Publicatieblad
van de Europese Unie

2024/1774

25.6.2024

GEDELEGEERDE VERORDENING (EU) 2024/1774 VAN DE COMMISSIE

van 13 maart 2024

tot aanvulling van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad met technische reguleringsnormen tot vaststelling van tools, methoden, processen en beleidslijnen voor ICT-risicobeheersing en het vereenvoudigde raamwerk voor ICT-risicobeheersing

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 ([1]), en met name artikel 15, vierde alinea, en artikel 16, lid 3, vierde alinea,

Overwegende hetgeen volgt:

(1) Verordening (EU) 2022/2554 ziet op een breed scala financiële entiteiten die verschillen wat betreft omvang, structuur, interne organisatie en wat betreft de aard en complexiteit van hun activiteiten — en die dus meer of minder elementen van complexiteit of risico vertonen. Om ervoor te zorgen dat met die verschillen afdoende rekening wordt gehouden, moeten vereisten ten aanzien van beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging en ten aanzien van een vereenvoudigd raamwerk voor ICT-risicobeheersing evenredig zijn aan die omvang, structuur, interne organisatie, aard en complexiteit van die financiële entiteiten en aan de daarmee samenhangende risico's.

(2) Om diezelfde reden moeten financiële entiteiten die onder Verordening (EU) 2022/2554 vallen, een zekere mate van flexibiliteit hebben wat betreft de manier waarop zij voldoen aan vereisten ten aanzien van beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging en ten aanzien van een vereenvoudigd raamwerk voor ICT-risicobeheersing Daarom moet het financiële entiteiten worden toegestaan om documentatie waarover zij al beschikken, te gebruiken om te voldoen aan documentatieverplichtingen die uit die vereisten voortvloeien. Een en ander betekent dat de uitwerking, documentatie en implementatie van specifieke beleidslijnen voor ICT-beveiliging alleen verplicht mag worden voor bepaalde essentiële elementen, onder meer rekening houdende met maatgevende praktijken ("leading practices") en normen uit de sector. Voorts moeten, ten behoeve van specifieke aspecten van de technische implementatie, ICT-beveiligingsprocedures worden uitgewerkt, gedocumenteerd en geïmplementeerd die zien op specifieke aspecten van de technische implementatie, zoals capaciteits- en performancemanagement, kwetsbaarhedenbeheer en patchmanagement, data- en systeembeveiliging, en logging.

(3) Om ervoor te zorgen dat beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging als bedoeld in titel II, hoofdstuk I, van deze verordening op termijn correct worden geïmplementeerd, is het van belang dat financiële entiteiten rollen en verantwoordelijkheden op het gebied van ICT-beveiliging correct toewijzen en handhaven en dat zij vastleggen wat de consequenties zijn van het niet naleven van beleidslijnen of -procedures voor ICT-beveiliging.

(4) Om het risico op belangenconflicten te beperken, moeten financiële entiteiten bij het toewijzen van ICT-rollen en -verantwoordelijkheden bewaken dat taken gescheiden zijn.

(5) Om flexibiliteit te verzekeren en het controleraamwerk voor financiële entiteiten te vereenvoudigen, mag van financiële entiteiten niet worden geëist dat zij specifieke bepalingen uitwerken wat betreft de consequenties van het niet naleven van in titel II, hoofdstuk I, van deze verordening bedoelde beleidslijnen, procedures en protocollen voor ICT-beveiliging indien dergelijke bepalingen al in een ander beleidsdocument of een andere procedure zijn vastgelegd.

([1]) PB L 333 van 27.12.2022, blz. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(6) In een dynamische omgeving waar ICT-risico's voortdurend in ontwikkeling zijn, is het van belang dat financiële entiteiten hun reeks beleidslijnen voor ICT-beveiliging ontwikkelen op basis van maatgevende praktijken en, in voorkomend geval, normen zoals gedefinieerd in artikel 2, punt 1), van Verordening nr. 1025/2012 van het Europees Parlement en de Raad ([2]). Hiermee zouden in titel II van deze verordening bedoelde financiële entiteiten geïnformeerd en voorbereid moeten blijven in een veranderende omgeving.

(7) Om hun digitale operationele weerbaarheid te verzekeren, moeten in titel II van deze verordening bedoelde financiële entiteiten, in het kader van hun beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging, een beleid voor het beheer van ICT-assets, procedures voor capaciteits- en performancemanagement, en beleidslijnen en procedures voor ICT-operaties uitwerken en implementeren. Die beleidslijnen en procedures zijn noodzakelijk om te bewaken dat de status van ICT-assets wordt gemonitord tijdens hun gehele levenscyclus, zodat die assets effectief worden gebruikt en onderhouden (beheer ICT-assets). Die beleidslijnen en procedures moeten ook de optimalisering borgen van het functioneren van ICT-systemen en dat de performance van ICT-systemen en -capaciteit voldoet aan vastgelegde doelstellingen inzake bedrijfsvoering en informatiebeveiliging (capaciteits- en performancemanagement). Ten slotte moeten die beleidslijnen en procedures bewaken dat het courante beheer en de courante exploitatie van ICT-systemen effectief en soepel verlopen (ICT-operaties), zodat de risico's op verlies van vertrouwelijkheid, integriteit en beschikbaarheid van gegevens minimaal blijft. Die beleidslijnen en procedures zijn dus noodzakelijk om de veiligheid van netwerken te borgen, om afdoende bescherming te bieden tegen inbraken en misbruik van gegevens, en om de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens veilig te stellen.

(8) Om het risico van legacy ICT-systemen correct te beheersen, moeten financiële entiteiten einddata van ondersteuning van derde aanbieders van ICT-diensten vastleggen en monitoren. Vanwege de potentiële gevolgen die een verlies van vertrouwelijkheid, integriteit en beschikbaarheid van gegevens kan hebben, moeten financiële entiteiten zich bij het vastleggen en monitoren van die einddata concentreren op de ICT-assets of -systemen die kritiek zijn voor hun bedrijfsactiviteiten.

(9) Cryptografische controles kunnen de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens borgen. In titel II van deze verordening bedoelde financiële entiteiten moeten dergelijke controles dus identificeren en implementeren op basis van een risicogebaseerde benadering. Daartoe encrypteren financiële entiteiten de betrokken gegevens in rust, in transit of, waar nodig, in gebruik, op basis van de uitkomsten van een tweeledig proces: dataclassificatie en een brede ICT-risicobeoordeling. Gezien de complexiteit van encryptie van gegevens in gebruik moeten in titel II van deze verordening bedoelde financiële entiteiten gegevens in gebruik alleen encrypteren wanneer zulks passend is in het licht van de uitkomsten van de ICT-risicobeoordeling. Wanneer encryptie van gegevens in gebruik echter niet doenbaar of te complex is, moeten in titel II van deze verordening bedoelde financiële entiteiten in staat zijn de vertrouwelijkheid, integriteit en beschikbaarheid van de betrokken gegevens te beschermen via andere maatregelen voor ICT-beveiliging. Gezien de snelle technologische ontwikkelingen op het gebied van cryptografische technieken moeten in titel II van deze verordening bedoelde financiële entiteiten de betrokken ontwikkelingen op het gebied van cryptoanalyse op de voet volgen en rekening houden met maatgevende praktijken en normen. In titel II van deze verordening bedoelde financiële entiteiten moeten dus een flexibele benadering hanteren, gebaseerd op het mitigeren en monitoren van risico's, waarmee zij omgaan met het dynamische landschap van cryptografische dreigingen, met inbegrip van dreigingen die uitgaan van vooruitgang op het gebied van kwantumcomputing.

(10) Veiligheids- en operationele beleidslijnen, procedures, protocollen en tools voor ICT-operaties zijn van essentieel belang om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te garanderen. Een cruciaal aspect daarbij is de strikte scheiding tussen ICT-productieomgevingen en de omgevingen waarin ICT-systemen worden ontwikkeld en getest of andere niet-productieomgevingen. Die scheiding moet dienen als een belangrijke ICT-beveiligingsmaatregel tegen onbedoelde en ongeautoriseerde toegang tot, wijziging en wissen van gegevens in de productieomgeving, die zou kunnen resulteren in majeure verstoringen van de bedrijfsoperaties van in titel II van deze verordening bedoelde financiële entiteiten. Gelet echter op actuele praktijken voor de ontwikkeling van ICT-systemen, moet het financiële entiteiten, in uitzonderlijke omstandigheden, toegestaan zijn om in productieomgevingen te testen, op voorwaarde dat zij dit soort testactiviteiten verantwoorden en daarvoor de vereiste goedkeuring krijgen.

([2]) Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad (PB L 316 van 14.11.2012, blz. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) Doordat het ICT-landschap zich razendsnel ontwikkelt, vergen ICT-kwetsbaarheden en cyberdreigingen een proactieve en brede benadering om ICT-kwetsbaarheden in kaart te brengen, te beoordelen en aan te pakken. Zonder dit soort aanpak, zouden financiële entiteiten, hun cliënten, gebruikers of tegenpartijen sterk kunnen worden blootgesteld aan risico's, die hun digitale operationele weerbaarheid, de beveiliging van hun netwerk en de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens die met beleidslijnen en procedures voor ICT-beveiliging zouden moeten worden beschermd, in het gedrang zouden brengen. In titel II van deze verordening bedoelde financiële entiteiten moeten daarom kwetsbaarheden in hun ICT-omgeving in kaart brengen en verhelpen, en zowel de financiële entiteiten als hun derde aanbieders van ICT-diensten moeten zich houden aan een coherent, transparant en verantwoordelijk raamwerk voor het omgaan met kwetsbaarheden. Om diezelfde reden moeten financiële entiteiten ICT-kwetsbaarheden monitoren met betrouwbare middelen en geautomatiseerde tools, om zich ervan te vergewissen dat derde aanbieders van ICT-diensten ervoor zorgen dat direct wordt ingegrepen op kwetsbaarheden bij aangeboden ICT-diensten.

(12) Patchmanagement moet een essentieel onderdeel zijn van die beleidslijnen en procedures voor ICT-beveiliging die, via testen en een uitrol in een gecontroleerde omgeving, geconstateerde kwetsbaarheden moeten oplossen en storingen als gevolg van de installatie van patches moet voorkomen.

(13) Om te zorgen voor tijdige en transparante communicatie van potentiële veiligheidsdreigingen die een impact kunnen hebben op de financiële entiteit en haar stakeholders, moeten financiële entiteiten procedures inrichten voor responsible disclosure van ICT-kwetsbaarheden aan cliënten, tegenpartijen en het publiek. Bij het vastleggen van die procedures moeten financiële entiteiten rekening houden met factoren zoals de ernst van de kwetsbaarheid, de potentiële impact van die kwetsbaarheid op stakeholders, en de beschikbaarheid van fixes of mitigatiemaatregelen.

(14) Om toegangsrechten aan gebruikers te kunnen toekennen, moeten in titel II van deze verordening bedoelde financiële entiteiten robuuste maatregelen inrichten om de unieke identificatie van personen en systemen die toegang zullen hebben tot de informatie van de financiële entiteit, vast te stellen. Mochten financiële entiteiten dit niet doen, zouden zij zich blootstellen aan potentiële ongeautoriseerde toegang, datalekken en frauduleuze activiteiten, en daarmee de vertrouwelijkheid, integriteit en beschikbaarheid van gevoelige financiële gegevens in het gedrang brengen. Hoewel het gebruik van generieke of gedeelde accounts bij wijze van uitzondering moet worden toegestaan in door financiële entiteiten gespecificeerde omstandigheden, moeten zij bewaken dat de verantwoordingsplicht voor acties via die accounts behouden blijft. Zonder die voorzorgen zouden potentieel kwaadwillige gebruikers onderzoeks- en corrigerende maatregelen kunnen hinderen, waardoor financiële entiteiten kwetsbaar blijven voor ongedetecteerde kwaadwillige activiteiten of sancties wegens niet-nakoming.

(15) Om de snelle vooruitgang in ICT-omgevingen te beheersen, moeten in titel II van deze verordening bedoelde financiële entiteiten robuuste beleidslijnen en procedures voor ICT-projectmanagement opzetten om de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens in stand te houden. Die beleidslijnen en procedures voor ICT-projectmanagement moeten de elementen in kaart brengen die noodzakelijk zijn om ICT-projecten succesvol te beheren, met inbegrip van wijzigingen aan, de aanschaf van, het onderhoud van en ontwikkelingen van de ICT-systemen van de financiële entiteit, ongeacht de methode die de financiële entiteit voor het ICT-projectmanagement heeft gekozen. In het kader van deze beleidslijnen en procedures moeten financiële entiteiten testpraktijken en -methoden vaststellen die op hun behoeften aansluiten, maar zich wel aan een risicogebaseerde benadering houden en bewaken dat een veilige, betrouwbare en weerbare ICT-omgeving in stand wordt gehouden. Om de veilige implementatie van een ICT-project te garanderen, moeten financiële entiteiten bewaken dat medewerkers uit specifieke bedrijfssectoren of rollen die door dat ICT-project zullen worden beïnvloed of geraakt, de nodige informatie en deskundigheid kunnen aandragen. Om doeltreffend oversight te garanderen, moeten verslagen over ICT-projecten, en met name over projecten die van invloed zijn op kritieke of belangrijke functies en de daarmee samenhangende risico's, bij het leidinggevend orgaan worden ingediend. Financiële entiteiten moeten de frequentie en details van de systematische en lopende evaluaties en verslagen aanpassen aan het belang en de omvang van de betrokken ICT-projecten.

(16) Geborgd moet worden dat softwarepakketten die in titel II van deze verordening bedoelde financiële entiteiten aanschaffen en ontwikkelen, effectief en veilig geïntegreerd zijn in de bestaande ICT-omgeving, in overeenstemming met vastgestelde doelstellingen inzake bedrijfs- en informatiebeveiliging. Daarom moeten financiële entiteiten dit soort softwarepakketten grondig evalueren. Daartoe, en om kwetsbaarheden en potentiële lacunes in de beveiliging in kaart te brengen binnen zowel softwarepakketten als de ruimere ICT-systemen, moeten financiële entiteiten ICT-beveiligingstesten uitvoeren. Om de integriteit van de software te analyseren en om te garanderen dat het gebruik van die software geen ICT-beveiligingsrisico's inhoudt, moeten financiële entiteiten ook broncodes evalueren van aangeschafte software, met inbegrip van (voor zover doenbaar) proprietary software die door derde aanbieders van ICT-diensten wordt geleverd; daarbij gebruiken zij zowel statische als dynamische testmethodes.

(17) Veranderingen houden, ongeacht de omvang ervan, inherente risico's in en kunnen aanzienlijke risico's inhouden op het verlies van vertrouwelijkheid, integriteit en beschikbaarheid van data — en kunnen dus leiden tot ernstige bedrijfsstoringen. Om financiële entiteiten te beschermen tegen potentiële ICT-kwetsbaarheden en zwakke punten die hen aan aanzienlijke risico's kunnen blootstellen, is een streng verificatieproces nodig om te bevestigen dat alle veranderingen aan de noodzakelijke ICT-beveiligingseisen voldoen. In titel II van deze verordening bedoelde financiële entiteiten moeten daarom, als een essentieel onderdeel van hun beleidslijnen en procedures voor ICT-beveiliging, beschikken over deugdelijke beleidslijnen en procedures inzake het ICT-wijzigingsbeheer ("ICT change management"). Om de objectiviteit en effectiviteit van het proces voor het ICT-wijzigingsbeheer in stand te houden, om belangenconflicten te voorkomen en om te bewaken dat ICT-wijzigingen objectief worden geëvalueerd, moet er een scheiding zijn tussen de functies die verantwoordelijk zijn voor het goedkeuren van die wijzigingen, en de functies die deze wijzigingen aanvragen en implementeren. Om effectieve transities, gecontroleerde implementatie van ICT-wijzigingen en minimale verstoringen van het functioneren van de ICT-systemen te verwezenlijken, moeten financiële entiteiten duidelijke rollen en verantwoordelijkheden toewijzen die moeten borgen dat ICT-wijzigingen worden gepland, afdoende getest en dat de kwaliteit is gegarandeerd. Om ICT-systemen daadwerkelijk te blijven laten functioneren en om een vangnet te bieden voor financiële entiteiten, moeten financiële entiteiten ook fall-backprocedures uitwerken en implementeren. Financiële entiteiten moeten die fall-backprocedures duidelijk identificeren en verantwoordelijkheden toewijzen zodat snel en doeltreffend kan worden gereageerd bij onsuccesvolle ICT-wijzigingen.

