

Dit document beschrijft hoe het HelloID Identity Management platform bijdraagt aan het ISO 27001, NEN 7510 en BIO compliant maken van klantorganisaties. Tools4ever is als ontwikkelaar van de IDaaS-oplossing HelloID volledig ISO 27001-gecertificeerd en daar richt dit document zich dus niet op. Deze checklist focust op hoe HelloID klantorganisaties ondersteunt bij het realiseren van de beveiligingsdoelstellingen en de bijbehorend maatregelen.

Voorbeeld: het role-based toegangsbeheer van HelloID vormt een centraal element in de toegangsbeveiliging van alle IT systemen binnen een klantorganisatie. Het feit dat HelloID back-ups maakt betekent enkel dat HelloID zelf aan de eisen voldoet.

A.5 Organisatorische beheersmaatregelen

A.5.1 Beleidsregels voor informatiebeveiliging Specifieke beleidsregels mbt de verstrekking van accounts en toegangsrechten op basis van gebruikersattributen (zoals functie, afdeling etc.) worden binnen HelloID eenduidig beheerd als business rules. HelloID vormt voor deze regels de Single Point of Truth. Optimalisatie van deze business rules wordt ondersteund met role mining functionaliteit.

A.5.3 Functiescheiding De verstrekking van accounts en toegangsrechten aan de hand van functies ondersteunt de implementatie van rolscheiding. Daarnaast kan men voor de verschillende self-service processen goedkeuringsprocedures inrichten met een duidelijke scheiding van taken. Met toxic policy management kan het verstrekken van conflicterende rechten worden voorkomen.

A.5.4 Managementverantwoordelijkheden Bij individueel verstrekte accounts en rechten kan via workflows worden geborgd dat de juiste managers de aanvraag beoordelen. Ook kunnen managers via delegated forms zelf eventueel rechten verstrekken aan eigen medewerkers. Recertification kan worden ingezet om eerder door managers aangevraagde of goedgekeurde licenties en rechten, planmatig opnieuw te laten beoordelen.

A.5.7 Informatie en analyses over dreigingen HelloID genereert logs en informatie die kunnen ondersteunen bij analyse van dreigingen: 1) Access Management inlogpogingen etc. 2) Provisioning business rules waarmee medewerkers aan accounts en rechten worden gekoppeld. 3) Service Automation logs van service-verzoeken, de afhandeling ervan en de status. Met 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.

- A.5.8** Informatiebeveiliging in projectmanagement
Service Automation ondersteunt de (tijdelijke) uitgifte van individuele accounts en toegangsrechten, bijvoorbeeld voor projecten. Daarbij is de goedkeuring door relevante functionarissen geborgd via configureerbare workflows. Recertification kan worden ingezet om eerder door managers aangevraagde of goedgekeurde individuele licenties en rechten, planmatig opnieuw te laten beoordelen.
- A.5.9** Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen
HelloID onderhoudt een registratie van gebruikers, beschikbare applicaties, data shares en de daarvoor verstrekte accounts en rechten. Met reconciliation kunnen we inconsistenties ontdekken en herstellen tussen deze inventarisatie binnen het IAM-platform en de aangesloten doelsystemen.
- A.5.10** Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen
De Provisioning module ondersteunt de automatische uitgifte en beheer van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast kunnen via Service Automation individuele toegangsrechten worden verstrekt en beheerd. Hierbij wordt de beoordeling van individuele verzoeken door relevante managers ondersteund met configureerbare workflows.
- A.5.11** Retourneren van bedrijfsmiddelen
HelloID verzorgt dat toegangsrechten en accounts automatisch worden gedeactiveerd en verwijderd bij beëindiging van het dienstverband, contract of overeenkomst. Ook kan het platform zorgen dat tijdig tickets worden aangemaakt in bijv. IT Service Management systemen voor het intrekken van fysieke bedrijfsmiddelen zoals laptops en telefoons.
- A.5.12** Classificeren van informatie
De via HelloID verstrekte en beheerde rechten kunnen afhankelijk zijn van specifieke gegevensklassen. De implementatie van deze fijnmazige toegang is afhankelijk het specifieke doelsysteem.
- A.5.14** Overdragen van informatie
De met HelloID verstrekte en beheerde toegangsrechten kunnen ook beperkingen bevatten mbt de overdracht van informatie. Ook ondersteunt het platform via de Access Management module extra authenticatie (Multi-Factor Authenticatie) om sommige rechten extra goed te beveiligen.
- A.5.15** Toegangsbeveiliging
De Provisioning module ondersteunt de automatische uitgifte en beheer van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast kunnen via Service Automation individuele toegangsrechten worden verstrekt en beheerd. Hierbij wordt de beoordeling van individuele verzoeken door relevante managers ondersteund met configureerbare workflows. Bij de provisioning kan de toxic policies functionaliteit worden gebruikt om de uitgifte van conflicterende accounts en rechten te voorkomen. Recertification kan worden ingezet om eerder door managers aangevraagde of goedgekeurde individuele licenties en rechten, planmatig opnieuw te laten beoordelen.

