elkaar afgestemd blijven; en

    d. het leidinggevend orgaan van de instelling de ICT-strategie en bijbehorende uitvoeringsplannen goedkeurt en toezicht houdt op de uitvoering ervan.

2.2.2 Uitvoering van de ICT-strategie

27. Indien er voor de ICT-strategie van de instelling belangrijke en complexe ICT-wijzigingen moeten worden uitgevoerd, of wijzigingen met wezenlijke implicaties voor het bedrijfsmodel van de instelling, beoordelen bevoegde autoriteiten of de instelling een risicobeheersingskader heeft dat aansluit bij haar omvang, haar ICT-activiteiten en het niveau van de wijzigingen, om de doeltreffende uitvoering van de ICT-strategie van de instelling te ondersteunen. Hierbij houden zij rekening met de vraag of het risicobeheersingskader:

[5] Directie en leidinggevend orgaan als gedefinieerd in Richtlijn 2013/36/EU van 26 juni 2013 in artikel 3, lid 1, punt 7), "leidinggevend orgaan" en artikel 3, lid 1, punt 9), "directie".

a. governanceprocessen (bijv. voortgangs- en begrotingsbewaking en -rapportage) en relevante organen (bijv. een bureau voor projectbeheer, een ICT-stuurgroep of een soortgelijke entiteit) omvat om de uitvoering van de strategische programma's op ICT-vlak effectief te ondersteunen;

b. de taken en verantwoordelijkheden voor de uitvoering van strategische programma's op ICT-vlak heeft omschreven en toegewezen, met speciale aandacht voor de ervaring van de voornaamste betrokkenen in het organiseren, sturen en bewaken van belangrijke en complexe ICT-wijzigingen en voor het beheer van de bredere gevolgen voor de organisatie en voor het personeel (bijv. omgaan met weerstand tegen veranderingen, opleiding, communicatie).

c. de onafhankelijke controle- en interne auditfuncties ertoe verplicht ervoor te zorgen dat de risico's in verband met de uitvoering van de ICT-strategie zijn vastgesteld, beoordeeld en doeltreffend beperkt en dat het governancekader voor de uitvoering van de ICT-strategie effectief is; en

d. een planning en een toetsing van de planning omvat die de flexibiliteit verschaffen om te reageren op belangrijke geconstateerde problemen (bijv. problemen met of vertraging in de uitvoering) of externe ontwikkelingen (bijv. belangrijke wijzigingen in de bedrijfsomgeving, technologische kwesties of innovaties) om een tijdige aanpassing van het strategische uitvoeringsplan te waarborgen.

2.3 Algeheel kader voor interne governance

28. Overeenkomstig titel 5 van de SREP-richtsnoeren van EBA beoordelen bevoegde autoriteiten of de instelling een passende en transparante bedrijfsstructuur heeft die ‘fit for purpose’ is, en of zij passende governanceregelingen ten uitvoer heeft gelegd. Specifiek wat betreft ICT-systemen en in overeenstemming met de richtsnoeren inzake interne governance van EBA omvat dit ook een beoordeling van de vraag of de instelling aantoont:

    a. dat zij een robuuste, transparante organisatiestructuur met duidelijke verantwoordelijkheden heeft, inclusief het leidinggevend orgaan en zijn comités, en dat belangrijke verantwoordelijke personen voor ICT (bijv. Chief Information Officer ‘CIO’, Chief Operating Officer ‘COO’ of gelijkwaardige functie) voldoende indirecte of directe toegang tot het leidinggevend orgaan hebben, om te garanderen dat belangrijke ICT-gerelateerde informatie of vraagstukken adequaat op het niveau van het leidinggevend orgaan worden gemeld en besproken en dat het leidinggevend orgaan daarover adequaat besluiten neemt; en

    b. dat het leidinggevend orgaan de risico's in verband met ICT kent en daarvoor een oplossing zoekt.

29. Op grond van paragraaf 5.2 van de SREP-richtsnoeren van EBA beoordelen bevoegde autoriteiten of bij het beleid en de strategie inzake uitbesteding van ICT, waar relevant, rekening wordt gehouden met de gevolgen van de uitbesteding van ICT voor de activiteiten en het bedrijfsmodel van de instelling.

2.4 ICT-risico in het risicobeheerkader van de instelling

30. Bij de beoordeling van het instellingsbrede risicobeheer en de interne risicobeheersing, als bedoeld in titel 5 van de SREP-richtsnoeren van EBA, bekijken bevoegde autoriteiten of het kader voor risicobeheer en interne risicobeheersing van de instelling de ICT-systemen van de instelling adequaat beschermt op een manier die past bij de omvang en activiteiten van de instelling en haar risicoprofiel als beschreven in titel 3. Bevoegde autoriteiten bepalen met name of:

    a. de risicobereidheid en de Icaap betrekking hebben op de ICT-risico's, als onderdeel van de bredere categorie van het operationele risico, met het oog op de omschrijving van de algehele risicostrategie en de vaststelling van het interne kapitaal; en

    b. de ICT-risico's zich binnen het bereik van de instellingsbrede kaders voor risicobeheer en interne risicobeheersing bevinden.

31. Bevoegde autoriteiten voeren de onder a) bedoelde beoordeling uit met gebruik van zowel verwachte als ongunstige scenario's, bijvoorbeeld scenario's die zijn opgenomen in de stresstest per instelling of voor toezichtsdoeleinden.

32. Specifiek met betrekking tot b) beoordelen bevoegde autoriteiten of de onafhankelijke controle- en interne auditfuncties, als beschreven in de punten 104, onder a), 104, onder d), 105, onder a) en 105,onder c) van de SREP-richtsnoeren van EBA, een toereikend niveau van onafhankelijkheid tussen de ICT- en de risicobeheersings- en auditfuncties garanderen, gezien de omvang en het ICT-risicoprofiel van de instelling.

2.5 Samenvatting van de bevindingen

33. Deze resultaten moeten tot uitdrukking komen in de samenvatting van de bevindingen op grond van titel 5 van de SREP-richtsnoeren van EBA en deel uitmaken van de respectieve scores overeenkomstig de overwegingen in tabel 3 van de SREP-richtsnoeren van EBA.

34. Voor de beoordeling van de ICT-strategie moeten de volgende punten in acht worden genomen bij het afsluiten van bovengenoemde beoordeling:

    a. Indien bevoegde autoriteiten tot de conclusie komen dat het governancekader van de instelling ontoereikend is om de in 2.2 vermelde ICT-strategie te ontwikkelen en uit te voeren, dient dit als input voor de beoordeling van de interne governance van de instelling als bedoeld in titel 5 van de SREP-richtsnoeren van EBA in punt 87, onder a).

    b. Indien bevoegde autoriteiten op grond van de in 2.2. bedoelde beoordelingen tot de conclusie komen dat de ICT-strategie en de bedrijfsstrategie in grote mate niet op elkaar zijn afgestemd en dat dit aanzienlijke negatieve gevolgen heeft voor de zakelijke en/of financiële doelstellingen van de instelling op lange termijn, de duurzaamheid en/of het bedrijfsmodel van de instelling, of de bedrijfsonderdelen/activiteiten van de instelling die als het wezenlijkst worden aangemerkt in punt 62 a) van de SREP-richtsnoeren van EBA, dient dit als input voor de beoordeling van het bedrijfsmodel als vermeld in titel 4 van de SREP GL in de punten 70, onder b) en c).

c. Indien bevoegde autoriteiten op grond van de in 2.2. bedoelde beoordelingen tot de conclusie komen dat de instelling wellicht onvoldoende ICT-middelen en ICT-uitvoeringsmogelijkheden heeft om belangrijke geplande strategische wijzigingen door te voeren en te ondersteunen, dient dit als input voor de beoordeling van het bedrijfsmodel als vermeld in titel 4 van de SREP-richtsnoeren van EBA in punt 70, onder b).

Titel 3 - Beoordeling van risicoblootstellingen en risicobeheersing van instellingen op ICT-gebied

3.1 Algemene overwegingen

35. Bevoegde autoriteiten beoordelen of de instelling haar ICT-risico's naar behoren heeft geïdentificeerd, beoordeeld en beperkt. Dit proces moet onderdeel zijn van het operationele risicobeheerkader en overeenkomen met de aanpak die geldt voor het operationele risico.

36. Bevoegde autoriteiten identificeren eerst de wezenlijke inherente ICT-risico's waaraan de instelling wordt of kan worden blootgesteld, gevolgd door een beoordeling waarbij wordt onderzocht hoe effectief deze risico's door het ICT-risicobeheerkader, de procedures en risicobeheersing worden beperkt. De uitkomst van de beoordeling wordt vastgelegd in een samenvatting van bevindingen die wordt meegenomen in de score voor operationeel risico als bedoeld in de SREP-richtsnoeren. Wanneer het ICT-risico als wezenlijk wordt beschouwd en bevoegde autoriteiten een afzonderlijke score willen toekennen, wordt tabel 1 gebruikt om een score als subrisico van het operationele risico toe te kennen.

