Richtsnoeren

EBA/GL/2019/04

28 november 2019

EBA-richtsnoeren inzake ICT en risicobeheer op het gebied van veiligheid

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 de richtsnoeren te voldoen.

2. Richtsnoeren geven weer wat in de opvatting van 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.

Rapportagevereisten

3. Overeenkomstig artikel 16, lid 3, van Verordening (EU) nr. 1093/2010 stellen bevoegde autoriteiten EBA vóór ([dd.mm.jjjj]) 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 door EBA 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/2019/04". 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 moet eveneens aan EBA worden gemeld.

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

Onderwerp, toepassingsgebied en definities

Onderwerp

5. Deze richtsnoeren bouwen voort op de bepalingen van artikel 74 van Richtlijn 2013/36/EU (RKV) betreffende interne governance, en vloeien voort uit het mandaat om richtsnoeren uit te vaardigen overeenkomstig artikel 95, lid 3, van Richtlijn (EU) 2015/2366 (RBD2).

6. Deze richtsnoeren lichten de risicobeheermaatregelen toe die financiële instellingen (zoals gedefinieerd in lid 9 hieronder) moeten treffen overeenkomstig artikel 74 van de RKV om hun ICT- en beveiligingsrisico's voor alle activiteiten te beheren, en die betalingsdienstaanbieders (zoals gedefinieerd in lid 9 hieronder) moeten treffen overeenkomstig artikel 95, lid 1, van de RBD2, om de operationele en beveiligingsrisico's (bedoeld als "ICT- en beveiligingsrisico's") met betrekking tot de betalingsdiensten die zij aanbieden te beheren. Deze richtsnoeren omvatten vereisten voor informatiebeveiliging, inclusief cyberbeveiliging, voor zover de informatie wordt bewaard in ICT-systemen.

Toepassingsgebied

7. Deze richtsnoeren zijn van toepassing voor het beheer van ICT- en beveiligingsrisico's binnen financiële instellingen (zoals gedefinieerd in lid 9). Voor de toepassing van deze richtsnoeren slaat de term "ICT- en beveiligingsrisico's" op de operationele en beveiligingsrisico's van artikel 95 van RBD2 voor de verlening van betalingsdiensten.

8. Voor betalingsdienstaanbieders (zoals gedefinieerd in lid 9) zijn deze richtsnoeren van toepassing op hun verlening van betalingsdiensten, in overeenstemming met het toepassingsgebied en mandaat van artikel 95 van RBD2. Voor instellingen (zoals gedefinieerd in lid 9) zijn deze richtsnoeren van toepassing op alle activiteiten die ze aanbieden.

Geadresseerden

9. Deze richtsnoeren zijn gericht op financiële instellingen, wat voor de toepassing van deze richtsnoeren verwijst naar 1) betalingsdienstaanbieders zoals gedefinieerd in artikel 4, lid 11, van RBD2; en 2) instellingen, dit wil zeggen kredietinstellingen en beleggingsondernemingen zoals bedoeld in punt 3 van artikel 4, lid 1, van Verordening (EU) nr. 575/2013. Deze richtsnoeren zijn ook van toepassing op bevoegde autoriteiten als gedefinieerd in artikel 4, lid 1, punt 40, van Verordening (EU) nr. 575/2013, met inbegrip van de Europese Centrale Bank voor zaken die verband houden met de taken die haar zijn toegewezen bij Verordening (EU) nr. 1024/2013, en bevoegde autoriteiten in het kader van RDB2 waarnaar wordt verwezen in artikel 4, lid 2, letter i), van Verordening (EU) nr. 1093/2010.

Definities

10. Tenzij anders aangegeven, hebben de termen die in Richtlijn 2013/36/EU (RKV), Verordening (EU) nr. 575/2013 (VKV) en Richtlijn 2366/2015/EU (RBD2) worden gebruikt en gedefinieerd, in deze richtsnoeren dezelfde betekenis. In deze richtsnoeren gelden bovendien de volgende definities:

ICT- en beveiligingsrisico	het risico van verliezen als gevolg van inbreuken op de geheimhouding, falende integriteit van systemen en data, ongeschiktheid of onbeschikbaarheid van systemen en data, of onvermogen om IT aan te passen binnen een redelijke termijn en met redelijke kosten wanneer de omgeving of de bedrijfsvereisten veranderen (d.w.z. flexibiliteit)[2]. Dit omvat beveiligingsrisico's die voortvloeien uit ontoereikende of falende interne processen of externe gebeurtenissen met inbegrip van cyberaanvallen of ontoereikende fysieke beveiliging.
Leidinggevend orgaan	(a) Voor kredietinstellingen en beleggingsondernemingen heeft deze term dezelfde betekenis als de definitie in punt 7 van artikel 3, lid 1, van Richtlijn 2013/36/EU. (b) Voor betalingsinstellingen of elektronischgeldinstellingen verwijst deze term naar de bestuurders of personen die verantwoordelijk zijn voor het bestuur van de betalingsinstellingen en elektronischgeldinstellingen en, waar dit relevant is, naar personen die verantwoordelijk zijn voor het beheer van de betalingsdienstactiviteiten van de betalingsinstellingen en elektronischgeldinstellingen. (c) Voor de betalingsdienstaanbieders waarnaar verwezen wordt in de punten c), e) en f) van artikel 1, lid 1, van Richtlijn (EU) 2015/2366, heeft deze term de betekenis die geldt in de toepasselijke nationale of EU-wetgeving.
Operationeel of veiligheidsincident	Een losse gebeurtenis of een reeks met elkaar verbonden gebeurtenissen die niet is gepland door de financiële instelling en die een nadelig effect heeft of waarschijnlijk zal hebben op de integriteit, beschikbaarheid, vertrouwelijkheid en/of authenticiteit van betalingsgerelateerde diensten.
Hogere leidinggevenden	(a) Voor kredietinstellingen en beleggingsondernemingen heeft deze term dezelfde betekenis als de definitie in punt 9 van artikel 3, lid 1, van Richtlijn 2013/36/EU. (b) Voor betalingsinstellingen en elektronischgeldinstellingen betekent deze term de natuurlijke personen die een uitvoerende functie uitoefenen in een instelling en die

[2] Definitie uit de EBA-richtsnoeren inzake gemeenschappelijke procedures en methoden voor het proces van toetsing en evaluatie door de toezichthouder van 19 december 2014 (EBA/GL/2014/13), gewijzigd door EBA/GL/2018/03.

	verantwoordelijk zijn voor het dagelijks bestuur van de instelling en hierover rekenschap moeten geven aan het leidinggevend orgaan. (c) Voor de betalingsdienstaanbieders waarnaar verwezen wordt in de punten c), e) en f) van artikel 1, lid 1, van Richtlijn (EU) 2015/2366, heeft deze term de betekenis die geldt in de toepasselijke nationale of EU-wetgeving.
Risicobereidheid	Het totale risiconiveau en de soorten risico's die de betalingsdienstaanbieders en instellingen binnen hun risicodraagkracht en overeenkomstig hun bedrijfsmodel bereid zijn te nemen om hun strategische doelen te bereiken.
Auditfunctie	(a) Voor kredietinstellingen en beleggingsondernemingen is de auditfunctie zoals bedoeld in artikel 22 van de EBA-richtsnoeren betreffende interne governance (EBA/GL/2017/11). (b) Voor andere betalingsdienstaanbieders dan kredietinstellingen moet de auditfunctie onafhankelijk zijn binnen of onafhankelijk zijn van de betalingsdienstaanbieder, en kan het een interne en/of externe auditfunctie betreffen.
ICT-projecten	Elk project, of onderdeel daarvan, waarbij ICT-systemen en -diensten worden gewijzigd, vervangen, afgewezen of uitgevoerd. ICT-projecten kunnen deel uitmaken van ruimere programma's voor ICT- of bedrijfstransformatie.
Derde partij	Een organisatie die zakelijke relaties is aangegaan of overeenkomsten heeft gesloten met een entiteit om een product of een dienst te verstrekken[3].
Informatie-activa	Een verzameling van informatie, al dan niet tastbaar, die het beschermen waard is.
ICT-activum	Een activum van software of hardware dat terug te vinden is binnen de bedrijfsomgeving.
ICT-systemen[4]	ICT-opstelling als onderdeel van een mechanisme of een verbindingsnetwerk dat de werkzaamheden van een financiële instelling ondersteunt.
ICT-diensten[5]	Diensten die door ICT-systemen aan een of meerdere interne of externe gebruikers worden verstrekt. Voorbeelden zijn onder meer diensten inzake gegevensinvoer, gegevensopslag, gegevensverwerking en rapportage, maar ook diensten inzake monitoring, en besluitvormings- en bedrijfsondersteuning.

