HelloID bijdrage aan DORA compliancy van klantorganisaties

Deze checklist toont hoe de HelloID dienstverlening bijdraagt aan het DORA compliant maken van klantorganisaties. De checklist richt zich dus specifiek op DORA verplichtingen bij klanten waaraan HelloID een bijdrage kan leveren. De checklist is opgesteld aan de hand van de artikelen in de DORA verordening (EU verordening 2022/2554) én de bijbehorende gedelegeerde verordening (gedelegeerde EU verordening 2024/1774). Alleen die artikelen zijn opgenomen in de checklist waarin HelloID een bijdrage kan leveren.

Let op: De checklist is dus géén volledige compliancylijst van de HelloID dienstverlening zelf. Tools4ever is binnen het DORA kader een aanbieder van ICT-diensten. Tools4ever en de HelloID dienstverlening zijn daarom ingericht om te voldoen aan de daarvoor geldende eisen.

VERORDENING (EU) 2022/2554 VAN HET EUROPEES PARLEMENT EN DE RAAD

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

Hfst I Algemene bepalingen

Art. 1	Onderwerp	n.v.t.
Art. 2	Toepassingsgebied	n.v.t.
Art. 3	Definities	n.v.t.
Art. 4	Evenredigheids-beginsel	n.v.t.

Hfst II ICT-risicobeheer

Afdeling I

Art. 5	Governance en organisatie	Binnen het ICT-risicobeheer verzorgt HelloID het toegangsbeheer tot systemen en gegevens binnen organisaties. Het platform genereert logs en informatie ten behoeve van analyses, rapportages en audits. ***Daarnaast is er een ruime set aan governance tools om individueel verstrekte rechten regelmatig planmatig te opnieuw te beoordelen, de uitgifte van conflicterende rechten te voorkomen, inconsistenties tussen de IAM-registratie en doelsystemen te detecteren, en het account- en rechtenbeheer periodiek te evalueren, actualiseren en verbeteren.***

Afdeling II

Art. 6	Kader voor ICT-risicobeheer	Binnen het ICT-risicobeheer, borgt HelloID het toegangsbeheer tot systemen en gegevens binnen organisaties. HelloID user provisioning automatiseert de uitgifte en het beheer van accounts en toegangsrechten voor gebruikers. Aanvullend kunnen individuele toegangsrechten worden verstrekt en beheerd met behulp van service automation en self-service. Voor het real-time access management kan HelloID gebruik maken van separate identity providers (IdP) zoals Active Directory of Entra ID, maar het platform beschikt ook over een ingebouwde IdP. HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits. ***Daarnaast is er een ruime set aan governance tools om individueel verstrekte rechten regelmatig planmatig te opnieuw te beoordelen, de uitgifte van conflicterende rechten te voorkomen, inconsistenties tussen de IAM-registratie en doelsystemen te detecteren, en het account- en rechtenbeheer periodiek te evalueren, actualiseren en verbeteren.***
Art. 7	ICT-systemen, -protocollen en -instrumenten	n.v.t.
Art. 8	Identificatie	HelloID biedt altijd een actueel overzicht van verstrekte accounts en rechten, inclusief de formele rol (functie, afdeling etc.) van de betreffende medewerker. ***Daarnaast kunnen governance functies zoals reconciliation en role mining inzicht geven in accounts en rechten die buiten HelloID om zijn verstrekt, bijvoorbeeld rechtstreeks door systeembeheerders. Dit helpt bij het inventariseren welke medewerkers in de praktijk welke systemen en gegevens gebruiken.***