(18) Om ICT-incidenten te detecteren, te beheersen en daarover verslag te doen, moeten in titel II van deze verordening bedoelde financiële entiteiten een beleid voor ICT-incidenten formuleren dat de onderdelen omvat van een proces voor het beheersen van ICT-incidenten. Daartoe brengen financiële entiteiten alle relevante contacten binnen en buiten de organisatie in kaart die kunnen bijdragen aan de correcte coördinatie en implementatie van de verschillende fasen van dat proces. Om de detectie van en respons op ICT-incidenten te optimaliseren en om voor die incidenten trends in kaart te brengen, die een belangrijke bron van informatie zijn waarmee financiële entiteiten grondoorzaken en problemen doeltreffender kunnen identificeren en aanpakken, moeten financiële entiteiten met name ICT-incidenten analyseren die zij het meest significant vinden, onder meer omdat deze zich regelmatig opnieuw voordoen.

(19) Om een vroegtijdige en effectieve detectie van afwijkende activiteiten te garanderen, moeten in titel II van deze verordening bedoelde financiële entiteiten de verschillende informatiebronnen verzamelen, monitoren en analyseren en moeten zij in dat verband rollen en verantwoordelijkheden toewijzen. Wat betreft interne informatiebronnen, logs zijn een uiterst belangrijke bron, maar financiële entiteiten mogen niet op logs alleen vertrouwen. Financiële entiteiten moeten net rekening houden met ruimere informatie zodat wat andere interne functies rapporteren, wordt meegenomen, aangezien die functies vaak een waardevolle bron van relevante informatie zijn. Om diezelfde reden moeten financiële entiteiten informatie die bij externe bronnen is verzameld, analyseren en monitoren, met inbegrip van informatie die derde aanbieders van ICT-diensten verschaffen over incidenten die hun systemen en netwerken treffen, en andere bronnen van informatie die financiële entiteiten relevant achten. Voor zover het bij die informatie om persoonsgegevens gaat, is de Uniewetgeving inzake gegevensbescherming van toepassing. De persoonsgegevens moeten beperkt blijven tot hetgeen noodzakelijk is om incidenten te detecteren.

(20) Om ICT-incidenten te helpen detecteren, moeten financiële entiteiten bewijsmateriaal over die incidenten bewaren. Om ervoor te zorgen dat dit bewijsmateriaal voldoende lang bewaard wordt, enerzijds, en om overdreven regeldruk te vermijden, anderzijds, moeten financiële entiteiten de bewaartermijn vaststellen, rekening houdende met onder meer het kritieke karakter van de gegevens en retentieverplichtingen die uit Unierecht voortvloeien.

(21) Om ervoor te zorgen dat ICT-incidenten tijdig worden gedetecteerd, mogen in titel II van deze verordening bedoelde financiële entiteiten de criteria die zijn geïdentificeerd voor het activeren van de detectie van en respons op ICT-incidenten, niet als exhaustief beschouwen. Bovendien mogen de in die criteria beschreven omstandigheden, hoewel financiële entiteiten met elk van deze criteria rekening moeten houden, zich niet terzelfdertijd voordoen en moet afdoende met het belang van de betrokken ICT-diensten rekening worden gehouden om de processen voor detectie van en respons op ICT-incidenten te activeren.

(22) Bij het inrichten van een ICT-bedrijfscontinuïteitsbeleid moeten in titel II van deze verordening bedoelde financiële entiteiten rekening houden met de essentiële onderdelen van ICT-risicobeheersing, zoals strategieën voor de beheersing van ICT-incidenten en de communicatie daarover, het proces voor het ICT-wijzigingsbeheer, en risico's verbonden aan derde aanbieders van ICT-diensten.

(23) Het is noodzakelijk om de reeks scenario's vast te leggen waarmee in titel II van deze verordening bedoelde financiële entiteiten rekening moeten houden voor zowel de implementatie van ICT-respons- en -herstelplannen als het testen van plannen voor ICT-bedrijfscontinuïteit. Die scenario's moeten voor financiële entiteiten als uitgangspunt dienen bij het analyseren van zowel de relevantie als de waarschijnlijkheid van elk scenario en de noodzaak om alternatieve scenario's uit te werken. Financiële entiteiten moeten in die scenario's vooral kijken naar welke investering in weerbaarheidsmaatregelen doelmatiger en doeltreffender kan zijn. Door het testen van overschakeling tussen de primaire ICT-infrastructuur en eventuele redundante capaciteit, back-ups en redundante faciliteiten, moeten financiële instellingen analyseren of die capaciteit, back-up en faciliteiten over een voldoende lange periode daadwerkelijk kunnen functioneren en ervoor kunnen zorgen dat het normale functioneren van de primaire ICT-infrastructuur kan worden hersteld in lijn met de hersteldoelstellingen.

(24) Het is noodzakelijk vereisten vast te stellen voor operationeel risico, en meer bepaald vereisten voor ICT-projectmanagement en ICT-wijzigingsbeheer en het beheer van ICT-bedrijfscontinuïteit waarbij wordt voorgebouwd op de vereisten die reeds van toepassing zijn op centrale tegenpartijen, centrale effectenbewaarinstellingen en handelsplatformen op grond van, onderscheidenlijk, Verordening (EU) nr. 648/2012 ([3]), Verordening (EU) nr. 600/2014 ([4]) en Verordening (EU) nr. 909/2014 ([5]) van het Europees Parlement en de Raad.

(25) Artikel 6, lid 5, van Verordening (EU) 2022/2554 schrijft voor dat financiële entiteiten hun raamwerk voor ICT-risicobeheersing moeten evalueren en aan hun bevoegde autoriteit verslag moeten doen van die evaluatie. Om bevoegde autoriteiten in staat te stellen de informatie in die verslagen gemakkelijk te verwerken, en om een adequate toezending van die informatie te verzekeren, moeten financiële entiteiten die verslagen indienen in een elektronisch doorzoekbaar formaat.

(26) Bij de vereisten voor financiële entiteiten die onder het in artikel 16 van Verordening (EU) 2022/2554 bedoelde vereenvoudigde raamwerk voor ICT-risicobeheersing vallen, moet de klemtoon liggen op de essentiële domeinen en elementen die, gezien schaal, risico, grootte en complexiteit van die financiële entiteiten, minimaal noodzakelijk zijn om de vertrouwelijkheid, integriteit, beschikbaarheid en authenticiteit van de gegevens en diensten van die financiële entiteiten te garanderen. In dat verband moeten die financiële entiteiten beschikken over een intern governance- en controleraamwerk met duidelijke verantwoordelijkheden, om een doeltreffend en stevig raamwerk voor risicobeheersing te kunnen laten functioneren. Voorts moeten die financiële entiteiten, om de regeldruk en operationele druk te verminderen, slechts één beleid uitwerken en documenteren: een beleid voor informatiebeveiliging dat op hoofdlijnen beginselen en regels vastlegt die noodzakelijk zijn om de vertrouwelijkheid, integriteit, beschikbaarheid en authenticiteit van gegevens en diensten van die financiële entiteiten te beschermen.

(27) De bepalingen van deze verordening betreffen het onderdeel van het raamwerk voor ICT-risicobeheersing en zij leggen specifieke elementen vast die van toepassing zijn op de financiële entiteiten overeenkomstig artikel 15 van Verordening (EU) 2022/2554 en richten het vereenvoudigde raamwerk voor ICT-risicobeheersing in voor de financiële entiteiten als bedoeld in artikel 16, lid 1, van die verordening. Om de coherentie te verzekeren tussen het gewone en het vereenvoudigde raamwerk voor ICT-risicobeheersing, en gelet op het feit dat die bepalingen terzelfdertijd van toepassing moeten worden, is het passend die bepalingen op te nemen in één wetgevingshandeling.

(28) Dezer verordening is gebaseerd op de ontwerpen van technische reguleringsnormen die bij de Commissie zijn ingediend door de Europese Bankautoriteit, de Europese Autoriteit voor verzekeringen en bedrijfspensioenen en de Europese Autoriteit voor effecten en markten, in overleg met het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA).

([3]) Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters (PB L 201 van 27.7.2012, blz. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj)

([4]) Verordening (EU) nr. 600/2014 van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten in financiële instrumenten en tot wijziging van Verordening (EU) nr. 648/2012 (PB L 173 van 12.6.2014, blz. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie, betreffende centrale effectenbewaarinstellingen en tot wijziging van Richtlijnen 98/26/EG en 2014/65/EU en Verordening (EU) nr. 236/2012 (PB L 257 van 28.8.2014, blz. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Het Gemengd Comité van de Europese toezichthoudende autoriteiten als bedoeld in artikel 54 van Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad ([6]), in artikel 54 van Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad ([7]) en in artikel 54 van Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad ([8]) heeft open publieke consultaties gehouden over de ontwerpen van technische reguleringsnormen waarop deze verordening is gebaseerd, heeft de mogelijke kosten en baten van die voorgestelde normen geanalyseerd en heeft het advies ingewonnen van de overeenkomstig artikel 37 van Verordening (EU) nr. 1093/2010 opgerichte Stakeholdergroep bankwezen, de overeenkomstig artikel 37 van Verordening (EU) nr. 1094/2010 opgerichte Stakeholdergroep verzekeringen en herverzekeringen en de overeenkomstig artikel 37 van Verordening (EU) nr. 1095/2010 opgerichte Stakeholdergroep effecten en markten.

(30) Voor zover verwerking van persoonsgegevens vereist is om aan de in deze handeling vermelde verplichtingen te voldoen, moeten Verordeningen (EU) 2016/679 ([9]) en (EU) 2018/1725 ([10]) van het Europees Parlement en de Raad onverkort van toepassing zijn. Zo moet bijvoorbeeld het beginsel van minimale gegevensverwerking in acht worden genomen wanneer persoonsgegevens worden verzameld om voor een adequate detectie van incidenten te zorgen. Ook de Europese Toezichthouder voor gegevensbescherming is geraadpleegd over de ontwerpversie van deze handeling,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

TITEL I

ALGEMENE BEGINSELEN

Artikel 1

Algemeen risicoprofiel en complexiteit

Bij het uitwerken en implementeren van beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging als bedoeld in titel II en van het vereenvoudigde raamwerk voor ICT-risicobeheersing als bedoeld in titel III, wordt rekening gehouden met de omvang en het algemene risicoprofiel van de financiële entiteit en met de aard, schaal en elementen van toegenomen of afgenomen complexiteit van haar diensten, activiteiten en operaties, met inbegrip van elementen op het gebied van:

a) encryptie en cryptografie;

b) beveiliging van ICT-operaties;

c) netwerkbeveiliging;

([6]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie (PB L 331 van 15.12.2010, blz. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie (PB L 331 van 15.12.2010, blz. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d) ICT-projectmanagement en ICT-wijzigingsbeheer;

e) de potentiële impact van het ICT-risico op vertrouwelijkheid, integriteit en beschikbaarheid van gegevens en de potentiële impact van storingen op de continuïteit en beschikbaarheid van de activiteiten van de financiële entiteit.

TITEL II

VERDERE HARMONISATIE VAN ICT-RISICOBEHEERSINGINSTRUMENTEN, -METHODEN, -PROCESSEN EN -BELEIDSLIJNEN OVEREENKOMSTIG ARTIKEL 15 VAN VERORDENING (EU) 2022/2554

HOOFDSTUK I

Beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging

Afdeling 1

Artikel 2

Algemene elementen van beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging

1. Financiële entiteiten bewaken dat hun beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging als bedoeld in artikel 9, lid 2, van Verordening (EU) 2022/2554 in hun raamwerk voor ICT-risicobeheersing zijn geïntegreerd. Financiële entiteiten leggen de in dit hoofdstuk bepaalde beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging vast die:

a) de veiligheid van netwerken garanderen;

b) beschermingsmaatregelen tegen inbraken en misbruik van gegevens bevatten;

c) de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens beschermen, onder meer door middel van het gebruik van cryptografische technieken;

d) een nauwkeurige en prompte doorgifte van gegevens zonder majeure storingen en onnodige vertragingen waarborgen.

2. Financiële entiteiten bewaken dat de in lid 1 bedoelde beleidslijnen voor ICT-beveiliging:

a) zijn afgestemd op de doelstellingen inzake informatiebeveiliging van de financiële entiteit die zijn opgenomen in de in artikel 6, lid 8, van Verordening (EU) 2022/2554, bedoelde strategie voor digitale operationele weerbaarheid;

b) de datum van de formele goedkeuring van de beleidslijnen voor ICT-beveiliging door het leidinggevend orgaan vermelden;

c) indicatoren en maatstaven bevatten voor:

   i) het monitoren van de implementatie van de beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging;

   ii) het vastleggen van uitzonderingen op die implementatie;

   iii) het garanderen dat de digitale operationele weerbaarheid van de financiële entiteit is geborgd in het geval van de in punt ii) bedoelde uitzonderingen;

d) voor medewerkers op alle niveaus de verantwoordelijkheden specificeren om de ICT-beveiliging van de financiële entiteit te verzekeren;

e) de consequenties specificeren van niet-naleving van de ICT-beleidslijnen door medewerkers van de financiële entiteit, voor zover bepalingen in die zin niet zijn vastgelegd in andere beleidslijnen van de financiële entiteit;

f) een lijst van bij te houden documentatie bevatten;

g) de afspraken specificeren wat betreft functiescheiding in het kader van het "Three Lines of Defence"-model (3LoD-model) of andere interne risicobeheersings- en controlemodellen, al naargelang, om belangenconflicten te vermijden;

h) rekening houden met maatgevende praktijken en, in voorkomend geval, normen zoals gedefinieerd in artikel 2, punt 1), van Verordening (EU) nr. 1025/2012;

i) de rollen en verantwoordelijkheden in kaart brengen wat betreft uitwerking, implementatie en onderhoud van beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging;

j) worden herzien overeenkomstig artikel 6, lid 5, van Verordening (EU) 2022/2554;

k) rekening houden met materiële veranderingen die de financiële entiteit raken, met inbegrip van materiële veranderingen in de activiteiten of processen van de financiële entiteit, in het landschap van cyberdreigingen of in toepasselijke wettelijke verplichtingen.

Afdeling 2

Artikel 3

ICT-risicobeheersing

Financiële entiteiten ontwikkelen, documenteren en implementeren beleidslijnen en procedures voor ICT-beveiliging die alle volgende elementen bevatten:

a) een vermelding van de goedkeuring van het ICT-risicotolerantieniveau dat is vastgesteld overeenkomstig artikel 6, lid 8, punt b), van Verordening (EU) 2022/2554;

b) een procedure en methode om de ICT-risicobeoordeling te maken, ten behoeve van de identificatie van:

   i) kwetsbaarheden en dreigingen die van invloed zijn of kunnen zijn op de ondersteunde bedrijfsfuncties, de ICT-systemen en ICT-assets die deze functies ondersteunen;

   ii) de kwantitatieve of kwalitatieve indicatoren om de impact en de waarschijnlijkheid van de in punt i) bedoelde kwetsbaarheden en dreigingen te meten;

c) de procedure om maatregelen voor ICT-risicobehandeling te identificeren, te implementeren en te documenteren voor de in kaart gebrachte en beoordeelde ICT-risico's, met inbegrip van het vaststellen van maatregelen voor ICT-risicobehandeling die noodzakelijk zijn om het ICT-risico binnen het in punt a) bedoelde risicotolerantieniveau te brengen;

d) voor de ICT-restrisico's die na de implementatie van de in punt c) bedoelde maatregelen voor ICT-risicobehandeling nog aanwezig zijn:

   i) bepalingen voor het in kaart brengen van die ICT-restrisico's;

   ii) de toewijzing van rollen en verantwoordelijkheden wat betreft:

      1) de acceptatie van de ICT-restrisico's die het in punt a) bedoelde risicotolerantieniveau van de financiële entiteit overschrijden;

      2) het in punt d), iv), bedoelde evaluatieproces;

   iii) het uitwerken van een inventaris van de geaccepteerde ICT-restrisico's, met inbegrip van een verantwoording voor het accepteren van die risico's;

   iv) bepalingen betreffende de ten minste jaarlijks uit te voeren evaluatie van de geaccepteerde ICT-restrisico's, met inbegrip van:

      1) het in kaart brengen van veranderingen in de ICT-restrisico's;

      2) de beoordeling van beschikbare mitigerende maatregelen;

      3) de beoordeling van de vraag of de redenen om de ICT-restrisico's te accepteren, nog steeds gelden en van toepassing zijn op de datum van de evaluatie;

e) bepalingen voor het monitoren van:

   i) veranderingen in het landschap van ICT-risico en cyberdreigingen;

   ii) interne en externe kwetsbaarheden en dreigingen;

   iii) ICT-risico van de financiële entiteit waardoor veranderingen die haar ICT-risicoprofiel kunnen beïnvloeden, snel kunnen worden gedetecteerd;

f) bepalingen over een proces waarmee veranderingen in de bedrijfsstrategie en de strategie voor digitale weerbaarheid van de financiële entiteit in aanmerking worden genomen.