[3] Definitie van de fundamentele elementen van de G7 voor het beheer van cyberrisico's van derden in de financiële sector.
[4] Definitie uit de richtsnoeren inzake ICT-risicobeoordeling in het kader van de procedure voor toetsing en evaluatie door de toezichthouder (EBA/GL/2017/05).
[5] ibid.

Tenuitvoerlegging

Toepassingsdatum

11. Deze richtsnoeren gelden vanaf 30 juni 2020.

Intrekking

12. De richtsnoeren inzake veiligheidsmaatregelen voor operationele en beveiligingsrisico's (EBA/GL/2017/17) die in 2017 werden gepubliceerd worden door deze richtsnoeren vervangen op het moment dat deze richtsnoeren van toepassing worden.

Richtsnoeren inzake ICT en risicobeheer op het gebied van veiligheid

1.1. Evenredigheid

1. Alle financiële instellingen moeten voldoen aan de bepalingen die in deze richtsnoeren zijn uiteengezet, op een manier die evenredig is aan en rekening houdt met de omvang en interne organisatie van de financiële instelling, en de aard, omvang, complexiteit en het risicogehalte van de diensten en producten die de financiële instellingen verstrekken of van plan zijn te verstrekken.

1.2. Governance en strategie

1.2.1. Governance

2. Het leidinggevend orgaan moet ervoor zorgen dat financiële instellingen over een passend kader voor interne governance en interne controle beschikken voor hun ICT- en beveiligingsrisico's. Het leidinggevend orgaan moet duidelijke taken en verantwoordelijkheden bepalen voor ICT-functies, risicobeheer in verband met informatiebeveiliging, en bedrijfscontinuïteit, ook deze voor het leidinggevende orgaan en de comités ervan.
3. Het leidinggevend orgaan moet ervoor zorgen dat de omvang en vaardigheden van het personeel van de financiële instellingen passend zijn om hun operationele ICT-behoeften en risicobeheerprocedures inzake ICT en beveiliging doorlopend te ondersteunen, en de implementatie van hun ICT-strategie te waarborgen. Het leidinggevend orgaan moet ervoor zorgen dat de toegekende begroting toereikend is om het bovenstaande te verwezenlijken. Verder moeten financiële instelling ervoor zorgen dat alle personeelsleden, met inbegrip van personen met een sleutelpositie, een passende opleiding over ICT- en beveiligingsrisico's

ontvangen, onder meer over informatiebeveiliging, op jaarbasis, of vaker indien nodig (zie ook punt 1.4.7).

4. Het leidinggevend orgaan heeft algemene verantwoordingsplicht voor het opzetten, goedkeuren en bewaken van de uitvoering van de ICT-strategie van de financiële instellingen als onderdeel van hun algemene bedrijfsstrategie, evenals voor de vaststelling van een doeltreffend risicobeheerkader voor ICT- en beveiligingsrisico's.

1.2.2. Strategie

5. De ICT-strategie moet worden afgestemd op de algemene bedrijfsstrategie van de financiële instellingen en moet bepalen:
    a) hoe de ICT van de financiële instelling moet evolueren om hun bedrijfsstrategie doeltreffend te ondersteunen en er deel van uit te maken, met inbegrip van de evolutie van de organisatiestructuur, ICT-systeemveranderingen en belangrijke afhankelijkheden van derden;
    b) de geplande strategie en evolutie van de ICT-architectuur, met inbegrip van afhankelijkheden van derden;
    c) duidelijke doelstellingen inzake informatiebeveiliging, met de nadruk op ICT-systemen en -diensten, personeel en processen.
6. Financiële instellingen moeten actieplannen opstellen waarin maatregelen zijn opgenomen die moeten worden getroffen om het doel van de ICT-strategie te bereiken. Deze moeten aan alle relevante personeelsleden worden bekendgemaakt (inclusief contractanten en derde aanbieders waar van toepassing en relevant). De actieplannen moeten regelmatig worden herzien om de relevantie en geschiktheid ervan te waarborgen. Financiële instellingen moeten ook processen ontwikkelen om de doeltreffendheid van de tenuitvoerlegging van hun ICT-strategie te monitoren en meten.

1.2.3. Gebruik van derde aanbieders

7. Onverminderd de EBA-richtsnoeren inzake uitbestedingsregelingen (EBA/GL/2019/02) en artikel 19 van RBD2, moeten financiële instellingen zorgen voor de doeltreffendheid van de risicobeperkingsmaatregelen zoals omschreven in hun risicobeheerkader, met inbegrip van de maatregelen die in deze richtsnoeren zijn uiteengezet, wanneer operationele functies van betalingsdiensten en/of ICT-diensten en -systemen van een activiteit worden uitbesteed, inclusief aan entiteiten van de groep, of wanneer een beroep wordt gedaan op derden.
8. Om de continuïteit van ICT-diensten en -systemen te waarborgen, moeten financiële instellingen ervoor zorgen dat contracten en overeenkomsten inzake dienstverleningsniveau (zowel onder normale omstandigheden als in het geval van verstoring van de diensten — zie ook punt 1.7.2) met aanbieders (uitbestedingsleveranciers, entiteiten van de groep of derde aanbieders) het volgende omvatten:

a) passende en evenredige beveiligingsgerelateerde doelstellingen en maatregelen inclusief vereisten zoals minimale cyberbeveiligingsvereisten; specificatie van de levenscyclus van de gegevens van de financiële instelling; vereisten met betrekking tot versleuteling van gegevens, netwerkbeveiliging en procedures voor beveiligingscontrole, en de locatie van datacentra;
b) operationele procedures en behandelingsprocedures inzake veiligheidsincidenten inclusief escalatie en rapportage.

9. Financiële instellingen moeten toezicht houden op en controleren in welke mate deze verstrekkers de beveiligingsdoelstellingen, maatregelen en prestatiedoelstellingen van de financiële instelling naleven.

1.3. Kader voor het beheer van ICT- en beveiligingsrisico's

1.3.1. Organisatie en doelstellingen

10. Financiële instellingen moeten hun ICT- en beveiligingsrisico's identificeren en beheren. De ICT-functies die verantwoordelijk zijn voor ICT-systemen, processen en beveiligingsoperaties moeten beschikken over passende processen en controles om ervoor te zorgen dat alle risico's in kaart worden gebracht, worden geanalyseerd, gemeten, gemonitord, beheerd, gerapporteerd en binnen de grenzen van de risicobereidheid van de financiële instelling worden gehouden, en dat de projecten en systemen die ze verstrekken en de activiteiten die ze uitvoeren in overeenstemming zijn met externe en interne vereisten.

11. Financiële instellingen moeten de verantwoordelijkheid voor het beheren en bewaken van ICT- en beveiligingsrisico's aan een controlefunctie toewijzen, om zich zo te houden aan de vereisten van afdeling 19 van de EBA-richtsnoeren inzake interne governance (EBA/GL/2017/11). Financiële instellingen moeten de onafhankelijkheid en objectiviteit van deze controlefunctie waarborgen door deze op passende wijze te scheiden van processen inzake ICT-activiteiten. Deze controlefunctie is rechtstreeks verantwoording verschuldigd aan het leidinggevend orgaan, en is verantwoordelijk voor het monitoren en controleren van de naleving van het kader voor het beheer van ICT- en beveiligingsrisico's. De functie moet waarborgen dat de ICT- en beveiligingsrisico's in kaart worden gebracht, worden gemeten, beoordeeld, beheerd, gemonitord en gerapporteerd. Financiële instellingen moeten ervoor zorgen dat deze controlefunctie niet verantwoordelijk is voor interne audits.

