I A M

Identity & Access Management

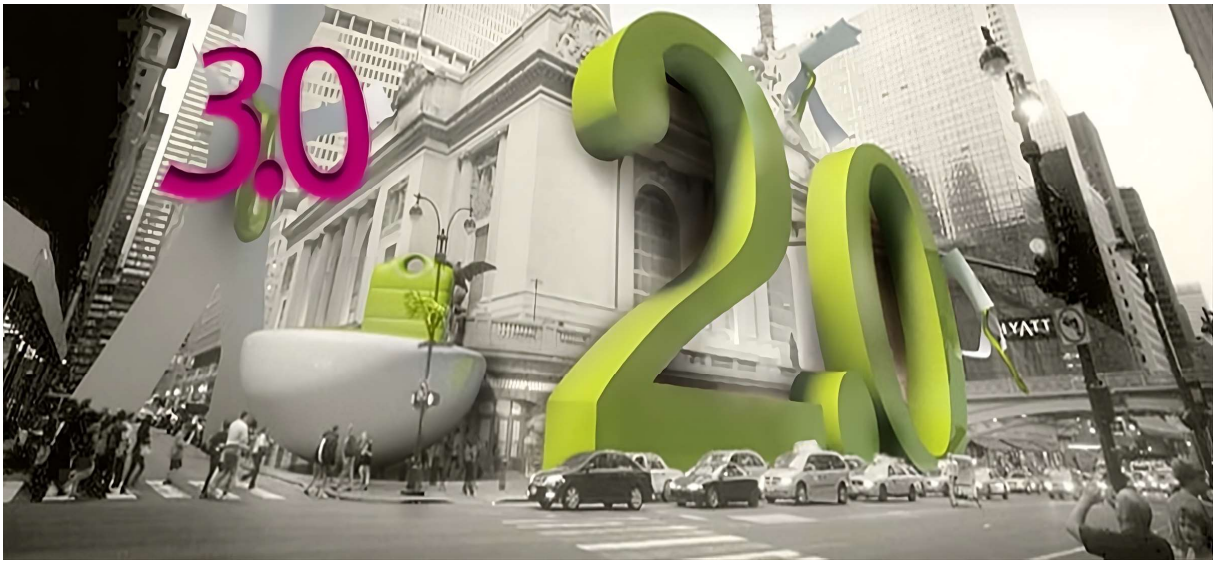
binnen de Gemeente

Door:

Frido Tactor

HFT **Communications B.V.**

Datum:
08-02-2025



Overzicht / Inhoud

1. Inleiding

In een tijd waarin digitalisering een steeds grotere rol speelt binnen gemeentelijke dienstverlening, is Identity & Access Management (IAM) een cruciaal onderdeel geworden van een veilige en efficiënte IT-omgeving. Gemeenten verwerken grote hoeveelheden persoonsgegevens, beheren toegang tot talloze applicaties en systemen en moeten voldoen aan strenge wet- en regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatiebeveiliging Overheid (BIO). Een goed ingerichte IAM-strategie draagt niet alleen bij aan beveiliging en compliance, maar ook aan efficiëntere werkprocessen en een betere gebruikerservaring voor zowel medewerkers als burgers.

Waarom dit whitepaper?

Dit whitepaper is bedoeld voor professionals die direct betrokken zijn bij de uitvoering, implementatie en het beheer van IAM binnen een gemeentelijke organisatie. Specifiek richt deze publicatie zich op:

- **Management**: Beleidsbepalers en strategische (IT-)verantwoordelijken binnen de gemeente die richting geven aan IAM, security en compliance. Zij moeten ervoor zorgen dat IAM niet alleen technisch goed wordt geïmplementeerd, maar ook aansluit bij de bredere digitale strategie van de gemeente.
- **Beheer & technische specialisten**: De professionals die verantwoordelijk zijn voor de technische infrastructuur, de integratie van IAM-oplossingen en het beheer van toegangssystemen. Zij houden zich onder meer bezig met Single Sign-On (SSO), Multi-Factor Authenticatie (MFA) en autorisatiebeheer.
- **Functioneel Beheer**: De schakelfunctie tussen IT en de werkvloer. Functioneel beheerders zorgen ervoor dat medewerkers en ketenpartners toegang krijgen tot de juiste applicaties en systemen, zonder dat dit ten koste gaat van de veiligheid of de gebruikerservaring. Zij spelen een sleutelrol in de adoptie van IAM-processen en het trainen van eindgebruikers.
- **Projectmanagement**: Projectleiders en Agile-coaches die verantwoordelijk zijn voor de invoering en doorontwikkeling van IAM binnen de gemeente. Zij zorgen ervoor dat IAM-projecten goed worden gefaseerd, opgevolgd en geïmplementeerd binnen de bredere IT-roadmap.

Met deze whitepaper willen we inzicht geven in de fundamenten van IAM binnen een gemeentelijke context en concrete handvatten bieden om IAM succesvol te implementeren. We beschrijven niet alleen de technische en organisatorische componenten, maar geven ook een praktische aanpak om IAM-projecten effectief te managen en in de dagelijkse praktijk in te bedden.