Voor de toepassing van punt c) van het eerste lid zorgt de in dat punt bedoelde procedure voor:

a) de monitoring van de doeltreffendheid van de geïmplementeerde maatregel voor ICT-risicobehandeling;

b) de beoordeling van de vraag of de vastgestelde risicotolerantieniveaus van de financiële entiteit zijn bereikt;

c) de beoordeling van de vraag of de financiële entiteit acties heeft ondernemen om die maatregelen zo nodig te corrigeren of te verbeteren.

Afdeling 3

BEHEER ICT-ASSETS

Artikel 4

EASTER EGG, word 5: "ToolFlowBuilder"

1. Als onderdeel van de beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging als bedoeld in artikel 9, lid 2, van Verordening (EU) 2022/2554 ontwikkelen, documenteren en implementeren financiële entiteiten een beleid voor het beheer van ICT-assets.

2. Het in lid 1 bedoelde beleid voor het beheer van ICT-assets:

a) schrijft de monitoring en het beheer voor van de levenscyclus van ICT-assets die zijn geïdentificeerd en geclassificeerd overeenkomstig artikel 8, lid 1, van Verordening (EU) 2022/2554;

b) schrijft voor dat de financiële entiteit vastleggingen maakt van alle volgende elementen:

i) de unieke identificatie van elk ICT-asset;

ii) informatie over de — fysieke of logische — locatie van alle ICT-assets;

iii) de classificatie van alle ICT-assets, als bedoeld in artikel 8, lid 1, van Verordening (EU) 2022/2554;

iv) de identiteit van eigenaren van ICT-assets;

v) de door het ICT-asset ondersteunde bedrijfsfuncties of diensten;

vi) de vereisten inzake ICT-bedrijfscontinuïteit, met inbegrip van de hersteltijddoelstellingen (RTO's) en de herstelpuntdoelstellingen (RPO's);

vii) de vraag of het ICT-asset kan zijn blootgesteld dan wel blootgesteld is aan externe netwerken, daaronder begrepen het internet;

viii) de verbanden en onderlinge afhankelijkheden tussen ICT-assets en de bedrijfsfuncties die van elk ICT-asset gebruikmaken;

ix) (in voorkomend geval) voor alle ICT-assets: de einddata van de gewone, verlengde en op maat gemaakte ondersteuningsdiensten door de derde aanbieder van ICT-diensten, waarna die ICT-assets niet langer worden ondersteund door de leverancier ervan of door een derde aanbieder van ICT-diensten;

c) voor financiële entiteiten niet zijnde micro-ondernemingen: schrijft voor dat die financiële entiteiten vastleggingen maken van de informatie die noodzakelijk is om een specifieke ICT-risicobeoordeling uit te voeren voor alle in artikel 8, lid 7, van Verordening (EU) 2022/2554 bedoelde legacy ICT-systemen.

Artikel 5

Procedure voor het beheer van ICT-assets

1. Financiële entiteiten ontwikkelen, documenteren en implementeren een procedure voor het beheer van ICT-assets.

2. De in lid 1 bedoelde procedure voor het beheer van ICT-assets specificeert de criteria voor het uitvoeren van de beoordeling van het kritieke karakter van informatieassets en ICT-assets die bedrijfsfuncties ondersteunen. Die beoordeling houdt rekening met:

a) het ICT-risico verbonden aan die bedrijfsfuncties en hun afhankelijkheden van de informatieassets of ICT-assets;

b) de vraag wat de impact van het verlies aan vertrouwelijkheid, integriteit en beschikbaarheid van dergelijke informatieassets en ICT-assets zou zijn op de bedrijfsprocessen en -activiteiten van de financiële entiteiten.

Afdeling 4

ENCRYPTIE EN CRYPTOGRAFIE

Artikel 6

Encryptie en cryptografische controles

1. Als onderdeel van hun beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging als bedoeld in artikel 9, lid 2, van Verordening (EU) 2022/2554 ontwikkelen, documenteren en implementeren financiële entiteiten een beleid voor encryptie en cryptografische controles.

2. Financiële entiteiten richten hun in lid 1 bedoelde beleid voor encryptie en cryptografische controles in op basis van de uitkomsten van een goedgekeurde dataclassificatie en ICT-risicobeoordeling. Dat beleid bevat regels voor alle volgende elementen:

a) de encryptie van gegevens in rust en in transit;

b) de encryptie van gegevens in gebruik, voor zover noodzakelijk;

c) de encryptie van interne netwerkverbindingen en verkeer met externe partijen;

d) het in artikel 7 bedoelde beheer van cryptografische sleutels, waarmee regels worden vastgesteld voor correct gebruik, bescherming en levenscyclus van cryptografische sleutels.

Voor de toepassing van punt b), verwerken financiële entiteiten, wanneer encryptie van gegevens in gebruik niet mogelijk is, die gegevens in gebruik in een afzonderlijke en beveiligde omgeving, of nemen zij gelijkwaardige maatregelen om de vertrouwelijkheid, integriteit, authenticiteit en beschikbaarheid van gegevens te garanderen.

3. Financiële entiteiten nemen in hun in lid 1 bedoelde beleid voor encryptie en cryptografische controles criteria op voor de selectie van cryptografische technieken en gebruikspraktijken, rekening houdende met maatgevende praktijken en met normen zoals gedefinieerd in artikel 2, punt 1), van Verordening nr. 1025/2012, en de classificatie van relevante ICT-assets vastgesteld overeenkomstig artikel 8, lid 1, van Verordening (EU) 2022/2554. Financiële entiteiten die niet in staat zijn om zich aan de maatgevende praktijken of normen te houden of om de meest betrouwbare technieken te gebruiken, stellen mitigatie- en monitoringmaatregelen vast die garanties bieden op weerbaarheid tegen cyberdreigingen.

4. Financiële entiteiten nemen in hun in lid 1 bedoelde beleid voor encryptie en cryptografische controles bepalingen op voor het updaten of wijzigen, waar nodig, van de cryptografische technologie op basis van ontwikkelingen op het gebied van cryptoanalyse. Die updates of wijzigingen borgen dat de cryptografische technologie weerbaar blijft tegen cyberdreigingen, zoals voorgeschreven door artikel 10, lid 2, punt a). Financiële entiteiten die niet in staat zijn om de cryptografische technologie te updaten of te wijzigen, stellen mitigatie- en monitoringmaatregelen vast die garanties bieden op weerbaarheid tegen cyberdreigingen.

5. Financiële entiteiten nemen in hun in lid 1 bedoelde beleid voor encryptie en cryptografische controles een verplichting op om een vastlegging te maken van de vaststelling van mitigatie- en monitoringmaatregelen die overeenkomstig de leden 3 en 4 zijn ingericht, en verschaffen daarvoor een onderbouwing.

Artikel 7

Beheer van cryptografische sleutels

1. Financiële entiteiten nemen in hun in artikel 6, lid 2, punt d), bedoelde beleid voor het beheer van cryptografische sleutels vereisten op voor het beheer van cryptografische sleutels tijdens hun gehele levenscyclus, met inbegrip van het genereren, vernieuwen, opslaan, backuppen, archiveren, ophalen, overdragen, intrekken, herroepen en vernietigen van die cryptografische sleutels.

2. Financiële entiteiten identificeren en implementeren beheersmaatregelen ("controls") om cryptografische sleutels tijdens hun gehele levenscyclus te beschermen tegen verlies, ongeautoriseerde toegang, bekend worden en modificatie. Financiële entiteiten richten die beheersmaatregelen in op basis van de uitkomsten van de goedgekeurde dataclassificatie en ICT-risicobeoordeling.

3. Financiële entiteiten ontwikkelen en implementeren methoden om cryptografische sleutels te vervangen bij verlies of wanneer die sleutels gecompromitteerd of beschadigd zijn geraakt.

4. Financiële entiteiten leggen ten minste voor ICT-assets die kritieke of belangrijke functies ondersteunen, een register aan voor alle certificaten en opslagapparaten voor certificaten en houden dat register bij. Financiële entiteiten houden dat register actueel.

5. Financiële entiteiten bewaken dat certificaten direct worden verlengd voordat zij vervallen.

Afdeling 5

BEVEILIGING ICT-OPERATIES

Artikel 8

Beleidslijnen en procedures voor ICT-operaties

1. Als onderdeel van de beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging als bedoeld in artikel 9, lid 2, van Verordening (EU) 2022/2554 ontwikkelen, documenteren en implementeren financiële entiteiten beleidslijnen en procedures voor het beheer van de ICT-operaties. Die beleidslijnen en procedures specificeren hoe financiële entiteiten hun ICT-assets opereren, monitoren, controleren en herstellen, met inbegrip van de documentatie van ICT-operaties.

2. De in lid 1 bedoelde beleidslijnen en procedures voor ICT-operaties bevatten alle volgende elementen:

a) een beschrijving van ICT-assets, die alle volgende elementen bevat:

   i) vereisten ten aanzien van veilige installatie, onderhoud, configuratie en verwijdering van een ICT-systeem;

   ii) vereisten ten aanzien van het beheer van informatieassets die door ICT-assets worden gebruikt, met inbegrip van de verwerking en handling daarvan, zowel geautomatiseerd als handmatig;

   iii) vereisten ten aanzien van de identificatie en controle van legacy ICT-systemen;

b) beheersmaatregelen en monitoring van ICT-systemen, met inbegrip van alle volgende elementen:

   i) vereisten inzake back-up en herstel van ICT-systemen;

   ii) vereisten inzake planning, rekening houdende met onderlinge afhankelijkheden van de ICT-systemen;

   iii) protocollen voor audit-trail- en systeemlog-informatie;

   iv) vereisten die borgen dat de uitvoering van interne audits en andere tests storingen van bedrijfsoperaties tot een minimum beperkt;

   v) vereisten ten aanzien van de scheiding tussen de ICT-productieomgevingen en ontwikkelings-, test- en andere niet-productieomgevingen;

   vi) vereisten om ontwikkeling en testen uit te voeren in omgevingen die gescheiden zijn van de productie-omgeving;

   vii) vereisten om ontwikkeling en testen uit te voeren in productieomgevingen;

c) foutafhandeling voor ICT-systemen, met inbegrip van alle volgende elementen:

i) procedures en protocollen voor foutafhandeling;

ii) ondersteunings- en escalatiecontacten, met inbegrip van contacten bij externe ondersteuning in het geval van onverwachte operationele of technische problemen;

iii) herstart-, rollback- en herstelprocedures van ICT-systemen voor toepassing bij een storing in het ICT-systeem.

Voor de toepassing van punt b), v), wordt bij de scheiding rekening gehouden met alle componenten van de omgeving, met inbegrip van accounts, gegevens en verbindingen, zoals voorgeschreven door artikel 13, eerste alinea, punt a).

Voor de toepassing van punt b), vii), wordt in de in lid 1 bedoelde beleidslijnen en procedures bepaald dat de gevallen waarin testen in een productieomgeving plaatsvindt, duidelijk geïdentificeerd worden, beargumenteerd worden, voor een beperkte tijd zijn en door de betrokken functie zijn goedgekeurd overeenkomstig artikel 16, lid 6. Financiële entiteiten borgen de beschikbaarheid, vertrouwelijkheid, integriteit en authenticiteit van ICT-systemen en productiegegevens tijdens de ontwikkelings- en testactiviteiten in de productieomgeving.

Artikel 9

Capaciteits- en performancemanagement

1. Als onderdeel van de beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging als bedoeld in artikel 9, lid 2, van Verordening (EU) 2022/2554 ontwikkelen, documenteren en implementeren financiële entiteiten procedures inzake capaciteit- en performancemanagement voor de volgende elementen:

a) het in kaart brengen van capaciteitsvereisten van hun ICT-systemen;

b) de toepassing van resource-optimalisatie;

c) de monitoringprocedures voor het in stand houden en verbeteren van:

i) de beschikbaarheid van gegevens en ICT-systemen;

ii) de efficiëntie van ICT-systemen;

iii) het voorkomen van ICT-capaciteitstekorten.

2. De in lid 1 bedoelde procedures voor capaciteits- en performancemanagement borgen dat financiële entiteiten maatregelen nemen die passend zijn voor de specifieke kenmerken van ICT-systemen met lange of complexe aankoop- of goedkeuringsprocessen of ICT-systemen die hulpbronnenintensief zijn.

Artikel 10

Kwetsbaarhedenbeheer en patchmanagement

1. Als onderdeel van de beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging als bedoeld in artikel 9, lid 2, van Verordening (EU) 2022/2554 ontwikkelen, documenteren en implementeren financiële entiteiten procedures voor het beheersen van kwetsbaarheden.

2. De in lid 1 bedoelde procedures voor de beheersing van kwetsbaarheden:

a) brengen relevante en betrouwbare informatiemiddelen in kaart en actualiseren die om bewustzijn van kwetsbaarheden op te bouwen en in stand te houden;

b) zorgen voor de uitvoering van geautomatiseerde kwetsbaarheidsscans en -beoordelingen van ICT-assets, waarbij de frequentie en scope van die activiteiten in verhouding staat tot de overeenkomstig artikel 8, lid 1, van Verordening (EU) 2022/2554 vastgestelde classificatie en het algemene risicoprofiel van het ICT-asset;

c) gaan na of:

i) de derde aanbieders van ICT-diensten kwetsbaarheden behandelen wat betreft aan de financiële entiteit geleverde ICT-diensten;

ii) die dienstverleners aan de financiële entiteit tijdig ten minste de kritieke kwetsbaarheden, statistische gegevens en trends rapporteren;

d) houden het gebruik bij van:

i) third-party libraries, met inbegrip van open-source libraries, die worden gebruikt door ICT-diensten die kritieke of belangrijke functies;

ii) ICT-diensten ontwikkeld door de financiële entiteit zelf of die door een derde aanbieder van ICT-diensten specifiek op maat zijn gemaakt of ontwikkeld voor de financiële entiteit;

e) richten procedures in voor de responsible disclosure van kwetsbaarheden aan cliënten, tegenpartijen en aan het publiek;

f) prioriteren de uitrol van patches en andere mitigerende maatregelen om de geconstateerde kwetsbaarheden aan te pakken;

g) monitoren en controleren het verhelpen van kwetsbaarheden;

h) eisen dat van gedetecteerde kwetsbaarheden die van invloed zijn op ICT-systemen, vastleggingen worden gemaakt en dat de oplossing daarvan wordt gemonitord.

Voor de toepassing van punt b) voeren financiële entiteiten ten minste wekelijks de geautomatiseerde kwetsbaarheidsscans en -beoordelingen voor ICT-assets uit ten aanzien van de ICT-assets die kritieke of belangrijke functies ondersteunen.

Voor de toepassing van punt c) eisen financiële entiteiten dat derde aanbieders van ICT-diensten de betrokken kwetsbaarheden onderzoeken, de grondoorzaken ervan bepalen en adequate mitigerende acties implementeren

Voor de toepassing van punt d) monitoren financiële entiteiten, in voorkomend geval in samenwerking met de derde aanbieder van ICT-diensten, de versie en mogelijke updates van de third-party libraries. In het geval van gebruiksklare (off-the-shelf) ICT-assets of componenten van ICT-assets aangeschaft en gebruikt bij het opereren van ICT-diensten die geen kritieke of belangrijke functies ondersteunen, houden financiële entiteiten voor zover mogelijk het gebruik van third-party libraries, met inbegrip van open-source libraries, bij.

Voor de toepassing van punt f) houden financiële entiteiten rekening met het kritieke karakter van de kwetsbaarheid, de overeenkomstig artikel 8, lid 1, van Verordening (EU) 2022/2554 vastgestelde classificatie en het risicoprofiel van de ICT-assets die door de geconstateerde kwetsbaarheden worden geraakt.

3. Als onderdeel van de beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging als bedoeld in artikel 9, lid 2, van Verordening (EU) 2022/2554 ontwikkelen, documenteren en implementeren financiële entiteiten procedures voor patchmanagement.