Art. 9	Bescherming en voorkoming	HelloID beschermt de toegang tot systemen en gegevens binnen organisaties. Dit kan ook de fysieke toegangsbeveiliging omvatten, via koppelingen met fysieke toegangbeheersystemen. HelloID user provisioning automatiseert de uitgifte en het beheer van accounts en toegangsrechten voor gebruikers. Dit dekt de hele identity lifecycle af, vanaf iemands onboarding tot en met diens vertrek. Hierbij wordt gebruik gemaakt van Attribute Based Access Control, waarbij de actuele gegevens uit HR-applicaties en andere bronsystemen worden geraadpleegd om te bepalen welke IT-faciliteiten nodig zijn. Aanvullend kunnen individuele toegangsrechten worden verstrekt en beheerd met behulp van service automation en self-service. Via configureerbare workflows kunnen individuele verzoeken worden beoordeeld door hiervoor aangewezen functionaris(sen). Voor gebruikers authenticatie kan HelloID gebruik maken van separate identity providers (IdP) zoals Active Directory of Entra ID, maar het platform beschikt ook over een ingebouwde IdP. Deze ondersteunt Single Sign-On (SSO) en meerdere Multi-Factor Authenticatie (MFA) methodes, inclusief FIDO2-compliant hardware keys. HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits. ***Daarnaast is er een ruime set aan governance tools om individueel verstrekte rechten regelmatig planmatig te opnieuw te beoordelen, de uitgifte van conflicterende rechten te voorkomen, inconsistenties tussen de IAM-registratie en doelsystemen te detecteren, en het account- en rechtenbeheer periodiek te evalueren, actualiseren en verbeteren.***
Art. 10	Detectie	HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits. Alle binnen en door HelloID uitgevoerde acties worden opgeslagen in Elastic reporting met uitgebreide rapportage mogelijkheden. Dat omvat onder andere: - Provisioning: Naast een overzicht van alle businessrules (en wijzigingen), per systeem en gebruiker alle acties omtrent het creëren, enablen, updaten, verplaatsen, disablen, het verwijderen van accounts, en het toekennen en intrekken van permissies. - Service Automation met alle (self) service acties omtrent aanvragen, workflows, goedkeuringen, formulierdata en configuratiewijzigingen. Zo worden bij alle wijzigingen binnen HelloID vastgelegd wie deze heeft aangevraagd, welke persoon het verzoek heeft goedgekeurd en tot welke exacte wijzigingen in achterliggende systemen dit heeft geleid. - Access Management met alle succesvolle en mislukte aanmeldingen, de geografische locatie van de gebruiker, gebruikte apparaten, geïnitieerde wachtwoordresets, toegangspogingen voor applicaties en mislukte toegangspogingen als gevolg van het toegangsbeleid.

		Deze gegevens kunnen worden geanalyseerd om kwetsbaarheden te herkennen en problemen te voorkomen. Ook kunnen gegevens worden gedeeld met bijvoorbeeld SIEM (Security Information and Event Management) systemen. ***Met governance functies zoals reconciliation kunnen we inconsistenties tussen registraties in het IAM platform en de doelsystemen identificeren, en daarmee onder andere onbeheerde accounts en rechten accounts en rechten ontdekken.***
Art. 11	Respons en herstel	Alle informatie en logs (zie artikel 10) zijn uiteraard beschikbaar voor respons en herstelacties. HelloID beheert centraal accounts en permissies binnen de aangesloten doelsystemen. Ten behoeve van herstelacties kunnen deze instellingen opnieuw worden doorgevoerd in die systemen. ***Ook is reconciliation functionaliteit beschikbaar om inconsistenties te detecteren tussen het HelloID platform en de doelsystemen, en deze te herstellen.***
Art. 12	Back-upbeleid en -procedures, terugzettings- en herstelprocedures en -methoden	Alle informatie en logs (zie artikel 10) zijn uiteraard beschikbaar voor respons en herstelacties. HelloID beheert centraal accounts en permissies binnen de aangesloten doelsystemen. Ten behoeve van herstelacties kunnen deze instellingen opnieuw worden doorgevoerd in die systemen. ***Ook is reconciliation functionaliteit beschikbaar om inconsistenties te detecteren tussen het HelloID platform en de doelsystemen, en deze te herstellen.***
Art. 13	Scholing en ontwikkeling	n.v.t.
Art. 14	Communicatie	n.v.t.
Art. 15	Verdere harmonisatie van ICT-risicobeheersinstrumenten, -methoden, -processen en -beleidslijnen	Dit is uitgewerkt in een aanvullende verordening (EU) 2024/1774. Deze omvat onder andere aanvullende eisen en detaillering op het gebied van toegangsbeveiliging. Deze werken we hieronder apart uit.
Art. 16	Vereenvoudigd kader voor ICT-risicobeheer	Dit vereenvoudigde kader is uitgewerkt in een aanvullende verordening (EU) 2024/1774. Met betrekking tot het identiteits- en toegangsbeheer geldt dat HelloID de functionaliteit biedt zoals omschreven bij bovenstaande artikelen 5 t/m 15. Deze functionaliteit kan ook worden ingezet voor het vereenvoudigd kader voor risico-beheer.