    De interne-auditfunctie moet, volgens een risicogebaseerde benadering, in staat zijn om op onafhankelijke wijze de naleving van het beleid en de procedures van de financiële instelling en van de externe eisen door alle ICT- en beveiligingsgerelateerde activiteiten en eenheden van een financiële instelling te beoordelen en objectief te waarborgen, om zich zo te houden aan de vereisten van afdeling 22 van de EBA-richtsnoeren inzake interne governance (EBA/GL/2017/11).

12. Financiële instellingen moeten sleutelfuncties en -verantwoordelijkheden bepalen en toewijzen, evenals relevante rapportagelijnen, opdat het kader voor het beheer van ICT- en beveiligingsrisico's doeltreffend is. Dit kader moet volledig worden opgenomen in en afgestemd op de algemene risicobeheerprocessen van de financiële instellingen.

13. Het kader voor het beheer van ICT- en beveiligingsrisico's bestaat uit processen om:

    a) de risicobereidheid voor ICT- en beveiligingsrisico's te bepalen, in overeenstemming met de risicobereidheid van de financiële instelling;
    b) de ICT- en beveiligingsrisico's waaraan een financiële instelling wordt blootgesteld, in kaart te brengen en te beoordelen;
    c) beperkingsmaatregelen, inclusief beheersmaatregelen, vast te stellen om ICT- en beveiligingsrisico's te verminderen;
    d) de doeltreffendheid van deze maatregelen te monitoren, evenals het aantal gerapporteerde incidenten, waaronder voor betalingsdienstaanbieders de gerapporteerde incidenten overeenkomstig artikel 96 van RBD2 die een invloed hebben op de ICT-gerelateerde activiteiten, en actie te ondernemen om de maatregelen waar nodig te corrigeren;
    e) verslag uit te brengen bij het leidinggevend orgaan over ICT- en beveiligingsrisico's en beheersmaatregelen;
    f) identificeren en beoordelen of er ICT- en beveiligingsrisico's voortvloeien uit grote wijzigingen in ICT-systemen of IT-diensten, processen of procedures, en/of na belangrijke operationele of veiligheidsincidenten.

14. Financiële instellingen moeten ervoor zorgen dat het kader voor het beheer van ICT- en beveiligingsrisico's wordt gedocumenteerd en voortdurend wordt verbeterd, op basis van tijdens de tenuitvoerlegging en monitoring "getrokken lessen". Het kader voor het beheer van ICT- en beveiligingsrisico's moet ten minste jaarlijks door het leidinggevend orgaan worden goedgekeurd en geëvalueerd.

1.3.2. Identificatie van functies, processen en activa

15. Financiële instellingen moeten hun bedrijfsfuncties, taken en ondersteunende processen identificeren, opstellen, in kaart brengen en steeds actualiseren om het belang van elk onderdeel te identificeren, evenals hun afhankelijkheden met betrekking tot ICT- en beveiligingsrisico's.

16. Daarnaast moeten financiële instellingen de informatie-activa die hun bedrijfsfuncties en ondersteunende processen ondersteunen, identificeren, opstellen, in kaart brengen en steeds actualiseren, zoals ICT-systemen, personeel, contractanten, derden en afhankelijkheden van andere externe en interne systemen en processen, om ten minste de informatie-activa die hun kritieke bedrijfsfuncties en processen ondersteunen te kunnen beheren.

1.3.3. Classificatie en risicobeoordeling

17. Financiële instellingen dienen de geïdentificeerde bedrijfsfuncties, ondersteunende processen en informatie-activa waarnaar verwezen wordt in de leden 15 en 16 te classificeren naargelang hun kritieke karakter.

18. Om het kritieke karakter van deze geïdentificeerde bedrijfsfuncties, ondersteunende processen en informatie-activa vast te stellen, dienen financiële instellingen ten minste de vereisten inzake vertrouwelijkheid, integriteit en beschikbaarheid in aanmerking te nemen. De verantwoordingsplicht en verantwoordelijkheid voor de informatie-activa moet duidelijk worden toegewezen.

19. Financiële instellingen dienen de geschiktheid van de classificatie van de informatie-activa en relevante documentatie te evalueren wanneer een risicobeoordeling wordt uitgevoerd.

20. Financiële instellingen moeten de ICT- en beveiligingsrisico's die een invloed hebben op de geïdentificeerde bedrijfsfuncties, ondersteunende processen en informatie-activa identificeren volgens hun kritieke karakter. Deze risicobeoordeling moet jaarlijks worden uitgevoerd en gedocumenteerd, of met kortere intervallen indien nodig. Dergelijke risicobeoordelingen moeten ook worden uitgevoerd bij alle grote wijzigingen in de infrastructuur, processen of procedures die een invloed hebben op de bedrijfsfuncties, ondersteunende processen en informatie-activa, en dientengevolge moet de huidige risicobeoordeling van financiële instellingen geactualiseerd worden.

21. Financiële instellingen moeten ervoor zorgen dat zij bedreigingen en kwetsbaarheden die relevant zijn voor hun bedrijfsprocessen, ondersteunende functies en informatie-activa voortdurend monitoren en moeten de risicoscenario's die deze beïnvloeden regelmatig evalueren.

1.3.4. Risicobeperking

22. Op basis van de risicobeoordelingen moeten financiële instellingen bepalen welke maatregelen nodig zijn om de geïdentificeerde ICT- en beveiligingsrisico's te verminderen tot een aanvaardbaar niveau, en of er wijzigingen moeten worden doorgevoerd aan de bestaande bedrijfsprocessen, controlemaatregelen, ICT-systemen en ICT-diensten. Een financiële instelling moet rekening houden met de tijd die vereist is om deze wijzigingen te implementeren, en met de tijd die nodig is om passende tussentijdse beperkingsmaatregelen te treffen om de ICT- en beveiligingsrisico's tot een minimum te beperken teneinde binnen de grenzen van de ICT- en beveiligingsrisicobereidheid van de financiële instelling te blijven.

23. Financiële instellingen moeten maatregelen vaststellen en implementeren om de geïdentificeerde ICT- en beveiligingsrisico's te verminderen en de informatie-activa te beschermen in overeenstemming met hun classificatie.

1.3.5. Rapportage

24. Financiële instellingen dienen de resultaten van risicobeoordelingen duidelijk en tijdig aan het leidinggevend orgaan te rapporteren. Die rapportage laat de verplichting van betalingsdienstaanbieders om een geactualiseerde en uitgebreide risicobeoordeling te verstrekken aan de bevoegde instanties zoals bedoeld in artikel 95, lid 2, van Richtlijn (EU) 2015/2366 onverlet.

1.3.6. Audit

25. De governance, systemen en processen voor de ICT- en beveiligingsrisico's van een financiële instelling moeten op regelmatige basis worden gecontroleerd door auditors met voldoende kennis, vaardigheden en deskundigheid inzake ICT- en beveiligingsrisico's en in betalingen (voor betalingsdienstaanbieders) om onafhankelijke assurance van de doeltreffendheid ervan te bieden aan het leidinggevend orgaan. De auditors moeten onafhankelijk zijn binnen of onafhankelijk zijn van de financiële instelling. De frequentie en gerichtheid van dergelijke audits moeten in evenwicht zijn met de relevante ICT- en beveiligingsrisico's.

26. Het leidinggevend orgaan van een financiële instelling moet het auditplan goedkeuren, met inbegrip van alle ICT-audits en alle essentiële wijzigingen hierin. Het auditplan en de uitvoering ervan, inclusief de auditfrequentie, moeten de inherente ICT- en beveiligingsrisico's in de financiële instelling weerspiegelen en hieraan evenredig zijn, en moeten regelmatig worden bijgewerkt.

27. Er dient een formeel proces voor opvolging te worden opgesteld met inbegrip van bepalingen voor tijdige verificatie en herstel van kritieke ICT-auditbevindingen.

1.4. Informatiebeveiliging

1.4.1. Beleid inzake informatiebeveiliging

28. Financiële instellingen moeten een beleid inzake informatiebeveiliging ontwikkelen en documenteren dat de overkoepelende beginselen en regels ter bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en informatie van financiële instellingen en hun klanten omschrijft. Voor betalingsdienstaanbieders wordt dit beleid vastgelegd in het document van het beveiligingsbeleid dat overeenkomstig artikel 5, lid 1, punt j), van Richtlijn (EU) 2015/2366 wordt vastgesteld. Het informatiebeveiligingsbeleid moet in overeenstemming zijn met de informatiebeveiligingsdoelstellingen van de financiële instelling en gebaseerd zijn op de relevante resultaten van het risicobeoordelingsproces. Het beleid wordt vastgesteld door het leidinggevend orgaan.

