

Identity & Acces Management

11 december 2025

Henk Links, Max Passet, Henry Meutstege

SAMENWERKEN AAN

CYBERVEILIGHEID

IN HET MBO



Agenda



1. Waarom is IAM belangrijk?
2. De neuzen dezelfde kant op
3. SURFaudit toetsingkader IB
4. Templates: SURF & MBO Digitaal
5. Discussie
6. Oproep: start IAM-werkgroep

Waarom is IAM belangrijk?

- IAM is een belangrijk domein om IB & Privacy aantoonbaar op orde te houden.
- Audits laten lage volwassenheid zien op IAM.
- IAM koppelt toegang aan betrouwbare brondata en rollen; minder handwerk, minder fouten en betere verantwoording.
- In de 2^{de} Security audit toetsen op werking
- Voor deelname aan de Cyberweerbaarheidspool is op het IAM-domein compliance vereist.



De neuzen dezelfde kant op....

(Definities)

Logisch Toegangsbeheer (Identity and Access Management): processen, technologieën en afspraken die bepalen wie toegang heeft tot wat, wanneer en onder welke voorwaarden.

Kernbegrippen:

- Identificatie: digitale identiteit (attributen)
- Authenticatie
- Autorisatie
- Provisioning & deprovisioning
- Levenscyclusbeheer (instroom, doorstroom, uitstroom)



SURFaudit toetsingskader IB

Statemen	Onderwerp	Waar het om gaat
OR.02	Functiescheiding	Taken worden gescheiden zodat één persoon geen kritieke processen kan beïnvloeden.
HR.04	Verandering of beëindiging van functie	Bij functiewijziging of vertrek worden verantwoordelijkheden opnieuw toegewezen en toegangsrechten direct verwijderd om continuïteit en veiligheid te borgen.
ID.01	Toegangsrechten	Rollen en rechten zijn vastgelegd in een autorisatie-matrix (SOLL) en herleidbaar per gebruiker.
ID.02	Administratie van toegangsrechten	Toegang wordt toegekend, gewijzigd en ingetrokken via formele, controleerbare procedures.
ID.03	Super-user toegang	Super-user rechten zijn beperkt, goedgekeurd en worden gemonitord.
ID.04	Noodtoegang	Noodprocedures zijn gedocumenteerd, gelogd en geëvalueerd.
ID.05	Periodieke toetsing	SOLL- en IST-situatie worden vergeleken, afwijkingen worden hersteld.
SM.02	Authenticatiemechanismes	Unieke accounts, centraal beheerd. Authenticatie volgens beleid (incl. MFA). Functiescheiding in aanvragen en toekennen. Inactieve accounts worden tijdig verwijderd.

Templates: SURF & MBO Digitaal

- SURF-templates

- Standaard identiteits- en toegangsbeheer
- Richtlijn toekennen en intrekken autorisaties
- Richtlijn autorisatiebeheer en controle
- Template Autorisatiematrix
- Handreiking Richtlijn Wachtwoorden
- Handreiking Wachtwoorden kluis

Bekrachtigd door: Bestuur, CvB
Looptijd: 3 – 5 jaar
Review: 1 jaar

Bekrachtigd door: CISO, Dir. ICT, CIO-office
Looptijd: 1 – 3 jaar
Review: 1 jaar

Bekrachtigd door: betreffend Management
Looptijd: 1 jaar
Review: 1 jaar

Bekrachtigd door: betreffend Management
Looptijd: 1 jaar
Review: 1 jaar

Beleid (waarom)
Strategisch en macro niveau

Standaard (wat)
Tactisch en meso niveau

Richtlijn (hoe)
Tactisch en meso niveau

Procedure en handleiding (hoe)
Operationeel en micro niveau

- Programma Cyberveiligheid: pragmatisch beleidsdocument (netwerk IB&P, afgeleid van SURF templates)
- Voor de 2^{de} Security audit, Identity Management statements worden op werking getoetst
- Voor Cyberweerbaarheidspool compliance: focus op de kroonjuwelen

IAM-processen

- **Administratieve Processen**

- Nieuwe Medewerker
- Nieuwe aanvraag (standaard)
- Nieuwe Rol / Verruimen bestaande rol
- Wijziging functie/ afdeling
- Uitdiensttreding
- Intrekken rollen / autorisatie (zonder uitdiensttreding)

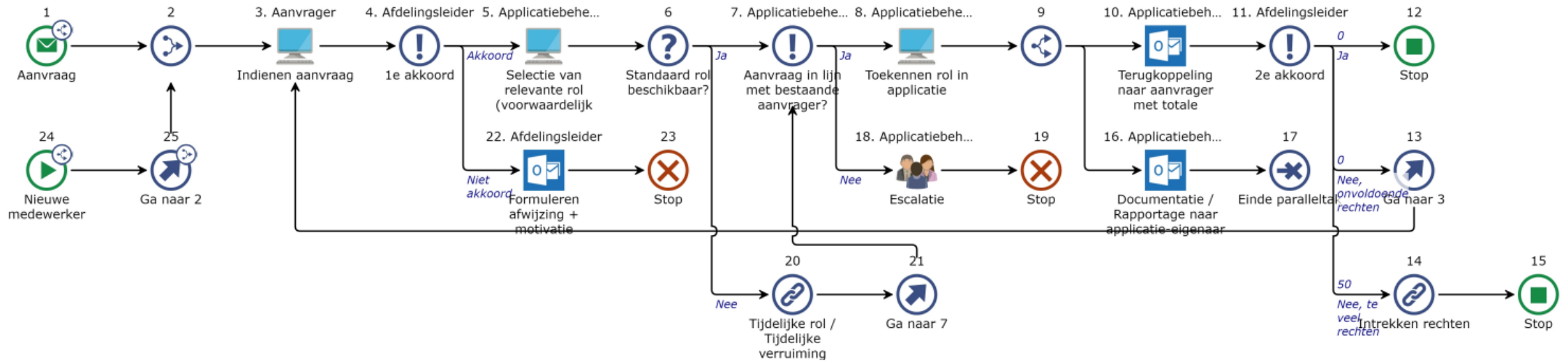
- **Controle processen**

- Evaluatie SOLL / IST
- Jaarevaluatie

- **Superuser processen**

- Creëren SuperUser Account
- Evaluatie SuperUser Account
- Envelop procedure

Voorbeeld: Nieuwe aanvraag



Discussie (1/3)

Stelling:

De data eigenaar bepaald wie toegang krijgt tot een applicatie

Eens of oneens?



Discussie (2/3)

Stelling:

Elke beheerder heeft super user rechten nodig om zijn werk goed te kunnen doen

Eens of oneens?



Discussie (3/3)

Stelling:

Een autorisatiematrix bestaat uit een overzicht van rollen, de rechten die bij de rol horen en een overzicht van gebruikers die deze rol hebben...

Eens of oneens?



Leeftijd is
als wijn
hoe ouder
hoe beter!

IAM-werkgroep

Doel:

- Delen best practices
- Concrete templates en procedures opleveren
(autorisatiematrix, processen, reviews).