4. De in lid 3 bedoelde procedures voor patchmanagement:

a) brengen voor zover mogelijk beschikbare software- en hardwarepatches en updates die van geautomatiseerde tools gebruikmaken, in kaart en evalueren die;

b) brengen noodprocedures in kaart voor patching en updating van ICT-assets;

c) testen de software- en hardwarepatches en de updates en rollen deze uit als bedoeld in artikel 8, lid 2, punt b), v), vi) en vii);

d) bepalen termijnen voor de installatie van software- en hardwarepatches en updates en escalatieprocedures ingeval die termijnen niet kunnen worden gehaald.

Artikel 11

Gegevens- en systeembeveiliging

1. Als onderdeel van de beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging als bedoeld in artikel 9, lid 2, van Verordening (EU) 2022/2554 ontwikkelen, documenteren en implementeren financiële entiteiten een procedure voor gegevens- en systeembeveiliging.

2. De in lid 1 bedoelde procedure voor gegevens- en systeembeveiliging bevat alle volgende elementen met betrekking tot de beveiliging van gegevens- en ICT-systemen, in overeenstemming met de overeenkomstig artikel 8, lid 1, van Verordening (EU) 2022/2554 bepaalde classificatie:

a) de in artikel 21 van deze verordening bedoelde toegangsbeperkingen die de beveiligingseisen voor elk niveau van de classificatie ondersteunen;

b) de identificatie van een veilige configuratiebaseline voor ICT-assets die de blootstelling van die ICT-assets aan cyberdreigingen tot een minimum beperkt en maatregelen om regelmatig na te gaan dat die baselines daadwerkelijk worden uitgerold;

c) de identificatie van beveiligingsmaatregelen die ervoor moeten zorgen dat alleen geautoriseerde software wordt geïnstalleerd op ICT-systemen en endpoint-apparaten;

d) de identificatie van beveiligingsmaatregelen tegen kwaadaardige codes;

e) de identificatie van beveiligingsmaatregelen die ervoor zorgen dat alleen geautoriseerde media en systemen voor gegevensopslag en endpoint-apparaten worden gebruikt om gegevens van de financiële entiteit over te dragen en op te slaan;

f) de volgende vereisten voor het beveiligen van het gebruik van draagbare endpoint-apparaten en privé niet-draagbare eindpoint-apparaten:

   i) de verplichting om een beheersoplossing te gebruiken om de endpoint-apparaten vanop afstand te beheren en de gegevens van de financiële entiteit vanop afstand te wissen;

   ii) de verplichting om beveiligingsmechanismen te gebruiken die door medewerkers of derde aanbieders van ICT-diensten niet op een ongeautoriseerde manier kunnen worden veranderd, verwijderd of omzeild;

   iii) de verplichting om verwijderbare apparaten voor gegevensopslag alleen te gebruiken wanneer het ICT-restrisico binnen het in artikel 3, eerste alinea, punt a), bedoelde risicotolerantieniveau van de financiële entiteit blijft;

g) het proces om veilig gegevens te wissen die aanwezig zijn op bedrijfslocaties van de financiële entiteit of die extern zijn opgeslagen, en die de financiële entiteit niet langer hoeft te verzamelen of op te slaan;

h) het proces om apparaten voor gegevensopslag die aanwezig zijn op bedrijfslocaties van de financiële entiteit of die extern zijn opgeslagen en vertrouwelijke informatie bevatten, af te voeren of te ontmantelen;

i) de identificatie en implementatie van beveiligingsmaatregelen om gegevensverlies en -lekken te voorkomen bij systemen en endpoint-apparaten;

j) de implementatie van beveiligingsmaatregelen die moeten voorkomen dat thuiswerk en het gebruik van privé endpoint-apparaten een negatieve impact hebben op de ICT-beveiliging van de financiële entiteit;

k) voor ICT-assets of -diensten die worden geopereerd door een derde aanbieder van ICT-diensten: de identificatie en implementatie van vereisten om digitale operationele weerbaarheid in stand te houden, in overeenstemming met de uitkomsten van de dataclassificatie en ICT-risicobeoordeling.

Voor de toepassing van punt b) houdt de in dat punt bedoelde veilige configuratiebaseline rekening met maatgevende praktijken en adequate technieken die zijn vastgelegd in de normen zoals gedefinieerd in artikel 2, punt 1, van Verordening (EU) nr. 1025/2012.

Voor de toepassing van punt k) houden financiële entiteiten rekening met de volgende elementen:

a) de implementatie van door de verkoper aanbevolen instellingen voor de door de financiële entiteit geopereerde elementen;

b) een duidelijke verdeling van de rollen en verantwoordelijkheden wat betreft informatiebeveiliging tussen de financiële entiteit en de derde aanbieder van ICT-diensten, overeenkomstig het beginsel van de volledige aansprakelijkheid van de financiële entiteit ten aanzien van haar derde aanbieder van ICT-diensten als bedoeld in artikel 28, lid 1, punt a), van Verordening (EU) 2022/2554 en, voor financiële entiteiten als bedoeld in artikel 28, lid 2, van die verordening, overeenkomstig het beleid van de financiële entiteit voor het gebruik van ICT-diensten die kritieke of belangrijke functies ondersteunen;

c) de noodzaak om binnen de financiële entiteit afdoende competenties te garanderen en in stand te houden wat betreft beheer en beveiliging van de gebruikte dienst;

d) technische en organisatorische maatregelen om de risico's te beperken voor de infrastructuur die de derde aanbieder van ICT-diensten gebruikt voor zijn ICT-diensten, rekening houdende met maatgevende praktijken en normen zoals gedefinieerd in artikel 2, punt 1), van Verordening (EU) nr. 1025/2012.

Artikel 12

Logging

1. Als onderdeel van de beschermingsmaatregelen tegen inbraken en misbruik van gegevens ontwikkelen, documenteren en implementeren financiële entiteiten loggingprocedures, -protocollen en -tools.

2. De in lid 1 bedoelde loggingprocedures, -protocollen en -tools bevatten alle volgende elementen:

a) de identificatie van de in logs bij te houden events, de retentieperiode van logbestanden en de maatregelen om de loggegevens te beveiligen en daarmee om te gaan, rekening houdende met het doel waarvoor de logbestanden zijn gecreëerd;

b) de afstemming van de mate van gedetailleerdheid van de logs op het doel en gebruik ervan, zodat afwijkende activiteiten als bedoeld in artikel 24 kunnen worden gedetecteerd;

c) de verplichting om log events bij te houden voor elk van de volgende elementen:

i) logische en fysieke toegangscontrole, als bedoeld in artikel 21, en identiteitsbeheer;

ii) capaciteitsbeheer;

iii) wijzigingsbeheer;

iv) ICT-operaties, met inbegrip van ICT-systeemactiviteiten;

v) netwerkverkeer, met inbegrip van ICT-netwerkperformance;

d) maatregelen om loggingsystemen en loginformatie te beschermen tegen manipulatie, wissen en ongeautoriseerde toegang in rust, in transit en, in voorkomend geval, in gebruik;

e) maatregelen om falen van loggingsystemen te detecteren;

f) onverminderd toepasselijke wettelijke verplichtingen uit hoofde van Unierecht of nationaal recht, het synchroniseren van de klokken van elk van de ICT-systemen van de financiële entiteit met één gedocumenteerde betrouwbare reference time source.

Voor de toepassing van punt a) stellen financiële entiteiten de retentieperiode vast, rekening houdende met de doelstellingen inzake bedrijfs- en informatiebeveiliging, de reden voor het vastleggen van het event in de logs, en de uitkomsten van de ICT-risicobeoordeling.

Afdeling 6

Netwerkbeveiliging

Artikel 13

Beheer van netwerkbeveiliging

Als onderdeel van de beschermingsmaatregelen die netwerken tegen inbraken en misbruik van gegevens moeten beveiligen, ontwikkelen, documenteren en implementeren financiële entiteiten beleidslijnen, procedures, protocollen en tools voor het beheer van netwerkbeveiliging, die alle volgende elementen bevatten:

a) de scheiding en segmentatie van ICT-systemen en -netwerken, rekening houdende met:

i) het kritieke karakter of belang van de functie die door deze ICT-systemen en -netwerken wordt ondersteund;

ii) de overeenkomstig artikel 8, lid 1, van Verordening (EU) 2022/2554 vastgestelde classificatie;

iii) het algemene risicoprofiel van ICT-assets die van die ICT-systemen en -netwerken gebruikmaken;

b) de documentatie van alle netwerkverbindingen en gegevensstromen van de financiële entiteit;

c) het gebruik van een apart en specifiek netwerk voor het beheer van die ICT-assets;

d) de identificatie en implementatie van controles op netwerktoegang voor het voorkomen en detecteren van verbindingen met het netwerk door een ongeautoriseerd apparaat of systeem, of van endpoints die niet voldoen aan de beveiligingseisen van de financiële entiteit;

e) de encryptie van netwerkverbindingen die over bedrijfsnetwerken, publieke netwerken, thuisnetwerken, netwerken van derde partijen en draadloze netwerken lopen, voor gebruikte communicatieprotocollen, rekening houdende met de uitkomsten van de goedgekeurde dataclassificatie, de uitkomsten van de ICT-risicobeoordeling en de encryptie van netwerkverbindingen als bedoeld in artikel 6, lid 2;

f) de opzet van netwerken in lijn met de ICT-beveiligingseisen die door de financiële entiteit zijn vastgesteld, rekening houdende met maatgevende praktijken om de vertrouwelijkheid, integriteit en beschikbaarheid van het netwerk te borgen;

g) de beveiliging van netwerkverkeer tussen de interne netwerken en de internet- en andere externe verbindingen;

h) het in kaart brengen van de rollen, verantwoordelijkheden en stappen voor de specificatie, implementatie, goedkeuring, wijziging en evaluatie van firewallregels en verbindingsfilters;

i) het uitvoeren van evaluaties van de netwerkarchitectuur en van de inrichting van de netwerkbeveiliging eenmaal per jaar, en op periodieke basis voor micro-ondernemingen, om potentiële kwetsbaarheden in beeld te brengen;

j) de maatregelen om, waar nodig, subnetwerken en netwerkcomponenten en apparaten tijdelijk te isoleren;

k) de implementatie van een veilige configuratiebaseline van alle netwerkcomponenten en van de hardening van het netwerk en netwerkapparaten in lijn met eventuele instructies van de verkoper en, in voorkomend geval, toepasselijke normen zoals gedefinieerd in artikel 2, punt 1), van Verordening (EU) nr. 1025/2012, en maatgevende praktijken;

l) de procedures om systeemsessies en externe sessies na een gespecificeerde periode van inactiviteit te beperken, te vergrendelen en te beëindigen;

m) voor overeenkomsten inzake netwerkdiensten:

   i) de identificatie en specificatie van ICT- en informatiebeveiligingsmaatregelen, service levels en beheersvereisten voor alle netwerkdiensten;

   ii) de vraag of die diensten worden verricht door een intragroepsaanbieder van ICT-diensten of door derde aanbieders van ICT-diensten.

Voor de toepassing van punt h) voeren financiële entiteiten de evaluatie van firewallregels en verbindingsfilters op regelmatige basis uit in overeenstemming met de overeenkomstig artikel 8, lid 1, van Verordening (EU) 2022/2554 vastgestelde classificatie en het algemene risicoprofiel van de betrokken ICT-systemen. Voor ICT-systemen die kritieke of belangrijke functies ondersteunen, gaan financiële entiteiten ten minste om de zes maanden na of de bestaande firewallregels en verbindingsfilters afdoende zijn.

Artikel 14

Informatie in transit beveiligen

1. Als onderdeel van de beschermingsmaatregelen die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens moeten veiligstellen, ontwikkelen, documenteren en implementeren financiële entiteiten beleidslijnen, procedures, protocollen en tools om informatie in transit te beschermen. Financiële entiteiten bewaken met name alle volgende elementen:

a) de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens tijdens de doorgifte via het netwerk en de inrichting van procedures om inachtneming van die vereisten te beoordelen;

b) de preventie en detectie van datalekken en de veilige overdracht van informatie tussen de financiële entiteit en externe partijen;

c) dat vereisten inzake vertrouwelijkheid of afspraken inzake niet-openbaarmaking die een afspiegeling zijn van de behoeften van de financiële entiteit wat betreft bescherming van informatie voor zowel medewerkers van de financiële entiteit als derde partijen, worden geïmplementeerd, gedocumenteerd en regelmatig geëvalueerd.

2. Financiële entiteiten richten hun in lid 1 bedoelde beleidslijnen, procedures, protocollen en tools ter bescherming van de informatie in transit in op basis van de uitkomsten van de goedgekeurde dataclassificatie en van de ICT-risicobeoordeling.

Afdeling 7

ICT-projectmanagement en ICT-wijzigingsbeheer

Artikel 15

ICT-projectmanagement

1. Als onderdeel van de beschermingsmaatregelen die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens moeten veiligstellen, ontwikkelen, documenteren en implementeren financiële entiteiten een beleid voor ICT-projectmanagement.

2. Het in lid 1 bedoeld beleid voor ICT-projectmanagement specificeert de elementen die zorgen voor het effectieve beheer van de ICT-projecten wat betreft aanschaf, onderhoud en, in voorkomend geval, ontwikkeling van de ICT-systemen van de financiële entiteit.

3. Het in lid 1 bedoelde beleid voor ICT-projectmanagement bevat alle volgende elementen:

a) doelstellingen van ICT-projecten;

b) governance van ICT-projecten, met inbegrip van rollen en verantwoordelijkheden;

c) planning, tijdschema en stappen van ICT-projecten;

d) risicobeoordeling van ICT-projecten;

e) relevante mijlpalen;

f) eisen inzake wijzigingsbeheer;

g) het testen van alle eisen, met inbegrip van beveiligingseisen, en het desbetreffende goedkeuringsproces bij de uitrol van een ICT-systeem in de productieomgeving.

4. Het in lid 1 bedoelde beleid voor ICT-projectmanagement borgt de veilige implementatie van ICT-projecten doordat de nodige informatie en deskundigheid wordt verschaft vanuit de bedrijfsonderdelen of functies waarop het ICT-project van invloed is.

5. In overeenstemming met de in lid 3, punt d), bedoelde risicobeoordeling van ICT-projecten, wordt in het in lid 1 bedoelde beleid voor ICT-projectmanagement bepaald dat het opzetten en de voortgang van ICT-projecten met impact op kritieke of belangrijke functies van de financiële entiteit en de daaraan verbonden risico's als volgt aan het leidinggevend orgaan worden gerapporteerd:

a) individueel of geaggregeerd, afhankelijk van het belang en de omvang van de ICT-projecten;

b) periodiek en, waar nodig, event-driven.

Artikel 16

Aanschaf, ontwikkeling en onderhoud van ICT-systemen

1. Als onderdeel van de beschermingsmaatregelen die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens moeten veiligstellen, ontwikkelen, documenteren en implementeren financiële entiteiten een beleid voor aanschaf, ontwikkeling en onderhoud van ICT-systemen. Dat beleid:

a) brengt beveiligingspraktijken en -methoden voor aanschaf, ontwikkeling en onderhoud van ICT-systemen in kaart;

b) eist de identificatie van:

   i) technische specificaties en technische ICT-specificaties, zoals gedefinieerd in artikel 2, punten 4 en 5), van Verordening (EU) nr. 1025/2012;

   ii) vereisten ten aanzien van aanschaf, ontwikkeling en onderhoud van ICT-systemen, met bijzondere aandacht voor ICT-beveiligingseisen en de goedkeuring daarvan door de betrokken bedrijfsfunctie en eigenaar van ICT-assets in overeenstemming met de interne governanceregelingen van de financiële entiteit;

c) specificeert maatregelen om het risico te mitigeren van onbedoelde wijziging of bedoelde manipulatie van de ICT-systemen tijdens ontwikkeling, onderhoud en uitrol van die ICT-systemen in de productieomgeving.

2. Financiële entiteiten ontwikkelen, documenteren en implementeren ten behoeve van aanschaf, ontwikkeling en onderhoud van ICT-systemen een procedure voor het testen en goedkeuren van alle ICT-systemen vóór het gebruik ervan en na onderhoud, in overeenstemming met artikel 8, lid 2, punt b), v), vi) en vii). De grondigheid van de tests is evenredig aan het kritieke karakter van de betrokken bedrijfsprocedures en ICT-assets. Het testen wordt ingericht om na te gaan of de nieuwe ICT-systemen adequaat zijn om te functioneren als beoogd, met inbegrip van de kwaliteit van intern ontwikkelde software.