37. Bij de uitvoering van de beoordeling op grond van deze titel maken bevoegde autoriteiten gebruik van alle beschikbare informatiebronnen als vermeld in punt 127 van titel 6 van de SREP-richtsnoeren van EBA, bijvoorbeeld activiteiten, verslaglegging en uitkomsten van de instelling op het gebied van risicobeheer, als basis voor het vaststellen van hun prioriteiten waar het gaat om de beoordeling door de toezichthouder. Bevoegde autoriteiten maken tevens gebruik van andere informatiebronnen om deze beoordeling te verrichten, waaronder, indien relevant, de volgende bronnen:

    a. zelfevaluaties van ICT-risico's en -risicobeheersing (indien opgenomen in de Icaap-informatie);
    b. aan ICT-risico's gerelateerde managementinformatie die aan het leidinggevend orgaan van de instelling wordt overgelegd, bijvoorbeeld periodieke en incidentele ICT-risicoverslaglegging (onder meer in de databank van operationele verliezen), en gegevens over blootstelling aan ICT-risico's van de risicobeheerfunctie van de instelling;
    c. ICT-gerelateerde uitkomsten van interne en externe audits die aan de auditcommissie zijn gemeld.

3.2 Identificatie van wezenlijke ICT-risico's

38. Bevoegde autoriteiten identificeren de risico's waaraan de instelling is of zou kunnen worden blootgesteld, door de onderstaande stappen te volgen:

3.2.1 Toetsing van het ICT-risicoprofiel van de instelling

39. Bij de toetsing van het ICT-risicoprofiel van de instelling kijken bevoegde autoriteiten naar alle relevante informatie over de blootstellingen van de instelling aan ICT-risico's, waaronder de informatie in punt 37 en de vastgestelde wezenlijke gebreken of tekortkomingen in de ICT-organisatie en de instellingsbrede ricisobeheersing op grond van titel 2 van deze richtsnoeren, en toetsen zij waar relevant deze informatie op evenredige wijze. Als onderdeel van deze toetsing nemen bevoegde autoriteiten de volgende aspecten in aanmerking:

    a. het mogelijke effect van een belangrijke verstoring van de ICT-systemen op het financiële systeem hetzij op binnenlands hetzij op internationaal niveau;
    b. of het mogelijk is dat de instelling gevoelig is voor ICT-beveiligingsrisico's of ICT-beschikbaarheids- en -continuïteitsrisico's als gevolg van de afhankelijkheid van internet, uitgebreide toepassing van innovatieve ICT-oplossingen of andere bedrijfsdistributiekanalen die haar een gemakkelijker doelwit voor cyberaanvallen maken;
    c. of het mogelijk is dat de instelling meer is blootgesteld aan ICT-beveiligingsrisico's, ICT-beschikbaarheids- en -continuïteitsrisico's, ICT-data-integriteitsrisico's of ICT-wijzigingsrisico's vanwege de complexiteit (bijv. als gevolg van fusies of overnames) of het verouderde karakter van haar ICT-systemen;
    d. of de instelling wezenlijke wijzigingen aan haar ICT-systemen en/of ICT-functie aanbrengt (bijv. als gevolg van fusies, overnames, afstotingen of de vervanging van haar centrale ICT-systemen), die een nadelige uitwerking op de stabiliteit of het ordelijk functioneren van de ICT-systemen kunnen hebben en kunnen leiden tot wezenlijke ICT-beschikbaarheids- en -continuïteitsrisico's, ICT-beveiligingsrisico's, ICT-wijzigingsrisico's of ICT-data-integriteitsrisico's;
    e. of de instelling ICT-diensten of ICT-systemen binnen of buiten de groep heeft uitbesteed, waardoor zij aan wezenlijke ICT-uitbestedingsrisico's kan worden blootgesteld;
    f. of de instelling ambitieuze kostenbesparende maatregelen op ICT-gebied treft die ertoe kunnen leiden dat er minder ICT-investeringen, - middelen en -expertise nodig zijn en dat zij sterker wordt blootgesteld aan alle typen ICT-risico's in de taxonomie;
    g. of de instelling door de ligging van belangrijke operationele centra/datacentra op ICT-gebied (bijv. regio's, landen) kan worden blootgesteld aan natuurrampen (bijv. overstromingen, aardbevingen), politieke instabiliteit of arbeidsconflicten en binnenlandse onlusten die kunnen leiden tot een wezenlijke toename van ICT-beschikbaarheids- en -continuïteitsrisico's en ICT-beveiligingsrisico's.

3.2.2 Toetsing van de kritieke ICT-systemen en -diensten

40. Als onderdeel van de identificatie van de ICT-risico's met een potentiële significante impact op de instelling toetsen bevoegde autoriteiten documentatie van de instelling en vormen zij zich een oordeel over welke ICT-systemen en diensten cruciaal zijn voor het adequate functioneren, de beschikbaarheid, continuïteit en beveiliging van de essentiële activiteiten van de instelling.

41. Hiertoe beoordelen bevoegde autoriteiten de methode en processen die door de instelling worden toegepast om de kritieke ICT-systemen en -diensten te identificeren, waarbij zij rekening houden met

het feit dat sommige ICT-systemen en -diensten door de instelling als kritiek kunnen worden beschouwd vanuit een perspectief van bedrijfscontinuïteit en beschikbaarheid, beveiliging (bijv. fraudepreventie) en/of geheimhouding (bijv. vertrouwelijke gegevens). Bevoegde autoriteiten geven zich er bij het verrichten van hun toetsing rekenschap van dat kritieke ICT-systemen en -diensten ten minste aan een van de volgende voorwaarden moeten voldoen:

a. Zij ondersteunen centrale bedrijfsactiviteiten en distributiekanalen (bijv. geldautomaten, internet- en mobiel bankieren) van de instelling.

b. Zij ondersteunen essentiële governanceprocessen en bedrijfsfuncties, waaronder risicobeheer (bijv. systemen voor risicobeheer en het beheer van financiële middelen).

c. Zij vallen onder speciale wet- of regelgeving (indien aanwezig) waarin hogere eisen worden gesteld aan de beschikbaarheid, veerkracht, vertrouwelijkheid of de beveiliging (bijv. wetgeving voor gegevensbescherming of mogelijke doelstellingen voor de hersteltijd ('Recovery Time Objectives' (RTO), de maximale tijd waarbinnen een systeem na een incident moet zijn hersteld) en de doelstelling voor het herstelpunt ('Recovery Point Objective' (RPO), de maximale tijdsperiode gedurende welke gegevens in geval van een incident verloren kunnen zijn) van enkele systeemrelevante diensten (indien en waar van toepassing).

d. Zij verwerken of bewaren vertrouwelijke of gevoelige gegevens, waarvoor geldt dat als onbevoegden daar toegang toe krijgen, dit aanzienlijke gevolgen kan hebben voor de reputatie en financiële resultaten van de instelling of voor de deugdelijkheid en continuïteit van haar activiteiten (bijv. databanken met gevoelige klantgegevens).

e. Zij verschaffen basisfunctionaliteiten die van groot belang zijn voor het adequaat functioneren van de instelling (bijv. diensten op het gebied van telecom en connectiviteit, diensten op het gebied van ICT- en cyberbeveiliging).

3.2.3 Identificatie van wezenlijke ICT-risico's voor kritieke ICT-systemen en -diensten

42. Rekening houdend met de verrichte toetsingen van het ICT-risicoprofiel en de kritieke ICT-systemen en -diensten van de instelling zoals hierboven beschreven, vormen bevoegde autoriteiten zich een oordeel over de wezenlijke ICT-risico's die volgens hen in hun hoedanigheid van toezichthouder een significante prudentiële impact op de kritieke ICT-systemen en -diensten van de instelling kunnen hebben.

43. Bij de beoordeling van de mogelijke effecten van ICT-risico's op de kritieke ICT-systemen en -diensten van een instelling kijken bevoegde autoriteiten naar:

a. de financiële gevolgen, waaronder (maar niet beperkt tot) het verlies van middelen of activa, mogelijke compensatie van klanten, juridische en herstelkosten, contractuele schade, gederfde inkomsten;

b. de mogelijkheid tot verstoring van de activiteiten, met onder andere aandacht voor het belang van de desbetreffende financiële diensten; het aantal klanten en/of vestigingen en werknemers dat erdoor getroffen wordt;

c. de mogelijke gevolgen voor de reputatie van de instelling op grond van het kritieke karakter van de desbetreffende bankdienst of operationele activiteit (bijv. diefstal van klantgegevens); het externe

profiel/zichtbaarheid van de getroffen ICT-systemen en -diensten (bijv. systemen voor mobiel bankieren of internetbankieren, verkooppunten, geldautomaten of betalingssystemen);

d. de gevolgen van regelgeving, waaronder de mogelijkheid dat de regelgever gebruik maakt van publieke terechtwijzing en boetes of zelfs van wijzigingen in vergunningen;

e. de strategische gevolgen voor de instelling, bijvoorbeeld wanneer strategische product- of bedrijfsplannen in gevaar worden gebracht of worden gestolen.

