



# IAM en ITAM strategisch gecombineerd

Whitepaper oktober 2025

# Inhoudsopgave

Management samenvatting.....	3
Introductie.....	3
Wat is IAM? .....	3
Wat is ITAM? .....	4
De verbinding tussen IAM en ITAM.....	4
Strategische waarde van de integrale aanpak.....	4
Praktijkvoorbeeld: onboarding en offboarding .....	5
Tot slot .....	5

## Management samenvatting

Organisaties zijn sterk afhankelijk geworden van digitale middelen. Identity & Access Management (IAM) en IT Asset Management (ITAM) zijn beide cruciaal, maar worden vaak los van elkaar benaderd. Door IAM en ITAM te integreren, ontstaat niet alleen meer grip op toegang en middelen, maar ook voorspelbaarheid in kosten, verhoogde wendbaarheid, eenvoudiger compliance en risicobeheersing. Organisaties die dit strategisch aanpakken benutten hun volledige IT-landschap en creëren concurrentievoordeel.

## Introductie

Organisaties zijn in toenemende mate afhankelijk van hun digitale middelen. (SaaS) applicaties, systemen, data en cloud resources zijn niet langer ondersteunend, maar vormen de kern van de bedrijfsvoering. Daarmee groeit ook de noodzaak om controle te hebben over wie toegang heeft tot welke middelen – autorisatie, het bewijzen van de bijbehorende identiteit – authenticatie, en welke kosten daartegenover staan.

Identity & Access Management (IAM) en IT Asset Management (ITAM) zijn disciplines die ieder op hun manier bijdragen aan grip en veiligheid. Toch worden ze vaak los van elkaar behandeld, terwijl juist hun samenhang een veel grotere waarde oplevert.

Dit whitepaper laat zien hoe IAM en ITAM elkaar versterken, hoe begrippen als RBAC en IGA daarbinnen passen, en waarom een geïntegreerde aanpak een sleutel is tot wendbaarheid, voorspelbaarheid en kostenbeheersing.

## Wat is IAM?

Identity & Access Management is het geheel aan processen en technologieën waarmee organisaties bepalen wie toegang heeft tot welke middelen. De essentie is eenvoudig samen te vatten: de juiste persoon, met de juiste rechten, op het juiste moment.

Binnen IAM onderscheiden we twee belangrijke pijlers. De eerste is Role Based Access Control (RBAC). Dit maakt gebruik van rollen die gekoppeld zijn aan functies, met binnen elke rol een standaard set aan gebruiksrechten voor bijvoorbeeld applicaties en opslaglocaties. Een medewerker in de rol van financial controller krijgt automatisch toegang tot de financiële applicaties die daarvoor nodig zijn, met daarbinnen o.a. de juiste rechten om facturen goed te keuren. Eén van de grote voordelen daarbij is dat wanneer de medewerker een andere functie gaat bekleden en de rol vervalt (de medewerker is dan een zogenaamde ‘mover’), de rechten ook automatisch weer ingetrokken worden. Hierdoor worden risico's met betrekking tot security (o.a. bij uitdiensttreding) verminderd, wordt bedrijfscontinuïteit vergroot en zijn kosten beter beheersbaar.

De tweede is Identity Governance & Administration (IGA), dat zich richt op het bredere beheer van de volledige lifecycle van autorisatie en authenticatie, ondersteund door gespecialiseerde tooling. Het omvat niet alleen processen zoals het aanvragen, goedkeuren en intrekken van rechten, maar ook periodieke controles, certificeringen en rapportages. Waar RBAC zorgt voor een gestandaardiseerde toekenning van rechten op basis van rollen, biedt IGA de middelen om dit continu te monitoren, te auditen en te automatiseren. Bijkomend voordeel is dat dit op zichzelf besparingen met zich meebrengt door de verlaging van belasting bij medewerkers. Denk aan selfservice portals voor toegang, workflows voor managers en dashboards waarmee compliance aantoonbaar wordt gemaakt. Daarmee waarborgt IGA

niet alleen dat rechten efficiënt worden toegekend, maar vooral ook dat ze in lijn blijven met zowel interne beleidsregels en externe wet- en regelgeving.

## Wat is ITAM?

ITAM is een volwassen discipline binnen de IT (met een nadruk op IT-governance) die zich richt op het beheren van IT-middelen gedurende hun gehele levenscyclus. Dit omvat o.a. software, hardware, licenties, cloud resources en Software as a Service (SaaS). ITAM speelt een cruciale rol in kostenbeheersing, risicomanagement, naleving van regelgeving en contractuele verplichtingen.

Een effectieve ITAM-practice begint met een actueel, volledig en centraal aangelegd overzicht van alle IT-assets binnen een organisatie. Dit stelt organisaties in staat om te bepalen welke middelen actief in gebruik zijn, welke overbodig zijn en waar optimalisaties (o.a. door het begrijpen van en voldoen aan complexe licentievoorwaarden) mogelijk zijn. Door het gehele lifecycle van IT-assets – van aanschaf tot uitfasering – centraal te stellen, kunnen organisaties strategische keuzes maken die zowel kostenbesparend als risicoverlagend werken.