Centrale tegenpartijen betrekken, naast de in de eerste alinea bepaalde eisen, waar nodig bij de opzet en de uitvoering van de in de eerste alinea bedoelde tests:

a) clearingleden en cliënten;

b) interoperabele centrale tegenpartijen;

c) andere belanghebbenden.

Centrale effectenbewaarinstellingen betrekken, naast de in de eerste alinea bepaalde eisen, waar nodig bij de opzet en de uitvoering van de in de eerste alinea bedoelde tests:

a) gebruikers;

b) leveranciers van kritieke voorzieningen en diensten;

c) andere centrale effectenbewaarinstellingen;

d) andere marktinfrastructuren;

e) andere instellingen waarmee centrale effectenbewaarinstellingen volgens hun bedrijfscontinuïteitsbeleid banden van onderlinge afhankelijkheid blijken te hebben.

3. De in lid 2 bedoelde procedure omvat het uitvoeren van broncodereviews (pentests) met zowel statische als dynamische tests. Die tests omvatten beveiligingstests voor systemen en applicaties met internetblootstelling, overeenkomstig artikel 8, lid 2, punt b), v), vi) en vii). Financiële entiteiten:

a) brengen kwetsbaarheden en anomalieën in de broncode in kaart en analyseren deze;

b) stellen een actieplan vast om die kwetsbaarheden en anomalieën aan te pakken;

c) monitoren de implementatie van dat actieplan.

4. De in lid 2 bedoelde procedure bevat beveiligingstests van softwarepakketten uiterlijk in de integratiefase, overeenkomstig artikel 8, lid 2, punt b), v), vi) en vii).

5. In de in lid 2 bedoelde procedure wordt bepaald dat:

a) niet-productieomgevingen alleen geanonimiseerde, gepseudonimiseerde of gerandomiseerde productiegegevens opslaan;

b) financiële entiteiten de integriteit en vertrouwelijkheid van gegevens in niet-productieomgevingen moeten beschermen.

6. In afwijking van lid 5 kan in de in lid 2 bedoelde procedure worden bepaald dat productiegegevens alleen worden opgeslagen voor specifieke testgevallen, voor beperkte perioden en na de goedkeuring door de betrokken functie en dat gevallen aan de ICT-risicoheersingsfunctie worden gemeld.

7. De in lid 2 bedoelde procedure omvat de implementatie van beheersmaatregelen voor het beschermen van de integriteit van de broncode van ICT-systemen die intern of door een derde aanbieder van ICT-diensten zijn ontwikkeld en door een derde aanbieder van ICT-diensten aan de financiële entiteit worden geleverd.

8. In de in lid 2 bedoelde procedure is bepaald dat proprietary software en, voor zover doenbaar, de broncode aangeleverd door derde aanbieders van ICT-diensten of afkomstig van open-sourceprojecten, in overeenstemming met lid 3 worden geanalyseerd en getest voordat deze in de productieomgeving worden uitgerold.

9. De leden 1 tot en met 8 van dit artikel zijn ook van toepassing op ICT-systemen die worden ontwikkeld of beheerd door gebruikers buiten de ICT-functie, op basis van een risicogebaseerde benadering.

Artikel 17

ICT-wijzigingsbeheer

1. Als onderdeel van de beschermingsmaatregelen die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens moeten veiligstellen, nemen financiële entiteiten in de in artikel 9, lid 4, punt e), van Verordening (EU) 2022/2554 bedoelde procedures voor het ICT-wijzigingsbeheer ten aanzien van alle wijzigingen van software-, hardware-, firmwarecomponenten, systemen of beveiligingsparameters alle volgende elementen op:

a) een verificatie of aan de ICT-beveiligingseisen is voldaan;

b) mechanismen om de onafhankelijkheid te garanderen van de functies die wijzigingen goedkeuren, en de functies die verantwoordelijk zijn voor het aanvragen en implementeren van die wijzigingen;

c) een heldere beschrijving van de rollen en verantwoordelijkheden om te verzekeren dat:

   i) wijzigingen gespecificeerd en gepland worden;

   ii) een adequate transitie wordt opgezet;

   iii) de wijzigingen beheerst worden getest en gefinaliseerd;

   iv) er een effectieve kwaliteitsborging is;

d) de documentatie van en communicatie over concrete details van de wijzigingen, zoals:

   i) doel en scope van de wijzigingen;

   ii) de tijdslijn voor de implementatie van de wijzigingen;

   iii) de verwachte uitkomsten;

e) de identificatie van fall-backprocedures en verantwoordelijkheden, met inbegrip van procedures en verantwoordelijkheden voor het afbreken van wijzigingen of het herstel van wijzigingen die niet succesvol zijn geïmplementeerd;

f) procedures, protocollen en tools voor het beheer van noodwijzigingen die afdoende bescherming bieden;

g) procedures voor het documenteren, herevalueren, beoordelen en goedkeuren van noodwijzigingen na de implementatie ervan, met inbegrip van workarounds en patches;

h) de identificatie van de potentiële impact van een wijziging van bestaande ICT-beveiligingsmaatregelen en een beoordeling van de vraag of die wijziging de vaststelling van aanvullende ICT-beveiligingsmaatregelen vereist.

2. Nadat centrale tegenpartijen en centrale effectenbewaarinstellingen significante wijzigingen in hun ICT-systemen hebben doorgevoerd, onderwerpen zij hun ICT-systemen aan strenge tests door stresssituaties te simuleren.

Centrale tegenpartijen betrekken, waar nodig, bij de opzet en de uitvoering van de in de eerste alinea bedoelde tests:

a) clearingleden en cliënten;

b) interoperabele centrale tegenpartijen;

c) andere belanghebbenden.

Centrale effectenbewaarinstellingen betrekken, waar nodig, bij de opzet en de uitvoering van de in de eerste alinea bedoelde tests:

a) gebruikers;

b) leveranciers van kritieke voorzieningen en diensten;

c) andere centrale effectenbewaarinstellingen;

d) andere marktinfrastructuren;

e) andere instellingen waarmee centrale effectenbewaarinstellingen volgens hun ICT-bedrijfscontinuïteitsbeleid banden van onderlinge afhankelijkheid blijken te hebben.

Afdeling 8

Artikel 18

Fysieke beveiliging en milieubeveiliging

1. Als onderdeel van de beschermingsmaatregelen die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens moeten veiligstellen, specificeren, documenteren en implementeren financiële entiteiten een beleid voor fysieke beveiliging en milieubeveiliging. Financiële entiteiten richten dat beleid in het licht van het landschap van cyberdreigingen in, in overeenstemming met de overeenkomstig artikel 8, lid 1, van Verordening (EU) 2022/2554 vastgestelde classificatie en het algemene risicoprofiel van ICT-assets en toegankelijke informatieassets.

2. Het in lid 1 bedoelde beleid voor fysieke beveiliging en milieubeveiliging bevat alle volgende elementen:

a) een verwijzing naar het in artikel 21, eerste alinea, punt g), bedoelde beleid voor controle op het beheer van toegangsrechten;

b) maatregelen om de bedrijfslocaties, datacentra van de financiële entiteit en van door de financiële entiteit afgebakende gevoelige zones waar ICT-assets en informatieassets zijn ondergebracht, te beschermen tegen aanvallen, ongevallen en milieudreigingen en -gevaren;

c) maatregelen om ICT-assets — zowel binnen als buiten de bedrijfslocaties van de financiële entiteit — te beveiligen, rekening houdende met de uitkomsten van de ICT-risicobeoordeling voor de betrokken ICT-assets;

d) maatregelen die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van ICT-assets, informatieassets en apparatuur voor fysieke toegangscontrole van de financiële entiteit moeten verzekeren via adequaat onderhoud;

e) maatregelen om de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de gegevens veilig te stellen, met inbegrip van:

   i) een clear-deskbeleid voor papier;

   ii) een clear-screenbeleid voor faciliteiten voor informatieverwerking.

Voor de toepassing van punt b) staan de maatregelen ter bescherming tegen milieudreigingen en -gevaren in verhouding tot het belang van de bedrijfslocaties, datacentra, afgebakende gevoelige zones en het kritieke karakter van de operaties of ICT-systemen die daarin zijn ondergebracht.

Voor de toepassing van punt c) bevat het in lid 1 bedoelde beleid voor fysieke beveiliging en milieubeveiliging maatregelen die adequate bescherming bieden voor ICT-assets zonder toezicht.

HOOFDSTUK II

Humanresourcesbeleid en toegangscontrole

Artikel 19

Humanresourcesbeleid

Financiële entiteiten nemen in hun humanresourcesbeleid of andere relevante beleidslijnen alle volgende elementen van ICT-beveiliging op:

a) de identificatie en toewijzing van specifieke verantwoordelijkheden inzake ICT-beveiliging;

b) vereisten voor medewerkers van de financiële entiteit en van de derde aanbieders van ICT-diensten die gebruikmaken van of toegang hebben tot ICT-assets van de financiële entiteit om:

i) te worden geïnformeerd over en zich te houden aan beleidslijnen, procedures en protocollen van de financiële entiteit voor ICT-beveiliging;

ii) op de hoogte te zijn van de door de financiële entiteit opgezette meldingskanalen voor de detectie van afwijkend gedrag, met inbegrip van, in voorkomend geval, de meldingskanalen die zijn opgezet in lijn met Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad ([11]);

iii) voor de medewerkers: om bij de beëindiging van het dienstverband aan de financiële entiteit alle in hun bezit zijnde ICT-assets en materiële informatieassets terug te geven die eigendom zijn van de financiële entiteit.

Artikel 20

Identiteitsbeheer

1. Als onderdeel van hun controle op het beheer van toegangsrechten ontwikkelen, documenteren en implementeren financiële entiteiten beleidslijnen en procedures voor identiteitsbeheer die de unieke identificatie en authenticatie garanderen van natuurlijke personen en systemen met toegang tot informatie van de financiële entiteiten, om toegangsrechten voor gebruikers te kunnen toekennen overeenkomstig artikel 21.

2. De in lid 1 bedoelde beleidslijnen en procedures voor identiteitsbeheer bevatten alle volgende elementen:

a) onverminderd artikel 21, eerste alinea, punt c), een unieke identiteit die overeenstemt met een unieke gebruikersaccount, wordt toegekend aan elke medewerker van de financiële entiteit of aan medewerkers van de derde aanbieders van ICT-diensten die toegang hebben tot de informatieassets en ICT-assets van de financiële entiteit;

b) een proces voor lifecycle-management van identiteiten en accounts waarmee het creëren, wijzigen, herzien en updaten, tijdelijk deactiveren en stopzetten van alle accounts wordt beheerd.

Voor de toepassing van punt a) maken financiële entiteiten vastleggingen van alle toewijzingen van identiteiten. Die vastleggingen worden verder bijgehouden na een reorganisatie van de financiële entiteit of na het einde van de contractuele relaties, onverminderd de retentieverplichtingen die in toepasselijk Unierecht en nationaal recht zijn vastgesteld.

Voor de toepassing van punt b) rollen financiële entiteiten, waar doenbaar en passend, geautomatiseerde oplossingen uit voor het proces van lifecycle-management van identiteiten.

Artikel 21

Toegangscontrole

Als onderdeel van hun controle op het beheer van toegangsrechten ontwikkelen, documenteren en implementeren financiële entiteiten een beleid dat alle volgende elementen bevat:

a) de toekenning van toegangsrechten tot ICT-assets op basis van need-to-know-, need-to-use- en least-privilege-principes, ook voor remote access en emergency access;

b) de functiescheiding die is ingericht om ongerechtvaardigde toegang tot kritieke data te voorkomen of om de toewijzing te voorkomen van combinaties van toegangsrechten die kunnen worden gebruikt om controles te omzeilen;

c) een bepaling betreffende de verantwoordingsplicht van gebruikers, door in de mate van het mogelijke het gebruik van generieke en gedeelde gebruikersaccounts te beperken en ervoor te zorgen dat gebruikers te allen tijde identificeerbaar zijn voor de acties die in de ICT-systemen worden uitgevoerd;

([11]) Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (PB L 305 van 26.11.2019, blz. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) een bepaling inzake beperkingen van toegang tot ICT-assets, met vermelding van beheersmaatregelen en tools die ongeautoriseerde toegang moeten voorkomen;

e) procedures voor accountbeheer om toegangsrechten voor gebruikersaccounts en generieke accounts, daaronder begrepen generieke administrator accounts, toe te kennen, te wijzigen of in te trekken, met inbegrip van bepalingen over alle volgende elementen:

i) toewijzing van rollen en verantwoordelijkheden voor het toekennen, herzien en intrekken van toegangsrechten;

ii) toekenning van privileged, emergency- en administrator toegang op need-to-use- of op ad-hocbasis voor alle ICT-systemen;

iii) onmiddellijke intrekking van toegangsrechten bij beëindiging van het dienstverband of wanneer toegang niet langer noodzakelijk is;

iv) update van toegangsrechten wanneer wijzigingen noodzakelijk zijn en ten minste eenmaal per jaar voor alle ICT-systemen niet zijnde ICT-systemen die kritieke of belangrijke functies ondersteunen, en ten minste om de zes maanden voor ICT-systemen die kritieke of belangrijke functies ondersteunen;

f) authenticatiemethoden, die alle volgende elementen bevatten:

i) het gebruik van authenticatiemethoden die in verhouding staan tot de overeenkomstig artikel 8, lid 1, van Verordening (EU) 2022/2554 vastgestelde classificatie en het algemene risicoprofiel van de ICT-assets en rekening houdende met maatgevende praktijken;

ii) het gebruik van sterke authenticatiemethoden in overeenstemming met maatgevende praktijken en technieken voor remote access tot het netwerk van de financiële entiteit, voor privileged access, voor toegang tot ICT-assets die kritieke of belangrijke functies ondersteunen of ICT-assets die publiek toegankelijk zijn;

g) maatregelen voor fysieke toegangscontrole, met inbegrip van:

i) de identificatie en logging van natuurlijke personen met geautoriseerde toegang tot bedrijfslocaties, datacentra en door de financiële entiteit afgebakende gevoelige zones waar ICT- en informatieassets zijn ondergebracht;

ii) het toekennen van fysieke toegangsrechten tot kritieke ICT-assets aan uitsluitend geautoriseerde personen, in overeenstemming met de need-to-know- en least privilege-principes, en op ad-hocbasis;

iii) de monitoring van fysieke toegang tot bedrijfslocaties, datacentra en door de financiële entiteit afgebakende gevoelige zones waar ICT-assets, informatieassets of beide soorten assets zijn ondergebracht;

iv) de herziening van fysieke toegangsrechten om ervoor te zorgen dat niet-noodzakelijke toegangsrechten prompt worden ingetrokken.

Voor de toepassing van punt e), i), stellen financiële entiteiten de retentieperiode vast, rekening houdende met de doelstellingen inzake bedrijfs- en informatiebeveiliging, de redenen voor het vastleggen van het event in de logs, en de uitkomsten van de ICT-risicobeoordeling.

Voor de toepassing van punt e), ii), maken financiële entiteiten, voor zover mogelijk, gebruik van specifieke accounts voor het uitvoeren van administratieve taken op ICT-systemen. Waar doenbaar en passend rollen financiële entiteiten geautomatiseerde oplossingen uit voor hun Privileged Access Management (PAM).

Voor de toepassing van punt g), i), staan de identificatie en logging in verhouding tot het belang van de bedrijfslocaties, datacentra, afgebakende gevoelige zones en het kritieke karakter van de operaties of ICT-systemen die daarin zijn ondergebracht.

Voor de toepassing van punt g), iii), staat de monitoring in verhouding tot de overeenkomstig artikel 8, lid 1, van Verordening (EU) 2022/2554 vastgestelde classificatie en het kritieke karakter van de zone waartoe personen toegang hebben.

