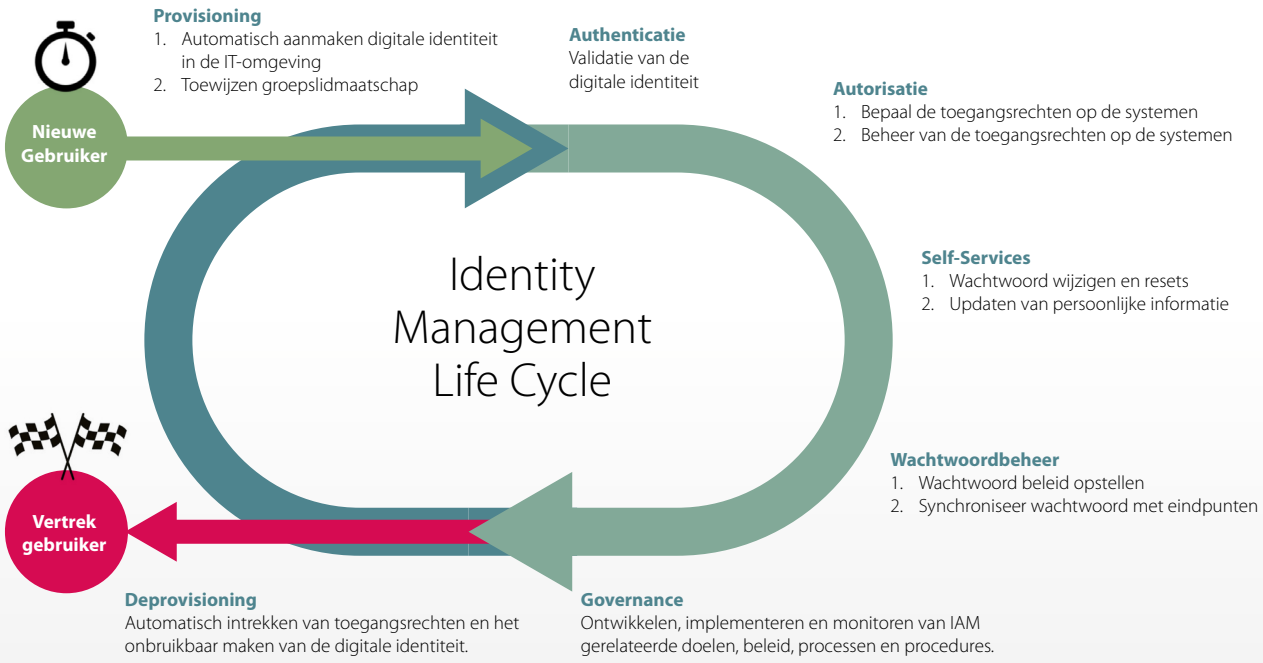
IAM het fundament van digitale beveiliging

Waarom IAM?

Identity and Acces Management (IAM) is van cruciaal belang in de digitale beveiliging van een organisatie. Op het moment dat een kwaadwillend persoon gebruik kan maken van een digitale identiteit, kan deze bij alle gegevens waartoe de digitale identiteit gemachtigd is. Alle geïmplementeerde processen en software om kwaadwillende personen de toegang te beletten, spelen op dat moment geen rol meer. IAM omvat het beheer van de digitale identiteit gedurende de volledige levenscyclus. Van de start van de relatie tot en met het einde van de relatie met de daaraan gerelateerde toegang tot gegevens. Op het moment dat IAM goed functioneert binnen de organisatie wordt een grote stap gezet in het beschermen van waardevolle gegevens, kan voldaan worden aan de gestelde audit en compliance eisen en wordt door middel van single sign-on de gebruikersvriendelijkheid van applicaties verhoogd.

De onderstaande afbeelding toont de onderwerpen die aan IAM gerelateerd zijn.



Aanpak IAM-traject

Uit het oogpunt van informatiebeveiliging en compliancy heeft de toename in het digitaal samenwerken tot gevolg dat IAM een belangrijk onderwerp is op de agenda van het management. Een IAM-traject heeft impact op de gehele organisatie en niet uitsluitend op de IT-afdeling. IAM vormt het fundament in de digitale beveiliging van de organisatie. IAM is een continu proces dat een belangrijke plaats in de organisatie verdient. Een goed functionerend IAM is onontbeerlijk voor elke organisatie.

Bauhaus helpt je IAM als fundament van digitale beveiliging neer te zetten.
Bij het neerzetten van IAM als fundament van digitale beveiliging, kan Bauhaus zowel de rol van adviseur als regisseur vervullen. De aanpak die Bauhaus hanteert als regisseur, bestaat uit de fasen:

FASE 1 **Status IAM-implementatie bepalen.** De status van de IAM-implementatie wordt bepaald op basis van principes met bijbehorende criteria. In een workshop wordt aan elk principe een risicowaarde toegekend. Deze fase levert een rapport op waarin de principes beschreven staan met de bijbehorende risico's, de status per principe met de vastgestelde risicowaarde en een globale beschrijving van de mogelijke mitigerende maatregel.

FASE 2 **Ontwikkelen en implementeren mitigerende maatregelen.** Op basis van het rapport uit fase 1 bepaalt de organisatie welke risico's onacceptabel zijn en direct moeten worden gemitigeerd en welke risico's (tijdelijk) worden geaccepteerd. Voor de risico's die direct gemitigeerd dienen te worden, worden (tijdelijke) maatregelen ontwikkeld en geïmplementeerd.

FASE 3 **Opstellen IAM-doelarchitectuur.** De IAM-doelarchitectuur heeft als doelgroep het management van de organisatie en heeft een horizon van drie jaar. De doelarchitectuur omvat de organisatie visie en strategie, de huidige situatie, de marktontwikkeling op IAM-gebied, de toekomstige situatie (het doel) en hoe de IAM-doelarchitectuur past in de security strategie van de organisatie.

FASE 4 **IAM-implementatie.** In de implementatie fase stelt Bauhaus samen met de organisatie de IAM-roadmap en planning op. Op basis van de doelarchitectuur wordt het IAM-beleid en de IAM-processen en procedures beschreven en vastgesteld. Ook worden verantwoordelijkheden behorend bij een IAM-rol opgesteld en productkeuzes gemaakt met betrekking tot ondersteunende middelen (tools) op IAM-gebied. Zodra deze zaken zijn afgerond vinden de wijzigingen in de organisatie plaats met betrekking tot de manier van werken op IAM-gebied en wijzigingen in de techniek. Omdat een IAM-implementatie niet alleen impact heeft op de IT-afdeling, wordt voor het wijzigen van de manier van werken samengewerkt met de Bauhaus specialisten van de afdeling People & Change. Voor wijzigingen in de techniek wordt samengewerkt met de One Zero IT specialisten van de afdeling Security.

BAUHAUS ARTITECH

Bauhaus ArtITech
Van Deventerlaan 30 - 40
3528 AE Utrecht

Tel. +31 30 711 88 44
info@bauhaus.nl
www.bauhaus.nl