TOOLS4EVER

Whitepaper V1.0 / 25 08 2022

ISO 27001

en de rol van Identity Management

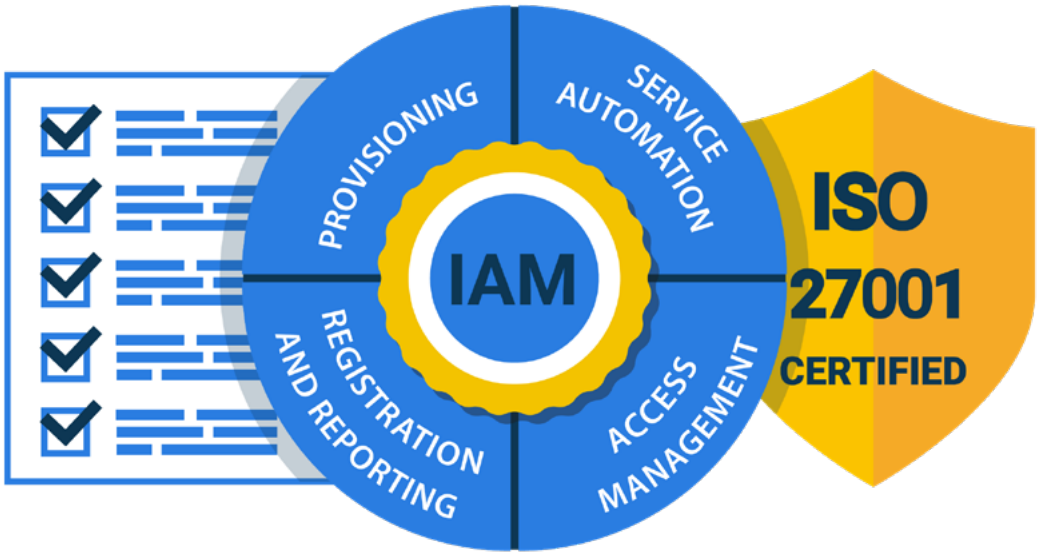
Inhoudsopgave

Inleiding

ISO 27001 is dé internationale standaard voor informatiebeveiligingsmanagement. De standaard helpt organisaties hun informatiesystemen op een gestructureerde, effectieve en efficiënte manier te beveiligen met een Information Security Management System (ISMS). ISO 27001 wordt breed toegepast en vormt ook de basis voor beveiligingsnormen binnen specifieke sectoren, zoals de Baseline Informatiebeveiliging Overheid (BIO) en de NEN 7510 (in de zorg).

ISO 27001 helpt organisaties op twee manieren. Allereerst met concrete richtlijnen om de informatiebeveiliging binnen de organisatie goed in te richten en te beheren. En daarnaast beschikken organisaties met een ISO 27001 certificatie over een algemeen geaccepteerd kwaliteitsstempel. Naar klanten en partners bevestig je hiermee dat je als organisatie de informatiebeveiliging volledig op orde hebt en voldoet aan de geldende eisen. Voor samenwerkingsovereenkomsten en contracten vormt zo'n ISO 27001 certificaat dus vaak een noodzakelijk 'tick in the box'.

In deze whitepaper geven we eerst een overzicht van de ISO 27001 norm. Vervolgens tonen we welke rol Identity Management speelt bij het ISO 27001 compliant maken van je organisatie.



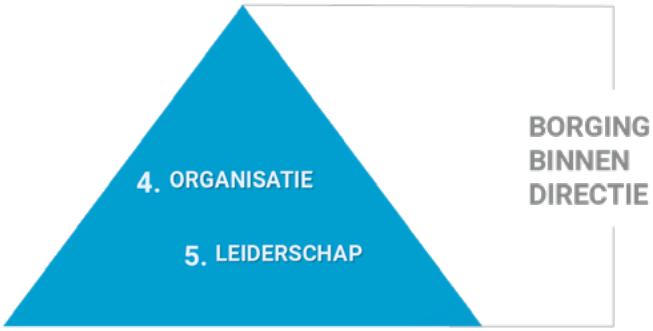
ISO 27001 overzicht

In ISO 27001 vind je geen gedetailleerde technische eisen voor onderwerpen als multi-factor authenticatie of data encryptie. De norm richt zich op informatiebeveiliging management-systemen en is vooral bedoeld om je organisatie en processen zodanig in te richten dat de vertrouwelijkheid, beschikbaarheid en integriteit van informatie is gegarandeerd. ISO 27001 sluit aan op de zogenaamde ISO High Level Structure (HLS). Deze HLS biedt een basisstructuur voor managementsystemen, met algemene richtlijnen op gebieden als leiderschap, risico-management en procesmanagement. Specifieke normen zoals ISO 9001 (kwaliteit), ISO 14001 (milieu) én ISO 27001 (informatiebeveiliging) kun je als het ware in het overall management-systeem 'klikken', zodat je als organisatie één samenhangend managementsysteem realiseert.