44. Vervolgens wijzen bevoegde autoriteiten de geïdentificeerde ICT-risico's die als wezenlijk worden beschouwd, toe aan de volgende ICT-risicocategorieën waarvoor in de bijlage aanvullende beschrijvingen en voorbeelden van risico's worden gegeven. Bevoegde autoriteiten denken na over de ICT-risico's in de bijlage als onderdeel van de beoordeling op grond van titel 3:

a. ICT-beschikbaarheids- en continuïteitsrisico
b. ICT-beveiligingsrisico
c. ICT-wijzigingsrisico
d. ICT-data-integriteitsrisico
e. ICT-uitbestedingsrisico

Deze categorisering heeft tot doel bevoegde autoriteiten te helpen bepalen welke risico's wezenlijk zijn (indien aanwezig) en derhalve tijdens de volgende beoordelingsstappen nader en grondiger dienen te worden getoetst.

3.3 Beoordeling van de risicobeheersing met het oog op de beperking van wezenlijke ICT-risico's

45. Om te beoordelen in hoeverre de instelling aan restrisico's op ICT-gebied is blootgesteld, toetsen bevoegde autoriteiten hoe de instelling de wezenlijke risico's die bevoegde autoriteiten tijdens de hierboven beschreven beoordeling hebben vastgesteld, identificeren, bewaken, beoordelen en beperken.

46. Hiertoe toetsen bevoegde autoriteiten, met het oog op de geïdentificeerde wezenlijke ICT-risico's, de (het) toepasselijke:

a. beleid en processen in verband met het ICT-risicobeheer en drempels van risicotolerantie;

b. kader voor organisatiebeheer en toezicht;

c. bereik van de interne audits en de bevindingen daarvan; en

d. ICT-risicobeheersing die specifiek is voor het geïdentificeerde wezenlijke ICT-risico.

47. Bij deze beoordeling wordt rekening gehouden met de uitkomsten van de analyse van het totale kader voor risicobeheer en interne risicobeheersing als bedoeld in titel 5 van de SREP-richtsnoeren van EBA, en tevens met de governance en strategie van de instelling die in titel 2 van deze richtsnoeren worden besproken; grote tekortkomingen op deze gebieden kunnen namelijk invloed hebben op het vermogen van de instelling om haar blootstellingen aan ICT-risico's te beheren en te beperken. Waar relevant

maken bevoegde autoriteiten ook gebruik van de in punt 37 van deze richtsnoeren vermelde informatiebronnen.

48. Bevoegde autoriteiten voeren de volgende beoordelingsstappen uit op een wijze die evenredig is met de aard, schaal en complexiteit van de activiteiten van de instelling en door als toezichthouder een toetsing te verrichten die is toegesneden op het ICT-risicoprofiel van de instelling.

3.3.1 Beleid en processen in verband met ICT-risicobeheer en tolerantiedrempels

49. Bevoegde autoriteiten toetsen of de instelling passend beleid en passende processen in verband met het ICT-risicobeheer en tolerantiedrempels heeft voor de geïdentificeerde wezenlijke ICT-risico's. Deze kunnen een onderdeel van het kader voor het beheer van operationele risico's of een afzonderlijk document vormen. Hiertoe houden zij rekening met de vraag of:

    a. het beleid inzake risico door het leidinggevend orgaan is geformaliseerd en goedgekeurd en voldoende richtlijnen voor de ICT-risicobereidheid van de instelling en voor de belangrijkste nagestreefde ICT-risicobeheerdoelstellingen en/of toegepaste tolerantiedrempels voor ICT-risico's bevat. Het relevante ICT-risicobeheerbeleid moet ook aan alle relevante belanghebbenden worden gecommuniceerd;

    b. het toepasselijke beleid betrekking heeft op alle belangrijke elementen voor het risicobeheer van de geïdentificeerde wezenlijke ICT-risico's;

    c. de instelling een proces en onderliggende procedures heeft uitgevoerd voor de identificatie (bijv. zelfevaluaties van risico's en risicobeheersing, analyse van risicoscenario's) en bewaking van de betrokken wezenlijke ICT-risico's; en

    d. de instelling een ICT-risicobeheerrapportage heeft dat tijdige informatie aan de directie en het leidinggevend orgaan verschaft en dat de directie en/of het leidinggevend orgaan in staat stelt te beoordelen en te bewaken of de plannen en maatregelen voor de beperking van ICT-risico's van de instelling stroken met de goedgekeurde risicobereidheid en/of tolerantiedrempels (waar relevant) en om zicht te houden op wijzigingen in wezenlijke ICT-risico's.

3.3.2 Kader voor organisatiebeheer en toezicht

50. Bevoegde autoriteiten beoordelen hoe de toepasselijke taken en verantwoordelijkheden op het gebied van risicobeheer in de interne organisatie zijn ingebed en geïntegreerd om de geïdentificeerde wezenlijke ICT-risico's te beheren en daarop toezicht te houden. Wat dit betreft beoordelen bevoegde autoriteiten of de instelling aantoont:

    a. dat zij duidelijke taken en verantwoordelijkheden heeft vastgesteld voor de identificatie, beoordeling, bewaking, beperking en rapportage van en toezicht op het betrokken wezenlijke ICT-risico;

    b. dat de verantwoordelijkheden en taken in verband met risico's duidelijk worden gecommuniceerd, toegewezen en ingebed in alle relevante onderdelen (bijv. bedrijfsonderdelen, IT) en processen van de organisatie, waaronder de taken en

verantwoordelijkheden voor het verzamelen en samenvoegen van de risico-informatie en het rapporteren daarover aan de directie en/of het leidinggevend orgaan;

c. dat de activiteiten inzake ICT-risicobeheer worden verricht met voldoende en kwalitatief toereikende personele en technische middelen. Om vast te stellen hoe geloofwaardig de toepasselijke plannen voor risicobeperking zijn, beoordelen bevoegde autoriteiten eveneens of de instelling voldoende begrotingsmiddelen en/of andere vereiste middelen met het oog op de uitvoering ervan heeft toegekend;
d. dat het leidinggevend orgaan zorg draagt voor een adequate follow-up van en reactie op belangrijke bevindingen van de onafhankelijke controlefuncties wat betreft het (de) ICT-risico('s), waarbij rekening wordt gehouden met het feit dat sommige aspecten aan een commissie, indien aanwezig, kunnen worden gedelegeerd; en
e. dat uitzonderingen op toepasselijk(e) ICT-regelgeving en -beleid worden geregistreerd en onderworpen aan een gedocumenteerde toetsing en rapportage door de onafhankelijke controlefunctie met speciale aandacht voor de bijbehorende risico's.

3.3.3 Bereik van interne audits en bevindingen daarvan

51. Bevoegde autoriteiten bekijken of de interne auditfunctie effectief is als het gaat om de controle op het toepasselijke ICT-risicobeheersingskader. Hiertoe toetsen zij of:

a. het ICT-risicobeheersingskader met de vereiste kwaliteit, grondigheid en frequentie wordt gecontroleerd op een wijze die past bij de omvang, de activiteiten en het ICT-risicoprofiel van de instelling;

b. het auditplan audits bevat met betrekking tot de kritieke ICT-risico's die de instelling heeft geïdentificeerd;

c. de belangrijke bevindingen van ICT-audits, inclusief overeengekomen acties, aan het leidinggevend orgaan worden gemeld; en

d. er gevolg wordt gegeven aan de bevindingen van ICT-audits, inclusief overeengekomen acties, en of voortgangsverslagen periodiek door de directie en/of de auditcommissie worden geëvalueerd.

3.3.4 ICT-risicobeheersing die specifiek is voor de geïdentificeerde wezenlijke ICT-risico's

52. Voor de geïdentificeerde wezenlijke ICT-risico's geldt dat bevoegde autoriteiten beoordelen of de instelling specifieke beheersingsmaatregelen heeft om deze risico's aan te pakken. De volgende paragrafen bieden een niet-volledige lijst van de specifieke beheersingsmaatregelen waarnaar gekeken wordt bij de beoordeling van de wezenlijke risico's die in punt 3.2.3 zijn geïdentificeerd en aan de volgende ICT-risicocategorieën zijn toegewezen:

a. ICT-beschikbaarheids- en continuïteitsrisico's;
b. ICT-beveiligingsrisico's;
c. ICT-wijzigingsrisico's;
d. ICT-data-integriteitsrisico's
e. ICT-uitbestedingsrisico's.