Hfst III Beheer, classificatie en rapportage van ICT-gerelateerde incidenten

Art. 17	Beheerproces voor ICT-gerelateerde incidenten	Alle informatie en logs (zie artikel 10) zijn uiteraard beschikbaar voor respons en herstelacties. HelloID beheert centraal accounts en permissies binnen de aangesloten doelsystemen. Ten behoeve van herstelacties kunnen deze instellingen opnieuw worden doorgevoerd in die systemen. ***Ook is reconciliation functionaliteit beschikbaar om inconsistenties te detecteren tussen het HelloID platform en de doelsystemen, en deze te herstellen.***
Art. 18	Classificatie van ICT-gerelateerde incidenten en cyberdreigingen	n.v.t.
Art. 19	Rapportage van ernstige ICT-gerelateerde incidenten en vrijwillige melding van significante cyberdreigingen	n.v.t.
Art. 20	Harmonisatie van inhoud en modellen van rapportage	n.v.t.
Art. 21	Centralisatie van meldingen van ernstige ICT-gerelateerde incidenten	n.v.t.
Art. 22	Feedback van toezichthouders	n.v.t.
Art. 23	Betalingsgerelateerde operationele of beveiligingsincidenten die kredietinstellingen, betalingsinstellingen, aanbieders van rekeninginformatiediensten en instellingen voor elektronisch geld betreffen	n.v.t.

Hfst IV Testen van digitale operationele weerbaarheid

Art. 24	Algemene vereisten voor uitvoering van tests van digitale operationele weer-baarheid	n.v.t.
Art. 25	Testen van ICT-in-strumenten en -systemen	n.v.t.
Art. 26	Geavanceerde tests van ICT-instrumen-ten, -systemen en -processen op basis van TLPT	n.v.t.
Art. 27	Vereisten voor testers voor het uitvoeren van TLPT	n.v.t.

Hfst V Beheer van ICT-risico van derde aanbieders

Afdeling I Basisbeginselen voor een degelijk beheer van het ICT- risico van derde aanbieders

Art. 28	Algemene beginselen	n.v.t.
Art. 29	Voorlopige beoorde-ling van het ICT-con-centratierisico op het niveau van de entiteit	n.v.t.
Art. 30	Belangrijke contrac-tuele bepalingen	n.v.t.

Afdeling II Oversightkader voor kritieke derde aanbieders van ICT-diensten

Art. 31	Aanwijzing van kritieke derde aanbieders van ICT-diensten	n.v.t.
Art. 32	Structuur van het oversightkader	n.v.t.