ISO 27001 omvat 10 hoofdstukken en een bijlage. De inhoudelijke eisen zijn beschreven in de hoofd-stukken 4 t/m 10 en vatten we hieronder samen. In bijlage A van ISO 27001 vind je concrete beheers-doelstellingen en -maatregelen die je – als ze relevant zijn binnen je organisatie - moet gebruiken om de informatiebeveiliging daadwerkelijk in te richten. Deze bijlage lichten we later in deze whitepaper toe.

Hoofdstuk 4-5: Business context

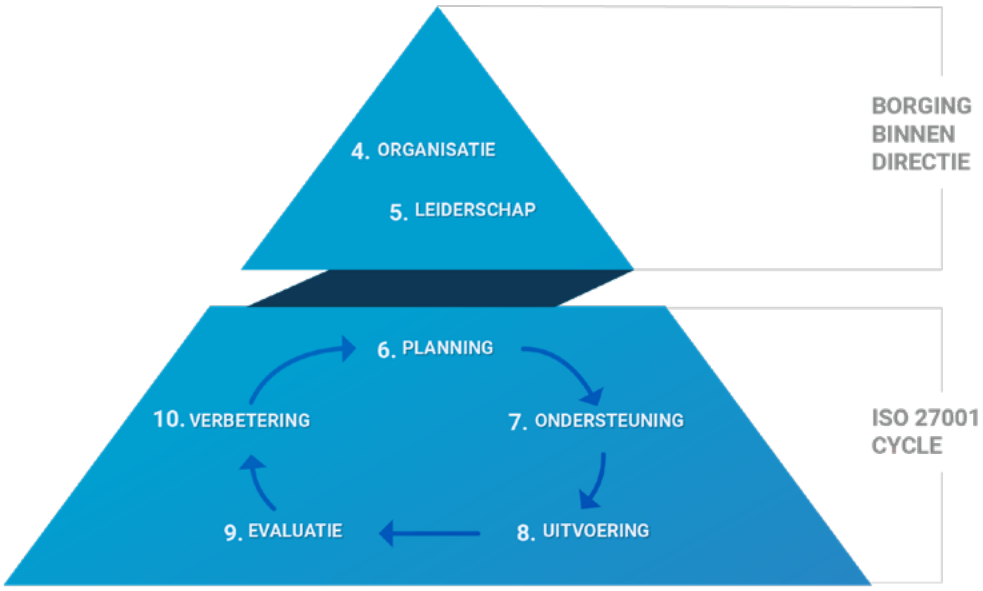
Belangrijk binnen ISO 27001 is dat informatiebeveiliging voldoende 'hoog' binnen de organi-satie is belegd. Het is niet voldoende om 'simpelweg een beveiligingsplan' te laten opstellen en beheren door de IT afdeling. Informatiebeveiliging moet aansluiten bij de businessdoelen en bedrijfsvoering en de beveiliging moet op de agenda staan bij de hoogste managementlaag. De eerste twee hoofdstukken (4 en 5) beschrijven deze eisen.



H4. Organisatie context	Hier inventariseren we de organisatiecontext voor de informatiebeveiliging. Een academisch ziekenhuis stelt bijvoorbeeld duidelijk andere beveiligingseisen dan een autodealer. Het is dus belangrijk om te inventariseren welke doelstellingen de organisatie heeft, welke interne en externe stakeholders er zijn, welke regelgeving van toepassing is etc. Hiermee bepaal je de kaders voor het uiteindelijke informatiebeveiligingsplan.
H5. Leiderschap	Leiderschap is een belangrijk onderdeel. Niet voor niets worden bij ISO audits ook senior managers geïnterviewd. Informatiebeveiliging moet namelijk de verantwoordelijkheid zijn van dat senior management en niet worden gedelegeerd naar een 'tandeloze' kwaliteitsmanager in een bijgebouw. De verschillende rollen en verantwoordelijkheden voor informatiebeveiliging moeten bovendien duidelijk zijn vastgelegd.