(a) Beheersingsmaatregelen voor het beheer van wezenlijke ICT-beschikbaarheids- en continuïteitsrisico's

53. Als aanvulling op de vereisten in de SREP-richtsnoeren van EBA (punten 279-281) beoordelen bevoegde autoriteiten of de instelling een passend kader heeft voor het identificeren, begrijpen, meten en beperken van ICT-beschikbaarheids- en continuïteitsrisico's.

54. Hiertoe houden zij met name rekening met de vraag of het kader:

a. de kritieke ICT-processen en de relevante ondersteunende ICT-systemen identificeert die deel dienen uit te maken van de plannen voor de veerkracht en continuïteit van het bedrijf, met:

   i. een alomvattende analyse van de afhankelijkheden tussen de kritieke bedrijfsprocessen en ondersteunende systemen;

   ii. vaststelling van de doelen voor het herstel van de ondersteunende ICT-systemen (die bijv. gewoonlijk door het bedrijf en/of de regelgeving worden vastgesteld in termen van RTO en RPO);

   iii. passende noodplannen om beschikbaarheid, continuïteit en herstel van kritieke ICT-systemen en -diensten mogelijk te maken om een verstoring van de activiteiten van de instelling zo veel mogelijk en binnen aanvaardbare grenzen te beperken.

b. beleid en normen inzake de controleomgeving voor de veerkracht en continuïteit van het bedrijf en operationele controles behelst die het volgende omvatten:

   i. maatregelen om te voorkomen dat één scenario, incident of ramp zowel de ICT- productie- als -herstelsystemen kan beïnvloeden;

   ii. procedures voor ICT-systeembackups en -herstel voor kritieke software en gegevens, die ervoor zorgen dat deze backups op een veilige en op voldoende afstand gelegen locatie worden opgeslagen, zodat deze kritieke gegevens niet door een incident of ramp kunnen worden vernietigd of corrupt raken;

   iii. toezichtoplossingen voor de tijdige opsporing van incidenten in verband met de beschikbaarheid of continuïteit van ICT;

   iv. een gedocumenteerd incidentenbeheer- en escalatieproces dat tevens richtlijnen verschaft voor de verschillende taken en verantwoordelijkheden op het gebied van incidentenbeheer en escalatie, de leden van de crisiscommissie(s) en de hiërarchische structuur in noodgevallen;

   v. fysieke maatregelen om de kritieke ICT-infrastructuur van de instelling (bijv. datacentra) tegen milieurisico's (bijv. overstromingen en andere natuurrampen) te beschermen en te zorgen voor een passende operationele omgeving voor ICT-systemen (bijv. airconditioning);

   vi. processen, taken en verantwoordelijkheden om ervoor te zorgen dat er ook voor uitbestede ICT-systemen en -diensten adequate oplossingen en plannen zijn met het oog op de veerkracht en continuïteit van het bedrijf;

vii. oplossingen voor ICT-prestatie- en capaciteitsplanning en -monitoring voor kritieke ICT-systemen en -diensten met welbepaalde beschikbaarheidseisen, om belangrijke beperkingen qua prestaties en capaciteit tijdig op te sporen;

viii. oplossingen om kritieke internetactiviteiten of -diensten (bijv. elektronisch bankieren) waar nodig en passend te beschermen tegen Denial-of-Service- en andere cyberaanvallen op internet, bedoeld om de toegang tot deze activiteiten en diensten onmogelijk te maken of te verstoren.

c. oplossingen voor de beschikbaarheid en continuïteit van ICT test, afgezet tegen een reeks realistische scenario's waaronder cyberaanvallen, en failovertests en tests van backups voor kritieke software en gegevens:

i. die gepland, geformaliseerd en gedocumenteerd zijn, en de testresultaten die gebruikt worden om de oplossingen voor de beschikbaarheid en continuïteit van ICT doeltreffender te maken;

ii. die betrekking hebben op de belanghebbenden en functies binnen de organisatie, zoals de leiding van de bedrijfsonderdelen, waaronder bedrijfscontinuïteit en incident- en crisisresponsteams, evenals relevante externe belanghebbenden in het ecosysteem;

iii. waarbij het leidinggevend orgaan en de directie op passende wijze zijn betrokken (bijv. als onderdeel van crisismanagementteams) en zij van de testresultaten op de hoogte worden gebracht.

(b) Beheersingsmaatregelen voor het beheer van wezenlijke ICT-beveiligingsrisico's

55. Bevoegde autoriteiten beoordelen of de instelling een effectief kader heeft voor het identificeren, begrijpen, meten en beperken van ICT-beveiligingsrisico's. Hiertoe houden zij met name rekening met de vraag of het kader de volgende zaken in ogenschouw neemt:

a. duidelijk omschreven taken en verantwoordelijkheden met betrekking tot:

i. de perso(o)n(en) en/of commissies die verantwoording en rekenschap moeten afleggen voor het dagelijkse ICT-veiligheidsbeheer en de uitwerking van het overkoepelende ICT-veiligheidsbeleid, met aandacht voor hun benodigde onafhankelijkheid;
ii. het ontwerpen, uitvoeren, beheren en monitoren van ICT-veiligheidscontroles;
iii. de bescherming van kritieke ICT-systemen en -diensten via bijvoorbeeld een proces voor de beoordeling van kwetsbaarheden, softwarepatchmanagement, eindpuntbescherming (bijv. malwarevirus) en instrumenten voor inbraakdetectie en -preventie;
iv. het monitoren, classificeren en afhandelen van externe of interne ICT-veiligheidsincidenten, inclusief incidentenrespons en het hervatten en herstellen van de ICT-systemen en diensten;
v. regelmatige en proactieve dreigingsevaluaties om de veiligheidscontroles op een adequaat niveau te houden.

b. een ICT-veiligheidsbeleid dat rekening houdt met en, waar nodig, voldoet aan internationaal erkende ICT-veiligheidsnormen en -beginselen (bijv. het 'beginsel van het minste privilege', d.w.z. beperken van de toegang tot het laagste niveau waarbij normaal functioneren voor het beheer van toegangsrechten mogelijk is, en het beginsel van 'diepteverdediging', d.w.z. gelaagde veiligheidsmechanismen, zorgen voor een grotere beveiliging van het systeem als geheel met het oog op het ontwerpen van een veiligheidsarchitectuur);

c. een proces om ICT-systemen en -diensten en daarop afgestemde veiligheidseisen te identificeren die in verband kunnen worden gebracht met mogelijke frauderisico's en/of mogelijk verkeerd gebruik en/of misbruik van vertrouwelijke gegevens, samen met gedocumenteerde veiligheidsverwachtingen waaraan voor deze geïdentificeerde ICT-systemen, -diensten en -gegevens moet worden voldaan, in lijn met de risicotolerantie van de instelling en met toezicht op de correcte uitvoering ervan;

d. een gedocumenteerd veiligheidsincidentenbeheer- en escalatieproces dat richtsnoeren verschaft voor de verschillende taken en verantwoordelijkheden op het gebied van incidentenbeheer en escalatie, de leden van de crisiscommissie(s) en de hiërarchische structuur in noodgevallen op het vlak van veiligheid;

e. het loggen van gebruikers- en administratieve activiteiten om doeltreffende monitoring van en de tijdige opsporing van en respons op ongeoorloofde activiteit mogelijk te maken; en om deel te nemen aan forensisch onderzoek naar veiligheidsincidenten of dit uit te voeren. De instelling moet loggingbeleid hebben waarin wordt beschreven welke typen logs bewaard moeten worden en voor hoe lang;

f. bewustwordings- en voorlichtingscampagnes of -initiatieven om alle geledingen in de instelling te informeren over het veilige gebruik en de bescherming van de ICT-systemen van de instelling en de voornaamste ICT-beveiligingsrisico's (en andere risico's) die zij moeten kennen, met name wat betreft de bestaande en groeiende cyberdreigingen (bijv. computervirussen, mogelijk intern(e) of extern(e) misbruik of aanvallen, cyberaanvallen) en de rol die zij spelen in het verminderen van de inbreuken op de veiligheid;

g. adequate fysieke veiligheidsmaatregelen (bijv. camerabewaking, inbraakalarm, veiligheidsdeuren) om ongeoorloofde fysieke toegang tot kritieke en gevoelige ICT-systemen (bijv. datacentra) te voorkomen;

h. maatregelen om de ICT-systemen tegen aanvallen vanaf internet (d.w.z. cyberaanvallen) of andere externe netwerken (bijv. traditionele telecomverbindingen of verbindingen met vertrouwde partners) te beschermen. Bevoegde autoriteiten toetsen of het kader van de instelling de volgende zaken in ogenschouw neemt:

    i. een proces en oplossingen om een complete actuele inventaris en overzicht bij te houden van alle naar buiten gerichte netwerkaansluitpunten (zoals websites, internettoepassingen, wifi, toegang op afstand) waardoor derden in de interne ICT-systemen kunnen inbreken;