A.5.16 Identiteitsbeheer

De Provisioning module verzorgt de identity lifecycle van digitale gebruikers, vanaf hun instroom en doorstroom tot de uitstroom bij beëindiging van het dienstverband, contract of overeenkomst. Accounts worden aangemaakt en up-to-date gehouden op basis van Attribute Based Access Control. Daarnaast kunnen via Service Automation individuele accounts worden verstrekt en beheerd. Bij de provisioning kan de toxic policies functionaliteit worden gebruikt om de uitgifte van conflicterende accounts en rechten te voorkomen. Recertification kan worden ingezet om eerder door managers aangevraagde of goedgekeurde individuele licenties en rechten planmatig opnieuw te laten beoordelen.

A.5.17 Authenticatie-informatie

Authenticatieinformatie wordt versleuteld opgeslagen in een Identiteitsprovider (IdP). HelloID kan zelf fungeren als IdP, maar gebruikelijker is dat HelloID gebruik maakt van bestaande IdP's zoals de lokale Active Directory of EntraID.

A.5.18 Toegangsrechten

De Provisioning module ondersteunt de automatische uitgifte en beheer van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast kunnen via Service Automation individuele toegangsrechten worden verstrekt en beheerd. Hierbij wordt de beoordeling van individuele verzoeken door relevante managers ondersteund met configureerbare workflows. Bij de provisioning kan de toxic policies functionaliteit worden gebruikt om de uitgifte van conflicterende accounts en rechten te voorkomen. Recertification kan worden ingezet om eerder door managers aangevraagde of goedgekeurde individuele licenties en rechten, planmatig opnieuw te laten beoordelen.

A.5.28 Verzamelen van bewijsmateriaal

HelloID genereert logs en informatie over de volgende zaken: 1) Access Management inlogpogingen etc. 2) Provisioning business rules waarmee medewerkers aan accounts en rechten worden gekoppeld. 3) Service Automation logs van service-verzoeken, de afhandeling ervan en de status. Met 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.

A.5.34 Privacy en bescherming van persoonsgegevens

De Provisioning module ondersteunt de automatische uitgifte en beheer van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast kunnen via Service Automation individuele toegangsrechten worden verstrekt en beheerd. Hierbij wordt de beoordeling van individuele verzoeken door relevante managers ondersteund met configureerbare workflows. Met bovenstaande mechanismes zorgen we dat alleen rechten worden verstrekt die nodig zijn voor iemands taken en verantwoordelijkheden.

Bij de provisioning kan de toxic policies functionaliteit worden gebruikt om de uitgifte van conflicterende accounts en rechten te voorkomen. Recertification kan worden ingezet om eerder door managers aangevraagde of goedgekeurde individuele licenties en rechten planmatig opnieuw te laten beoordelen.

A.5.35 Onafhankelijke beoordeling van informatiebeveiliging

HelloID werkt met transparante business rules en beschikt daarnaast over overzichten van de individueel verstrekte toegangsrechten (en wie deze heeft goedgekeurd). Reconciliation kun je inzetten om inconsistenties te ontdekken en herstellen tussen het IAM-platform en de aangesloten doelsystemen. Hiermee kunnen bijvoorbeeld ongewenst handmatig verstrekte rechten worden geïdentificeerd. Role mining kun je gebruiken om sub optimalisaties en onvolkomenheden te herkennen binnen de gebruikte business rules. Met Recertification kunnen eerder door managers aangevraagde of goedgekeurde licenties en rechten regulier opnieuw worden beoordeeld.