Hoofdstuk 6-10: ISO 27001 'cyclus'

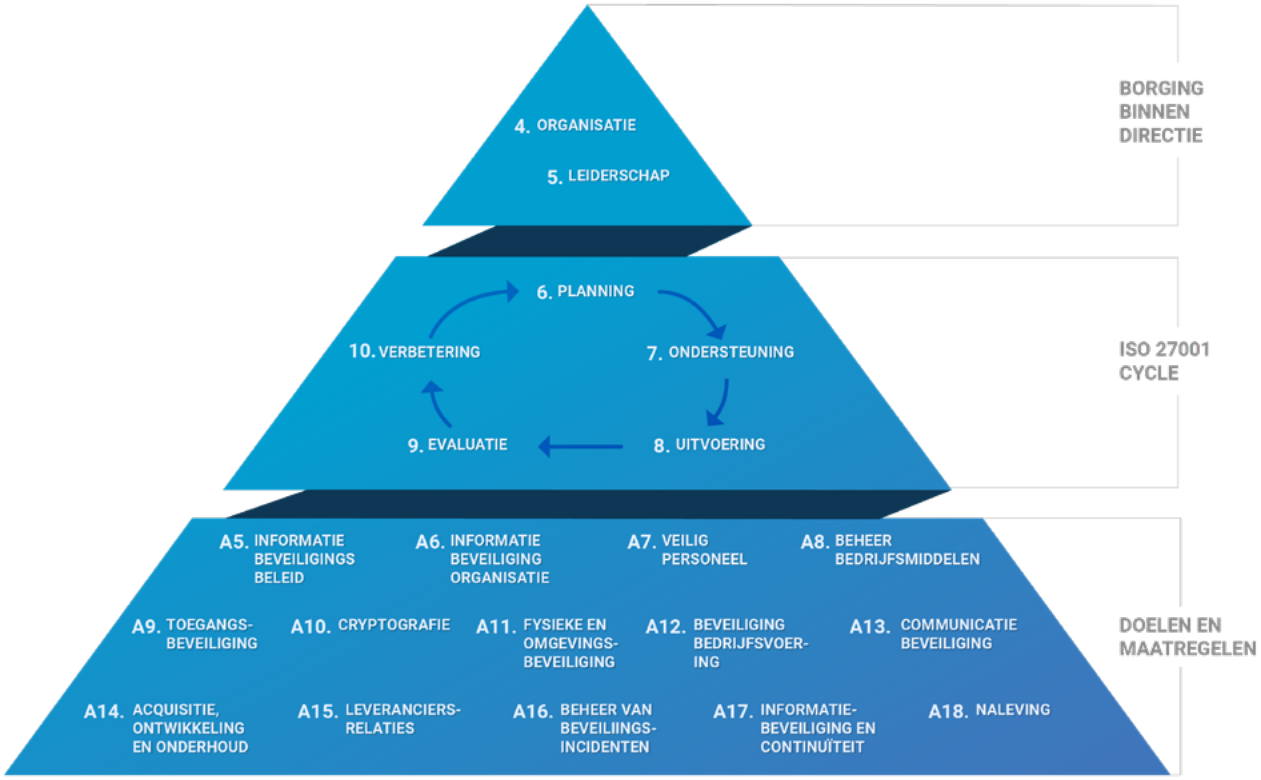
Met hoofdstuk 4 en 5 zorg je dat je de organisatiekaders duidelijk zijn en dat senior management voldoende betrokken is. In de volgende hoofdstukken 6-10 vind je vervolgens richtlijnen hoe je de informatiebeveiliging concreet organiseert, plant, implementeert en voortdurend aanpast aan de actuele omstandigheden:



H6. Planning	De basis bestaat uit een uitgebreide risico analyse met de risico's die voor deze organisatie van toepassing zijn. Per risico wordt de kans op dat risico bepaald en wat de impact daarvan zou zijn. Aan de hand hiervan stel je de benodigde maatregelen op om de risico's te beheersen. Je formuleert concrete beveiligingsdoelen en hoe je die doelen gaat realiseren.
H7. Ondersteuning	Daarbij moet uiteraard de organisatie in staat zijn deze plannen ook uit te voeren. De juiste vaardigheden, kennis, systemen en 'security awareness' moeten aanwezig zijn. Ook moet er voldoende worden geïnvesteerd in interne communicatie en documentatie.
H8. Uitvoering	De beveiligingsprocessen moeten zijn geïmplementeerd met de passende maatregelen om de veiligheidsrisico's te beheersen. Gedurende de uitvoering van de plannen moeten de resultaten voortdurend worden gemonitord en de risicoanalyses moeten regelmatig worden geactualiseerd.
H9. Evaluatie	Structureel moeten de resultaten van de beveiligingsmaatregelen worden geëvalueerd. Onderdeel daarvan zijn interne audits en ook moet er regelmatig een zogenaamde directiebeoordeling worden opgesteld en besproken binnen de directie.
H10. Verbetering	Tenslotte moet geborgd zijn dat niet alleen eventuele tekortkomingen uit die evaluaties worden opgelost. Ook moeten de processen en competenties aanwezig zijn om steeds nieuwe en verbeterde beveiligingsmaatregelen te ontwikkelen en implementeren.