    ii. zorgvuldig beheerde en gecontroleerde veiligheidsmaatregelen (bijv. firewalls, proxyservers, mailrelays, antivirus- en contentscanners) om het inkomende en uitgaande netwerkverkeer (bijv. e-mail) en de naar buiten gerichte netwerkaansluitingen waardoor derden in de interne ICT-systemen kunnen inbreken, te beveiligen;

iii. processen en oplossingen om websites en toepassingen te beveiligen die rechtstreeks vanaf internet en/of van buitenaf kunnen worden aangevallen en die als toegangspunt voor de interne ICT-systemen kunnen dienen. Over het algemeen gaat het hierbij om een combinatie van erkende veilige ontwikkelingspraktijken, maatregelen om de ICT-systemen te harden en op kwetsbaarheden te scannen en/of de implementatie van aanvullende veiligheidsoplossingen zoals firewalls en/of inbraakdetectie- en/of inbraakpreventiesystemen;

iv. periodieke penetratietests om te beoordelen hoe effectief de uitgevoerde cyber- en interne ICT-veiligheidsmaatregelen en -processen zijn. Deze tests worden door personeel en/of externe deskundigen met de benodigde expertise verricht; de testresultaten en conclusies worden gedocumenteerd en aan de directie en/of het leidinggevend orgaan worden gemeld. Wanneer nodig en van toepassing, dient de instelling op basis van deze tests inzicht te krijgen in waar de veiligheidscontroles en -processen verder moeten worden verbeterd en/of hoe de effectiviteit ervan beter kan worden gewaarborgd.

(c) Beheersingsmaatregelen voor het beheer van wezenlijke ICT-wijzigingsrisico's

56. Bevoegde autoriteiten beoordelen of de instelling een effectief kader heeft voor het identificeren, begrijpen, meten en beperken van risico's in verband met wijzigingen in ICT, dat past bij de aard, schaal en complexiteit van de activiteiten van de instelling en het ICT-risicoprofiel van de instelling. Het kader van de instelling dient betrekking te hebben op de risico's die zich voordoen bij het ontwikkelen, testen en goedkeuren van ICT-systeemwijzigingen, waaronder de ontwikkeling van of wijzigingen in software, voordat deze naar de productieomgeving worden gemigreerd, en een adequaat ICT-levenscyclusbeheer te waarborgen. Hiertoe houden bevoegde autoriteiten met name rekening met de vraag of het kader de volgende zaken in ogenschouw neemt:

a. gedocumenteerde processen voor het beheren en controleren van wijzigingen in ICT-systemen (bijv. configuratie- en patchmanagement) en -gegevens (bijv. reparatie van bugs of gegevenscorrecties), waarbij ervoor wordt gezorgd dat het ICT-risicobeheer voldoende ingezet wordt bij belangrijke ICT-wijzigingen die een grote invloed op het risicoprofiel of de risicoblootstelling van de instelling kunnen hebben;

b. specificaties betreffende de vereiste scheiding van taken gedurende de verschillende fasen van de uitgevoerde ICT-wijzigingen (bijv. bedenken en ontwikkelen van oplossingen, testen en goedkeuren van nieuwe software en/of wijzigingen, migratie en implementatie in de productieomgeving, en reparatie van bugs), met speciale aandacht voor de geïmplementeerde oplossingen en scheiding van taken om wijzigingen te beheren en te controleren die door ICT-personeel (bijv. ontwikkelaars, ICT-systeembeheerders, databankbeheerders) of een andere partij (bijv. zakelijke gebruikers, dienstverleners) in de ICT-productiesystemen zijn aangebracht;

c. testomgevingen die productieomgevingen adequaat weerspiegelen;

d. een inventaris van de activa van de bestaande toepassingen en ICT-systemen in de productieomgeving en de test- en ontwikkelingsomgeving, zodat de vereiste wijzigingen (bijv. versie-updates of -upgrades, patchen van systemen, wijzigingen in de configuratie) voor de betrokken ICT-systemen op de juiste wijze kunnen worden beheerd, geïmplementeerd en gecontroleerd.

e. een proces om de levenscyclus van de gebruikte ICT-systemen te bewaken en te beheren, om ervoor te zorgen dat zij de huidige bedrijfs- en risicobeheervereisten blijven naleven en ondersteunen en dat de gebruikte ICT-oplossingen en -systemen bij voortduring door de verkopers ervan worden ondersteund; en dat dit vergezeld gaat van adequate procedures voor de ontwikkelingscyclus van software;

f. een systeem voor de controle van softwarebroncodes en passende procedures om ongeoorloofde wijzigingen in de broncode van intern ontwikkelde software te voorkomen;

g. een proces om de veiligheid en kwetsbaarheid van nieuwe of in wezenlijk opzicht gewijzigde ICT-systemen en software te screenen, alvorens deze vrij te geven voor productie en ze aan mogelijke cyberaanvallen bloot te stellen;

h. een proces en oplossingen om de ongeoorloofde of onbedoelde openbaarmaking van vertrouwelijke gegevens tijdens het vervangen, archiveren, verwijderen of vernietigen van ICT-systemen te voorkomen;

i. onafhankelijke toetsings- en validatieprocessen om de risico's op menselijke fouten te verkleinen wanneer er wijzigingen op de ICT-systemen worden aangebracht die een belangrijk nadelig effect op de beschikbaarheid, continuïteit of beveiliging van de instelling (bijv. belangrijke wijzigingen in de firewallconfiguratie) of de beveiliging van de instelling (bijv. wijzigingen in de firewalls) kunnen hebben.

(d) Beheersingsmaatregelen voor het beheer van wezenlijke ICT-data-integriteitsrisico's

57. Bevoegde autoriteiten beoordelen of de instelling een effectief kader heeft voor het identificeren, begrijpen, meten en beperken van ICT-data-integriteitsrisico's, dat past bij de aard, schaal en complexiteit van de activiteiten van de instelling en het ICT-risicoprofiel van de instelling. Het kader van de instelling moet oog hebben voor de risico's ten aanzien van het behoud van de integriteit van de door de ICT-systemen opgeslagen en verwerkte gegevens. Hiertoe houden zij met name rekening met de vraag of het kader de volgende zaken in ogenschouw neemt:

a. een beleid waarin de taken en verantwoordelijkheden worden beschreven voor het beheer van de integriteit van de gegevens in de ICT-systemen (bijv. gegevensarchitect (data architect), gegevensfunctionarissen (data officers) [6], gegevensbewaarders (data custodians) [7], eigenaars/beheerders van de gegevens (data owners/stewards)[8]) en waarin richtlijnen worden verschaft over welke gegevens vanuit het oogpunt van integriteit kritiek zijn en in de verschillende fasen van de levenscyclus van de ICT-gegevens aan specifieke ICT-controles (bijv. geautomatiseerde invoervalidatiecontroles, controles op gegevensoverdracht, afstemming, enz.) of toetsingen (bijv. een controle van compatibiliteit met de gegevensarchitectuur) moeten worden onderworpen;

[6] Een gegevensfunctionaris is verantwoordelijk voor de verwerking en het gebruik van gegevens.

[7] Een gegevensbewaarder is verantwoordelijk voor de bewaking, het veilige vervoer en de veilige opslag van gegevens.

[8] Een gegevensbeheerder is verantwoordelijk voor het beheer en de geschiktheid van gegevenselementen – zowel wat de inhoud als wat de metadata betreft.

b. een gedocumenteerde gegevensarchitectuur, gegevensmodel en/of data dictionary, die samen met relevante zakelijke en IT-belanghebbenden worden gevalideerd ter ondersteuning van de benodigde consistentie van de gegevens in alle ICT-systemen en om ervoor te zorgen dat de gegevensarchitectuur, het gegevensmodel en/of - woordenboek afgestemd blijven op de bedrijfs- en risicobeheerbehoeften;

c. een beleid betreffende het toegestane gebruik en dito afhankelijkheid van End User Computing, vooral aangaande de identificatie, registratie en documentatie van belangrijke computeroplossingen voor eindgebruikers (bijv. bij de verwerking van belangrijke gegevens) en de verwachte veiligheidsniveaus om ongeoorloofde wijzigingen te voorkomen, zowel in het instrument zelf als in de daarin opgeslagen gegevens.

d. gedocumenteerde processen voor de behandeling van uitzonderingen om geïdentificeerde problemen met betrekking tot de integriteit van ICT-gegevens overeenkomstig het kritieke en gevoelige karakter ervan op te lossen.

58. Voor onder toezicht staande instellingen die onder BCBS 239, beginselen voor effectieve samenvoeging van risicogegevens en risicorapportage[9], vallen, toetsen bevoegde autoriteiten de wijze waarop de instelling haar mogelijkheden voor risicorapportage en gegevensaggregatie analyseert vergeleken met de beginselen en de opgestelde documentatie op dat gebied, met inachtneming van het uitvoeringsschema en de overgangsgregelingen die in deze beginselen zijn vervat.