Art. 33	Taken van de lead overseer	n.v.t.
Art. 34	Operationele coördinatie tussen de lead overseers	n.v.t.
Art. 35	Bevoegdheden van de lead overseer	n.v.t.
Art. 36	Uitoefening van de bevoegdheden van de lead overseer buiten de Unie	n.v.t.
Art. 37	Verzoek om informatie	n.v.t.
Art. 38	Algemene onderzoeken	n.v.t.
Art. 39	Inspecties	n.v.t.
Art. 40	Oversight tijdens de uitvoering	n.v.t.
Art. 41	Harmonisatie van de voorwaarden voor de uitoefening van de oversightactiviteiten	n.v.t.
Art. 42	Vervolgmaatregelen van de bevoegde autoriteiten	n.v.t.
Art. 43	Oversight-vergoedingen	n.v.t.
Art. 44	Internationale samenwerking	n.v.t.

Hfst VI Regelingen voor de uitwisseling van informatie

Art. 45	Regelingen voor uitwisseling van informatie en inlichtingen over cyberdreiging	n.v.t.

Hfst VII Bevoegde autoriteiten

Art. 46	Bevoegde autoriteiten	n.v.t.
Art. 47	Samenwerking met structuren en autoriteiten die zijn opgericht bij Richtlijn (EU) 2022/2555	n.v.t.
Art. 48	Samenwerking tussen autoriteiten	n.v.t.
Art. 49	Sectoroverschrijdende financiële oefeningen, communicatie en samenwerking	n.v.t.
Art. 50	Administratieve strafmaatregelen en corrigerende maatregelen	n.v.t.
Art. 51	Uitoefening van de bevoegdheid tot het nemen van administratieve strafmaatregelen en corrigerende maatregelen	n.v.t.
Art. 52	Strafrechtelijke maatregelen	n.v.t.
Art. 53	Kennisgevingsverplichting	n.v.t.
Art. 54	Bekendmaking van administratieve strafmaatregelen	n.v.t.
Art. 55	Beroepsgeheim	n.v.t.
Art. 56	Gegevensbescherming	n.v.t.

Hfst VIII Gedelegeerde handelingen

Art. 57	Uitoefening van de bevoegdheids-delegatie	n.v.t.

Hfst IX Overgangs- en slotbepalingen

Afdeling I

Art. 58	Evaluatieclausule	n.v.t.
Art. 59	Wijzigingen van Verordening (EG) nr. 1060/2009	n.v.t.
Art. 60	Wijzigingen van Verordening (EU) nr. 648/2012	n.v.t.
Art. 61	Wijzigingen van Verordening (EU) nr. 909/2014	n.v.t.
Art. 62	Wijzigingen van Verordening (EU) nr. 600/2014	n.v.t.
Art. 63	Wijziging van Verordening (EU) 2016/1011	n.v.t.
Art. 64	Inwerkingtreding en toepassing	n.v.t.

GEDELEGEERDE VERORDENING (EU) 2024/1774 VAN DE COMMISSIE (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

Titel I ALGEMENE BEGINSELEN

Art. 1	Algemeen risicoprofiel en complexiteit	n.v.t.

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

Hfst I Beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging

Afdeling 1

Art. 2	Algemene elementen van beleidslijnen, procedures, protocollen en tools voor ICT-beveiliging	Binnen het ICT-risicobeheer verzorgt HelloID het toegangsbeheer tot systemen en gegevens binnen organisaties. Het platform genereert logs en informatie ten behoeve van analyses, rapportages en audits. ***Daarnaast is er een ruime set aan governance tools om individueel verstrekte rechten regelmatig planmatig te opnieuw te beoordelen, de uitgifte van conflicterende rechten te voorkomen, inconsistenties tussen de IAM-registratie en doelsystemen te detecteren, en het account- en rechtenbeheer periodiek te evalueren, actualiseren en verbeteren.***

Afdeling 2

Art. 3	ICT-risicobeheersing	Met behulp van rapportages en informatie van het HelloID platform, kan het account- en rechtenbeheer als onderdeel van het risk management periodiek worden beoordeeld, aangepast en verbeterd. ***Hiervoor biedt HelloID ook aanvullende governance tools zoals reconsiliation en role mining.***

Afdeling 3 BEHEER ICT-ASSETS

Art. 4	Beleid voor het beheer van ICT-assets	n.v.t.
Art. 5	Procedure voor het beheer van ICT-assets	n.v.t.