29. Het beleid omvat een omschrijving van de belangrijkste taken en verantwoordelijkheden inzake informatiebeveiligingsbeheer, en zet de vereisten voor personeel en contractanten, processen en technologie met betrekking tot informatiebeveiliging uiteen, waarbij wordt erkend dat personeelsleden en contractanten op alle niveaus verantwoordelijkheid dragen om de informatiebeveiliging van de financiële instelling te waarborgen. Het beleid dient de

vertrouwelijkheid, integriteit en beschikbaarheid van kritieke logische en fysieke activa van een financiële instelling, middelen en gevoelige betalingsgegevens van de betalingsdienstgebruikers te verzekeren, zowel in rust-, als in overgangs- of gebruikstoestand. Het beleid inzake informatiebeveiliging dient aan alle personeelsleden en contractanten van de financiële instelling bekendgemaakt te worden.

30. Op basis van het informatiebeveiligingsbeleid treffen financiële instellingen veiligheidsmaatregelen om de ICT- en beveiligingsrisico's waaraan zij worden blootgesteld te verminderen, en implementeren deze. Deze maatregelen hebben onder meer betrekking op:

    a) organisatie en governance in overeenstemming met de leden 10 en 11;
    b) logische beveiliging (afdeling 1.4.2);
    c) fysieke beveiliging (afdeling 1.4.3);
    d) beveiliging van ICT-activiteiten (afdeling 1.4.4);
    e) beveiligingsmonitoring (afdeling 1.4.5);
    f) evaluaties, beoordeling en testen informatiebeveiliging (afdeling 1.4.6);
    g) opleiding en bewustmaking inzake informatiebeveiliging (afdeling 1.4.7).

1.4.2. Logische beveiliging

31. Financiële instellingen moeten procedures voor logische toegangscontrole (identiteits- en toegangsbeheer) vaststellen, documenteren en implementeren. Deze procedures dienen te worden uitgevoerd, gehandhaafd, gemonitord en regelmatig geëvalueerd. In deze procedures zijn ook controles voor het monitoren van afwijkingen opgenomen. Deze procedures moeten ten minste de volgende maatregelen treffen, waarbij de term "gebruiker" ook technische gebruikers omvat:

    (a) **"Need-to-know", "least privilege" en functiescheiding:** financiële instellingen dienen toegangsrechten voor informatica-activa en hun ondersteunende systemen te beheren volgens het beginsel van "kennisnemingsbehoefte", met inbegrip van toegang op afstand. Gebruikers krijgen minimale toegangsrechten toegekend die strikt noodzakelijk zijn om hun taken uit te voeren (beginsel van "least privilege"), d.w.z. om ongerechtvaardigde toegang tot een grote reeks gegevens te voorkomen of om de toewijzing van combinaties van toegangsrechten te voorkomen die kunnen worden gebruikt om controles te omzeilen (beginsel van "functiescheiding").
    (b) **Gebruikersverantwoordelijkheid:** financiële instellingen dienen het gebruik van generieke en gedeelde gebruikersaccounts zo veel mogelijk te beperken, en te verzekeren dat gebruikers kunnen worden geïdentificeerd voor de acties die ze in de ICT-systemen hebben uitgevoerd.
    (c) **Geprivilegieerde toegangsrechten:** financiële instellingen dienen beheersmaatregelen te treffen voor geprivilegieerde systeemtoegang door accounts met meer systeemtoegangsrechten (bijv. beheerdersaccounts) strikt te beperken en hier nauw op toe te zien. Om een veilige communicatie te garanderen en risico's te verminderen, dient de toegang op afstand tot kritieke ICT-systemen alleen toegekend te worden

volgens kennisnemingsbehoefte en wanneer er sterke authenticatiemiddelen worden gebruikt.

(d) **Logbestanden bijhouden van gebruikersactiviteiten:** alle activiteiten van geprivilegieerde gebruikers via logbestanden moeten ten minste worden bijgehouden en gemonitord. Logbestanden dienen beveiligd te zijn om ongeoorloofde wijziging of verwijdering te voorkomen, en dienen bijgehouden te worden gedurende een periode die in verhouding staat tot het kritieke karakter van de geïdentificeerde bedrijfsfuncties, ondersteunende processen en informatie-activa, in overeenstemming met afdeling 1.3.3, onverminderd de gegevensbewaringsvereisten van de nationale en EU-wetgeving. Een financiële instelling dient deze gegevens te gebruiken om de identificatie en het onderzoek te vergemakkelijken van afwijkende activiteiten die geconstateerd werden bij het verlenen van de diensten.

(e) **Toegangsbeheer:** toegangsrechten dienen tijdig toegekend, ingetrokken of gewijzigd te worden, volgens vooraf bepaalde goedkeuringsprocessen waarbij de bedrijfseigenaar van de informatie waartoe toegang wordt verleend (eigenaar van de informatie-activa), betrokken is. In het geval van beëindiging van het dienstverband, dienen de toegangsrechten onmiddellijk ingetrokken te worden.

(f) **Hernieuwing van toegangscertificering:** toegangsrechten dienen regelmatig herzien te worden om te garanderen dat gebruikers geen buitensporige voorrechten hebben en dat toegangsrechten zijn ingetrokken wanneer ze niet langer noodzakelijk zijn.

(g) **Authenticatiemethoden:** financiële instellingen dienen authenticatiemethoden te handhaven die voldoende robuust zijn om er passend en doeltreffend voor te zorgen dat het beleid en de procedures inzake toegangscontrole worden nageleefd. Authenticatiemethoden dienen in verhouding te staan tot het kritieke karakter van de ICT-systemen, informatie of het proces waar toegang tot wordt verkregen. Dit betreft ten minste complexe wachtwoorden of sterkere authenticatiemethoden (zoals bifactoriële authenticatie), gebaseerd op relevante risico's.

32. Elektronische toegang van applicaties tot gegevens en ICT-systemen dient beperkt te worden tot het minimum dat nodig is om de desbetreffende diensten te kunnen aanbieden.

1.4.3. Fysieke beveiliging

33. Fysieke veiligheidsmaatregelen voor financiële instellingen dienen vastgesteld, gedocumenteerd en geïmplementeerd te worden om hun gebouwen, datacentra en gevoelige gebieden te beschermen tegen toegang door onbevoegden en tegen milieugevaren.

34. De fysieke toegang tot ICT-systemen mag alleen toegestaan worden aan bevoegde personen. Autorisaties moeten verleend worden overeenkomstig de taken en verantwoordelijkheden van de persoon, en beperkt worden tot personen die naar behoren opgeleid en gecontroleerd worden. De fysieke toegang moet regelmatig worden herzien om te waarborgen dat onnodige toegangsrechten onmiddellijk worden ingetrokken wanneer ze niet noodzakelijk zijn.

35. Passende maatregelen ter bescherming tegen milieugevaren moeten in verhouding zijn tot het belang van de gebouwen en het kritieke karakter van de werkzaamheden of ICT-systemen die in deze gebouwen gevestigd zijn.

1.4.4. Beveiliging van ICT-activiteiten

36. Financiële instellingen dienen procedures ten uitvoer te leggen om te voorkomen dat zich beveiligingsproblemen voordoen in ICT-systemen en ICT-diensten, en dienen de impact ervan op de ICT-dienstverlening tot een minimum te beperken. In deze procedures moeten de volgende maatregelen opgenomen zijn:

    a) identificatie van potentiële kwetsbaarheden die geëvalueerd en hersteld dienen te worden door ervoor te zorgen dat software en firmware bijgewerkt zijn, met inbegrip van de software die door de instellingen aan hun interne en externe gebruikers wordt verstrekt, door kritieke veiligheidspatches uit te rollen, of door compenserende controles te implementeren;
    b) implementatie van beveiligde configuratiebaselines van alle netwerkonderdelen;
    c) implementatie van netwerksegmentatie, systemen voor de voorkoming van gegevensverlies en de versleuteling van netwerkverkeer (in overeenstemming met de gegevensclassificatie);
    d) implementatie van bescherming van eindpunten inclusief servers, werkstations en mobiele toestellen; financiële instellingen dienen te evalueren of eindpunten voldoen aan de beveiligingsnormen die zij hebben vastgesteld alvorens deze toegang te verlenen tot het bedrijfsnetwerk;
    e) garantie dat er mechanismen in gebruik zijn om de integriteit van software, firmware en gegevens te controleren;
    f) versleuteling van gegevens in rust- en in overgangstoestand (in overeenstemming met de gegevensclassificatie).