Een volwassen ITAM-practice voorkomt verspilling, ondersteunt financiële sturing, mitigeert veiligheidsrisico's en levert de basis voor compliance en audits. Waar IAM zich richt op toegang, richt ITAM zich op IT-middelen. Beide domeinen zijn onlosmakelijk verbonden, maar worden in de praktijk vaak vanuit gescheiden teams en doelstellingen benaderd.

## De verbinding tussen IAM en ITAM

IAM bepaalt wie toegang krijgt tot welke middelen. ITAM registreert welke middelen aanwezig zijn, wat ze kosten en hoe en waar ze gebruikt worden.

Die verbinding maakt dat de data waar ITAM gebruik van maakt, verrijkt kan worden via IAM-data, en vice versa. Voor het inrichten van RBAC en het in kaart brengen van daadwerkelijk gebruik van IT-middelen kan IAM leunen op ITAM. Wanneer de toewijzing, mutaties en het intrekken van rechten niet goed zijn ingericht, heeft dit ook impact op het gebruik van IT-middelen en resulteert dit in bijkomende risico's.

Een voorbeeld: stel dat een medewerker overstapt van de financiële afdeling naar HR. Zonder een goed ingericht IAM-proces behoudt die medewerker vaak de gebruiksrechten voor financiële applicaties, opslaglocaties en mogelijk rechten om facturen goed te keuren, terwijl daar geen enkele functionele noodzaak meer voor is. Vanuit ITAM-perspectief lijkt het dan alsof er nog steeds licenties in gebruik zijn, tenzij het daadwerkelijke gebruik gemeten kan worden. In de werkelijkheid is dat vaak niet zo is. De organisatie betaalt voor onnodige licenties én loopt daarnaast een verhoogd risico.

Wanneer RBAC en IGA goed zijn ingericht, worden rechten zoals eerder vermeld ook automatisch aangepast bij functiewijzigingen. IAM wordt zo een betrouwbare bron voor ITAM.

## Strategische waarde van de integrale aanpak

De koppeling tussen IAM en ITAM levert strategische voordelen op die verder gaan dan kostenbesparingen en compliance.

Een eerste voordeel is voorspelbaarheid. IAM-data geeft direct inzicht in wie welke middelen nodig heeft. ITAM kan dit vertalen naar verwachte kosten, toekomstige licentiebehoeften, kostenefficiënt licentiëren

en investeringsscenario's die verbonden zijn aan bijvoorbeeld de IT-strategie. Ook maakt dit doorbelasting op basis van rollen mogelijk.

Een tweede voordeel is wendbaarheid. Organisaties die IAM en ITAM verbinden, kunnen sneller reageren op veranderingen. Nieuwe medewerkers krijgen direct de juiste toegang én bijbehorende middelen. Bij reorganisaties of fusies kan de verdeling van rechten en IT-middelen eenvoudig worden herzien.

Een derde voordeel is compliance en risicobeheersing. Door toegang en IT-middelen integraal te managen, kan een organisatie eenvoudig laten zien wie waar toegang toe heeft, waarom dat zo is, en welke kosten eraan verbonden zijn. Zo borgen zij dat (gevoelige) data niet onnodig wordt ingezien.

## Praktijkvoorbeeld: onboarding en offboarding

De waarde van de integrale aanpak wordt duidelijk in iets ogenschijnlijk eenvoudigs als het in- en uit dienst treden van medewerkers, ook wel bekend als joiners-movers-leavers processen.

Bij onboarding is snelheid cruciaal. Als IAM en ITAM los van elkaar functioneren, leidt dat vaak tot vertraging en fouten: wel toegang tot de applicatie, maar geen licentie. Of juist wel een licentie, maar geen hardware of geïnstalleerde software. Met een geïntegreerde aanpak waarborgt de organisatie dat deze twee naadloos op elkaar aansluiten. De rol van de medewerker bepaalt de rechten (IAM), die automatisch gekoppeld zijn aan de benodigde IT-middelen, zoals software en hardware (ITAM).

Bij offboarding is het risico minstens zo groot. Zonder integratie blijven rechten en licenties vaak onnodig toegekend aan het account van de uit dienst getrede medewerker. Dat kost onnodig geld en verhoogt het risico op misbruik. Met een geïntegreerde aanpak wordt dit in één keer opgelost: het intrekken van een identiteit leidt direct tot het vrijgeven van bijbehorende middelen.

## Tot slot

IAM en ITAM worden vaak benaderd vanuit verschillende invalshoeken, waaronder security en kostenbeheersing. Maar de organisaties die IAM en ITAM integraal aanpakken, benutten hun volle strategische potentieel. IAM zorgt voor de juiste toegang, ITAM voor inzicht in middelen en kosten. Samen zorgen ze voor inzicht, voorspelbaarheid, wendbaarheid en compliance. Echter is elke organisatie anders: de manier waarop IAM en ITAM samenkomen, hangt sterk af van het IT-landschap, de processen en de cultuur. Wilt u weten welke waarde er in uw organisatie te behalen is? Dan kan een verkennend gesprek met The ITAM-Unit al veel inzicht bieden!