A.5.36 Naleving van beleid, regels en normen voor informatiebeveiliging

HelloID werkt met transparante business rules en beschikt daarnaast over overzichten van de individueel verstrekte toegangsrechten (en wie deze heeft goedgekeurd). Reconciliation kun je inzetten om inconsistenties te ontdekken en herstellen tussen het IAM-platform en de aangesloten doelsystemen. Hiermee kunnen bijvoorbeeld ongewenst handmatig verstrekte rechten worden geïdentificeerd. Role mining kun je gebruiken om sub optimalisaties en onvolkomenheden te herkennen binnen de gebruikte business rules. Met Recertification kunnen eerder door managers aangevraagde of goedgekeurde licenties en rechten regulier opnieuw worden beoordeeld.

A.5.37 Gedocumenteerde bedieningsprocedures

Service automation ondersteunt gedelegeerde formulieren. Hiermee kunnen niet specifiek getrainde medewerkers zelf beheeracties uitvoeren zonder directe toegang tot kritische beheersystemen.

A.6 Mensgerichte beheersmaatregelen

A.6.1 Screening

Screening van kandidaten valt buiten de scope van HelloID. Wel kunnen specifieke criteria (bijv. behaalde certificaten) die worden geregistreerd in het HR-systeem, als onderdeel van de Provisioning worden gebruikt in business rules tbv de uitgifte van accounts en/of rechten. Bij individueel verstrekte accounts en rechten kunnen voor de gebruiker specifieke voorwaarden gelden (zoals een vergunning of training) die regulier opnieuw moeten worden beoordeeld. Hiervoor kan de Recertification functionaliteit worden gebruikt.

A.6.2 Arbeidsovereenkomst

Contractuele afspraken m.b.t. informatiebeveiliging, waarvan de bevestiging is geregistreerd in het HR-systeem, kunnen als onderdeel van de Provisioning worden gebruikt in business rules tbv de

uitgifte van accounts en/of rechten. Bij individuele verstrekking van accounts en rechten mbv Service Automation, kan een bevestiging in de workflow worden opgenomen. De gebruiker moet bijv. akkoord gaan met specifieke voorwaarden.

A.6.4 Disciplinaire procedure

Als een disciplinaire procedure leidt tot intrekken van bevoegdheden die staan geregistreerd in het HR-systeem, kan dit als onderdeel van de provisioning automatisch leiden tot ingetrokken accounts of toegangsrechten. Of via Service Automation formulieren kunnen snel acties worden uitgevoerd op accounts welke niet kunnen wachten op de Provisioning flow, dit met extra informatie omtrent de actie en logging daarvan.

A.6.5 Verantwoordelijkheden na beëindiging of wijziging van het dienstverband

De Provisioning module zorgt dat bij een wijziging van het dienstverband, functie, afdeling etc. die invloed heeft op de benodigde accounts en rechten, deze wijzigingen automatisch worden doorgevoerd. Bij het einde van iemands dienstverband worden automatisch accounts geblokkeerd. Bij individueel verstrekte accounts en rechten kan via de Recertification functionaliteit een periodieke herbeoordeling worden ingepland. Daarbij kan worden gecontroleerd of de rechten nog passen bij het actuele dienstverband, functie, afdeling etc.

A.6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten

Een geheimhoudingsverklaring, waarvan de bevestiging is geregistreerd in het HR-systeem, kan als onderdeel van de Provisioning worden gebruikt in business rules tbv de uitgifte van accounts en/of rechten. Bij individuele verstrekking van accounts en rechten mbv Service Automation, kan een bevestiging in de workflow worden opgenomen. De gebruiker moet bijv. akkoord gaan met specifieke geheimhoudingseisen.

A.6.7 Werken op afstand

HelloID Access Management ondersteunt contextuele factoren waaronder toegang vanaf externe netwerkomgevingen. Afhankelijk van de context kunnen bepaalde mogelijkheden worden geblokkeerd of alleen toegankelijk na een extra authenticatie. Naast soft of FIDO2 compliant hard tokens en sms biedt HelloID ook verschillende one time passwords (OTP's) als tweede factor.

A.7 Fysieke beheersmaatregelen

A.7.2 Fysieke toegangsbeveiliging

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.

A.7.3 Beveiligen van kantoren, ruimten en faciliteiten

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.