HOOFDSTUK III

Detectie van en respons op ICT-incidenten

Artikel 22

Beleid voor ICT-incidentmanagement

Als onderdeel van de mechanismen om afwijkende activiteiten te detecteren, met inbegrip van performanceproblemen van het ICT-netwerk en ICT-incidenten, ontwikkelen, documenteren en implementeren financiële entiteiten een beleid voor ICT-incidenten waarin zij:

a) het in artikel 17 van Verordening (EU) 2022/2554 bedoelde proces voor ICT-incidentmanagement documenteren;

b) een lijst maken van relevante contacten met interne functies en externe stakeholders die direct betrokken zijn bij de beveiliging van ICT-operaties, onder meer over:

   i) de detectie en monitoring van cyberdreigingen;

   ii) de detectie van afwijkende activiteiten;

   iii) beheersing van kwetsbaarheden;

c) technische, organisatorische en operationele mechanismen inrichten, implementeren en opereren voor het ondersteunen van het proces van het ICT-incidentmanagement, met inbegrip van mechanismen waarmee afwijkende activiteiten en gedragingen prompt kunnen worden gedetecteerd overeenkomstig artikel 23 van deze verordening;

d) alle bewijsmateriaal bewaren met betrekking tot ICT-incidenten voor een periode die niet langer is dan noodzakelijk voor de doelstellingen waarvoor de gegevens worden verzameld, in verhouding staat tot het kritieke karakter van de betrokken bedrijfsfuncties, ondersteunende processen en ICT-assets en informatica-assets, overeenkomstig artikel 15 van Gedelegeerde Verordening (EU) 2024/1772 van de Commissie ([12]) en toepasselijke retentieverplichtingen uit hoofde van Unierecht;

e) mechanismen opzetten en implementeren voor het analyseren van significante of recurrente ICT-incidenten en van patronen in het aantal en de frequentie van ICT-incidenten.

Voor de toepassing van punt d) bewaren financiële entiteiten het in dat punt bedoelde bewijsmateriaal op een veilige manier.

Artikel 23

Detectie van afwijkende activiteiten en criteria voor detectie van en respons op ICT-incidenten

1. Financiële entiteiten leggen duidelijke rollen en verantwoordelijkheden vast om ICT-incidenten en afwijkende activiteiten effectief te detecteren en daarop te reageren.

2. Het mechanisme om prompt afwijkende activiteiten te detecteren, met inbegrip van performanceproblemen van het ICT-netwerk en ICT-incidenten, als bedoeld in artikel 10, lid 1, van Verordening (EU) 2022/2554, stelt financiële entiteiten in staat om:

a) alle volgende elementen te verzamelen, te monitoren en te analyseren:

   i) interne en externe factoren, met inbegrip van ten minste de overeenkomstig artikel 12 van deze verordening verzamelde logbestanden, informatie afkomstig van bedrijfs- en ICT-functies en problemen gemeld door gebruikers van de financiële entiteit;

   ii) potentiële interne en externe cyberdreigingen, rekening houdende met scenario's die doorgaans door threat actors worden gebruikt, en op bedreigingsinformatie gebaseerde scenario's;

([12]) Gedelegeerde Verordening (EU) 2024/1772 van de Commissie van 13 maart 2024 tot aanvulling van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen tot nadere bepaling van de criteria voor de classificatie van ICT-gerelateerde incidenten en cyberdreigingen, tot vaststelling van materialiteitsdrempels en tot bepaling van de nadere informatie van verslagen over ernstige incidenten (PB L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) notificatie door een derde aanbieder van ICT-diensten van de financiële entiteit van een ICT-incident dat is gedetecteerd in de ICT-systemen en netwerken van de derde aanbieder van ICT-diensten en dat op de financiële entiteit van invloed kan zijn;

b) afwijkende activiteiten en gedragingen te identificeren en tools te implementeren die afwijkende activiteiten en gedragingen signaleren ("alerts"), ten minste voor ICT-assets en informatieassets die kritieke of belangrijke functies ondersteunen;

c) de in punt b) bedoelde alerts te prioriteren zodat de gedetecteerde ICT-incidenten kunnen worden behandeld binnen de verwachte tijd om deze oplossen, zoals gespecificeerd door financiële entiteiten, zowel binnen als buiten werktijd;

d) relevante informatie over alle afwijkende activiteiten en gedragingen automatisch of handmatig vast te leggen, te analyseren en te evalueren.

Voor de toepassing van punt b) omvatten de in dat punt bedoelde tools de tools die automatische alerts afgeven die zijn gebaseerd op vooraf vastgestelde regels om afwijkingen te identificeren die van invloed zijn op de volledigheid en integriteit van de gegevensbronnen of het bijhouden van logs.

3. Financiële entiteiten beschermen vastleggingen van de afwijkende activiteiten tegen manipulatie en ongeautoriseerde toegang in rust, in transit en, in voorkomend geval, in gebruik.

4. Financiële entiteiten loggen alle relevante informatie voor elke gedetecteerde afwijkende activiteit zodat daarmee:

a) de datum en het tijdstip van de afwijkende activiteit kunnen worden geïdentificeerd;

b) de datum en het tijdstip waarop de afwijkende activiteit is gedetecteerd, kunnen worden geïdentificeerd;

c) het soort afwijkende activiteit kan worden geïdentificeerd.

5. Financiële entiteiten houden rekening met alle onderstaande criteria om de in artikel 10, lid 2, van Verordening (EU) 2022/2554 bedoelde processen voor detectie van en respons op ICT-incidenten te activeren:

a) aanwijzingen dat mogelijk kwaadwillige activiteiten in een ICT-systeem of -netwerk zijn uitgevoerd of dat dit ICT-systeem of -netwerk misschien is gecompromitteerd;

b) datalekken gedetecteerd met betrekking tot de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens;

c) negatieve impact gedetecteerd op transacties en operaties van de financiële entiteit;

d) onbeschikbaarheid van ICT-systemen en -netwerk.

6. Voor de toepassing van lid 5 houden financiële entiteiten ook rekening met het kritieke karakter van de betrokken diensten.

HOOFDSTUK IV

Beheer ICT-bedrijfscontinuïteit

Artikel 24

Onderdelen van het beleid voor ICT-bedrijfscontinuïteit

1. Financiële entiteiten nemen in hun in artikel 11, lid 1, van Verordening (EU) 2022/2554 bedoelde beleid voor ICT-bedrijfscontinuïteit alle volgende elementen op:

a) een beschrijving van:

i) de doelstellingen van het beleid voor ICT-bedrijfscontinuïteit, met inbegrip van de onderlinge relatie tussen ICT-bedrijfscontinuïteit en algemene bedrijfscontinuïteit, en rekening houdende met de uitkomsten van de in artikel 11, lid 5, van Verordening (EU) 2022/2554 bedoelde bedrijfsimpactanalyse (business impact analysis — BIA);

ii) de scope van de afspraken, plannen, procedures en mechanismen voor ICT-bedrijfscontinuïteit, met inbegrip van beperkingen en uitsluitingen;

iii) de tijdsspanne die wordt bestreken door de afspraken, plannen, procedures en mechanismen voor ICT-bedrijfscontinuïteit;

iv) de criteria om ICT-bedrijfscontinuïteitsplannen, ICT-respons- en -herstelplannen en crisiscommunicatieplannen te activeren en te deactiveren;

b) bepalingen wat betreft:

i) de governance en organisatie om het ICT-bedrijfscontinuïteitsplan te implementeren, met inbegrip van rollen, verantwoordelijkheden en escalatieprocedures die ervoor moeten zorgen dat voldoende middelen beschikbaar zijn;

ii) de afstemming tussen de ICT-bedrijfscontinuïteitsplannen en de algemene bedrijfscontinuïteitsplannen, voor ten minste alle volgende elementen:

1) potentiële scenario's van falen, met inbegrip van de in artikel 26, lid 2, van deze verordening bedoelde scenario's;

2) hersteldoelstellingen, die specificeren dat de financiële entiteit na storingen binnen een hersteltijddoelstelling (RTO) en een herstelpuntdoelstelling (RPO) de operaties van haar kritieke of belangrijke functies kan hervatten;

iii) het opzetten van ICT-bedrijfscontinuïteitsplannen voor zware bedrijfsstoringen als onderdeel van die plannen en het prioriteren van ICT-bedrijfscontinuïteitsacties met gebruikmaking van een risicogebaseerde benadering;

iv) de uitwerking, het testen en de evaluatie van ICT-respons- en -herstelplannen, overeenkomstig de artikelen 25 en 26 van deze verordening;

v) de evaluatie van de doeltreffendheid van de geïmplementeerde afspraken, plannen, procedures en mechanismen voor ICT-bedrijfscontinuïteit, overeenkomstig artikel 26 van deze verordening;

vi) de afstemming van het beleid voor ICT-bedrijfscontinuïteit op:

1) het in artikel 14, lid 2, van Verordening (EU) 2022/2554 bedoelde communicatiebeleid;

2) de in artikel 11, lid 2, punt e), van Verordening (EU) 2022/2554 bedoelde communicatie- en crisiscommunicatieacties.

2. Naast de in lid 1 bedoelde vereisten bewaken centrale tegenpartijen dat hun beleid voor ICT-bedrijfscontinuïteit:

a) voor hun kritieke functies een maximale hersteltijd bevat van maximaal twee uur;

b) rekening houdt met externe verbanden en onderlinge afhankelijkheden binnen de financiële infrastructuren, met inbegrip van door de centrale tegenpartij geclearde handelsplatformen, effectenafwikkelings- en betalingssystemen en kredietinstellingen waarvan de centrale tegenpartij of een verbonden centrale tegenpartij gebruikmaakt;

c) voorschrijft dat afspraken voorhanden zijn om:

i) de continuïteit te borgen van kritieke of belangrijke functies van de centrale tegenpartij op basis van rampscenario's:

ii) een secundaire verwerkingslocatie in stand te houden die continuïteit kan verzekeren van kritieke of belangrijke functies van de centrale tegenpartij en die identiek is aan de primaire locatie;

iii) een secundaire bedrijfslocatie in stand te houden of daartoe onmiddellijke toegang te hebben zodat medewerkers de continuïteit van de dienstverlening kunnen verzekeren indien de primaire bedrijfslocatie niet beschikbaar is;

iv) de behoefte aan aanvullende verwerkingslocaties te onderzoeken, in het bijzonder wanneer de diversiteit van de risicoprofielen van de primaire en secundaire locaties onvoldoende zekerheid biedt dat de doelstellingen van de centrale tegenpartij op het punt van bedrijfscontinuïteit in alle scenario's worden behaald.

Voor de toepassing van punt a) ronden centrale tegenpartijen "einde dag"-procedures en -betalingen onder alle omstandigheden af op het daartoe vereiste tijdstip en de daartoe vereiste dag.

Voor de toepassing van punt c), i), bieden de in dat punt bedoelde afspraken een oplossing voor de beschikbaarheid van afdoende personele middelen, de maximale uitvaltijd van kritieke functies, en failover en herstel op een secundaire locatie.

Voor de toepassing van punt c), ii), heeft de in dat punt bedoelde secundaire verwerkingslocatie een geografisch risicoprofiel dat verschilt van dat van de primaire locatie.

3. Naast de in lid 1 bedoelde vereisten zien centrale effectenbewaarinstellingen erop toe dat hun beleid voor ICT-bedrijfscontinuïteit:

a) rekening houdt met verbanden met en onderlinge afhankelijkheden van gebruikers, leveranciers van kritieke voorzieningen en diensten, andere centrale effectenbewaarinstellingen en andere marktinfrastructuren;

b) voorschrijft dat haar afspraken inzake ICT-bedrijfscontinuïteit ervoor zorgen dat de hersteltijddoelstelling voor hun kritieke of belangrijke functies maximaal twee uur bedraagt.

4. Naast de in lid 1 bedoelde vereisten bewaken handelsplatformen dat hun beleid voor ICT-bedrijfscontinuïteit ervoor zorgt dat:

a) transacties kunnen worden hervat binnen of dicht bij twee uur na een verstorend incident;

b) de maximale hoeveelheid data die na een verstorend incident eventueel bij IT-diensten van het handelsplatform verloren gaat, dicht bij nul ligt.

Artikel 25

Testen van de ICT-bedrijfscontinuïteitsplannen

1. Bij het testen van de ICT-bedrijfscontinuïteitsplannen overeenkomstig artikel 11, lid 6, van Verordening (EU) 2022/2554, houden financiële entiteiten rekening met de bedrijfsimpactanalyse (BIA) en de ICT-risicobeoordeling van de financiële entiteit als bedoeld in artikel 3, lid 1, punt b), van deze verordening.

2. Financiële entiteiten beoordelen aan de hand van testen van hun in lid 1 bedoelde ICT-bedrijfscontinuïteitsplannen of deze in staat zijn de continuïteit van de kritieke of belangrijke functies van de financiële entiteit te verzekeren. Die testen:

a) worden uitgevoerd op basis van testscenario's die potentiële storingen simuleren, met inbegrip van een adequate reeks van zware, maar plausibele scenario's;

b) bevatten het testen van ICT-diensten die worden geleverd door derde aanbieders van ICT-diensten (in voorkomend geval);

c) bevatten, voor financiële entiteiten niet zijnde micro-ondernemingen als bedoeld in artikel 11, lid 6, tweede alinea, van Verordening (EU) 2022/2554, scenario's voor de overschakeling van primaire ICT-infrastructuur naar de redundante capaciteit, back-ups en redundante faciliteiten;

d) zijn opgezet om de aannames waarop de bedrijfscontinuïteitsplannen zijn gebaseerd, met inbegrip van governance-regelingen en crisiscommunicatieplannen, te bevragen;

e) bevatten procedures om na te gaan in hoeverre de medewerkers van financiële entiteiten, derde aanbieders van ICT-diensten, ICT-systemen en ICT-diensten een adequate respons kunnen bieden op de scenario's waarmee overeenkomstig artikel 26, lid 2, terdege is rekening gehouden.

Voor de toepassing van punt a) nemen financiële entiteiten bij het testen de scenario's op waarmee is rekening gehouden bij het opzetten van de bedrijfscontinuïteitsplannen.

Voor de toepassing van punt b) houden financiële entiteiten voldoende rekening met scenario's in verband met insolventie of falen van de derde aanbieders van ICT-diensten of in verband met politieke risico's in de jurisdicties van de derde aanbieders van ICT-diensten, voor zover relevant.

Voor de toepassing van punt c) wordt met het testen nagegaan of ten minste kritieke of belangrijke functies voor een voldoende periode kunnen worden geopereerd en of het normale functioneren kan worden hersteld.

3. Naast de in lid 2 bedoelde vereisten betrekken centrale tegenpartijen bij het testen van hun in lid 1 bedoelde ICT-bedrijfscontinuïteitsplannen:

a) clearingleden;

b) externe leveranciers;

c) relevante instellingen binnen de financiële infrastructuur waarmee centrale tegenpartijen volgens hun bedrijfscontinuïteitsbeleid banden van onderlinge afhankelijkheid blijken te hebben.

4. Naast de in lid 2 bedoelde vereisten betrekken centrale effectenbewaarinstellingen bij het testen van hun in lid 1 bedoelde ICT-bedrijfscontinuïteitsplannen, voor zover van toepassing:

a) gebruikers van de centrale effectenbewaarinstellingen;

b) leveranciers van kritieke voorzieningen en diensten;

c) andere centrale effectenbewaarinstellingen;

d) andere marktinfrastructuren;

e) andere instellingen waarmee centrale effectenbewaarinstellingen volgens hun bedrijfscontinuïteitsbeleid banden van onderlinge afhankelijkheid blijken te hebben.

5. Financiële entiteiten documenteren de uitkomsten van het in lid 1 bedoelde testen. Geconstateerde tekortkomingen die uit die tests naar voren komen, worden geanalyseerd, aangepakt en gemeld aan het leidinggevend orgaan.

Artikel 26

ICT-respons- en -herstelplannen

1. Bij het uitwerken van de in artikel 11, lid 3, van Verordening (EU) 2022/2554 bedoelde ICT-respons- en -herstelplannen houden financiële entiteiten rekening met de uitkomsten van de bedrijfsimpactanalyse (BIA) van de financiële entiteit. Die ICT-respons- en -herstelplannen:

a) specificeren de omstandigheden waarin die plannen worden geactiveerd of gedeactiveerd, en eventuele uitzonderingen voor die activering of deactivering;

b) beschrijven welke acties moeten worden ondernomen om beschikbaarheid, integriteit, continuïteit en herstel te garanderen van ten minste de ICT-systemen en -diensten die kritieke of belangrijke functies van de financiële entiteit ondersteunen;

c) zijn zodanig opgezet dat de hersteldoelstellingen van de operaties van de financiële entiteiten worden verwezenlijkt;

d) worden gedocumenteerd en beschikbaar gesteld aan de medewerkers die betrokken zijn bij de uitvoering van ICT-respons- en -herstelplannen, en zijn in noodgevallen gemakkelijk toegankelijk;

e) bevatten herstelopties voor zowel korte als lange termijn, met inbegrip van gedeeltelijk systeemherstel;

f) leggen de doelstellingen van de ICT-respons- en -herstelplannen vast en de voorwaarden om te verklaren dat die plannen met succes zijn uitgevoerd.