Bijlage A: Beheersdoelstellingen en -maatregelen

Je moet voldoen aan alle eisen in de hoofdstukken van ISO 27001 om als organisatie gecertificeerd te kunnen worden. De invulling van de eisen mag afhangen van het type organisatie en doelstellingen. In bijlage A van ISO 27001 vind je een overzicht van 114 verschillende beheersdoelstellingen en maatregelen, in 14 categorieën. Die kun je zien als een catalogus, waaruit iedere organisatie maatregelen moet inzetten die van toepassing zijn bij de eigen organisatie en risico's. Ook is er nog de norm ISO 27002 waarin de verschillende maatregelen nog verder zijn uitgewerkt. Hieronder vind je een kort overzicht van de categorieën met de doelstellingen en maatregelen in bijlage A.

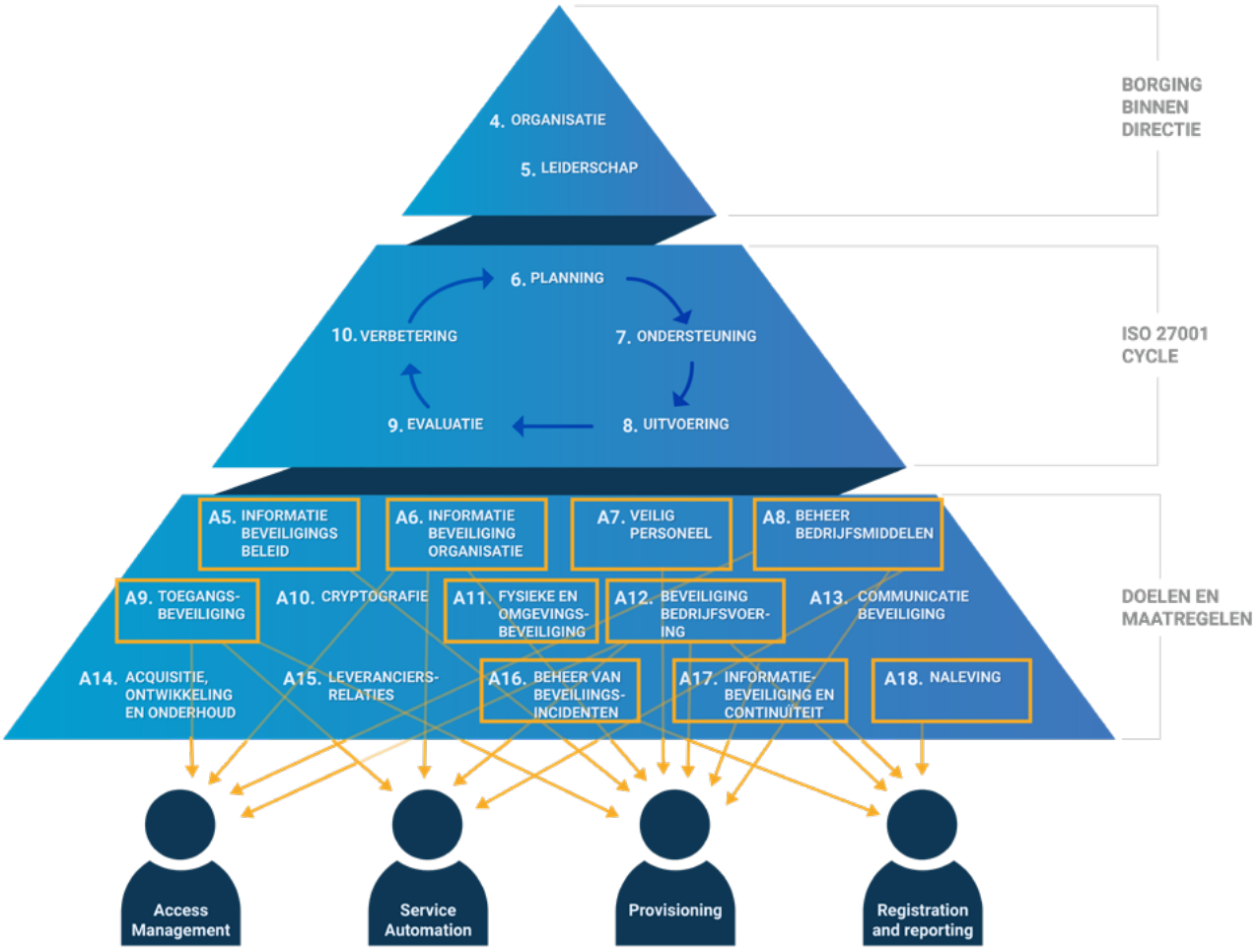


A5. Informatiebeveiligings-beleid	Als aanvulling op het algemene organisatiebeleid moet ook een specifiek informatiebeveiligingsbeleid worden opgesteld en regelmatig geëvalueerd.
A6. Organisatie van informatiebeveiliging	Er is niet alleen een informatiebeveiligingsbeleid nódig, het moet ook worden geïmplementeerd en beheerd. Welke rollen zijn nodig met welke verantwoordelijkheden en bevoegdheden? Rolscheiding is daarbij een belangrijk aandachtspunt en ook is er vandaag de dag veel aandacht nodig voor online werken en het gebruik van (eigen) mobiele apparaten.
A7. Veilig personeel	Uiteraard moeten medewerkers voldoende zijn opgeleid en zich bewust zijn van het belang van informatiebeveiliging. Dat betreft het hele 'dienstverband', van de juiste werving van medewerkers tot en met de benodigde beveiligingsmaatregelen als mensen de organisatie weer verlaten.

A8. Beheer van bedrijfsmiddelen	Bedrijfsmiddelen om informatie te verwerken (zoals software en computersystemen) moeten goed geregistreerd en beheerd worden. Wie mag de systemen gebruiken en worden bedrijfsmiddelen en gebruiksrechten na beëindiging van de werkzaamheden weer teruggegeven? Alle informatie moet goed worden geclassificeerd en voldoende veilig opgeslagen.
A9. Toegangsbeveiliging	Er zijn maatregelen nodig om te zorgen dat medewerkers alleen toegang krijgen tot netwerken, systemen en gegevens die ze nodig hebben voor hun eigen werkzaamheden.