37. Verder dienen financiële instellingen op doorlopende basis na te gaan of wijzigingen in de bestaande operationele omgeving de bestaande veiligheidsmaatregelen beïnvloeden en of er bijkomende maatregelen genomen moeten worden om de daaraan verbonden risico's naar behoren te verminderen. Deze wijzigingen dienen deel uit te maken van het formele wijzigingenbeheerproces ("change management") van de financiële instellingen, dat ervoor moet zorgen dat de wijzigingen naar behoren worden gepland, getest, gedocumenteerd, geautoriseerd en uitgerold.

1.4.5. Beveiligingsmonitoring

38. Financiële instellingen dienen beleid en procedures op te stellen en toe te passen om afwijkende activiteiten die een invloed kunnen hebben op de informatiebeveiliging van de financiële instellingen op te sporen, en passend op deze gebeurtenissen te reageren. Als onderdeel van deze continue monitoring moeten financiële instellingen geschikte en effectieve middelen toepassen om fysieke of digitale binnendringing te detecteren en rapporteren,

evenals inbreuken op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie-activa. De continue monitoring- en detectieprocessen dienen betrekking te hebben op:

a) relevante interne en externe factoren, inclusief bedrijfs- en ICT-beheersfuncties;
b) transacties om misbruik van toegang door derden of andere entiteiten en intern misbruik van toegang te detecteren;
c) potentiële interne en externe bedreigingen.

39. Financiële instellingen dienen processen en organisatorische structuren op te stellen en toe te passen om beveiligingsbedreigingen die een wezenlijk effect kunnen hebben op hun vermogen om diensten aan te bieden te identificeren en te monitoren. Financiële instellingen dienen de technologische ontwikkelingen actief te volgen om ervoor te zorgen dat ze zich bewust zijn van de beveiligingsrisico's. Financiële instellingen moeten detectiemaatregelen nemen, bijvoorbeeld om eventuele gegevenslekken, malware en andere beveiligingsbedreigingen te identificeren, evenals publiek bekende kwetsbaarheden van software en hardware, en controleren op de beschikbaarheid van hiervoor geschikte beveiligingsupdates.

40. Het beveiligingsmonitoringproces moet een financiële instelling ook helpen om inzicht te krijgen in de aard van operationele of beveiligingsincidenten, om trends vast te stellen en om de onderzoeken van de organisatie te ondersteunen.

1.4.6. Evaluaties, beoordeling en testen van informatiebeveiliging

41. Financiële instellingen dienen een verscheidenheid aan evaluaties, beoordelingen en testen van de informatiebeveiliging uit te voeren om de doeltreffende identificatie van kwetsbaarheden in hun ICT-systemen en ICT-diensten te waarborgen. Zo kunnen financiële instellingen bijvoorbeeld gapanalyses uitvoeren op het gebied van informatiebeveiligingsnormen, nalevingscontroles, interne en externe audits van de informatiesystemen, of fysieke beveiligingsevaluaties. Verder moet de instelling goede praktijken in aanmerking nemen zoals evaluaties van broncodes, kwetsbaarheidsbeoordelingen, penetratietests en Red Team-oefeningen.

42. Financiële instellingen moeten een toetsingskader voor informatiebeveiliging opstellen en toepassen dat de robuustheid en doeltreffendheid van hun informatiebeveiligingsmaatregelen valideert, en ervoor zorgen dat dit kader bedreigingen en kwetsbaarheden in aanmerking neemt, die zijn geïdentificeerd via monitoring van bedreigingen en het risicobeoordelingsproces inzake ICT en beveiliging.

43. Het toetsingskader voor informatiebeveiliging moet ervoor zorgen dat tests:

a) worden uitgevoerd door onafhankelijke testers met voldoende kennis, vaardigheden en deskundigheid inzake het testen van informatiebeveiligingsmaatregelen, en die niet betrokken zijn bij de ontwikkeling van de informatiebeveiligingsmaatregelen;
b) kwetsbaarheidsscans en penetratietests omvatten (inclusief bedreigingsgerichte penetratietests waar nodig en passend) in verhouding tot het bij de bedrijfsprocessen en -systemen geïdentificeerde risiconiveau.

44. Financiële instellingen dienen doorlopende en herhaalde tests uit te voeren op de veiligheidsmaatregelen. Voor alle kritieke ICT-systemen (lid 17) moeten deze tests minstens op jaarbasis worden uitgevoerd en, voor betalingsdienstaanbieders maken ze deel uit van de uitgebreide beoordeling van de beveiligingsrisico's die verband houden met de betalingsdiensten die ze verstrekken, in overeenstemming met artikel 95, lid 2, van RBD2. Niet-kritieke systemen dienen regelmatig getest te worden door middel van een risicogebaseerde benadering, maar minstens een keer per drie jaar.

45. Financiële instellingen moeten ervoor zorgen dat tests van veiligheidsmaatregelen worden uitgevoerd in het geval van wijzigingen aan de infrastructuur, processen of procedures, en indien wijzigingen worden doorgevoerd wegens grote operationele of beveiligingsincidenten, of wegens de vrijgave van nieuwe of aanzienlijk gewijzigde internetgerichte kritieke toepassingen.

46. Financiële instellingen moeten de resultaten van de beveiligingstests controleren en evalueren, en hun veiligheidsmaatregelen dienovereenkomstig aanpassen, onverwijld wanneer het gaat om kritische ICT-systemen.

47. Het toetsingskader voor betaaldienstaanbieders dient controles te bevatten voor 1) betalingsterminals en -toestellen die gebruikt worden voor het aanbieden van betalingsdiensten, 2) betalingsterminals en -toestellen die gebruikt worden om de betalingsdienstgebruiker te authenticeren en 3) toestellen en software die door de betalingsdienstaanbieder ter beschikking gesteld worden aan de betalingsdienstgebruiker om een authenticatiecode te genereren/ontvangen.

48. Op basis van de waargenomen beveiligingsdreigingen en de aangebrachte wijzigingen, moeten er tests worden uitgevoerd waarin scenario's van relevante en bekende potentiële aanvallen zijn opgenomen.

1.4.7. Opleiding en bewustmaking inzake informatiebeveiliging

49. Financiële instellingen moeten een opleidingsprogramma opstellen, met inbegrip van periodieke bewustmakingsprogramma's inzake bewaking, voor alle personeelsleden en contractanten om te waarborgen dat zij zijn opgeleid om hun taken en verantwoordelijkheden uit te voeren in overeenstemming met het relevante beveiligingsbeleid en bijbehorende procedures om menselijke fouten, diefstal, fraude, misbruik of verlies te verminderen, en beveiligingsgerelateerde risico's kunnen aanpakken. Financiële instellingen moeten ervoor zorgen dat het opleidingsprogramma minstens eenmaal per jaar opleiding regelt voor alle personeelsleden en contractanten.

1.5. Beheer van ICT-activiteiten

50. Financiële instellingen moeten hun ICT-activiteiten beheersen op basis van gedocumenteerde en toegepaste processen en procedures (die voor betaaldienstaanbieders het document inzake beveiligingsbeleid omvat overeenkomstig artikel 5, lid 1, punt j), van RBD2) die zijn goedgekeurd door het leidinggevend orgaan. In deze reeks documenten moet worden

omschreven hoe financiële instellingen hun ICT-systemen en -diensten exploiteren, monitoren en controleren, met inbegrip van het documenteren van kritieke ICT-activiteiten, en ze moeten financiële instellingen in staat stellen om een geactualiseerde inventaris van ICT-activa bij te houden.

51. Financiële instellingen dienen ervoor te zorgen dat de uitvoering van hun ICT-activiteiten afgestemd is op hun bedrijfsvereisten. Financiële instellingen moeten de doeltreffendheid van hun ICT-activiteiten waar mogelijk handhaven en verbeteren, onder meer de noodzaak om te bedenken hoe potentiële fouten die het gevolg zijn van de uitvoering van manuele taken, tot een minimum kunnen worden beperkt.