(e) Beheersingsmaatregelen voor het beheer van wezenlijke ICT-uitbestedingsrisico's

59. Bevoegde autoriteiten beoordelen of de uitbestedingsstrategie van de instelling, in lijn met de vereisten van de uitbestedingsrichtlijnen van het CEBT (2006) en met de vereiste in punt 85, onder d), van de SREP-richtsnoeren van EBA, adequaat op de ICT-uitbesteding van toepassing is, waaronder uitbesteding van ICT-diensten binnen de groep. Bij de beoordeling van de ICT-uitbestedingsrisico's houden bevoegde autoriteiten er rekening mee dat de ICT-uitbestedingsrisico's ook kunnen worden geanalyseerd als onderdeel van de beoordeling van inherente operationele risico's op grond van punt 240, onder j), van de SREP-richtsnoeren van EBA, om dubbel werk of dubbeltellingen te voorkomen.

60. In het bijzonder beoordelen bevoegde autoriteiten of de instelling een effectief kader heeft voor het identificeren, begrijpen en meten van het ICT-uitbestedingsrisico en met name of zij controles uitvoert en een controleomgeving heeft om risico's in verband met wezenlijke uitbestede ICT-diensten te beperken, die passen bij de omvang, activiteiten en het ICT-risicoprofiel van de instelling en die het volgende omvatten:

a. een beoordeling van het effect van de ICT-uitbesteding op het risicobeheer van de instelling in verband met het gebruik van dienstverleners (bijv. aanbieders van clouddiensten) en hun diensten tijdens het aanbestedingsproces, die door de directie of het leidinggevend orgaan wordt gedocumenteerd en wordt meegenomen in de besluitvorming rondom het al dan niet uitbesteden van de diensten. De instelling toetst het beleid inzake het ICT-risicobeheer en de ICT-controles en

[9] Bazels Comité voor bankentoezicht, Principles for effective risk data aggregation and risk reporting, januari 2013, online beschikbaar: http://www.bis.org/publ/bcbs239.pdf.

controleomgeving van de dienstverlener, zodat deze voldoen aan de doelstellingen op het gebied van intern risicobeheer en risicobereidheid van de instelling. Deze toetsing moet tijdens de contractuele uitbestedingsperiode periodiek worden geactualiseerd, met inachtneming van de kenmerken van de uitbestede diensten;

b. bewaking van de ICT-risico's van de uitbestede diensten tijdens de contractuele uitbestedingsperiode als onderdeel van het risicobeheer van de instelling, die de instelling meeneemt in haar verslaglegging over het ICT-risicobeheer (bijv. rapportage over de bedrijfscontinuïteit en over de beveiliging);

c. monitoring en vergelijking van de niveaus van de ontvangen diensten met de contractueel overeengekomen dienstverleningsniveaus, die onderdeel van het uitbestedingscontract of de Service Level Agreement (SLA) dienen te vormen; en

d. voldoende personeel, middelen en vaardigheden om de ICT-risico's van de uitbestede diensten te bewaken en te beheren.

3.4 Samenvatting van de bevindingen en toekenning van scores

61. Na de voorgaande beoordeling vormen bevoegde autoriteiten zich een oordeel over het ICT-risico van de instelling. Dit oordeel wordt verwoord in een samenvatting van bevindingen waarmee bevoegde autoriteiten rekening houden bij de toekenning van de score van het operationele risico in tabel 6 van de SREP-richtsnoeren van EBA. Bevoegde autoriteiten baseren hun standpunt over wezenlijke ICT-risico's op basis van de volgende overwegingen die in de beoordeling van het operationele risico worden meegenomen:

a. Risico-overwegingen

i. het ICT-risicoprofiel en de blootstelling aan ICT-risico's van de instelling;
ii. de geïdentificeerde kritieke ICT-systemen en -diensten; en
iii. de wezenlijkheid van ICT-risico's als het gaat om kritieke ICT-systemen.

b. Overwegingen over beheer en riscobeheersing

i. Of het beleid en de strategie van de instelling op het gebied van het beheer van ICT-risico's en haar algehele strategie en risicobereidheid met elkaar in overeenstemming zijn.
ii. of het organisatiekader voor het ICT-risicobeheer robuust is, met duidelijke verantwoordelijkheden en een duidelijke scheiding van taken tussen risico-eigenaars en de beheer- en -risicobeheersingsfuncties.
iii. of de systemen voor het meten, bewaken en rapporteren van het ICT-risico passend zijn, en
iv. of er deugdelijke kaders zijn voor de beheersing van wezenlijke ICT-risico's.

62. Indien bevoegde autoriteiten het ICT-risico als wezenlijk beschouwen en de bevoegde autoriteit besluit dit risico als subcategorie van het operationele risico te beoordelen en een score te geven, verschaft onderstaande tabel (tabel 1) de volgende overwegingen over de score van ICT-risico's.

Tabel 1: Overwegingen van de toezichthouder voor het toekennen van een score voor het ICT-risico

Risicoscore	Standpunt toezichthouder	Overwegingen voor inherent risico	Overwegingen voor adequaat beheer & risicobeheersing
1	Er is geen waarneembaar risico van een significante prudentiële impact op de instelling, gezien het niveau van inherent risico en het beheer en de risicobeheersing.	• De informatiebronnen waarnaar op grond van punt 37 moet worden gekeken, hebben geen belangrijke blootstellingen aan ICT-risico's aan het licht gebracht. • De aard van het ICT-risicoprofiel van de instelling heeft, in samenhang met de toetsing van de kritieke ICT-systemen en de wezenlijke ICT-risico's voor de ICT-systemen en -diensten, geen wezenlijke ICT-risico's aan het licht gebracht.	• Het beleid en de strategie van de instelling op het gebied van het ICT-risico is afgestemd op haar algehele strategie en risicobereidheid. • Het organisatiekader voor het ICT-risico is robuust, met duidelijke verantwoordelijkheden en een duidelijke scheiding van taken tussen risico-eigenaars en de beheer- en risicobeheersingsfuncties. • De systemen voor hetmeten, bewaken en rapporteren van het ICT-risico zijn passend. • Er is een deugdelijk kader voor de beheersing van het ICT-risico.
2	Er is een laag risico van een significante prudentiële impact op de instelling, gezien het niveau van het inherente risico en het beheer en de risicobeheersing.	• De informatiebronnen waarnaar op grond van punt 37 moet worden gekeken, hebben geen belangrijke blootstellingen aan ICT-risico's aan het licht gebracht. • De aard van het ICT-risicoprofiel van de instelling heeft, in samenhang met de toetsing van de kritieke ICT-systemen en de wezenlijke ICT-risico's voor de ICT-systemen en -diensten, een beperkte blootstelling aan ICT-risico's (bijv. niet meer dan 2 van de 5 vooraf vastgestelde ICT-risicocategorieën) aan het licht gebracht.	
3	Er is een middelhoog risico van een significante prudentiële impact op de instelling, gezien het niveau van het inherente risico en het beheer en de risicobeheersing.	• De informatiebronnen waarnaar op grond van punt 37 moet worden gekeken, hebben aanwijzingen voor mogelijke belangrijke blootstellingen aan ICT-risico's aan het licht gebracht. • De aard van het ICT-risicoprofiel van de instelling heeft, in samenhang met de toetsing van	

		de kritieke ICT-systemen en de wezenlijke ICT-risico's voor de ICT-systemen en -diensten, een verhoogde blootstelling aan ICT-risico's (bijv. 3 van de 5 vooraf vastgestelde ICT-risicocategorieën) aan het licht gebracht.	
4	Er is een hoog risico van een significante prudentiële impact op de instelling, gezien het niveau van het inherente risico en het beheer en de risicobeheersing.	• De informatiebronnen waarnaar op grond van punt 37 moet worden gekeken, hebben meerdere aanwijzingen voor belangrijke blootstellingen aan ICT-risico's verschaft. • De aard van het ICT-risicoprofiel van de instelling heeft, in samenhang met de toetsing van de kritieke ICT-systemen en de wezenlijke ICT-risico's voor de ICT-systemen en -diensten, een grote blootstelling aan ICT-risico's (bijv. 4 of 5 van de 5 vooraf vastgestelde ICT-risicocategorieën) aan het licht gebracht.	