A10. Cryptografie	Gegevens moeten voldoende versleuteld worden om zowel de vertrouwelijkheid als de integriteit van gegevens te kunnen garanderen.
A11. Fysieke beveiliging en beveiliging van de omgeving	Organisaties moeten voorkomen dat onbevoegden toegang krijgen tot computers en gegevensdragers op kantoorlocaties. Dat betekent ook dat bij bijvoorbeeld stroomuitval of een calamiteit de informatiebeveiliging intact moet blijven. En bij afvoer van apparatuur moeten de gegevens verwijderd zijn.
A12. Beveiliging bedrijfsvoering	Er moeten duidelijke afspraken en procedures zijn om informatiesystemen veilig te gebruiken en de systemen te beschermen tegen malware. Ook zijn er duidelijke back-up en monitoring maatregelen nodig.
A13. Communicatiebeveiliging	Zowel de interne netwerkfaciliteiten als de externe netwerkcommunicatie moeten beveiligd zijn tegen onbevoegde toegang en misbruik.
A14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	Organisaties moeten bij inkoop, ontwikkeling en beheer van IT systemen rekening houden met de beveiliging van de systemen en data. Daarbij gaat het niet alleen om operationele systemen. Ook bijvoorbeeld ontwikkel-, demo- en testsystemen moeten voldoende beveiligd zijn.
A15. Leveranciersrelaties	Organisaties zijn afhankelijk van leveranciers voor hun IT systemen. Dat geldt zowel voor systemen en software die on-premises worden geleverd, als leveranciers die gevoelige cloud data beheren. Er zijn duidelijke afspraken met leveranciers nodig om de informatiebeveiliging te garanderen.
A16. Beheer van beveiligingsincidenten	Ondanks alle beveiligingsmaatregelen kan er toch een incident plaatsvinden. Hiervoor moeten goede procedures met duidelijke verantwoordelijkheden aanwezig zijn, inclusief afspraken over de verdere rapportage en oplossing.
A17. Informatiebeveiligings-aspecten van bedrijfs-continuïteitsbeheer	Bij incidenten met de IT voorzieningen moet er specifiek op worden gelet dat de continuïteit van de informatiebeveiliging altijd gegarandeerd blijft.
A18. Naleving	Als organisatie moet je voortdurend kunnen aantonen dat je voldoet aan alle geldende wet- en regelgeving.