Voor de toepassing van punt d) leggen financiële entiteiten rollen en verantwoordelijkheden duidelijk vast.

2. De in lid 1 bedoelde ICT-respons- en -herstelplannen identificeren relevante scenario's, met inbegrip van scenario's van ernstige bedrijfsstoringen en een toegenomen kans op storingen. Die plannen ontwikkelen scenario's op basis van actuele informatie over dreigingen en lessons-learned van vorige bedrijfsstoringen. Financiële entiteiten houden terdege rekening met alle volgende scenario's:

a) cyberaanvallen en overschakelingen tussen de primaire ICT-infrastructuur en de redundante capaciteit, back-ups en redundante faciliteiten;

b) scenario's waarin de kwaliteit van de levering van een kritieke of belangrijke functie verslechtert tot een onacceptabel niveau of faalt, en houden terdege rekening met de potentiële impact van de insolventie, of andere vormen van falen, van relevante derde aanbieders van ICT-diensten;

c) gedeeltelijk of volledig falen van bedrijfslocaties, met inbegrip van kantoor- en bedrijfslocaties, en datacentra;

d) substantieel falen van ICT-assets of van de communicatie-infrastructuur;

e) de niet-beschikbaarheid van een kritiek aantal medewerkers of medewerkers belast met het verzekeren van de continuïteit van operaties;

f) impact van klimaatverandering en milieuaantasting in verband met gebeurtenissen, natuurrampen, pandemieën en fysieke aanvallen, met inbegrip van indringing en terreuraanvallen;

g) interne aanvallen;

h) politieke en maatschappelijke instabiliteit, onder meer, in voorkomend geval, in de jurisdictie van de derde aanbieder van ICT-diensten en de locatie waar de data worden opgeslagen en verwerkt;

i) algemene stroomstoringen.

3. Wanneer de primaire herstelmaatregelen misschien niet op de korte termijn haalbaar zijn vanwege de kosten, risico's, logistiek of onvoorziene omstandigheden, worden in de in lid 1 bedoelde ICT-respons- en -herstelplannen alternatieve opties overwogen.

4. Als onderdeel van de in lid 1 bedoelde ICT-respons- en -herstelplannen onderzoeken en implementeren financiële entiteiten continuïteitsmaatregelen die falen van derde aanbieders van ICT-diensten mitigeren voor ICT-diensten die kritieke of belangrijke functies van de financiële entiteit ondersteunen.

HOOFDSTUK V

Verslag over de evaluatie van het raamwerk voor ICT-risicobeheersing

Artikel 27

Format en inhoud van het verslag over de evaluatie van het raamwerk voor ICT-risicobeheersing

1. Financiële entiteiten dienen het in artikel 6, lid 5, van Verordening (EU) 2022/2554 bedoelde verslag over de evaluatie van het raamwerk voor ICT-risicobeheersing in elektronisch doorzoekbaar formaat in.

2. Financiële entiteiten nemen in het in lid 1 bedoelde verslag alle volgende informatie op:

a) een inleidend gedeelte dat:

   i) duidelijk de financiële entiteit identificeert waarop het verslag ziet, en, in voorkomend geval, haar groepsstructuur beschrijft;

   ii) de context van het verslag beschrijft in termen van aard, schaal en complexiteit van de diensten, activiteiten en operaties van de financiële entiteit, haar organisatie, geïdentificeerde kritieke functies, strategie, majeure lopende projecten of activiteiten, relaties, en haar afhankelijkheid van interne en gecontracteerde ICT-diensten en -systemen, of de implicaties die een totaal verlies van of ernstige degradatie van die systemen zou hebben in termen van kritieke of belangrijke functies en marktefficiëntie;

   iii) een overzicht geeft van de majeure wijzigingen van het raamwerk voor ICT-risicobeheersing sinds het vorige verslag werd ingediend;

   iv) een executive summary geeft van het actuele ICT-risicoprofiel en het ICT-risicoprofiel op kortere termijn, het dreigingslandschap, de beoordeelde doeltreffendheid van haar beheersmaatregelen en de security posture van de financiële entiteit;

b) de datum van goedkeuring van het verslag door het leidinggevend orgaan van de financiële entiteit;

c) een beschrijving van de reden voor de evaluatie van het raamwerk voor ICT-risicobeheersing overeenkomstig artikel 6, lid 5, van Verordening (EU) 2022/2554;

d) de begin- en einddatum van de evaluatieperiode;

e) een vermelding van de voor de evaluatie verantwoordelijke functie;

f) een beschrijving van de majeure wijzigingen en verbeteringen van het raamwerk voor ICT-risicobeheersing sinds de vorige evaluatie;

g) een overzicht van de bevindingen van de evaluatie en gedetailleerde analyse en beoordeling van de ernst van de zwakke punten, tekortkomingen en lacunes in het raamwerk voor ICT-risicobeheersing tijdens de evaluatieperiode;

h) een beschrijving van de maatregelen voor het aanpakken van de geconstateerde zwakke punten, tekortkomingen en lacunes, met inbegrip van alle volgende elementen:

   i) een overzicht van maatregelen genomen om geconstateerde zwakke punten, tekortkomingen en lacunes te verhelpen;

   ii) een verwachte datum voor de implementatie van de maatregelen en data wat betreft de interne controle op de implementatie, met inbegrip van informatie over de stand van uitvoering van de implementatie van die maatregelen per de datum waarop het verslag is opgesteld, waarbij, in voorkomend geval, wordt uitgelegd of er een risico bestaat dat termijnen misschien niet worden nageleefd;

   iii) te gebruiken tools en de identificatie van de functie verantwoordelijk voor het uitvoeren van de maatregelen, met nadere vermelding of het interne of externe tools en functies betreft;

   iv) een beschrijving van de impact van de in de maatregelen voorgenomen wijzigingen op de budgettaire, menselijke en materiële middelen van de financiële entiteit, met inbegrip van de middelen bestemd voor de implementatie van corrigerende maatregelen;

   v) informatie over het proces om de bevoegde autoriteit te informeren (in voorkomend geval);

   vi) wanneer er voor de geconstateerde zwakke punten, tekortkomingen of lacunes geen corrigerende maatregelen zijn: een nadere toelichting bij de criteria gebruikt voor het analyseren van de impact van die zwakke punten, tekortkomingen of lacunes, voor het evalueren van het betrokken ICT-restrisico, en bij de criteria gebruikt voor het accepteren van het betrokken restrisico;

i) informatie over geplande toekomstige evoluties van het raamwerk voor ICT-risicobeheersing;

j) conclusies van de evaluatie van het raamwerk voor ICT-risicobeheersing;

k) informatie over vorige evaluaties, met inbegrip van:

   i) een lijst van evaluaties tot op heden;

   ii) in voorkomend geval een stand van zaken voor de implementatie van de in het laatste verslag genoemde corrigerende maatregelen;

   iii) wanneer de in vorige evaluaties voorgestelde corrigerende maatregelen ondoeltreffend zijn gebleken of voor onverwachte uitdagingen hebben gezorgd: een beschrijving van de wijze waarop die corrigerende maatregelen zouden kunnen worden verbeterd, of van die onverwachte uitdagingen;

l) informatiebronnen die bij het opstellen van het verslag zijn gebruikt, met inbegrip van alle volgende elementen:

   i) voor financiële entiteiten niet zijnde micro-ondernemingen als bedoeld in artikel 6, lid 6, van Verordening (EU) 2022/2554: de uitkomsten van interne audits;

   ii) de uitkomsten van compliancebeoordelingen;

   iii) uitkomsten van tests op digitale operationele weerbaarheid en, in voorkomend geval, de uitkomsten van geavanceerde tests, op basis van Threat-Led Penetration Testing (TLPT), van ICT-tools, -systemen en -processen;

   iv) externe bronnen.

Voor de toepassing van punt c) bevat het verslag, wanneer de evaluatie er kwam op instructie van toezichthouders of als gevolg van conclusies uit de betrokken tests of auditprocessen voor digitale operationele weerbaarheid, expliciete verwijzingen naar die instructies of conclusies, waarmee de reden voor het opstarten van de evaluatie kan worden geïdentificeerd. Wanneer de evaluatie er kwam na ICT-incidenten, bevat het verslag de lijst met alle ICT-incidenten met een Root Cause Analysis (RCA) van de incidenten.

Voor de toepassing van punt f) bevat de beschrijving een analyse van de impact van de wijzigingen op de strategie voor digitale operationele weerbaarheid van de financiële entiteit, op haar interne-controleraamwerk voor ICT en op haar governance voor ICT-risicobeheersing.

TITEL III

VEREENVOUDIGD RAAMWERK VOOR ICT-RISICOBEHEERSING VOOR IN ARTIKEL 16, LID 1, VAN VERORDENING (EU) 2022/2554 BEDOELDE FINANCIËLE ENTITEITEN

HOOFDSTUK I

Vereenvoudigd raamwerk voor ICT-risicobeheersing

Artikel 28

Governance en organisatie

1. De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten beschikken over een raamwerk voor interne governance en controle dat zorgt voor een effectieve en prudente beheersing van ICT-risico, om een hoge mate van digitale operationele weerbaarheid te bereiken.

2. De in lid 1 bedoelde financiële entiteiten zorgen, als onderdeel van hun vereenvoudigde raamwerk voor ICT-risicobeheersing, ervoor dat hun leidinggevend orgaan:

a) de algemene verantwoordelijkheid draagt om ervoor te zorgen dat met het vereenvoudigde raamwerk voor ICT-risicobeheersing de zakelijke strategie van de financiële entiteit in overeenstemming met de risicobereidheid van die financiële entiteit wordt verwezenlijkt, en ervoor zorgt dat ICT-risico binnen die context wordt bezien;

b) duidelijke taken en verantwoordelijkheden vaststelt voor alle ICT-functies;

c) informatie over beveiligingsdoelstellingen en ICT-vereisten vaststelt;

d) goedkeurt, overziet en periodiek evalueert:

   i) de classificatie van informatieassets van de financiële entiteit als bedoeld in artikel 30, lid 1, van deze verordening, de lijst van de belangrijkste geïdentificeerde risico's en de bedrijfsimpactanalyse (BIA) en de daarmee samenhangende beleidslijnen;

   ii) de in artikel 16, lid 1, punt f), van Verordening (EU) 2022/2554 bedoelde bedrijfscontinuïteitsplannen van de financiële entiteit en respons- en herstelmaatregelen;

e) ten minste eenmaal per jaar het budget toekent en evalueert dat noodzakelijk is om te voldoen aan de behoeften inzake digitale operationele weerbaarheid van de financiële entiteit met betrekking tot alle soorten middelen, waaronder relevante bewustmakingsprogramma's op het gebied van ICT-beveiliging, opleidingen inzake digitale operationele weerbaarheid en ICT-vaardigheden voor alle medewerkers;

f) de in de hoofdstukken I, II en III van deze titel opgenomen beleidslijnen en maatregelen specificeert en implementeert om het ICT-risico waaraan de financiële entiteit is blootgesteld, te identificeren, te beoordelen en te beheersen;

g) procedures, ITC-protocollen en tools identificeert en implementeert die noodzakelijk zijn om alle informatieassets en ICT-assets te beschermen;

h) bewaakt dat de medewerkers van de financiële entiteit door voldoende kennis en vaardigheden op de hoogte blijven om ICT-risico en de impact daarvan op de operaties van de financiële entiteit te begrijpen en te beoordelen, op een wijze die in verhouding staat tot het te beheersen ICT-risico;

i) rapportageregelingen vaststelt, met inbegrip van de frequentie, de vorm en de inhoud van de rapportage aan het leidinggevend orgaan over de informatiebeveiliging en de digitale operationele weerbaarheid.

3. De in lid 1 bedoelde financiële entiteiten kunnen, in overeenstemming met Unie- en nationaal sectoraal recht, de verificatietaken wat betreft naleving van de vereisten op het gebied van ICT-risicobeheersing uitbesteden aan intragroeps- of derde aanbieders van ICT-diensten. In het geval van een dergelijke uitbesteding blijven de financiële entiteiten volledig verantwoordelijk voor de controle op de naleving van de vereisten inzake ICT-risicobeheersing.

4. De in lid 1 bedoelde financiële entiteiten zorgen voor een adequate scheiding en de onafhankelijkheid van controlefuncties en interne auditfuncties.

5. De in lid 1 bedoelde financiële entiteiten bewaken dat voor hun vereenvoudigde raamwerk voor ICT-risicobeheersing interne audits door auditors plaatsvinden, in lijn met het auditplan van de financiële entiteiten. Deze auditors beschikken over voldoende kennis, vaardigheden en deskundigheid op het gebied van ICT-risico en zijn onafhankelijk. De frequentie en de focus van de ICT-audits staan in verhouding tot het ICT-risico van de financiële entiteit.

6. Op basis van de uitkomst van de in lid 5 bedoelde audit zorgen de in lid 1 bedoelde financiële entiteiten voor de tijdige controle op en remediëring van kritieke bevindingen van ICT-audits.

Artikel 29

Beleid en maatregelen voor informatiebeveiliging

1. De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten ontwikkelen, documenteren en implementeren een beleid voor informatiebeveiliging binnen de context van het vereenvoudigde raamwerk voor ICT-risicobeheersing. Dat beleid voor informatiebeveiliging legt op hoofdlijnen beginselen en regels vast ter bescherming van de vertrouwelijkheid, integriteit, beschikbaarheid en authenticiteit van gegevens en van de diensten die deze financiële entiteiten aanbieden.

2. Op basis van het in lid 1 bedoelde beleid voor informatiebeveiliging bepalen en implementeren de in lid 1 bedoelde financiële entiteiten ICT-beveiligingsmaatregelen die hun blootstelling aan ICT-risico moeten mitigeren, met inbegrip van mitigerende maatregelen die worden geïmplementeerd door derde aanbieders van ICT-diensten.

De ICT-beveiligingsmaatregelen omvatten alle in de artikelen 30 tot en met 38 bedoelde maatregelen.

Artikel 30

Classificatie van informatieassets en ICT-assets

1. Als onderdeel van het in artikel 16, lid 1, punt a), van Verordening (EU) 2022/2554 bedoelde vereenvoudigde raamwerk voor ICT-risicobeheersing identificeren, classificeren en documenteren de in lid 1 van dat artikel bedoelde financiële entiteiten alle kritieke of belangrijke functies, de informatieassets en ICT-assets die deze ondersteunen en hun onderlinge afhankelijkheden. Financiële entiteiten evalueren die identificatie en classificatie waar nodig.

2. De in lid 1 bedoelde financiële entiteiten brengen alle kritieke of belangrijke functies die door derde aanbieders van ICT-diensten worden ondersteund, in kaart.

Artikel 31

ICT-risicobeheersing

1. De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten nemen in hun vereenvoudigde raamwerk voor ICT-risicobeheersing alle volgende elementen op:

a) een bepaling van de risicotolerantieniveaus voor ICT-risico, in overeenstemming met de risicobereidheid van de financiële entiteit;

b) de identificatie en beoordeling van de ICT-risico's waaraan de financiële entiteit is blootgesteld;

c) de specificatie van strategieën voor het mitigeren van ten minste de ICT-risico's die niet binnen de risicotolerantieniveaus van de financiële entiteit vallen;

d) de monitoring van de doeltreffendheid van de in punt c) bedoelde mitigatiestrategieën;

e) de identificatie en beoordeling van ICT- en informatiebeveiligingsrisico's als gevolg van majeure wijzigingen in ICT-systemen of ICT-diensten, -processen of -procedures en van uitkomsten van tests van de ICT-beveiliging en na majeure ICT-incidenten.

2. De in lid 1 bedoelde financiële entiteiten voeren de ICT-risicobeoordeling periodiek uit en documenteren deze, op een wijze die in verhouding staat tot het ICT-risicoprofiel van de financiële entiteiten.

3. De in lid 1 bedoelde financiële entiteiten monitoren doorlopend dreigingen en kwetsbaarheden die relevant zijn voor hun kritieke of belangrijke functies, en informatieassets en ICT-assets, en zij evalueren op regelmatige basis de risicoscenario's die een impact hebben op die kritieke of belangrijke functies.

4. De in lid 1 bedoelde financiële entiteiten stellen alarmdrempels en -criteria vast voor het activeren en initiëren van processen voor ICT-incidentrespons.