Afdeling 4 ENCRYPTIE EN CRYPTOGRAFIE

Art. 6	Encryptie en cryptografische controles	n.v.t.

Art. 7	Beheer van crypto-grafische sleutels	n.v.t.

Afdeling 5 BEVEILIGING ICT-OPERATIES

Art. 8	Beleidslijnen en procedures voor ICT-operaties	n.v.t.
Art. 9	Capaciteits- en performancema-nagement	n.v.t.
Art. 10	Kwetsbaarheden-beheer en patch-management	HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits. dit is een belangrijk hulpmiddel bij het identi-ficeren en verhelpen van kwetsbaarheden. ***Daarbij helpen ook de governance tools om individueel verstrekte rechten regelmatig planmatig te opnieuw te beoordelen, de uitgifte van conflicterende rechten te voorkomen, inconsistenties tussen de IAM-registratie en doelsystemen te detecteren, en het account- en rechtenbeheer periodiek te evalueren, actualiseren en verbeteren.***
Art. 11	Gegevens- en systeembeveiliging	In het kader van de gegevens- en systeembeveiliging, verzorgt HelloID specifiek het toegangsbeheer tot systemen en gegevens binnen organisaties. HelloID ondersteunt de eisen op het gebied van de toegangsbeveiliging, zorgt dat gebruikers de maatregelen niet kunnen omzeilen of manipuleren, en voorkomt datalekken. Onder-deel hiervan is het bieden van veilige remote toegang door gebrui-kers .
Art. 12	Logging	HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits. Alle binnen en door HelloID uitgevoerde acties worden opgeslagen in Elastic reporting met uitgebreide rapportage mogelijkheden. Dat omvat onder andere: - Provisioning: Naast een overzicht van alle businessrules (en wijzi-gingen), per systeem en gebruiker alle acties omtrent het creëren, enablen, updaten, verplaatsen, disablen, het verwijderen van accounts, en het toekennen en intrekken van permissies. - Service Automation met alle (self) service acties omtrent aanvra-gen, workflows, goedkeuringen, formulierdata en configuratiewijzi-gingen. Zo worden bij alle wijzigingen binnen HelloID vastgelegd wie deze heeft aangevraagd, welke persoon het verzoek heeft goedge-keurd en tot welke exacte wijzigingen in achterliggende systemen dit heeft geleid.

		- Access Management met alle succesvolle en mislukte aanmeldingen, de geografische locatie van de gebruiker, gebruikte apparaten, geïnitieerde wachtwoordresets, toegangspogingen voor applicaties en mislukte toegangspogingen als gevolg van het toegangsbeleid. Deze gegevens kunnen worden geanalyseerd om kwetsbaarheden te herkennen en problemen te voorkomen. Ook kunnen gegevens worden gedeeld met bijvoorbeeld SIEM (Security Information and Event Management) systemen.

Afdeling 6 Netwerkbeveiliging

Art. 13	Beheer van netwerkbeveiliging	n.v.t.
Art. 14	Informatie in transit beveiligen	n.v.t.

Afdeling 7 ICT-projectmanagement en ICT-wijzigingsbeheer

Art. 15	ICT projectmanagement	n.v.t.
Art. 16	Aanschaf, ontwikkeling en onderhoud van ICT-systemen	n.v.t.
Art. 17	ICT-wijzigingsbeheer	n.v.t.

Afdeling 8

Art. 18	Fysieke beveiliging en milieubeveiliging	Via een koppeling tussen HelloID en beheersystemen van toegangspasjes kunnen ook fysieke toegangsrechten worden verstrekt en beheerd. De provisioning functionaliteit kan worden ingezet om toegangsrechten automatisch te verstrekken aan de hand van iemands functie/afdeling/locatie etc.