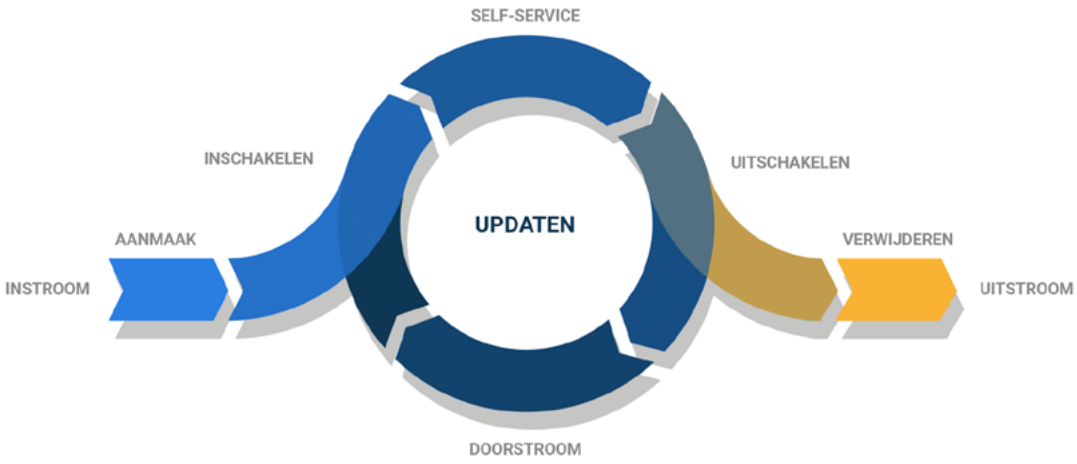
Identity Management en ISO 27001

Bijlage A van ISO 27001 geeft dus een wat verder uitgewerkt beeld van de maatregelen die een organisatie moet nemen om informatie goed te beveiligen. Het beheer van eindgebruikers en hun rechten worden daarbij steeds belangrijker. Medewerkers, partners en klanten mogen alleen toegang krijgen tot applicaties en data op een 'need to know' basis. Ook is het noodzakelijk dat alle IT activiteiten zijn te traceren tot het niveau van individuele gebruikers. Het maakt Identity Management een belangrijk gereedschap bij de realisatie van een 'ISO 27001 proof' informatiebeveiliging. In dit hoofdstuk mappen we de verschillende categorieën met maatregelen in bijlage A op de mogelijkheden binnen een state-of-the-art Identity Management oplossing. Dit illustreren we aan de hand van onze eigen HelloID cloudbased Identity & Access Management (IAM) platform.



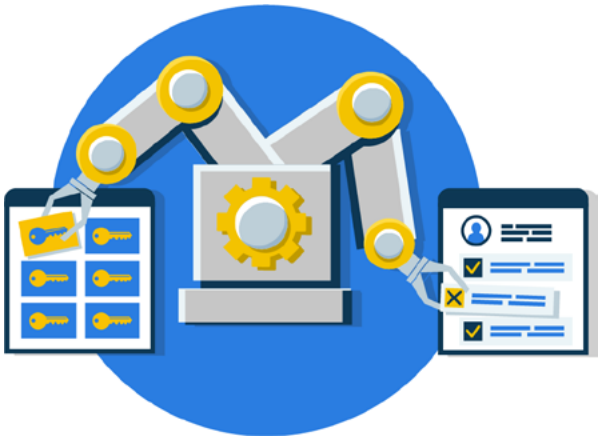
Provisioning van gebruiksaccounts en -rechten

Groepsaccounts zijn binnen ISO 27001 not done, evenals het 'copy user' principe voor nieuw binnenkomende medewerkers. Toegangsrechten moeten vandaag de dag eenduidig zijn gekoppeld aan individuele gebruikersaccounts. Er moet op ieder moment duidelijk zijn wie er toegang heeft tot data en applicaties en wie bepaalde handelingen uitvoert. En natuurlijk moeten de accountgegevens en toegangsrechten altijd up-to-date zijn. Dus steeds in lijn met iemands huidige rol en positie binnen de organisatie. Professioneel en geautomatiseerd gebruikersaccountmanagement is daarvoor cruciaal.



Binnen HelloID borgen we dit door middel van geautomatiseerde provisioning. Hiermee zijn iemands digitale identiteit en toegangsrechten altijd in lijn met de informatie zoals geregistreerd in het HR systeem. Dankzij een rechtstreeks koppeling tussen dat HR systeem en HelloID ontvangt de nieuwe medewerker bij onboarding direct een gebruikersaccount met daaraan gekoppeld de faciliteiten en rechten die passen bij diens rol. Ook tijdens het verdere dienstverband houden we dit automatisch actueel. Verandert iemands rol, dan past HelloID ook direct de toegangsrechten aan. En verlaat iemand de organisatie, dan zorgt HelloID dat automatisch het account wordt geblokkeerd en de vertrekkende medewerker geen toegang meer heeft. Stapeling van rechten en accounts die per ongeluk toegankelijk blijven zijn niet langer mogelijk.