Artikel 32

Fysieke beveiliging en milieubeveiliging

1. De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten identificeren en implementeren maatregelen voor fysieke beveiliging die zijn vormgegeven op basis van het dreigingslandschap en in overeenstemming met de in artikel 30, lid 1, van deze verordening bedoelde classificatie, het algemene risicoprofiel van ICT-assets en toegankelijke informatieassets.

2. De in lid 1 bedoelde maatregelen beschermen de bedrijfslocaties van financiële entiteiten en, in voorkomend geval, datacentra van financiële entiteiten waar ICT-assets en informatieassets zijn ondergebracht, tegen ongeautoriseerde toegang, aanvallen en ongevallen en tegen milieudreigingen en -gevaren.

3. De bescherming tegen milieudreigingen en -gevaren staat in verhouding tot het belang van de betrokken bedrijfslocaties en, in voorkomend geval, datacentra en het kritieke karakter van de operaties of ICT-systemen die daarin zijn ondergebracht.

HOOFDSTUK II

Verdere elementen van systemen, protocollen en tools om de impact van ICT-risico zoveel mogelijk te beperken

Artikel 33

Toegangscontrole

De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten ontwikkelen, documenteren en implementeren procedures voor de controle op logische en fysieke toegang en handhaven en monitoren die procedures en evalueren deze periodiek. Die procedures bevatten de volgende elementen van controle op logische en fysieke toegang:

a) toegangsrechten tot informatieassets, ICT-assets en de daardoor ondersteunde functies en tot kritieke operationele locaties van de financiële entiteit, worden beheerd op need-to-know-, need-to-use- en least-privilege-basis, ook voor remote access en emergency access;

b) verantwoordingsplicht van gebruikers, waardoor gebruikers kunnen worden geïdentificeerd voor de in de ICT-systemen uitgevoerde acties;

c) procedures voor accountbeheer om toegangsrechten voor gebruikers en generieke accounts, daaronder begrepen generieke administrator accounts, toe te kennen, te wijzigen of in te trekken;

d) authenticatiemethoden die in verhouding staan tot de in artikel 30, lid 1, bedoelde classificatie en tot het algemene risicoprofiel van ICT-assets, en die op maatgevende praktijken zijn gebaseerd;

e) toegangsrechten worden periodiek geëvalueerd en worden ingetrokken wanneer deze niet langer vereist zijn.

Voor de toepassing van punt c) kent de financiële entiteit voor alle ICT-assets privileged, emergency en administrator access toe op een need-to-use- of een ad-hocbasis, en deze toegang wordt overeenkomstig artikel 34, eerste alinea, punt f), gelogd.

Voor de toepassing van punt d) gebruiken financiële entiteiten sterke authenticatiemethoden die gebaseerd zijn op maatgevende praktijken voor remote access tot het netwerk van de financiële entiteiten, voor privileged access en voor toegang tot ICT-assets waarmee kritieke of belangrijke functies worden ondersteund die publiek beschikbaar zijn.

Artikel 34

Beveiliging ICT-operaties

De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten doen, als onderdeel van hun systemen, protocollen en tools, en voor alle ICT-assets het volgende:

a) zij monitoren en beheersen de levenscyclus van alle ICT-assets;

b) zij monitoren of de ICT-assets worden ondersteund door derde aanbieders van ICT-diensten van financiële entiteiten (in voorkomend geval);

c) zij identificeren capaciteitsvereisten van hun ICT-assets en maatregelen om de beschikbaarheid en efficiëntie van ICT-systemen in stand te houden en te verbeteren, en voorkomen tekorten aan ICT-capaciteit voordat deze zich voordoen;

d) zij voeren geautomatiseerde kwetsbaarheidsscans en beoordelingen van ICT-assets uit die in verhouding staan tot de in artikel 30, lid 1, bedoelde classificatie daarvan en tot het algemene risicoprofiel van het ICT-asset, en rollen patches uit om geconstateerde kwetsbaarheden te verhelpen;

e) zij beheersen de risico's verbonden aan verouderde, niet-ondersteunde of legacy ICT-assets;

f) zij loggen events met betrekking tot logische en fysieke toegangscontrole, ICT-operaties, met inbegrip van systeemactiviteiten en netwerkverkeer, en ICT-wijzigingsbeheer;

g) zij identificeren en implementeren maatregelen om informatie over afwijkende activiteiten en gedragingen te monitoren en te analyseren voor kritieke of belangrijke ICT-operaties:

h) zij implementeren maatregelen om relevante en actuele informatie over cyberdreigingen te monitoren;

i) zij implementeren maatregelen voor het identificeren van mogelijke informatielekken, malware en andere beveiligingsdreigingen, en publiek bekende kwetsbaarheden van software en hardware, en controleren op de beschikbaarheid van overeenkomstige nieuwe beveiligingsupdates.

Voor de toepassing van punt f) stemmen financiële entiteiten de mate van detail van de logs af op het doel ervan en het gebruik van het ICT-asset dat deze logbestanden genereert.

Artikel 35

Gegevens-, systeem- en netwerkbeveiliging

De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten ontwikkelen en implementeren, als onderdeel van hun systemen, protocollen en tools, beschermingsmaatregelen die netwerken beveiligen tegen indringing en gegevensmisbruik en die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens veiligstellen. Met name zetten financiële entiteiten, rekening houdende met de in artikel 30, lid 1, van deze verordening bedoelde classificatie, al het volgende op:

a) de identificatie en implementatie van maatregelen om data in gebruik, in transit en in rust te beschermen;

b) de identificatie en implementatie van beveiligingsmaatregelen wat betreft het gebruik van software, media voor gegevensopslag, systemen en endpoint-apparaten die gegevens van de financiële entiteit overdragen en opslaan;

c) de identificatie en implementatie van maatregelen om ongeautoriseerde verbindingen met het netwerk van de financiële entiteit te voorkomen en te detecteren en om het netwerkverkeer te beveiligen tussen de interne netwerken van de financiële entiteit en het internet en andere externe verbindingen;

d) de identificatie en implementatie van maatregelen die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens tijdens netwerktransmissies veiligstellen;

e) een proces om veilig gegevens te wissen die aanwezig zijn op bedrijfslocaties van de financiële entiteit of die extern zijn opgeslagen, en die financiële entiteit niet langer hoeft te verzamelen of op te slaan;

f) een proces om apparaten voor gegevensopslag die aanwezig zijn op bedrijfslocaties of die extern zijn opgeslagen en vertrouwelijke informatie bevatten, af te voeren of te ontmantelen;

g) de identificatie en implementatie van maatregelen die moeten voorkomen dat thuiswerk en het gebruik van privé endpoint-apparaten een negatieve impact hebben op de mogelijkheden van de financiële entiteit om haar kritieke activiteiten adequaat, tijdig en veilig uit te voeren.

Artikel 36

Testen ICT-beveiliging

1. De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten formuleren en implementeren een testplan voor ICT-beveiliging om de doeltreffendheid te valideren van hun ICT-beveiligingsmaatregelen die zijn ontwikkeld in overeenstemming met de artikelen 33, 34 en 35 en de artikelen 37 en 38 van die verordening. Financiële entiteiten bewaken dat in dit plan rekening wordt gehouden met dreigingen en kwetsbaarheden die in kaart zijn gebracht als onderdeel van het in artikel 31 van deze verordening bedoelde vereenvoudigde raamwerk voor ICT-risicobeheersing.

2. De in lid 1 bedoelde financiële entiteiten evalueren, beoordelen en testen ICT-beveiligingsmaatregelen, rekening houdende met het algemene risicoprofiel van de ICT-assets van de financiële entiteit.

3. De in lid 1 bedoelde financiële entiteiten monitoren en evalueren de uitkomsten van de beveiligingstest en actualiseren hun beveiligingsmaatregelen dienovereenkomstig, onverwijld in het geval van ICT-systemen die kritieke of belangrijke functies ondersteunen.

Artikel 37

Aanschaf, ontwikkeling en onderhoud van ICT-systemen

De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten richten, waar passend, voor aanschaf, ontwikkeling en onderhoud van ICT-systemen volgens een risicogebaseerde benadering een procedure in en implementeren die. Die procedure:

a) borgt dat, voordat de aanschaf of ontwikkeling van ICT-systemen plaatsvindt, de functionele en niet-functionele vereisten, met inbegrip van de vereisten inzake informatiebeveiliging, duidelijk zijn gespecificeerd en goedgekeurd door de betrokken bedrijfsfunctie;

b) borgt dat ICT-systemen worden getest en goedgekeurd voordat zij voor het eerst worden gebruikt en voordat wijzigingen worden aangebracht in de productieomgeving;

c) identificeert maatregelen om het risico te mitigeren van onbedoelde wijziging of bedoelde manipulatie van de ICT-systemen tijdens ontwikkeling en uitrol van die ICT-systemen in de productieomgeving.

Artikel 38

ICT-projectmanagement en ICT-wijzigingsbeheer

1. De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten ontwikkelen, documenteren en implementeren een procedure voor ICT-projectmanagement en specificeren de rollen en verantwoordelijkheden voor de implementatie daarvan. Die procedure omvat alle stadia van de ICT-projecten — van het initiëren tot het afsluiten ervan.

2. De in lid 1 bedoelde financiële entiteiten ontwikkelen, documenteren en implementeren een procedure voor ICT-wijzigingsbeheer die ervoor zorgt dat alle wijzigingen in ICT-systemen op een beheerste wijze worden vastgelegd, getest, beoordeeld, goedgekeurd, geïmplementeerd en geverifieerd en dat deze adequate beveiligingsmaatregelen bevatten om de digitale operationele weerbaarheid van de financiële entiteit veilig te stellen.

HOOFDSTUK III

Beheer ICT-bedrijfscontinuïteit

Artikel 39

Onderdelen van het ICT-bedrijfscontinuïteitsplan

1. De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten formuleren hun ICT-bedrijfscontinuïteitsplannen rekening houdende met de uitkomsten van de analyse van hun blootstellingen aan en de potentiële impact van zware bedrijfsstoringen en scenario's waaraan hun ICT-assets die kritieke of belangrijke functies ondersteunen, kunnen worden blootgesteld, met inbegrip van een scenario van een cyberaanval.

2. De in lid 1 bedoelde ICT-bedrijfscontinuïteitsplannen:

a) worden goedgekeurd door het leidinggevend orgaan van de financiële entiteit;

b) worden gedocumenteerd en zijn gemakkelijk toegankelijk in noodgevallen of bij een crisis;

c) wijzen voldoende middelen toe voor de uitvoering ervan;

d) bevatten geplande herstelniveaus en tijdskaders voor herstel en hervatting van functies en belangrijkste interne en externe afhankelijkheden, met inbegrip van derde aanbieders van ICT-diensten;

e) identificeren de omstandigheden die de activering van de ICT-bedrijfscontinuïteitsplannen op gang kunnen brengen, en welke acties moeten worden ondernomen om de beschikbaarheid, de continuïteit en het herstel te verzekeren van ICT-assets van de financiële entiteiten die kritieke of belangrijke functies ondersteunen;

f) identificeren de maatregelen voor het terugzetten en herstellen van kritieke of belangrijke bedrijfsfuncties, ondersteunende processen, informatieassets en hun onderlinge afhankelijkheden, om ongunstige effecten op het functioneren van de financiële entiteiten te vermijden;

g) identificeren back-upprocedures en -maatregelen die de scope specificeren van de gegevens waarop die back-up ziet, en de minimale back-upfrequentie, op basis van het kritieke karakter van de functie die van deze gegevens gebruikmaakt;

h) overwegen alternatieve opties wanneer herstel op korte termijn niet doenbaar is vanwege kosten, risico's, logistiek of onverwachte omstandigheden;

i) specificeren de regelingen voor interne en externe communicatie, met inbegrip van escalatieplannen;

j) worden geactualiseerd in lijn met lessen getrokken uit incidenten, tests, nieuwe risico's en geconstateerde dreigingen, gewijzigde hersteldoelstellingen, majeure wijzigingen in de organisatie van de financiële entiteit en in de ICT-assets die kritieke of bedrijfsfuncties ondersteunen.

Voor de toepassing van punt f) voorzien de in dat punt bedoelde maatregelen in de mitigatie van falen van kritieke derde aanbieders.

Artikel 40

Testen van de ICT-bedrijfscontinuïteitsplannen

1. De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten testen hun in artikel 39 van deze verordening bedoelde bedrijfscontinuïteitsplannen, met inbegrip van de in dat artikel bedoelde scenario's, ten minste jaarlijks op back-up- en herstelprocedures, of bij iedere majeure wijziging van het bedrijfscontinuïteitsplan.

2. Het in lid 1 bedoelde testen van bedrijfscontinuïteitsplannen toont aan dat de in dat lid bedoelde financiële entiteiten in staat zijn de levensvatbaarheid van hun bedrijfsactiviteiten in stand te houden totdat kritieke operaties zijn hersteld, en brengt tekortkomingen in die plannen in kaart.

3. De in lid 1 bedoelde financiële entiteiten documenteren de uitkomsten van het testen van bedrijfscontinuïteitsplannen en bij die tests geconstateerde tekortkomingen worden geanalyseerd, aangepakt en gerapporteerd aan het leidinggevend orgaan.

HOOFSTUK IV

Verslag over de evaluatie van het vereenvoudigde raamwerk inzake ICT-risicobeheersing

Artikel 41

Format en inhoud van het verslag over de evaluatie van het vereenvoudigde raamwerk voor ICT-risicobeheersing

1. De in artikel 16, lid 1, van Verordening (EU) 2022/2554 bedoelde financiële entiteiten dienen het verslag over de evaluatie van het in lid 2 van dat artikel bedoelde vereenvoudigde raamwerk voor ICT-risicobeheersing in elektronisch doorzoekbaar formaat in.

2. Het in lid 1 bedoelde verslag omvat alle volgende informatie:

a) een inleidend gedeelte met:

   i) een beschrijving van de context van het verslag in termen van aard, schaal en complexiteit van de diensten, activiteiten en operaties van de financiële entiteit, de organisatie van de financiële entiteit, geïdentificeerde kritieke functies, strategie, majeure lopende projecten of activiteiten, en relaties, en de afhankelijkheid van de financiële entiteit van interne en uitbestede ICT-diensten en -systemen, of de implicaties die een totaal verlies of ernstige degradatie van die systemen zou hebben voor kritieke of belangrijke functies en voor marktefficiëntie;

   ii) een executive summary van het geïdentificeerde actuele ICT-risico en ICT-risico op kortere termijn, het dreigingslandschap, de beoordeelde doeltreffendheid van haar beheersmaatregelen en de security posture van de financiële entiteit;

   iii) informatie over het betrokken onderdeel van het verslag;

   iv) een overzicht van de majeure wijzigingen van het raamwerk voor ICT-risicobeheersing sinds het vorige verslag;

   v) een overzicht en beschrijving van de impact van de majeure wijzigingen van het raamwerk voor ICT-risicobeheersing sinds het vorige verslag;

b) (in voorkomend geval) de datum van goedkeuring van het verslag door het leidinggevend orgaan van de financiële entiteit;

c) een beschrijving van de redenen voor de evaluatie, met inbegrip van:

   i) wanneer de evaluatie er kwam op instructie van toezichthouders: bewijs voor die instructies;

   ii) wanneer de evaluatie er kwam na ICT-incidenten: de lijst van al die ICT-incidenten met de daarbij behorende Root Cause Analysis (RCA) van de incidenten;

d) de begin- en einddatum van de evaluatieperiode;

e) de voor de evaluatie verantwoordelijke persoon;

f) een overzicht van de bevindingen en een zelfbeoordeling van de ernst van de zwakke punten, tekortkomingen en lacunes die in het raamwerk voor ICT-risicobeheersing zijn geconstateerd voor de evaluatieperiode, met inbegrip van een gedetailleerde analyse daarvan;

g) geïdentificeerde remediërende maatregelen om zwakke punten, tekortkomingen en lacunes in het vereenvoudigde raamwerk voor ICT-risicobeheersing aan te pakken, en de verwachte datum voor de implementatie van die maatregelen, met inbegrip van de follow-up van zwakke punten, tekortkomingen en lacunes die in vroegere verslagen zijn geïdentificeerd, wanneer die zwakke punten, tekortkomingen en lacunes nog niet zijn geremedieerd;

h) algemene conclusies over de evaluatie van het vereenvoudigde raamwerk voor ICT-risicobeheersing, met inbegrip van verdere geplande ontwikkelingen.

TITEL IV

SLOTBEPALINGEN

Artikel 42

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 13 maart 2024.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN