



**van hall
larenstein**
university of applied sciences

Aanbesteding

USE-Cases

Hogeschool Van Hall Larenstein

Inhoud

1. INSTRUCTIE	3
2. In-, door- en uitstroomproces van medewerkers.....	4
2.1 Organisatie inrichting	4
2.2 Eisen	4
2.3 Nieuwe student instroom	4
2.4 Nieuwe medewerker instroom.....	5
2.5 Medewerker wisselt functie	5
2.6 Iemand verlaat HVHL.....	6
2.7 Student klaar met opleiding.....	6
3. AANVRAAG EN TOEKENNING VAN ROLLEN EN RECHTEN	8
3.1 Organisatie inrichting	8
3.2 Eisen	8
3.3 Iemand vraagt extra toegang aan.....	8
3.4 Rechten dienen per direct ingetrokken te worden.....	8
3.5 Tijdelijke toegang moet verleent worden.....	9
4. BEHEER VAN INTEGRATIES MET BRON- EN DOELSYSTEMEN	10
4.1 Organisatie inrichting	10
4.2 Eisen	10
4.3 Integratie van nieuw doelsysteem	10
4.4 Aanpassen van volgorde, thresholds en attributen in de koppeling	11
4.5 Technisch beheer op koppeling met doelsystemen.	11
5. AUTORISATIEMATRIX, ATTESTATIE EN RAPPORTAGE.....	12
5.1 Organisatie inrichting	12
5.2 Eisen	12
5.3 Self-detectie van ongeautoriseerde rechten.....	12
5.4 Auditrapportage.....	13
5.5 Attestatie	14
6. ROLBEHEER PROCES.....	15
6.1 Organisatie inrichting	15
6.2 Eisen	15
6.3 Aanmaken van een nieuwe rol	15
6.4 Wijzigen van een bestaande rol.....	16
6.5 Bulk wijzigingen doorvoeren.....	16

1. INSTRUCTIE

De scenario's in dit document zijn gebaseerd op de inventarisatie van eisen binnen de organisatie. Samen beschrijven zij de vijf belangrijkste deelgebieden van Identity & Access Management (IAM) en daarmee de functionaliteiten die de organisatie verwacht van een toekomstig IAM-pakket en de bijbehorende leverancier.

Ieder scenario start met een beschrijving van de huidige organisatie-inrichting. Deze beschrijving geeft context aan de use-cases en laat zien hoe processen, rollen, systemen en verantwoordelijkheden binnen de organisatie zijn ingericht.

Per scenario zijn vervolgens één of meerdere use-cases uitgewerkt. Een use-case bestaat uit een fictieve praktijksituatie en een aantal concrete stappen. De use-cases zijn gebaseerd op situaties die binnen de organisatie kunnen voorkomen en maken inzichtelijk hoe de oplossing in de praktijk moet functioneren.

Aan ieder scenario is een set eisen of wensen gekoppeld. Deze eisen vormen het beoordelingskader voor de use-cases en zijn tevens opgenomen in het requirements-overzicht.

We verwachten dat inschrijver per use-case aantoont hoe de oplossing de beschreven situatie ondersteunt. Dit kan bijvoorbeeld door middel van een demonstratie, screenshots, procesbeschrijvingen of andere vormen van onderbouwing. Op basis hiervan beoordeelt de organisatie in welke mate de oplossing voldoet aan de gestelde eisen en wensen wat meegerekend wordt als kwaliteitsbeoordeling van de aanbesteding.

2. In-, door- en uitstroomproces van medewerkers

2.1 Organisatie inrichting

HVHL gebruikt HR2Day als bronsysteem voor medewerkersgegevens. In HR2Day worden medewerkers geregistreerd met onder andere functie, afdeling, leidinggevende, dienstverband, startdatum en einddatum. Binnen HR2Day wordt gewerkt met een functiehuis. Dit functiehuis bevat formele functies, zoals invoeren van een nieuwe medewerker, aanpassen van een medewerkersgegevens, uitdiensttreding van een medewerker. Deze formele functies vormen de basis voor het bepalen van standaardrollen en basisrechten. Deze use case beschrijft hoe het IAM-pakket medewerkersgegevens uit HR2Day gebruikt om de toegang van medewerkers bij instroom, doorstroom en uitstroom automatisch en herleidbaar te verwerken. Bronsysteem HR2Day. Ook vermelden en beschrijven. Opbouw identiteit opbouw vanuit welke attributen.

2.2 Eisen

T-100	Medewerker identiteiten vanuit HR-brongegevens.
F-13	Inzicht in accounts per unieke identiteit.
F-49	Afbakening van organisatorische rollen per dienstverband.
F-42	Relatie tussen accounttypen en unieke identiteit.
T-65	Synchronisatie van AD- en Entra ID-groepen.
T-82	Studentidentiteiten vanuit OSIRIS-brongegevens.

2.3 Nieuwe student instroom

Situatie

Een nieuwe student wordt ingeschreven in het Student Informatie Systeem (Osiris) en wil de opleiding Bedrijfskunde en Agribusiness gaan volgen. Ze krijgt hiervoor basisrechten van student en toegang in de applicatie Moodle van de opleiding die ze wil volgen. Haar gegevens zijn; C.J (Chantal) de Vries geboren in Leeuwarden op 10-06-2005. Er is al iemand onder dezelfde naam ingeschreven Chantal de Vries die ook nog studeert, dit is niet dezelfde persoon. Er moet een nieuwe identiteit aangemaakt worden. Chantal.devries@hvhl.nl bestaat reeds.

Opdracht

- De student automatisch detecteert. (eis monitoren bronsysteem Osiris attributen op mutaties, 298)
- Een digitaal uniek account (Emailadres) aanmaakt. (eis controle op dezelfde naam etc., aanmaken account unieke identiteit met Emailadres)
- Dat aan het account ook het attribuut HVHL-ID heeft dat uniek is (eis HVHL-ID zelfde lay-out, uniek HVHL-ID, ...)

- d) De juiste rol(len) toekent. (student basis M365 met rechten in AD & Entra en wifi HVHL)
- e) Toegang verleent tot de benodigde applicaties. (toegang Moodle met juiste opleiding)
- f) De acties registreert in auditlogging. (traceerbaarheid, registratie)

2.4 Nieuwe medewerker instroom

Situatie

Een nieuwe medewerker wordt geregistreerd in het HR-systeem HR2Day. Zij start als docent Bedrijfskunde en Agribusiness binnen de betreffende onderwijsafdeling. Op basis van haar functie en afdeling moet zij basisrechten krijgen als medewerker en toegang tot de applicaties die nodig zijn voor het uitvoeren van haar werkzaamheden. Zijn gegevens zijn: H (Henk) de Jong, geboren in Leeuwarden op 23-09-1985. Henk.dejong@hvhl.nl

Opdracht

- a) De nieuwe medewerker automatisch detecteert vanuit het bronsysteem HR2Day.
- b) Controleert of er al een persoon met dezelfde naam of vergelijkbare persoonsgegevens bestaat.
- c) Een unieke digitale identiteit en account aanmaakt.
- d) Aan het account een uniek HVHL-ID koppelt.
- e) De juiste medewerkersrol(len) toekent op basis van functie, afdeling en status.
- f) Basisrechten toekent, zoals toegang tot groepen in AD & Entra, M365, wifi en medewerkersportalen.

2.5 Medewerker wisselt functie

Situatie

Medewerker M.J. (Marieke) Jansen, geboren op 14-03-1988 in Zwolle, is in dienst bij HVHL. Zij werkt op dit moment als administratief medewerker binnen de afdeling Studentzaken. In HR2Day wordt geregistreerd dat Marieke per 01-10-2026 een nieuwe functie krijgt. Zij wordt teamleider Studentzaken binnen dezelfde afdeling. De rechten die horen bij haar oude functie als administratief medewerker mogen niet automatisch actief blijven als deze niet meer passen bij haar nieuwe functie. Tegelijk moeten de standaardrollen en basisrechten worden toegekend die horen bij haar nieuwe functie als teamleider. Voor sommige aanvullende rechten binnen de nieuwe functie is goedkeuring nodig van een rolbeheerder of leidinggevende.

Opdracht

- a) De functiewijziging van M.J. Jansen automatisch detecteert vanuit HR2Day.
- b) Bepaalt welke rollen en rechten horen bij de oude functie.
- c) Bepaalt welke rollen en rechten horen bij de nieuwe functie.
- d) Oude rechten verwijdert die niet meer passen bij de functie teamleider.

- e) Nieuwe rechten toekent die horen bij de functie teamleider Studentzaken.
- f) De gewijzigde rollen en rechten zichtbaar maakt bij het gebruikersaccount

2.6 Iemand verlaat HVHL

Situatie

Medewerker R.P. (Ruben) Meijer, geboren op 22-11-1984 in Groningen, is in dienst als docent Bedrijfskunde binnen de afdeling Onderwijs Bedrijfskunde en Agribusiness. In HR2Day wordt geregistreerd dat Ruben per 31-12-2026 uit dienst gaat. Vanaf deze datum mag hij geen toegang meer hebben tot applicaties, systemen, rollen, autorisaties en bedrijfsinformatie van HVHL. Een deel van de doelsystemen is via provisioning aangesloten op het IAM-pakket. Voor deze systemen moeten accounts en rollen automatisch worden beëindigd. Andere doelsystemen zijn niet technisch gekoppeld, maar worden via een workflow opgevolgd. Voor deze systemen moeten de systeemeigenaren worden genotificeerd om accounts te disablen en rollen handmatig in te trekken.

Opdracht

- a) De uitdienstdatum van R.P. Meijer automatisch detecteert vanuit HR2Day.
- b) Het centrale account automatisch disabled op het moment dat de uitdienstdatum is aangebroken.
- c) Accounts in doelsystemen die via provisioning zijn aangesloten automatisch disabled.
- d) Rollen en rechten in provisioning-doelsystemen automatisch intrekt.
- e) Herkent welke doelsystemen niet via provisioning zijn aangesloten en daarbij een notificatie stuurt om het account te disablen.
- f) De systeemeigenaren een overzicht geeft van rollen en rechten die handmatig moeten worden ingetrokken.

2.7 Student klaar met opleiding

Situatie

Student T. Kooistra (Tessa), geboren op 26-04-2009 in Leeuwarden, doet de studie Bedrijfskunde en Agribusiness. In Osiris wordt geregistreerd dat Tessa per 1-7-2026 de studie succesvol heeft behaald. Vanaf deze datum plus 15 aantal dagen (grace period) mag deze persoon geen toegang meer hebben tot applicaties, systemen, rollen, autorisaties en bedrijfsinformatie van HVHL. Een deel van de doelsystemen is via provisioning aangesloten op het IAM-pakket. Voor deze systemen moeten accounts en rollen automatisch worden beëindigd. Andere doelsystemen zijn niet technisch gekoppeld, maar worden via een workflow opgevolgd. Voor deze systemen moeten de systeemeigenaren worden genotificeerd om accounts te disablen en rollen handmatig in te trekken.

Opdracht

- a) Studie afgerond wordt geadministreerd in Osiris.
- b) Het centrale account automatisch disabled 15 aantal dagen nadat de studie is afgerond.
- c) Accounts in doelsystemen die via provisioning zijn aangesloten automatisch disabled.

- d) Rollen en rechten in provisioning-doelsystemen automatisch intrekt.
- e) Herkent welke doelsystemen niet via provisioning zijn aangesloten en daarbij een notificatie stuurt om het account te disabelen.
- f) De systeemeigenaren een overzicht geeft van rollen en rechten die handmatig moeten worden ingetrokken.

3. AANVRAAG EN TOEKENNING VAN ROLLEN EN RECHTEN

3.1 Organisatie inrichting

Binnen HVHL vindt automatische toekenning van rollen plaats via role-based provisioning, op basis van kenmerken zoals functie, afdeling en status. Voor rechten die niet automatisch worden toegekend, wordt gebruikgemaakt van een aanvraagproces via het servicemanagementsysteem Topdesk. Deze aanvragen worden gekoppeld aan een referentienummer, zodat herleidbaar is waarom en op basis waarvan rechten zijn aangevraagd. HVHL gebruikt een rollenboek waarin is vastgelegd welke rollen en rechten aan functies, afdelingen of gebruikersgroepen mogen worden toegekend. Dit rollenboek wordt gebruikt om aanvragen en toekenningen te verifiëren.

3.2 Eisen

T-78	Ondersteuning voor privileged access.
T-81	Tijdelijke toegang met automatische vervaldatum.
F-45	Toewijzingsflow voor rollen door managers.

3.3 Iemand vraagt extra toegang aan

Medewerker S. (Sanne) Bakker, geboren op 18-05-1991 in Assen, werkt als administratief medewerker binnen de afdeling Studentzaken. Op basis van haar functie en afdeling krijgt zij automatisch de standaardrollen die horen bij haar functie. Voor een tijdelijk project rond diplomaverwerking heeft Sanne aanvullende toegang nodig tot een applicatie waarin studentdossiers kunnen worden ingezien. Deze toegang valt buiten haar standaardrollen. De manager van Sanne vraagt daarom extra toegang aan en doet een aanvraag met een omschrijving. De aanvraag wordt geregistreerd met Topdesk-referentienummer TD-2026-18472.

Opdracht

- Inzicht geeft in de rollen die automatisch zijn toegekend op basis van functie en afdeling.
- Een manager in staat stelt om aanvullende toegang aan te vragen met een verwijzing naar het TopDesk referentie nummer TD-2026-18472.
- De aanvraag routeert naar de juiste rolbeheerder of applicatie-eigenaar die de toegang toewijst af de aanvraag afwijst.
- Na goedkeuring de aanvullende rol of het recht toekent.
- Voor niet-aangesloten doelsystemen een workflow start voor handmatige opvolging.

3.4 Rechten dienen per direct ingetrokken te worden

Medewerker R. (Ruben) de Jong, geboren op 07-09-1983 in Groningen, werkt als functioneel beheerder binnen de afdeling ICT. Door een ernstig incident moet zijn toegang per direct worden ingetrokken. Dit kan bijvoorbeeld gaan om ontslag op staande voet, een vermoeden van misbruik of een datalek waarbij directe beperking van toegang noodzakelijk is.

De rolbeheerder moet rechten direct kunnen intrekken. Daarnaast moet bij calamiteiten ook een tweede bevoegde persoon deze actie kunnen uitvoeren, zodat HVHL niet afhankelijk is van één functionaris.

Opdracht

- a) De gebruiker **Ruben de Jong** opzoekt binnen het IAM-systeem en inzicht geeft in de actieve accounts, rollen en rechten.
- b) Een noodactie of directe intrekking van rechten ondersteunt en de account direct blokkeert.
- c) Rollen en rechten worden via provisioning-doelsystemen direct ingetrokken en de systemen die via workflow zijn aangesloten worden genotificeerd.
- d) Ondersteunt dat een tweede bevoegde persoon deze noodactie kan uitvoeren.
- e) Vastlegt wie de intrekking heeft uitgevoerd, wanneer dit is gedaan en waarom.

3.5 Tijdelijke toegang moet verleent worden

Medewerker L. (Linda) Vermeer, geboren op 12-01-1990 in Zwolle, werkt als projectmedewerker binnen de afdeling Onderwijsontwikkeling. Linda ondersteunt tijdelijk een project voor de implementatie van een nieuw onderwijsplatform. Voor dit project heeft zij gedurende drie maanden aanvullende toegang nodig tot een projectomgeving en een applicatie voor testgegevens. De toegang is tijdelijk en mag na afloop van het project niet actief blijven. De manager vraagt tijdelijke toegang aan met een startdatum van 01-09-2026 en een einddatum van 30-11-2026.

- a) De medewerker **Linda Vermeer** toont met haar bestaande standaardrollen.
- b) Een manager in staat stelt om tijdelijke toegang aan te vragen met daarin een begin- en einddatum
- c) Een toelichting vastlegt waarom de tijdelijke toegang nodig is.
- d) De aanvraag routeert naar de juiste goedkeurder die bij goedkeuring de tijdelijke rol of het tijdelijke recht toekent.
- e) De tijdelijke toegang automatisch intrekt op 30-11-2026.

4. BEHEER VAN INTEGRATIES MET BRON- EN DOELSYSTEMEN

4.1 Organisatie inrichting

Binnen HVHL worden identiteitsgegevens, attributen, rollen en autorisaties uitgewisseld tussen het IAM-pakket en verschillende bron- en doelsystemen. De huidige integratiefunctie via het ESB moet voor IAM-gerelateerde koppelingen zoveel mogelijk worden vervangen door functionaliteit binnen het nieuwe IAM-pakket. Nieuwe doelsystemen moeten met beperkte inspanning kunnen worden aangesloten en bestaande koppelingen moeten aanpasbaar zijn, bijvoorbeeld door attributen toe te voegen, attributen te wijzigen of de frequentie van gegevensuitwisseling aan te passen. Daarnaast moet duidelijk zichtbaar zijn wanneer een gegevensoverdracht fout gaat. Als een gebruiker, rol of recht niet goed wordt aangemaakt in een doelsysteem, moet het IAM-pakket inzicht geven in waar de fout zit, welke data is overgedragen en waarom de verwerking niet is gelukt.

4.2 Eisen

T-84	Instelbare frequentie voor ophalen brongegevens.
T-103	De leverancier biedt standaardconnectoren voor gangbare systemen en maakt inzichtelijk voor welke koppelingen maatwerk noodzakelijk is.
T-59	Synchronisatie kent varianten in timing (realtime, near realtime, batch).
T-17	Het IAM pakket moet een interface bevatten die OSIRIS kan aansluiten.

4.3 Integratie van nieuw doelsysteem

Binnen HVHL wordt een nieuw doelsysteem in gebruik genomen voor het beheren van stageplaatsen en praktijkopdrachten. De applicatie heet StageConnect en wordt gebruikt door studenten, docenten en stagecoördinatoren. Voor het gebruik van StageConnect moeten gebruikers automatisch worden herkend op basis van gegevens uit de bronsystemen. Studenten moeten toegang krijgen wanneer zij actief staan ingeschreven in Osiris en gekoppeld zijn aan een opleiding waarvoor stageonderdelen gelden. Docenten en stagecoördinatoren moeten toegang krijgen op basis van hun medewerker gegevens uit HR2Day, zoals functie, afdeling en dienstverbandstatus. HVHL wil StageConnect aansluiten op het IAM-pakket, zodat identiteiten, rollen en autorisaties automatisch kunnen worden doorgegeven. Daarbij moet worden bepaald welke attributen nodig zijn, welke rollen in StageConnect moeten worden aangemaakt en hoe mutaties vanuit Osiris en HR2Day worden verwerkt.

Opdracht

- Het nieuwe doelsysteem **StageConnect** registreert, inclusief doel, eigenaar en type koppeling.
- Vastlegt welke bronsystemen gegevens leveren, zoals **Osiris** voor studenten en **HR2Day** voor medewerkers.
- Configureert welke attributen worden uitgewisseld, zoals opleiding, studentstatus, functie, afdeling en dienstverbandstatus.
- Bepaalt welke rollen en autorisaties in StageConnect worden aangemaakt of toegekend.

- e) De provisioning naar StageConnect uitvoert en zichtbaar maakt welke gebruikers, rollen en rechten zijn doorgezet.
- f) Logging toont van succesvolle en mislukte transacties, inclusief beheerinformatie voor opvolging.

4.4 Aanpassen van volgorde, thresholds en attributen in de koppeling

Binnen HVHL wordt de koppeling tussen Osiris, het IAM-pakket en Moodle gebruikt om studenten toegang te geven tot digitale leeromgevingen. De toegang wordt bepaald op basis van attributen zoals studentstatus, opleiding, inschrijving, onderwijseenheid en startdatum. De opleiding Bedrijfskunde en Agribusiness wijzigt het onderwijsproces. Studenten moeten voortaan toegang krijgen tot Moodle zodra de inschrijving in Osiris voorlopig is goedgekeurd, in plaats van pas bij definitieve inschrijving. Daarvoor moet de attributenflow worden aangepast. De thresholds voor toegang wijzigt van definitief ingeschreven naar voorlopig goedgekeurd. Ook wordt een extra attribuut toegevoegd waarmee het startmoment van de student zichtbaar is. Het IAM-systeem moet laten zien hoe de functioneel beheerder deze wijziging zelf kan uitvoeren, welke attributen worden gebruikt en wat de impact is op studenten, rollen en Moodle-toegang. Ook moet de volgorde worden aangepast zodat de AD koppeling altijd voor de Moodle koppeling is met een bepaalde tijd tussen de koppelingen.

Opdracht

- a) De bestaande koppeling tussen Osiris, het IAM-pakket en Moodle toont, inclusief gebruikte attributen.
- b) De huidige toegangsvoorwaarde toont, bijvoorbeeld toegang bij status definitief ingeschreven.
- c) De toegangsvoorwaarde wijzigt naar status voorlopig goedgekeurd.
- d) Een extra attribuut toevoegt, bijvoorbeeld startmoment opleiding, en dit opneemt in de attributenflow.
- e) Een impactanalyse toont van de wijziging op studenten, rollen en Moodle-toegang. De wijziging gecontroleerd opslaat, activeert en vastlegt in logging.
- f) Zet de AD/Entra koppeling met tussentijd voor de Moodle koppeling.

4.5 Technisch beheer op koppeling met doelsystemen.

De technisch beheerder binnen HVHL controleert periodiek de werking van het IAM-systeem. Daarbij wordt in het bijzonder gelet op de verbindingen tussen de bron- en doelsystemen. Dagelijks wordt de log gecontroleerd op meldingen die onmiddellijke aandacht vereisen. Hiervoor wordt gebruikgemaakt van een eenvoudig toegankelijk, vooraf gedefinieerd filter in het systeem.

- a) De technisch beheerder opent de IAM-tool en controleert de log met behulp van een vooraf gedefinieerd filter, zodat relevante meldingen direct zichtbaar zijn.
- b) De technisch beheerder beoordeelt de meldingen.
- c) Indien verdere acties nodig zijn, worden deze uitgevoerd.
- d) Het resultaat van de controle wordt vastgelegd, eventueel in een externe tool zoals Excel.

5. AUTORISATIEMATRIX, ATTESTATIE EN RAPPORTAGE

5.1 Organisatie inrichting

Binnen HVHL is het belangrijk om inzicht te hebben in wie toegang heeft tot specifieke informatie, applicaties en systemen. Daarbij moet zichtbaar zijn welke rechten een persoon krijgt op basis van kenmerken zoals functie, afdeling, status of andere attributen. HVHL wil kunnen vergelijken wat de gewenste autorisatiesituatie is ten opzichte van de werkelijke situatie. In de gewenste situatie is vastgelegd welke rollen en rechten horen bij een bepaalde functie, afdeling of gebruikersgroep. In de werkelijke situatie is zichtbaar welke rollen en rechten daadwerkelijk zijn toegekend. Deze vergelijking is belangrijk voor rolbeheerders, applicatie-eigenaren, security en auditors. Zij moeten periodiek kunnen controleren of er afwijkingen zijn, bijvoorbeeld door losse aanvragen, foutieve toekenningen, handmatige wijzigingen of rechten die na uitdiensttreding niet correct zijn ingetrokken.

Daarnaast wil HVHL kunnen rapporteren over de werking van de in-, door- en uitstroomprocessen. Daarbij moet zichtbaar zijn of actieve medewerkers de juiste rechten hebben gekregen en of medewerkers die uit dienst zijn geen actieve rollen, rechten of accounts meer hebben, behalve wanneer sprake is van een gecontroleerde grace period.

5.2 Eisen

F-51	Controleerbaarheid van rechten.
F-4	Notificaties bij taak-, fout- en lifecycle gebeurtenissen.
G-14	Rapportages over aantallen studenten, cursisten, medewerkers en tijdelijke gebruikers per bronstroom moeten beschikbaar zijn.
F-46	Accounts zonder geldige actieve inschrijving, cursusdeelname of dienstverband moeten inzichtelijk zijn.
T-105	Er moet aantoonbaar worden gecontroleerd of uitgeschreven studenten / medewerkers uit dienst en beëindigde cursisten geen actieve rechten meer hebben.
T-74	Afwijkingen tussen bronregistraties, accounts en autorisaties in doelsystemen moeten kunnen worden signaleerd.
T-82	Studentidentiteiten vanuit OSIRIS-brongegevens.

5.3 Self-detectie van ongeautoriseerde rechten

Medewerker T. (Thomas) van Dijk, geboren op 03-02-1987 in Arnhem, werkt als docent Bedrijfskunde binnen de afdeling Onderwijs Bedrijfskunde en Agribusiness. Op basis van zijn functie en afdeling heeft Thomas standaard toegang tot M365, wifi, Moodle en de onderwijsapplicaties die bij zijn opleiding horen. Deze rechten zijn via het IAM-systeem toegekend. Tijdens een controle blijkt dat Thomas in een doelsysteem ook een beheerdersrol heeft gekregen. Deze rol is niet via het IAM-systeem aangevraagd, niet goedgekeurd en staat niet in de autorisatiematrix voor zijn functie. Het IAM-systeem moet deze afwijking automatisch signaleren. In het gebruikersprofiel moet zichtbaar zijn welk recht buiten het

IAM-proces is toegekend, in welk doelsysteem dit is gebeurd en waarom dit afwijkt van de verwachte autorisaties.

Opdracht

- a) Bij een gebruiker zichtbaar maakt welke rollen en rechten zijn toegekend via het IAM-systeem en welke rechten buiten het IAM-systeem om in een doelsysteem zijn toegekend.
- b) Signaleert wanneer een gebruiker rechten heeft die niet passen bij de autorisatiematrix, de functie, afdeling of actuele status van de gebruiker.
- c) Rechten toont die zijn verlopen, maar nog steeds actief zijn in het IAM-systeem of in een gekoppeld doelsysteem.
- d) Visueel onderscheid maakt tussen correcte rechten, afwijkende rechten, verlopen rechten en rechten die buiten het IAM-proces om zijn toegekend.
- e) De afwijking koppelt aan het betreffende doelsysteem, de rol, de datum van toekenning en de mogelijke oorzaak.
- f) Ondersteunt dat de rolbeheerder of beheerder de afwijking kan beoordelen en corrigeren, bijvoorbeeld door het recht in te trekken of opnieuw onder beheer van het IAM-systeem te brengen.

5.4 Auditrapportage

Security Officer M. (Maaïke) de Boer, geboren op 11-08-1981 in Leeuwarden, voert maandelijks een IAM-controle uit als onderdeel van de risicoanalyse op privacy en informatiebeveiliging. Zij gebruikt rapportages uit het IAM-systeem om te controleren of uitdienstmedewerkers geen actieve accounts, rollen of rechten meer hebben. Ook controleert zij of hoog geclassificeerde rollen correct zijn aangevraagd en goedgekeurd. Tijdens de controle ziet Maaïke dat medewerker R. (Ruben) Meijer op 31-05-2026 uit dienst is gegaan, maar in één doelsysteem nog een actief account heeft. Daarnaast ziet zij dat medewerker S. (Sanne) Bakker een hoog geclassificeerde rol heeft gekregen zonder vastgelegde tweede goedkeuring. Maaïke registreert deze bevindingen als afwijkingen. De rapportage toont per afwijking welke gebruiker, rol of systeem geraakt is, wat het risico is en welke opvolging nodig is. Op basis hiervan kan HVHL rechten intrekken, accounts disablen of het aanvraag- en goedkeuringsproces verbeteren.

Opdracht

- a) Periodieke auditrapportages kan genereren, bijvoorbeeld maandelijks, waarin afwijkingen binnen het IAM-proces zichtbaar worden gemaakt.
- b) Rapporteer over de werking van geautomatiseerde processen, zoals accountaanmaak, provisioning, deprovisioning, roltoekenning, rolintrekking en verwerking van einddatums.
- c) Inzicht geeft in afwijkingen buiten de afgesproken proceswerking, zoals accounts die te laat zijn disabled, rechten die niet tijdig zijn ingetrokken of tijdelijke rechten die langer actief zijn dan toegestaan.

- d) Rapporteert over handmatige acties, zoals handmatige toekenningen, handmatige intrekkingen, noodblokkades, goedkeuringen en correcties.
- e) Laat zien wanneer toegang is geblokkeerd, wanneer accounts zijn disabled, wanneer rechten zijn toegekend en wanneer rechten zijn ingetrokken.
- f) Auditinformatie beschikbaar stelt voor beoordeling van ontwerp, werking, afwijkingen en verbetermaatregelen binnen de PDCA-cyclus.

5.5 Attestatie

Rolbeheerder M. (Maaïke) Visser, geboren op 19-06-1982 in Zwolle, beoordeelt periodiek de rollen binnen de afdeling Studentzaken. In de autorisatiematrix is vastgelegd welke rollen horen bij functies binnen deze afdeling. Tijdens de attestatie vergelijkt Maaïke de gewenste situatie uit de autorisatiematrix met de feitelijke rollen uit het IAM-systeem en de gekoppelde doelsystemen. Daarbij blijkt dat medewerker L. (Laura) Smit, administratief medewerker Studentzaken, nog een rol heeft uit haar vorige functie binnen Examenadministratie. Deze rol hoort niet bij haar huidige functie. De rolbeheerder moet deze afwijking kunnen beoordelen en vastleggen of de rol terecht is, tijdelijk mag blijven bestaan of moet worden ingetrokken. De uitkomst van de attestatie wordt geregistreerd, zodat aantoonbaar is dat de rollen periodiek zijn beoordeeld

Opdracht

- a) Een rolbeheerder inzicht geeft in de rollen waarvoor hij of zij verantwoordelijk is, inclusief standaardrollen, uitzonderingsrollen en hoog geclassificeerde rollen.
- b) Per rol laat zien welke medewerkers deze rol volgens de autorisatiematrix zouden moeten hebben en welke medewerkers deze rol feitelijk hebben.
- c) Een is-/soll-vergelijking uitvoert waarbij afwijkingen in twee richtingen zichtbaar worden: medewerkers die een rol missen en medewerkers die een rol onterecht hebben.
- d) Ondersteunt dat per rol kan worden vastgelegd wie de aanvraag of toekenning mag accorderen, bijvoorbeeld een manager, rolbeheerder of andere aangewezen persoon.
- e) De rolbeheerder in staat stelt om afwijkingen te beoordelen en direct opvolging te geven, bijvoorbeeld door een rol te bevestigen, in te trekken of alsnog toe te kennen.
- f) De uitkomst van de attestatie vastlegt, zodat deze gebruikt kan worden als onderbouwing voor auditrapportage en verdere verbetering van het autorisatiebeheer.

6. ROLBEHEER PROCES

6.1 Organisatie inrichting

Binnen HVHL worden rollen gebruikt om toegang tot applicaties, gegevens en voorzieningen gecontroleerd toe te kennen. Rollen vormen de verbinding tussen functie, afdeling, proces, applicatie en de rechten die een gebruiker krijgt.

Voor iedere rol moet duidelijk zijn waarvoor de rol bedoeld is, welke rechten eraan gekoppeld zijn en wie eigenaar is van de rol. De rolbeheerder of eigenaar is verantwoordelijk voor het actueel houden van de rol, het beoordelen van wijzigingen en het bewaken van het juiste gebruik. Rollen moeten beheersbaar blijven gedurende de volledige levenscyclus. Dit betekent dat rollen kunnen worden aangemaakt, gewijzigd, goedgekeurd, gepubliceerd, ingetrokken of beëindigd. Wijzigingen in rollen moeten herleidbaar zijn, zodat duidelijk is wie een rol heeft aangepast, waarom dit is gedaan en welke gebruikers of systemen daardoor worden geraakt.

6.2 Eisen

F-83	Koppeling tussen rollen en functies.
F-44	Aantoonbaarheid van standaardrechten en afwijkingen.
F-53	Meerdere rollen en rechten per medewerker.
T-79	Classificatie van data en rollen.
F-45	Wijzigingen kunnen simuleren zonder deze daadwerkelijk door te voeren naar doelsystemen.

6.3 Aanmaken van een nieuwe rol

Binnen HR2Day wordt gewerkt met de formele functie administratief medewerker. Voor deze functie moet een nieuwe IAM-rol worden ingericht, omdat medewerkers toegang nodig hebben tot een nieuw administratief informatiesysteem. HR, de rolbeheerder en de applicatie-eigenaar bepalen samen welke autorisaties bij deze functie horen. HR geeft aan voor welke functie en doelgroep de rol bedoeld is. De applicatie-eigenaar geeft aan welke rechten binnen het informatiesysteem nodig zijn. De rolbeheerder vertaalt dit naar een nieuwe rol in het IAM-systeem. De rol krijgt een naam, omschrijving, eigenaar, doelgroep, gekoppelde autorisaties en een toekenningspolicy. Daarbij wordt bepaald of de rol automatisch wordt toegekend op basis van de functie administratief medewerker, of apart moet worden aangevraagd. Het IAM-systeem moet laten zien hoe een nieuwe rol wordt aangemaakt, gekoppeld aan HR2Day, opgenomen in de autorisatiematrix en voorzien van eigenaarschap, rechten en policy.

Opdracht

- Een nieuwe rol kan aanmaken voor de functie administratief medewerker op basis van het functiehuis uit HR2Day.
- Kan vastleggen welke doelgroep, functie, afdeling en eigenaar bij de rol horen.

- c) Autorisaties uit het betreffende informatiesysteem kan koppelen aan de nieuwe rol.
- d) Kan bepalen of de rol automatisch wordt toegekend via een policy of apart moet worden aangevraagd.
- e) Geef een classificatie aan een rol.
- f) De nieuwe rol kan opnemen in het rollenmodel en de autorisatiematrix.

6.4 Wijzigen van een bestaande rol

Binnen HR2Day wordt de nieuwe formele functie coördinator studentadministratie aangemaakt. Deze functie lijkt op administratief medewerker Studentzaken, maar bevat extra taken voor controle, rapportage en procesbewaking. Medewerker L. (Laura) Smit, geboren op 08-04-1990 in Arnhem, wordt in HR2Day geregistreerd met deze nieuwe functie. Er blijkt nog geen passende IAM-rol te bestaan. De bestaande rol Studentzaken Administratie geeft te weinig rechten; de teamleider rol geeft te veel rechten. De rolbeheerder bespreekt met HR en de applicatie-eigenaren welke autorisaties nodig zijn. Besloten wordt om de bestaande rol uit te breiden met een aparte variant voor coördinatoren. Deze rol krijgt extra rapportagerechten, maar geen beheerrechten. Het IAM-systeem moet laten zien hoe een bestaande rol wordt aangepast, welke rechten wijzigen, wie eigenaar is van de rol en welke goedkeuring is vastgelegd

Opdracht

- a) De bestaande rol Studentzaken Administratie toont, inclusief gekoppelde rechten, gebruikers, eigenaar en toekenningspolicy.
- b) Inzicht geeft in welke rechten ontbreken voor de nieuwe functie coördinator studentadministratie.
- c) Ondersteunt dat extra rapportagerechten worden toegevoegd en beheerrechten uitgesloten blijven.
- d) Laat zien welke gebruikers geraakt worden door de wijziging van de rol.
- e) De gewijzigde rol koppelt aan de nieuwe formele functie uit HR2Day en verwerkt in de autorisatiematrix.

6.5 Bulk wijzigingen doorvoeren

Binnen HR2Day wordt de organisatiestructuur gewijzigd. De afdeling Studentzaken wordt samengevoegd met Onderwijsadministratie. Hierdoor veranderen de functies, afdelingen en de bijbehorende roltoekenningen van meerdere medewerkers. Voordat de wijzigingen worden doorgevoerd, wil de rolbeheerder inzicht krijgen in de gevolgen van deze wijziging. De organisatie wil voorkomen dat medewerkers onbedoeld rechten verliezen of juist extra rechten krijgen. Het IAM-systeem moet daarom een simulatie kunnen uitvoeren waarin zichtbaar wordt welke rollen worden ingetrokken, welke nieuwe rollen worden toegekend en welke medewerkers hierdoor worden geraakt. Pas nadat de uitkomst is gecontroleerd en akkoord is bevonden, worden de wijzigingen definitief uitgevoerd.

Opdracht

- a) Een wijziging in functies, afdelingen of het rollenmodel kan simuleren zonder direct wijzigingen door te voeren.

- b) Inzicht geeft welke medewerkers door de wijziging worden geraakt.
- c) Laat zien welke rollen en rechten worden ingetrokken en welke nieuwe rollen worden toegekend.
- d) De impact van de wijziging toont voordat deze wordt uitgevoerd, inclusief eventuele conflicten of uitzonderingen.
- e) Ondersteunt dat de simulatie wordt beoordeeld en goedgekeurd voordat de wijzigingen definitief worden verwerkt.
- f) De definitieve rolwijzigingen na akkoord automatisch doorvoert en vastlegt in auditlogging.