Service Automation: standaardisatie met ruimte voor uitzonderingen



Goede informatiebeveiliging leunt op duidelijke beleidsregels, heldere processen en weinig ruimte voor individueel en ongecontroleerd maatwerk. Om dat te borgen willen we identity management processen zoveel als mogelijk standaardiseren en automatiseren. Daarbij moet het mogelijk zijn concepten als Role Based access te ondersteunen en processen te implementeren met een duidelijke scheiding van rollen. Tegelijkertijd zijn er altijd uitzonderingen en moet iedere organisatie een eigen balans zoeken tussen gebruiksvriendelijkheid en bedrijfsveiligheid. Automatisch te veel rechten verstrekken, leidt tot ongewenste beveiligingsrisico's. Maar medewerkers steeds onnodig laten wachten op hun toegangsrechten belemmert hun werk.

HelloID biedt die gewenste combinatie van standaardisatie en uitzonderingen:

- Standaard kun je binnen HelloID rechten toekennen met behulp van de zogenaamde Attribute Based Access Control (ABAC) functionaliteit. De organisatiestructuur met rollen en bijbehorende werkzaamheden vertalen we in HelloID naar configureerbare business rules die automatisch bepalen welke toegangsrechten een medewerker krijgt. Vanaf de automatisch onboarding bij indiensttreding tot en met de vertrekprocedure bij vertrek.

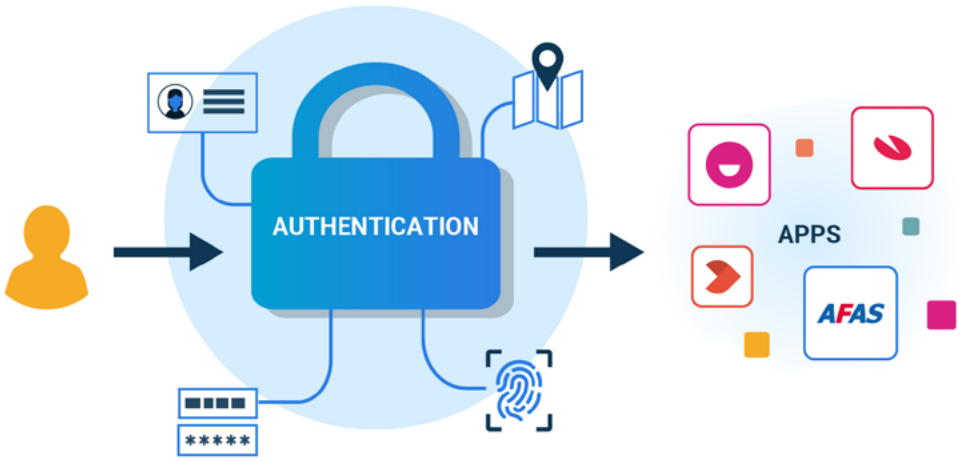
- Het merendeel van de rechten wordt dus volledig geautomatiseerd uitgegeven, maar zo'n standaard rollenmatrix is nooit volledig dekkend en daarom voorziet HelloID ook in uitzonderingen. Voor specifiekere en moeilijker automatisch uitdeelbare rechten kun je

self-service processen ontwerpen. Gebruikers kunnen hiermee zelf online toegang vragen tot applicaties of datashares waarbij automatisch de juiste goedkeuringsstappen worden gevolgd. Na goedkeuring zorgt het geautomatiseerde proces voor de verdere activering zonder risicovolle uitzonderingen of vergissingen.

Geautomatiseerde configuratieregels zorgen dat de dienstencatalogus automatisch up-to-date blijft. Een nieuwe share wordt bijvoorbeeld direct zichtbaar in de catalogus. Op ieder moment kan het systeem een overzicht geven van welke medewerkers actief zijn en welke licenties, applicaties, shares, et cetera zij in gebruik hebben.

Access management

Een state-of-the-art toegangsmanagement zorgt dat medewerkers - en zo nodig ook partners en klanten - eenvoudig en uniform toegang krijgen tot applicaties en data. Zoals hiervoor uitgelegd is het uitgangspunt daarbij dat iedere gebruiker is voorzien van één persoonlijk gebruikersaccount. Met een concept als Single Sign-On (SSO) zorg je vervolgens dat mensen maar één keer hoeven in te loggen. Juist zo'n combinatie van gebruiksvriendelijke én veilige toegangsoplossingen voorkom je dat medewerkers onveilige work-arounds verzinnen.