52. Financiële instellingen moeten procedures inzake het bijhouden van logbestanden en monitoring toepassen voor kritieke ICT-activiteiten zodat fouten kunnen worden opgespoord, geanalyseerd en gecorrigeerd.

53. Financiële instellingen moeten een geactualiseerde inventaris bijhouden van hun ICT-activa (inclusief ICT-systemen, netwerktoestellen, databanken, enz.). In de administratie van de ICT-activa moet de configuratie van de ICT-activa en de koppelingen en afhankelijkheden tussen de verschillende ICT-activa worden geregistreerd, zodat een degelijke configuratie en wijzigingenbeheerproces mogelijk zijn.

54. De inventaris van de ICT-activa moet voldoende gedetailleerd zijn om de onmiddellijke identificatie van een ICT-activum, de locatie, de beveiligingsclassificatie en het eigenaarschap ervan mogelijk te maken. Afhankelijkheden tussen activa moeten worden gedocumenteerd om bij te dragen aan de reactie op beveiligings- en operationele incidenten, waaronder cyberaanvallen.

55. Financiële instellingen moeten de levenscyclus van ICT-activa monitoren en beheren, om te waarborgen dat deze blijven voldoen aan vereisten inzake bedrijfs- en risicobeheer, en deze ondersteunen. Financiële instellingen moeten monitoren of hun ICT-activa ondersteund worden door externe of interne verkopers en ontwikkelaars, en of alle relevante patches en upgrades zijn toegepast op basis van de gedocumenteerde processen. De risico's die afkomstig zijn van verouderde of niet-ondersteunde ICT-activa moeten worden beoordeeld en verminderd.

56. Financiële instellingen moeten plannings- en monitoringsprocessen met betrekking prestaties en capaciteit implementeren om belangrijke prestatieproblemen van ICT-systemen en ICT-capaciteitstekorten te voorkomen en tijdig op te sporen en aan te pakken.

57. Financiële instellingen moeten back-up- en herstelprocedures voor gegevens en ICT-systemen vaststellen en implementeren zodat deze waar nodig kunnen worden hersteld. De omvang en frequentie van back-ups moeten worden vastgesteld in overeenstemming met de bedrijfsvereisten inzake herstel, en het kritieke karakter van de gegevens en de ICT-systemen, en moeten worden geëvalueerd volgens de uitgevoerde risicobeoordeling. De back-up- en herstelprocedures moeten op regelmatige basis worden getest.

58. Financiële instellingen moeten ervoor zorgen dat de back-ups van de gegevens en ICT-systemen veilig zijn opgeslagen en op een toereikende afstand van de hoofdvestiging zodat ze niet aan dezelfde risico's zijn blootgesteld.

3.5.1 Beheer van ICT-incidenten en -problemen

59. Financiële instellingen moeten een beheerproces voor incidenten en problemen opstellen en toepassen om operationele en beveiligingsincidenten inzake ICT te monitoren en hiervan logbestanden bij te houden, en om financiële instellingen in staat te stellen om kritieke bedrijfsfuncties en -processen voort te zetten of tijdig weer op te nemen wanneer verstoringen optreden. Financiële instellingen dienen de gepaste criteria en drempelwaarden te bepalen om een gebeurtenis te classificeren als een operationeel of veiligheidsincident, zoals beschreven in het hoofdstuk "Definities" van deze richtsnoeren, evenals vroegtijdige waarschuwingsindicatoren om een vroegtijdige detectie van deze incidenten mogelijk te maken. Dergelijke criteria en drempelwaarden gelden voor betaaldienstaanbieders onverminderd de classificatie van ernstige incidenten overeenkomstig artikel 96 van RBD2 en de richtsnoeren voor het melden van ernstige incidenten in het kader van RBD2 (EBA/GL/2017/10).

60. Om de impact van ongewenste voorvallen tot een minimum te beperken en tijdig herstel mogelijk te maken, moeten financiële instellingen passende processen en organisatiestructuren inrichten om een consistente en geïntegreerde monitoring, behandeling en opvolging van operationele en veiligheidsincidenten te waarborgen, en ervoor zorgen dat de onderliggende oorzaken worden geïdentificeerd en geëlimineerd om te voorkomen dat incidenten zich herhaaldelijk voordoen. Het proces voor incident- en probleembeheer moet het volgende omvatten:

    a) de procedures om incidenten te identificeren, registreren via logbestanden, categoriseren en classificeren volgens een prioriteit die is gebaseerd op het bedrijfskritieke karakter ervan;
    b) de taken en verantwoordelijkheden voor verschillende incidentenscenario's (bijv. fouten, slecht functioneren, cyberaanvallen);
    c) probleembeheerprocedures om de onderliggende oorzaak van één of meerdere incidenten te identificeren, analyseren en op te lossen — een financiële instelling moet de operationele of veiligheidsincidenten analyseren die naar alle waarschijnlijkheid een invloed hebben op de financiële instelling en die werden geïdentificeerd of die zich voordeden binnen of buiten de organisatie, en zij moet belangrijke lessen trekken uit deze analyses en de veiligheidsmaatregelen dienovereenkomstig bijwerken;
    d) effectieve plannen voor interne communicatie, inclusief procedures voor incidentmelding en escalatie, die ook beveiligingsgerelateerde klachten van klanten omvatten, om te waarborgen dat:
        i) incidenten met potentieel zware negatieve gevolgen op kritieke ICT-systemen en ICT-diensten worden gemeld aan de relevante hogere leidinggevenden en hogere ICT-leidinggevenden;

ii) het leidinggevend orgaan in het geval van ernstige incidenten op een ad-hocbasis in kennis wordt gesteld en ten minste op de hoogte wordt gebracht van de impact, de reactie en de aanvullende maatregelen die moeten worden vastgesteld als gevolg van de incidenten.

e) procedures voor de reactie op incidenten om de effecten die verband houden met de incidenten te verminderen en waarborgen dat de dienst snel operationeel en veilig wordt;

f) specifieke externe communicatieplannen voor kritieke bedrijfsfuncties en -processen om:

i) samen te werken met de relevante belanghebbenden teneinde effectief te reageren op en te herstellen van het incident;

ii) tijdige informatie te verstrekken aan externe partijen (bijv. klanten, andere marktdeelnemers, de toezichthoudende autoriteit) op passende wijze en in overeenstemming met geldende regelgeving.

1.6. ICT-project en wijzigingenbeheer

1.6.1. ICT-projectbeheer

61. Een financiële instelling moet een programma- en/of projectgovernanceproces inrichten dat taken, verantwoordelijkheden en aansprakelijkheden vaststelt om de tenuitvoerlegging van de ICT-strategie effectief te ondersteunen.

62. Een financiële instelling moet de risico's die voortvloeien uit de portefeuille van ICT-projecten (programmabeheer) op gepaste wijze monitoren en verminderen, ook rekening houdend met de risico's die het gevolg kunnen zijn van onderlinge afhankelijkheden tussen verschillende projecten en van afhankelijkheden van meerdere projecten van dezelfde hulpbronnen en/of deskundigheid.

63. Een financiële instelling moet een beleid voor ICT-projectbeheer opstellen en implementeren dat minstens het volgende omvat:

a) projectdoelstellingen;
b) taken en verantwoordelijkheden;
c) een projectrisicobeoordeling;
d) een projectplan, tijdschema en stappen;
e) belangrijke mijlpalen;
f) vereisten voor wijzigingenbeheer.

64. Het beleid voor ICT-projectbeheer moet ervoor zorgen dat vereisten inzake informatiebeveiliging worden geanalyseerd en goedgekeurd door een functie die onafhankelijk is van de ontwikkelingsfunctie.

65. Een financiële instelling moet ervoor zorgen dat alle gebieden die beïnvloed worden door een ICT-project vertegenwoordigd zijn in het projectteam en dat het projectteam over de vereiste kennis beschikt om een veilige en succesvolle projectimplementatie te waarborgen.