Chapter II Humanresourcesbeleid en toegangscontrole

Art. 19	Humanresources-beleid	HelloID ondersteunt de automatische uitgifte en beheer van accounts en rechten op basis van beleidsregels (business rules). Daarnaast kan worden geconfigureerd dat individuele verzoeken om IT-faciliteiten altijd worden beoordeeld door relevante managers via een configureerbare goedkeuringsflow. Hiermee is geborgd dat alleen rechten worden verstrekt die nodig zijn voor iemands taken en verantwoordelijkheden. Het platform beheert een 'identity lifecycle' waarmee ook aan het eind van een dienstverband rechten en faciliteiten van gebruikers weer tijdig kunnen worden ingetrokken.
Art. 20	Identiteitsbeheer	HelloID verstrekt persoonlijke accounts en rechten, op basis van gebruikersgegevens uit betrouwbare bronsystemen zoals HR-applicaties. Accounts en rechten worden zoveel mogelijk automatisch verstrekt aan de hand van attributen zoals iemands functie, afdeling etc. Hiermee beheert het platform een identity lifecycle waarin bij iedere verandering - functie, afdeling, locatie en dergelijke - automatisch ook de gebruikersaccounts en -rechten zonodig worden aangepast. Ook worden rechten tijdig ingetrokken als een medewerker de organisatie verlaat. Daarnaast worden individuele wijzigingsverzoeken aan de hand van goedkeuringsflows beoordeeld door de relevante functionaris(sen). Alle gebruikte beleidsregels, wijzigingen en wijzigingsverzoeken worden gelogd, inclusief de indiener, goedkeurende functionaris en behandelaar van het verzoek.
Art. 21	Toegangscontrole	HelloID beschermt de toegang tot systemen en gegevens binnen organisaties. Dit kan ook de fysieke toegangsbeveiliging omvatten, via koppelingen met fysieke toegangbeheersystemen. HelloID user provisioning automatiseert de uitgifte en het beheer van accounts en toegangsrechten voor gebruikers. Dit dekt de hele identity lifecycle af, vanaf iemands onboarding tot en met diens vertrek. Hierbij wordt gebruik gemaakt van Attribute Based Access Control, waarbij de actuele gegevens uit HR-applicaties en andere bronsystemen worden geraadpleegd, om te bepalen welke IT-faciliteiten nodig zijn op welk moment. Zelfs informatie uit roosterapplicaties kunnen zonodig als brongegevens worden ingezet. Met ABAC ondersteunt HelloID vanuit één plek de need-to-know, need-to-use en least-privilege principes. Het is ook een belangrijk hulpmiddel om rolscheiding te implementeren. Aanvullend kunnen individuele toegangsrechten worden verstrekt en beheerd met behulp van service automation en self-service. Via configureerbare workflows kunnen individuele ad hoc verzoeken worden beoordeeld door hiervoor aangewezen functionaris(sen). Voor gebruikers authenticatie kan HelloID gebruik maken van separate identity providers (IdP) zoals Active Directory of Entra ID, maar het platform beschikt ook over een ingebouwde IdP. Deze ondersteunt Single Sign-On (SSO) en meerdere Multi-Factor Authenticatie (MFA) methodes, inclusief FIDO2-compliant hardware keys. HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits.

		Daarnaast is er een ruime set aan governance tools om individueel verstrekte rechten regelmatig planmatig opnieuw te beoordelen, de uitgifte van conflicterende rechten te voorkomen, inconsistenties tussen de IAM-registratie en doelsystemen te detecteren, en het account- en rechtenbeheer periodiek te evalueren, actualiseren en te verbeteren.