HelloID ondersteunt alle gangbare Single Sign-On protocollen om gebruikers per applicatie te authentiseren. Voor toegang tot applicaties zonder ingebouwde SSO faciliteiten, biedt HelloID andere methodes om de toegang te verzorgen. Voor de primaire authenticatie kunnen we HelloID integreren met Active Directory en andere zogenaamde Identity Providers zoals Azure, Google, Salesforce, SAML en OpenID. Ook ondersteunt het platform extra beveiligingsopties zoals Two Factor Authentication (2FA). HelloID herkent contextuele factoren zoals de inloglocatie en het tijdstip en kan afhankelijk daarvan de gebruiker vragen om een extra authenticatie. Naast soft of hard tokens en sms biedt HelloID ook verschillende one time passwords (OTP's) als tweede factor.

HelloID verzorgt Identity & Access Management vanuit de cloud met als voordeel lagere investeringen, een snelle installatie en configuratie terwijl Tools4ever het technische beheer verzorgt, inclusief automatische updates. De oplossing wordt gerealiseerd met behulp van maximaal beveiligde Microsoft Azure- en Google Cloudomgevingen, die bovendien iedere zes maanden grondig wordt gecontroleerd door Deloitte Risk Services. Compliance aan de strenge security-eisen is dan ook gewaarborgd. De dienstverlening heeft bovendien een zeer hoge beschikbaarheid dankzij de ingebouwde redundantie.

Reporting

Voor ISO 27001 compliancy is registratie en rapportage essentieel. Als organisatie moet je kunnen aantonen dat de verschillende processen conform de relevante wet- en regelgeving worden uitgevoerd. Ook moet je bij een beveiligingsincident zoals een datalek kunnen traceren welke gebruikers binnen het netwerk welke handelingen hebben uitgevoerd.

Als cloud based oplossing moet HelloID voldoen aan steeds strengere wet- en regelgeving op het gebied van audits en beveiliging. Alle toegangspogingen, geautomatiseerde en handmatige processen, en het gebruik van ons platform worden daarom geregistreerd en inzichtelijk gemaakt. Zo wordt het authenticatieproces automatisch gemonitord en is via rapportages altijd inzichtelijk wie welke applicaties heeft geraadpleegd, op welk moment en vanaf welke locatie. Dit geeft niet alleen een gedetailleerd beeld van het doorlopen authenticatietraject, maar toont bijvoorbeeld ook inlogpogingen vanaf verdachte IP-adressen. Mogelijke dreigingen kunnen tijdig worden herkend om tegenmaatregelen te nemen.

Extra onderscheidend is dat binnen HelloID de volledige identity lifecycle per systeem én per gebruiker auditable is. Alle uitgevoerde acties worden gelogd, zoals het creëren, inschakelen, updaten, verplaatsen, disablen en verwijderen van accounts. Hetzelfde geldt voor het toekennen en intrekken van permissies. Zijn rechten ad hoc toegekend (buiten de reguliere rollenmatrix) dan is via HelloID precies te zien wie dit heeft aangevraagd, welke persoon het verzoek heeft goedgekeurd en tot welke exacte wijzigingen in achterliggende systemen dit heeft geleid. Daarmee is het HelloID proces volledig transparant, toetsbaar en aanpasbaar.

Meer weten?

Identity Management vormt vandaag de dag een centrale rol binnen je IT beveiliging. Medewerkers, partners en klanten mogen alleen nog met een eigen account toegang krijgen tot applicaties en data. Rechten moeten altijd worden verstrekt op een ‘need to know’ basis. We moeten bovendien alle IT activiteiten tot het niveau van individuele gebruikers kunnen traceren. Het maakt je Identity Management platform een belangrijk element bij het inrichten van je ISO 27001 compliant informatiebeveiligingssysteem.

Meer weten over de rol die Identity Management kan spelen bij de ISO 27001 compliancy binnen je organisatie? En hoe kun je je IT omgeving veilig houden zonder in te leveren op gebruiksvriendelijkheid? We vertellen je hier graag meer over. Bijvoorbeeld aan de hand van onze checklist ISO 27001 – HelloID. In deze lijst behandelen we alle ISO 27001 Annex A maatregelen met per maatregel een toelichting of – en zo ja, hoe – HelloID Identity Management hieraan een bijdrage kan leveren.

TOOLS4EVER

Adres	Amalialaan 126c 3743 KJ Baarn Nederland
Telefoon	+31 (0) 35 54 832 55
Website	Tools4ever.nl
Mail	info@tools4ever.com
Sales	sales@tools4ever.com
Support	tools4ever.nl/support