Bijlage – ICT-risicotaxonomie

5 ICT-risicocategorieën met een niet-volledige lijst van ICT-risico's met mogelijk grote impact en/of operationele of financiële gevolgen of gevolgen voor de reputatie

ICT-risicocategorieën	ICT-risico's (niet-volledig[10])	Risicobeschrijving	Voorbeelden
ICT-beschikbaarheids- en continuïteitsrisico's	Onvoldoende capaciteitsbeheer	Door een gebrek aan middelen (bijv. hardware, software, personeel, dienstverleners) kan het onmogelijk worden om de dienstverlening af te stemmen op bedrijfsbehoeften en systeemonderbrekingen, verslechtering van de dienstverlening en/of operationele fouten te verhelpen.	• Een capaciteitstekort kan de transmissiesnelheid en de beschikbaarheid van het netwerk (internet) voor diensten als internetbankieren negatief beïnvloeden. • Een gebrek aan personeel (intern of derden) kan leiden tot systeemonderbrekingen en/of operationele fouten.
	Falen van de ICT-systemen	Verminderde beschikbaarheid door falende hardware.	• Falen/slecht functioneren van opslag (harde schijven), server of andere ICT-apparatuur, bijvoorbeeld veroorzaakt door gebrek aan onderhoud.
		Verminderde beschikbaarheid door falende software en bugs.	• Door een oneindige lus in applicatiesoftware wordt transactie niet uitgevoerd. • Uitval als gevolg van het blijven gebruiken van verouderde ICT-systemen en -oplossingen die niet langer aan de huidige eisen voor beschikbaarheid en veerkracht voldoen en/of niet langer door de verkopers ervan worden ondersteund.
	Ontoereikende planning voor ICT-continuïteit en -calamiteitenherstel	Falen van geplande ICT-beschikbaarheids- en/of -continuïteitsoplossingen en/of calamiteitenherstel (bijv. uitwijkdatacentra) wanneer deze als reactie op een incident worden geactiveerd.	• Configuratieverschillen tussen het primaire en secundaire datacentrum kunnen ertoe leiden dat het uitwijkdatacentrum de geplande continuïteit van de dienstverlening niet kan waarborgen.

[10] ICT-risico's worden vermeld in de risicocategorie waarop zij het grootste effect hebben, maar zij kunnen ook gevolgen hebben voor andere categorieën

ICT-risicocategorieën	ICT-risico's (niet-volledig[10])	Risicobeschrijving	Voorbeelden
	Ontwrichtende en destructieve cyberaanvallen	Aanvallen om verschillende redenen (activisme, chantage), die leiden tot overbelasting van systemen en het netwerk, waardoor rechtmatige gebruikers geen toegang tot onlinecomputerdiensten kunnen krijgen.	• Distributed Denial of Service (DDOS)-aanvallen worden uitgevoerd door een groot aantal computersystemen op internet die door een hacker worden gecontroleerd, waarbij een grote hoeveelheid ogenschijnlijk legitieme dienstverleningsverzoeken naar internetdiensten (bijv. elektronisch bankieren) worden verzonden.
ICT-beveiligingsrisico's	Cyberaanvallen en andere externe op ICT gebaseerde aanvallen	Aanvallen die vanaf internet of externe netwerken voor verschillende doeleinden (bijv. fraude, spionage, activisme/sabotage, cyberterrorisme) worden uitgevoerd met behulp van diverse technieken (bijv. social engineering, inbraakpogingen door gebruik te maken van kwetsbare plekken, toepassing van kwaadaardige software) waardoor controle over interne ICT-systemen wordt verkregen.	Verschillende typen aanvallen: • Geavanceerde en aanhoudende dreiging (Advanced Persistent Threat, APT) dat interne systemen worden overgenomen of informatie wordt gestolen (bijv. aan identiteitsdiefstal gerelateerde informatie, creditcardinformatie). • Kwaadaardige software (bijv. ransomware) die gegevens met het oog op chantage versleutelt. • Infectie van interne ICT-systemen met Trojaanse paarden om op verborgen wijze kwaadaardige systeemacties te verrichten. • Benutten van kwetsbaarheden in ICT-systemen en/of (web)applicaties (bijv. SQL-injectie) om toegang tot het interne ICT-systeem te krijgen.
		Verrichten van frauduleuze betalingstransacties door hackers die de beveiliging van diensten op het gebied van elektronisch bankieren en betalen doorbreken of omzeilen en/of kwetsbare plekken in de beveiliging van de interne betalingssystemen van de instelling aanvallen en benutten.	• Aanvallen tegen diensten op het gebied van elektronisch bankieren en betalen, met als doel ongeoorloofde transacties te verrichten. • Creëren en verzenden van frauduleuze betalingstransacties vanuit de interne betalingssystemen van de instelling (bijv. frauduleuze SWIFT-berichten).
		Verrichten van frauduleuze effectentransacties door hackers die de beveiliging van de diensten op het gebied van elektronisch bankieren	• Pump-and-dump-aanvallen waarbij toegang wordt verkregen tot elektronische effectenrekeningen van klanten en frauduleuze inkoop- of verkooporders

ICT-risicocategorieën	ICT-risico's (niet-volledig[10])	Risicobeschrijving	Voorbeelden
		doorbreken of omzeilen waardoor zij ook toegang tot de effectenrekeningen van de klant krijgen.	worden geplaatst om de marktprijs te beïnvloeden en/of winst te maken op basis van eerder vastgestelde effectenposities.
		Aanvallen op communicatieverbindingen en allerlei soorten conversaties of ICT-systemen met als doel informatie te verzamelen en/of fraude te plegen.	• Afluisteren/onderscheppen van de onbeschermde overdracht van ongecodeerde authenticatiegegevens.
	Ontoereikende interne ICT-beveiliging	Verkrijgen van ongeoorloofde toegang tot kritieke ICT-systemen vanuit de instelling voor verschillende doeleinden (bijv. fraude, uitvoeren en verbergen van rogue-trading-activiteiten, gegevensdiefstal, activisme/sabotage) met behulp van diverse technieken (bijv. misbruiken en/of escaleren van privileges, identiteitsdiefstal, social engineering, benutten van kwetsbaarheden in ICT-systemen, toepassing van kwaadaardige software).	• Installeren van key stroke loggers (key loggers) om gebruikersnamen en wachtwoorden te stelen om ongeoorloofde toegang to vertrouwelijke gegevens te krijgen en/of fraude te plegen. • Kraken/raden van zwakke wachtwoorden om onrechtmatige of verhoogde toegangsrechten te krijgen. • Systeembeheerder gebruikt besturingssystemen of databankhulpprogramma's (voor het rechtstreeks aanbrengen van wijzigingen in de databank) om fraude te plegen
		Ongeoorloofde ICT-handelingen vanwege ontoereikende procedures en praktijken op het gebied van ICT-toegangsbeheer.	• Niet blokkeren of verwijderen van onnodige accounts, bijv. van personeel dat een andere functie heeft gekregen en/of de instelling heeft verlaten, inclusief gasten of leveranciers voor wie toegang niet langer nodig is, waardoor ongeoorloofde toegang tot ICT-systemen wordt verkregen. • Toekennen van buitensporige toegangsrechten en privileges, zodat het mogelijk wordt ongeoorloofde toegang te verkrijgen en/of malafide activiteiten te verbergen.
		Bedreigingen voor de veiligheid door gebrek aan veiligheidsbewustzijn, waarbij werknemers ICT-veiligheidsbeleid en -procedures niet begrijpen of negeren of zich daar niet aan houden.	• Werknemers die om de tuin worden geleid en op die manier hulp bieden bij een aanval (d.w.z. social engineering). • Slechte praktijken met betrekking tot

ICT-risicocategorieën	ICT-risico's (niet-volledig[10])	Risicobeschrijving	Voorbeelden
			identificatiegegevens: delen van wachtwoorden, gebruik van 'eenvoudig' te raden wachtwoorden, gebruik van hetzelfde wachtwoord voor veel verschillende doeleinden, enz. • Opslaan van niet-versleutelde vertrouwelijke gegevens op laptops en draagbare opslagoplossingen (bijv. USB-sticks) die vatbaar zijn voor verlies of diefstal.
		De ongeoorloofde opslag of overdracht van vertrouwelijke informatie buiten de instelling.	• Personen die vertrouwelijke informatie stelen of deze bewust lekken of smokkelen naar onbevoegde personen of het publiek.
	Ontoereikende fysieke ICT-beveiliging	Verkeerd gebruik of diefstal van ICT-activa via fysieke toegang met schade, verlies van activa of gegevens en eventuele andere dreigingen tot gevolg.	• Fysiek inbreken in kantoorgebouwen en/of datacentra om ICT-apparatuur te stelen (bijv. computers, laptops, oplossingen voor opslag) en/of gegevens te kopiëren door fysieke toegang tot ICT-systemen.
		Opzettelijke of onopzettelijke schade aan fysieke ICT-activa veroorzaakt door terrorisme, ongevallen of ongelukkige/verkeerde handelingen van personeel van de instelling en/of derden (leveranciers, reparateur).	• Fysiek terrorisme (d.w.z. bomaanslagen) of sabotage van ICT-activa. • Vernietiging van datacentra door brand, lekkage of andere factoren.
		Onvoldoende fysieke bescherming tegen natuurrampen met als gevolg gedeeltelijke of volledige vernietiging van ICT-systemen/datacentra door natuurrampen.	• Aardbevingen, extreme hitte, stormen, zware sneeuwstormen, overstromingen, branden, blikseminslagen.
ICT-wijzigingsrisico's	Ontoereikende controle op wijzigingen in ICT-systemen en op ICT-ontwikkelingen	Incidenten veroorzaakt door onopgemerkte fouten of kwetsbaarheden als gevolg van wijzigingen (bijv. onvoorziene effecten van een wijziging of een slecht beheerde wijziging door het ontbreken van tests of onjuiste wijzigingsbeheerpraktijken) in bijv. software, ICT-systemen en gegevens.	• In productie gaan van onvoldoende geteste software of configuratiewijzigingen met onverwachte nadelige gevolgen voor gegevens (bijv. corruptie, wissen) en/of de prestaties van ICT-systemen (bijv. uitval, verslechtering van prestaties). • Ongecontroleerde wijzigingen in ICT-systemen of

ICT-risicocategorieën	ICT-risico's (niet-volledig[10])	Risicobeschrijving	Voorbeelden
			gegevens in de productieomgeving. • In productie gaan van slecht beveiligde ICT-systemen en internettoepassingen, wat hackers de mogelijkheid biedt de verleende internetdiensten aan te vallen en/of de interne ICT-systemen te doorbreken. • Ongecontroleerde wijzigingen in de broncode van intern ontwikkelde software. • Onvoldoende testen doordat een adequate testomgeving ontbreekt.
	Ontoereikende ICT-architectuur	Een zwak ICT-architectuurbeheer bij het ontwerpen, bouwen en onderhouden van ICT-systemen (bijv. software, hardware, gegevens) kan uiteindelijk leiden tot complexe, moeilijke en rigide ICT-systemen waarvan het beheer veel geld kost en die niet langer voldoende zijn afgestemd op de bedrijfsbehoeften en ten opzichte van de actuele vereisten op het gebied van risicobeheer tekortschieten.	• Niet adequaat beheerde wijzigingen in ICT-systemen, software en/of gegevens over een langdurige periode, die leiden tot complexe, heterogene en moeilijk te beheren ICT-systemen en -architecturen, met talrijke nadelige gevolgen voor de bedrijfsvoering en het risicobeheer (bijv. ontbreken van flexibiliteit en wendbaarheid, ICT-incidenten en -storingen, hoge operationele kosten, verzwakte ICT-beveiliging en -veerkracht, verminderde gegevenskwaliteit en verslagleggingsmogelijkheden). • Buitensporige aanpassing en uitbreiding van commerciële softwarepakketten met intern ontwikkelde software, waardoor er in de toekomst geen nieuwe versies en upgrades van de commerciële software kunnen worden geïmplementeerd en de ondersteuning door de verkoper dreigt te verdwijnen.
	Ontoereikende levenscyclus- en patchmanagement	Niet bijhouden van een adequate inventaris van alle ICT-activa ter ondersteuning van, en in combinatie met, deugdelijke praktijken op het gebied van levenscyclus- en patchmanagement.	• Ongepatchte en verouderde ICT-systemen met mogelijk negatieve gevolgen voor de bedrijfsvoering en voor het risicobeheer (bijv. ontbreken van flexibiliteit en wendbaarheid, ICT-uitval, verzwakte

ICT-risicocategorieën	ICT-risico's (niet-volledig[10])	Risicobeschrijving	Voorbeelden
		Dit leidt tot onvoldoende gepatchte (en dus kwetsbaardere) en verouderde ICT-systemen die de bedrijfs- en risicobeheerbehoeften wellicht niet ondersteunen.	ICT-beveiliging en -veerkracht).
ICT-data-integriteitsrisico's	Slechte ICT-gegevensverwerking of -behandeling	Door fouten of storingen in systemen, communicatie en/of toepassingen of verkeerd uitgevoerde extractie, overdracht en laden (ETL) van gegevens kunnen gegevens corrupt raken of verloren gaan.	• IT-systeemfout tijdens batchverwerking, waardoor onjuiste saldi op de bankrekeningen van klanten ontstaan. • Verkeerd uitgevoerde zoekopdrachten. • Gegevensverlies door datareplicatie- (backup-)fout.
	Slecht ontworpen gegevensvalidatiecontroles in ICT-systemen	Fouten in verband met ontbrekende of ineffectieve controles betreffende de geautomatiseerde invoer en goedkeuring van gegevens (bijv. voor gebruikte gegevens van derden) en controles betreffende de overdracht, verwerking en uitvoer van gegevens in de ICT-systemen (bijv. controles op de validiteit van de invoer, afstemming van gegevens).	• Onvoldoende of ongeldige opmaak/validatie van gegevensinvoer in applicaties en/of gebruikersinterfaces. • Geen controles betreffende de afstemming van gegevens verricht op de geproduceerde uitvoer. • Geen controles verricht op de uitgevoerde gegevensextractieprocessen (bijv. zoekopdrachten in databanken), wat leidt tot foutieve gegevens. • Gebruik van onjuiste externe gegevens.
	Slecht gecontroleerde wijzigingen in de ICT-productiesystemen	Fouten in gegevens als gevolg van onvoldoende controle of de gegevensbehandeling tijdens de productie van ICT-systemen correct is en of de wijze waarop die behandeling plaatsvindt, gerechtvaardigd is.	• Ontwikkelaars of beheerders van databanken die zich op ongecontroleerde wijze rechtstreeks toegang tot de ICT-productiesystemen verschaffen en de gegevens daarvan wijzigen, bijv. in geval van een ICT-incident.
	Slecht ontworpen en/of beheerde gegevensarchitectuur, gegevensstromen, gegevensmodellen of gegevenswoordenb	Slecht beheerde gegevensarchitecturen, gegevensmodellen, gegevensstromen of gegevenswoordenboeken kunnen leiden tot meerdere versies van dezelfde gegevens in alle ICT-systemen, die niet langer consistent zijn vanwege op verschillende wijze toegepaste gegevensmodellen of gegevensdefinities, en/of verschillen in het onderliggende proces van de	• Het bestaan van verschillende klantendatabanken per product of bedrijfseenheid met verschillende gegevensdefinities en -velden, wat leidt tot niet onderling afgestemde en moeilijk te vergelijken en te integreren klantgegevens op het niveau van de gehele financiële instelling of groep.

ICT-risicocategorieën	ICT-risico's (niet-volledig[10])	Risicobeschrijving	Voorbeelden
	oeken	ontwikkeling van en wijzigingen in gegevens.	
ICT-uitbestedingsrisico's	Ontoereikende veerkracht van diensten verleend door een derde of een andere entiteit van de groep	De niet-beschikbaarheid van kritieke uitbestede ICT-diensten, telecommunicatiediensten en nutsvoorzieningen. Verlies of corruptie van kritieke/gevoelige gegevens die aan de dienstverlener zijn toevertrouwd.	• Niet-beschikbaarheid van centrale diensten als gevolg van fouten in (uitbestede) ICT-systemen of -toepassingen van leveranciers. • Verstoring van telecommunicatieverbindingen. • Gebrekkige stroomvoorziening.
	Ontoereikende governance inzake uitbesteding	Belangrijke verslechtering van de dienstverlening of fouten als gevolg van ondoeltreffende paraatheids- of controleprocessen van de verlener van de uitbestede diensten. Ineffectieve governance inzake uitbesteding kan resulteren in een tekort aan passende vaardigheden en mogelijkheden om de ICT-risico's volledig te identificeren, te beoordelen, te beperken en te bewaken en kan de operationele mogelijkheden van instellingen verminderen.	• Gebrekkige procedures voor het afhandelen van incidenten, contractuele controlemechanismen en garanties die in de dienstverleningsovereenkomst zijn ingebouwd en die ervoor zorgen dat belangrijke medewerkers afhankelijker worden van derden en verkopers. • Ongeschikte controles op het wijzigingsbeheer betreffende de ICT-omgeving van de dienstverlener kunnen een belangrijke verslechtering van de dienstverlening of storingen veroorzaken.
	Ontoereikende beveiliging van een derde of een andere entiteit van de groep	Hacken van de ICT-systemen van de dienstverlener, met rechtstreekse gevolgen voor de uitbestede diensten of kritieke/vertrouwelijke gegevens die bij de dienstverlener zijn opgeslagen. Personeel van de dienstverlener krijgt ongeoorloofde toegang tot kritieke/gevoelige gegevens die bij de dienstverlener zijn opgeslagen.	• Hacken van dienstverleners door criminelen of terroristen, als toegangspunt voor de ICT-systemen van instellingen of om inzage te krijgen in kritieke of gevoelige gegevens die bij de dienstverlener zijn opgeslagen, of deze te vernietigen. • Kwaadwillende insiders van de dienstverlener proberen gevoelige gegevens te stelen en te verkopen.