Chapter III Detectie van en respons op ICT-incidenten

Art. 22	Beleid voor ICT-incidentmanagement	HelloID genereert logs en informatie ten behoeve van analyses, rapportages en audits (zie artikel 12). Deze gegevens kunnen worden geanalyseerd om kwetsbaarheden te herkennen en problemen te voorkomen. Ook kunnen gegevens worden gedeeld met bijvoorbeeld SIEM (Security Information and Event Management) systemen. ***Met governance functies zoals reconciliation kunnen we inconsistenties tussen registraties in het IAM platform en de doelsystemen identificeren, en daarmee onder andere onbeheerde accounts en rechten accounts en rechten ontdekken.***
Art. 23	Detectie van afwijkende activiteiten en criteria voor detectie van en respons op ICT-incidenten	Zie artikel 22

Chapter IV Beheer ICT-bedrijfscontinuïteit

Art. 24	Onderdelen van het beleid voor ICT-bedrijfscontinuïteit	Alle informatie en logs (zie artikel 22) zijn uiteraard beschikbaar voor respons en herstelacties. HelloID beheert centraal accounts en permissies binnen de aangesloten doelsystemen. Ten behoeve van herstelacties kunnen deze instellingen opnieuw worden doorgevoerd in die systemen. ***Ook is de reconciliation functionaliteit beschikbaar om inconsistenties te detecteren tussen het HelloID platform en de doelsystemen, en deze te herstellen.***
Art. 25	Testen van de ICT-bedrijfs-continuïteitsplannen	n.v.t.
Art. 26	ICT-respons- en -herstelplannen	Zie artikel 24

Chapter V Verslag over de evaluatie van het raamwerk voor ICT-risicobeheersing

Art. 27	Format en inhoud van het verslag over de evaluatie van het raamwerk voor ICT-risicobeheersing	n.v.t.

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

Chapter I Vereenvoudigd raamwerk voor ICT-risicobeheersing

Art. 28	Governance en organisatie	Als onderdeel van de vereiste functionaliteit om alle informatieassets en ICT-assets te beschermen, is identity en access management een belangrijk element. De HelloID functionaliteit zoals omschreven bij artikel 21, vult dit in.
Art. 29	Beleid en maatregelen voor informatiebeveiliging	De functionaliteit zoals beschreven in artikel 21, vult binnen dit beleid het identity en access management in.
Art. 30	Classificatie van informatieassets en ICT-assets	n.v.t.
Art. 31	ICT-risicobeheersing	De bijdrage van het HelloID platform aan de ICT-risicobeheersing is toegelicht bij artikel 3.
Art. 32	Fysieke beveiliging en milieubeveiliging	Het HelloID platform ondersteunt ook het beheer van fysieke toegangsbeveiliging, zoals omschreven bij artikel 18.

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

Art. 33	Toegangscontrole	De realisatie van toegangscontrole met behulp van het HelloID platform is uitgebreid uitgewerkt bij artikel 21.
Art. 34	Beveiliging ICT-operaties	De HelloID functionaliteit om specifiek events te loggen met betrekking tot logische en fysieke toegangscontrole, is omschreven bij artikel 12.
Art. 35	Gegevens-, systeem- en netwerkbeveiliging	HelloID richt zich hierbij specifiek op gegevens- en systeembeveiliging, zoals uitgebreid uitgewerkt bij artikel 21.

Art. 36	Testen ICT-beveiliging	n.v.t.
Art. 37	Aanschaf, ontwikkeling en onderhoud van ICT-systemen	n.v.t.
Art. 38	ICT-projectmanagement en ICT-wijzigingsbeheer	n.v.t.

Chapter III Beheer ICT-bedrijfscontinuïteit

Art. 39	Onderdelen van het ICT-bedrijfscontinuïteitsplan	De bijdrage van het HelloID platform aan het ICT-bedrijfscontinuïteitsplan is toegelicht bij artikel 24.
Art. 40	Testen van de ICT-bedrijfscontinuïteitsplannen	n.v.t.

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

Art. 41	Format en inhoud van het verslag over de evaluatie van het vereenvoudigde	n.v.t.

Titel IV SLOTBEPALINGEN

Art. 42	Inwerkingtreding	n.v.t.