66. De opzet en voortgang van ICT-projecten en hun bijbehorende risico's moeten afzonderlijk of samen, naargelang het belang en de omvang van de ICT-projecten, regelmatig en op een ad-hocbasis waar nodig, aan het leidinggevend orgaan worden gemeld. Financiële instellingen moeten projectrisico's in hun risicobeheerkader opnemen.

1.6.2. Aankoop en ontwikkeling van ICT-systemen

67. Financiële instellingen moeten een proces ontwikkelen en inrichten dat de aankoop, ontwikkeling en het onderhoud van ICT-systemen regelt. Dit proces moet worden ontworpen door middel van een risicogebaseerde benadering.

68. Een financiële instelling moet ervoor zorgen dat, voordat enige aankoop of ontwikkeling van ICT-systemen plaatsvindt, de functionele en niet-functionele vereisten (inclusief vereisten inzake informatiebeveiliging) duidelijk zijn gedefinieerd en goedgekeurd door het relevante bedrijfsbestuur.

69. Een financiële instelling moet ervoor zorgen dat er maatregelen zijn getroffen om het risico van onbedoelde wijzigingen of doelbewuste manipulatie van de ICT-systemen tijdens de ontwikkeling en tenuitvoerlegging in de productieomgeving te verminderen.

70. Financiële instellingen hebben een methodologie in gebruik om ICT-systemen te testen en goed te keuren vóór het eerste gebruik ervan. Deze methodologie dient rekening te houden met de kritieke aard van bedrijfsprocessen en -activa. Het testen moet ervoor zorgen dat de nieuwe ICT-systemen presteren zoals gepland. Ze moeten ook testomgevingen gebruiken die een adequate weerspiegeling vormen van de productieomgeving.

71. Financiële instellingen moeten ICT-systemen, ICT-diensten en informatiebeveiligingsmaatregelen testen om potentiële zwakheden in de beveiliging, inbreuken en incidenten te identificeren.

72. Een financiële instelling moet afzonderlijke ICT-omgevingen opzetten om een gepaste functiescheiding te waarborgen en de impact van ongecontroleerde wijzigingen aan productiesystemen te verminderen. In het bijzonder moet een financiële instelling de scheiding van productieomgevingen en ontwikkelings-, test- en andere niet-productieomgevingen waarborgen. Een financiële instelling moet de integriteit en vertrouwelijkheid van productiegegevens in niet-productieomgevingen waarborgen. Alleen bevoegde gebruikers hebben toegang tot productiegegevens.

73. Financiële instellingen moeten maatregelen treffen om de integriteit van de broncodes van ICT-systemen die intern zijn ontwikkeld te beschermen. Ook moeten ze de ontwikkeling, implementatie, werking en/of configuratie van de ICT-systemen uitvoerig documenteren om alle onnodige afhankelijkheden van deskundigen over het onderwerp te verminderen. De documentatie van de ICT-systemen moet indien van toepassing minstens gebruikersdocumentatie, technische systeemdocumentatie en werkwijzen omvatten.

74. De processen van een financiële instelling voor de aankoop en ontwikkeling van ICT-systemen moeten ook van toepassing zijn op de ICT-systemen die worden ontwikkeld of beheerd door de eindgebruikers van de bedrijfsfunctie buiten de ICT-organisatie (bijv. informaticatoepassingen

voor eindgebruikers) door middel van een risicogebaseerde benadering. De financiële instelling moet een register bijhouden van deze toepassingen die kritieke bedrijfsfuncties of -processen ondersteunen.

1.6.3. ICT-wijzigingenbeheer

75. Financiële instellingen moeten een proces voor ICT-wijzigingenbeheer opstellen en implementeren om te waarborgen dat alle veranderingen aan ICT-systemen op gecontroleerde wijze worden geregistreerd, getest, beoordeeld, goedgekeurd, geïmplementeerd en gecontroleerd. Financiële instellingen moeten de wijzigingen tijdens noodsituaties afhandelen (bijv. wijzigingen die zo snel mogelijk moeten worden doorgevoerd) op grond van procedures die passende garanties bieden.

76. Financiële instellingen dienen op doorlopende basis na te gaan of wijzigingen in de bestaande operationele omgeving de bestaande veiligheidsmaatregelen beïnvloeden en of er bijkomende maatregelen genomen moeten worden om het risico in kwestie te verminderen. Deze wijzigingen moeten overeenstemmen met het formele wijzigingenbeheerproces van de financiële instelling.

1.7. Bedrijfscontinuïteitsbeheer

77. Financiële instellingen moeten een degelijk proces voor bedrijfscontinuïteitsbeheer opzetten om hun vermogen om op een doorlopende basisdiensten te verlenen te maximaliseren en de verliezen te beperken in het geval van een ernstige verstoring van de bedrijfsactiviteiten overeenkomstig artikel 85, lid 2, van Richtlijn 2013/36/EU en Titel IV van de EBA-richtsnoeren betreffende interne governance (EBA/GL/2017/11).

1.7.1. Bedrijfseffectbeoordeling

78. Als onderdeel van een degelijk bedrijfscontinuïteitsbeheer, moeten financiële instellingen bedrijfseffectbeoordelingen uitvoeren door te analyseren in welk mate zij zijn blootgesteld aan ernstige verstoringen van de bedrijfsactiviteiten en de potentiële impact ervan te beoordelen (inclusief vertrouwelijkheid, integriteit en beschikbaarheid), zowel kwantitatief als kwalitatief, door interne en/of externe gegevens (bijv. gegevens van derde aanbieders die relevant zijn voor een bedrijfsproces of gegevens die openbaar zijn en die mogelijk relevant zijn voor de bedrijfseffectbeoordeling) en scenario-analyses te gebruiken. De bedrijfseffectbeoordeling moet ook rekening houden met het kritieke karakter van de geïdentificeerde en geclassificeerde bedrijfsfuncties, ondersteunende processen, derde partijen en informatie-activa, en met hun onderlinge afhankelijkheden overeenkomstig afdeling 1.3.3.

79. Financiële instellingen moeten ervoor zorgen dat hun ICT-systemen en ICT-diensten ontworpen en afgestemd zijn op hun bedrijfseffectbeoordeling, bijvoorbeeld door het dubbel uitvoeren van bepaalde kritieke onderdelen om verstoringen te voorkomen die het gevolg zijn van gebeurtenissen die een invloed hebben op deze onderdelen.

1.7.2. Bedrijfscontinuïteitsplanning

80. Op basis van hun bedrijfseffectbeoordeling moeten financiële instellingen plannen opstellen om de bedrijfscontinuïteit te waarborgen (bedrijfscontinuïteitsplannen), die moeten worden gedocumenteerd en goedgekeurd door hun leidinggevende organen. In het bijzonder moeten de plannen rekening houden met risico's die nadelige gevolgen kunnen hebben voor de ICT-systemen en ICT-diensten. De plannen moeten doelstellingen ondersteunen om de vertrouwelijkheid, integriteit en beschikbaarheid van hun bedrijfsfuncties, ondersteunende processen en informatie-activa te beschermen, en indien nodig, te herstellen. Financiële instellingen moeten samenwerken met relevante interne en externe belanghebbenden, indien van toepassing, tijdens de opstelling van deze plannen.

81. Financiële instellingen moeten bedrijfscontinuïteitsplannen in gebruik nemen om te waarborgen dat zij gepast kunnen reageren op potentiële scenario's van falen en dat zij in staat zijn na verstoringen de werkzaamheden van hun kritieke bedrijfsactiviteiten weer te herstellen binnen een beoogd herstelmoment (RTO, recovery time objective; de maximumtermijn waarbinnen een systeem of proces hersteld moet zijn na een incident) en een beoogd herstelpunt (RPO, recovery point objective; de maximumtermijn waarin het aanvaardbaar is dat gegevens verloren gaan in geval van een incident). In gevallen van ernstige verstoringen van de bedrijfsactiviteiten die specifieke bedrijfscontinuïteitsplannen activeren, moeten financiële instellingen prioriteiten stellen aan bedrijfscontinuïteitsacties door middel van een risicogebaseerde benadering, die gebaseerd kan worden op de risicobeoordelingen die in het kader van afdeling 1.3.3 werden uitgevoerd. Voor betaaldienstaanbieders kan dit bijvoorbeeld inhouden dat de verdere verwerking van kritieke transacties wordt vergemakkelijkt terwijl inspanningen voor herstel worden voortgezet.

82. Een financiële instelling dient een aantal verschillende scenario's in aanmerking te nemen in haar bedrijfscontinuïteitsplannen, inclusief extreme maar plausibele scenario's, waaraan zij blootgesteld kan zijn, inclusief een scenario inzake cyberaanvallen, en de potentiële impact van deze scenario's te beoordelen. Op basis van deze scenario's moet een financiële instelling beschrijven hoe de continuïteit van de ICT-systemen en -diensten, evenals de informatiebeveiliging van de financiële instelling, worden gewaarborgd.

1.7.3. Interventie- en herstelplannen

83. Op basis van de bedrijfseffectbeoordeling (lid 78) en plausibele scenario's (lid 82) moeten financiële instellingen interventie- en herstelplannen ontwikkelen. Deze plannen moeten toelichten welke omstandigheden activering van de plannen op gang kunnen brengen, en welke acties moeten worden ondernomen om de beschikbaarheid, continuïteit en het herstel van ten minste de kritieke ICT-systemen en ICT-diensten te waarborgen. De interventie- en herstelplannen moeten de hersteldoelstellingen van de activiteiten van de financiële instellingen nastreven.

84. De interventie- en herstelplannen moeten herstelmogelijkheden op zowel korte als lange termijn in aanmerking nemen. De plannen moeten:

a) gericht zijn op het herstel van de activiteiten van kritieke bedrijfsfuncties, ondersteunende processen, informatie-activa en hun onderlinge afhankelijkheden om nadelige gevolgen voor de werking van de financiële instellingen en op het financiële systeem te vermijden, inclusief op betalingssystemen en betalingsdienstgebruikers, en de uitvoering van hangende betalingstransacties te waarborgen;
b) gedocumenteerd en beschikbaar zijn voor de bedrijfs- en ondersteunende afdelingen en gemakkelijk raadpleegbaar zijn in geval van nood;
c) bijgewerkt worden in overeenstemming met de lessen die getrokken werden uit de incidenten, tests, nieuwe risico's die geïdentificeerd worden en bedreigingen, en wijzigende hersteldoelstellingen en -prioriteiten.

85. De plannen moeten ook rekening houden met alternatieve mogelijkheden indien herstel op korte termijn niet haalbaar is omwille van de kosten, risico's, logistiek of onvoorziene omstandigheden.

86. Verder moet een financiële instelling als onderdeel van de interventie- en herstelplannen, continuïteitsmaatregelen treffen om gevolgen te mitigeren van gebreken bij derde aanbieders die een belangrijke rol spelen bij de ICT-bedrijfscontinuïteit van een financiële instelling (in overeenstemming met de bepalingen van de EBA-richtsnoeren over uitbestedingsregelingen (EBA/GL/2019/02) met betrekking tot bedrijfscontinuïteitsplannen).

1.7.4. Plannen testen

87. Financiële instellingen moeten hun bedrijfscontinuïteitsplannen regelmatig testen. Met name moeten zij ervoor zorgen dat de bedrijfscontinuïteitsplannen van hun kritieke bedrijfsfuncties, ondersteunende processen, informatie-activa en onderlinge afhankelijkheden (inclusief die welke verstrekt worden door derden, indien van toepassing) minstens eenmaal per jaar worden getest, in overeenstemming met lid 89.

88. Bedrijfscontinuïteitsplannen moeten ten minste jaarlijks worden geactualiseerd, op basis van testresultaten, huidige inlichtingen inzake dreigingen en lessen die werden getrokken uit eerdere gebeurtenissen. Wijzigingen in hersteldoelstellingen (inclusief RTO's en RPO's) en/of wijzigingen in bedrijfsfuncties, ondersteunende processen en informatie-activa, moeten indien relevant ook in aanmerking worden genomen als basis voor het actualiseren van de bedrijfscontinuïteitsplannen.

89. Het testen door financiële instellingen van hun bedrijfscontinuïteitsplannen moet aantonen dat zij in staat zijn om de levensvatbaarheid van hun bedrijfsactiviteiten in stand te houden tot kritieke activiteiten hersteld zijn. Zij dienen in het bijzonder:

a) een geschikte reeks ernstige maar plausibele scenario's te testen, onder meer die welke in aanmerking worden genomen voor de ontwikkeling van de bedrijfscontinuïteitsplannen (evenals het testen van diensten die door derden worden verstrekt, indien van toepassing); dit omvat de overschakeling van kritieke bedrijfsfuncties, ondersteunende processen en informatie-activa naar de noodherstelomgeving, en aantonen dat deze voor een voldoende representatieve

periode op die wijze kunnen worden beheerd en dat nadien de normale werking kan worden hersteld;

b) zodanig ontworpen te zijn dat ze de veronderstellingen testen waarop de bedrijfscontinuïteitsplannen berusten, met inbegrip van regelingen op het gebied van bestuur (governance) en crisiscommunicatieplannen;

c) procedures te bevatten om na te gaan of hun personeelsleden en contractanten, ICT-systemen en ICT-diensten in staat zijn om passend te reageren op de scenario's die zijn vastgelegd in lid 89, punt a).

90. Testresultaten moeten gedocumenteerd worden en alle geïdentificeerde tekortkomingen die het resultaat zijn van de tests moeten geanalyseerd en behandeld worden, en gerapporteerd worden aan het leidinggevend orgaan.

1.7.5. Crisiscommunicatie

91. In geval van een verstoring of noodsituatie, en tijdens de tenuitvoerlegging van de bedrijfscontinuïteitsplannen, moeten financiële instellingen ervoor zorgen dat ze doeltreffende maatregelen gebruiken voor inzake crisiscommunicatie zodat alle relevante interne en externe belanghebbenden, inclusief de bevoegde autoriteiten indien vereist bij nationale wetgeving, en relevante aanbieders (uitbestedingsleveranciers, entiteiten van de groep of derde aanbieders) hiervan tijdig en passend in kennis worden gesteld.

1.8. Beheer van de relatie met de betalingsdienstgebruikers

92. Betalingsdienstaanbieders dienen processen op te stellen en toe te passen om het bewustzijn van de betalingsdienstgebruiker te verhogen op het gebied van de beveiligingsrisico's die met de betalingsdiensten verbonden zijn door betalingsdienstgebruikers ondersteuning en richtlijnen aan te bieden.

93. Deze ondersteuning en richtlijnen voor de betalingsdienstgebruikers moeten bijgewerkt worden in het licht van nieuwe bedreigingen en kwetsbaarheden, en wijzigingen dienen meegedeeld te worden aan de betalingsdienstgebruikers.

94. Wanneer de producteigenschappen dit toelaten, dienen betalingsdienstaanbieders het voor betalingsdienstgebruikers mogelijk te maken om specifieke betalingsfuncties uit te schakelen in het kader van de betalingsdiensten die door de betalingsdienstaanbieder aangeboden worden aan de betalingsdienstgebruiker.

95. Wanneer een betalingsdienstaanbieder overeenkomstig artikel 68, lid 1, van Richtlijn (EU) 2015/2366 ingestemd heeft met de uitgavenlimieten voor betalingstransacties die met specifieke betalingsinstrumenten worden uitgevoerd, dient de betalingsdienstaanbieder de betaler de mogelijkheid te geven om deze limieten aan te passen tot de overeengekomen maximumlimiet.

96. Betalingsdienstaanbieders moeten betalingsdienstgebruikers de mogelijkheid geven om waarschuwingen te ontvangen over geïnitieerde en/of mislukte pogingen om

betalingstransacties te verrichten, waarmee zij frauduleus of onrechtmatig gebruik van hun rekening kunnen detecteren.

97. Betalingsdienstaanbieders dienen betalingsdienstgebruikers op de hoogte te houden van updates van de veiligheidsprocedures die gevolgen hebben voor de betalingsdienstgebruikers betreffende het aanbieden van de betalingsdiensten.

98. Betalingsdienstaanbieders moeten de betalingsdienstgebruikers helpen bij alle vragen, verzoeken om hulp en kennisgevingen van afwijkingen of problemen betreffende de beveiliging van betalingsdiensten. Betalingsdienstgebruikers moeten naar behoren geïnformeerd worden over de wijze waarop zij om hulp kunnen vragen.