A.8 Technologische beheersmaatregelen

- | | | |
|---------------|--|---|
| A.8.1 | User endpoint devices | Met behulp van Conditional Access kunnen toegangsrechten afhankelijk worden gemaakt van het type gebruikersapparaat, zoals Windows-, iOS, Android of macOS-apparaten. Ook het gebruikte toegangsnetwerk of inlogtijdstip kan als conditie worden gebruikt bij het bepalen van iemands rechten. |
| A.8.2 | Speciale toegangsrechten | HelloID biedt geen Private Access Management (PAM) functionaliteit voor speciale toegang. Wel kan via de Provisioning ABAC functionaliteit aan gebruikers met specifieke functies/deskundigheden, bijzondere toegangsrechten worden verstrekt. En door roostersystemen te koppelen als bronsysteem kun je ook toegang tot systemen afhankelijk maken van werkroosters en zo de toegangstijd te beperken. Door gebruik te maken van de delegated forms binnen de Service Automation module kun je 'reguliere' medewerkers beheertaken laten uitvoeren zonder speciale toegangsrechten. |
| A.8.3 | Beperking toegang tot informatie | De Provisioning module ondersteunt de automatische uitgifte en beheer van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast kunnen via Service Automation individuele toegangsrechten worden verstrekt en beheerd. Hierbij wordt de beoordeling van individuele verzoeken door relevante managers ondersteund met configureerbare workflows. Met bovenstaande mechanismes zorgen we dat alleen rechten worden verstrekt die nodig zijn voor iemands taken en verantwoordelijkheden. |
| A.8.4 | Toegangsbeveiliging op broncode | De Provisioning module ondersteunt de automatische uitgifte en beheer van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast kunnen via Service Automation individuele toegangsrechten worden verstrekt en beheerd. Hierbij wordt de beoordeling van individuele verzoeken door relevante managers ondersteund met configureerbare workflows. Met bovenstaande mechanismes zorgen we dat alleen rechten worden verstrekt die nodig zijn voor iemands taken en verantwoordelijkheden. Hiermee kunnen we ook de toegang tot ontwikkeltools beheeren. |
| A.8.5 | Beveiligde authenticatie | HelloID access management ondersteunt onder andere Multi-Factor Authenticatie (ook met FIDO2 compliant hardware keys en One-Time Passwords). |
| A.8.8 | Beheer van technische kwetsbaarheden | Reconciliation kan worden ingezet om onbeheerde accounts en toegangsrechten binnen doelsystemen te identificeren. |
| A.8.12 | Voorkomen van gegevenslekken (data leakage prevention) | Door accounts en toegangsrechten te beheeren via HelloID kunnen we het Principle of Least Privilege borgen waarbij alleen de noodzakelijke accounts en rechten worden verstrekt. Dit is een belangrijk hulpmiddel bij het voorkomen van datalekken. Reconciliation kan |

worden ingezet om onbeheerde accounts en toegangsrechten binnen doelsystemen te identificeren. Met toxic policy management voorkomen we het verstrekken van conflicterende rechten. Met recertification kan de herbeoordeling van individueel verstrekte rechten planmatig worden uitgevoerd.

A.8.14 Redundantie van informatieverwerkende faciliteiten

Reconciliation kan worden ingezet om inconsistenties te ontdekken tussen accounts en rechten zoals die zijn geregistreerd binnen het IAM platform maar niet correct zijn doorgevoerd binnen doelsystemen. Of instellingen die onbedoeld nog actief zijn in de doelsystemen.

A.8.15 Logging

HelloID genereert logs en informatie over de volgende zaken: 1) Access Management inlogpogingen etc. 2) Provisioning business rules waarmee medewerkers aan accounts en rechten worden gekoppeld. 3) Service Automation logs van service-verzoeken, de afhandeling ervan en de status.

Reconciliation kan worden ingezet om inconsistenties te ontdekken tussen accounts en rechten zoals die zijn geregistreerd binnen het IAM platform maar niet correct zijn doorgevoerd binnen doelsystemen. Of instellingen die onbedoeld nog actief zijn in de doelsystemen.

A.8.16 Monitoren van activiteiten

Reconciliation kan worden ingezet om onbeheerde accounts en rechten binnen doelsystemen te identificeren.

A.8.34 Bescherming van informatiesystemen tijdens audits

Reconciliation kan planmatig worden uitgevoerd zodat de belasting van doelsystemen beperkt blijft.