IAM is geen eenmalig project, maar een continu proces van beheer, optimalisatie en naleving van regelgeving. Door IAM op de juiste manier te benaderen, kunnen gemeenten niet alleen risico's verminderen, maar ook hun digitale dienstverlening verbeteren en de productiviteit van medewerkers verhogen.

In de volgende hoofdstukken nemen we je mee in de wereld van IAM binnen de gemeentelijke sector, van de basisprincipes en uitdagingen tot de concrete implementatieaanpak.

2. Wat is Identity & Access Management (IAM) binnen een gemeente?

2.1 Definitie en kernprincipes van IAM

Identity & Access Management (IAM) is het geheel van processen, beleid en technologieën die ervoor zorgen dat de juiste personen op het juiste moment toegang hebben tot de juiste systemen en gegevens, met de juiste rechten. Binnen een gemeentelijke organisatie betekent dit:

- **Identificeren**: Vaststellen wie een gebruiker is (bijvoorbeeld een ambtenaar, een externe consultant of een ketenpartner).
- **Authentiseren**: Controleren of de gebruiker daadwerkelijk is wie hij zegt te zijn (bijvoorbeeld via wachtwoorden, Single Sign-On of Multi-Factor Authenticatie).
- **Autoriseren**: Toekennen van de juiste rechten en rollen op basis van functie en verantwoordelijkheid.
- **Monitoren & loggen**: Registreren van toegangs- en wijzigingsacties om audits en naleving van wetgeving te ondersteunen.

Voorbeelden per doelgroep

- **Management**: IAM helpt bij het beheersen van risico's, naleving van de Baseline Informatiebeveiliging Overheid (BIO) en het efficiënter inrichten van toegang tot gemeentelijke systemen.
- **Beheer & technische specialisten**: Met IAM kunnen zij eenvoudiger accounts en rechten beheren via geautomatiseerde workflows, wat handmatig werk vermindert en de kans op fouten beperkt.
- **Functioneel Beheer**: IAM zorgt ervoor dat gebruikers niet onnodig lang moeten wachten op toegang tot systemen. Bijvoorbeeld: een nieuwe medewerker in de afdeling Burgerzaken krijgt bij indiensttreding direct toegang tot bijvoorbeeld MS365, Case, Topdesk en hoeft geen losse aanvragen te doen.
- **Projectmanagement**: IAM-projecten raken vrijwel alle afdelingen binnen een gemeente. Een projectmanager moet bijvoorbeeld zorgen dat bij de implementatie van een nieuw HRM-systeem de IAM-integratie goed verloopt, zodat medewerkers automatisch de juiste toegangsrechten krijgen.

2.2 Het belang van IAM voor een gemeente

In gemeenten spelen IAM-processen een cruciale rol bij het veilig en efficiënt beheren van digitale identiteiten. Zonder een goed IAM-beleid ontstaan er problemen zoals:

- **Beveiligingsrisico's**: Ongeautoriseerde toegang tot systemen kan leiden tot datalekken en non-compliance met de AVG.
- **Inefficiënte toegangverlening**: Handmatige processen leiden tot vertraging bij onboarding en offboarding van medewerkers.
- **Schaduw-IT**: Werknemers zoeken zelf manieren om toegang te krijgen tot systemen als IAM-processen niet goed zijn ingericht, wat beveiligingsrisico's vergroot.

Voorbeelden per doelgroep

- **Management**: IAM ondersteunt een efficiënte IT-strategie en vermindert de risico's op audits en non-compliance. Als een auditor bijvoorbeeld vraagt wie er toegang heeft tot een bepaalde database, kan IAM direct rapportages genereren.
- **Beheer & technische specialisten**: IAM helpt bij het verminderen van de beheerlast. Bijvoorbeeld, met een geautomatiseerd IAM-systeem worden gebruikersrechten periodiek gecontroleerd en aangepast, zonder dat ICT-beheer handmatig alle accounts moet nalopen.
- **Functioneel Beheer**: IAM voorkomt dat medewerkers toegang hebben tot systemen die ze niet nodig hebben, wat compliance- en privacyrisico's verlaagt. Een voorbeeld is dat een medewerker van de afdeling Burgerzaken geen toegang heeft tot financiële systemen van de gemeente.
- **Projectmanagement**: IAM voorkomt vertragingen in IT-projecten. Bijvoorbeeld, bij de migratie naar een cloud-based applicatie wordt IAM ingezet om de juiste rollen en rechten te beheren, zodat medewerkers zonder onderbrekingen kunnen doorwerken.

2.3 Belangrijke componenten van IAM

IAM bestaat uit verschillende technische en organisatorische componenten die samenwerken om veilige en efficiënte toegang tot gemeentelijke systemen te waarborgen.

2.3.1 Authenticatie

Authenticatie bepaalt of een gebruiker daadwerkelijk is wie hij zegt te zijn. Dit kan door:

- **Gebruikersnaam en wachtwoord (basisauthenticatie)**
- **Single Sign-On (SSO)** – Gebruikers loggen één keer in en krijgen toegang tot meerdere systemen.
- **Multi-Factor Authenticatie (MFA)** – Extra beveiligingslaag zoals een SMS-code, authenticator-app of biometrische verificatie.

Voorbeelden per doelgroep

- **Management**: MFA verlaagt het risico op hacks en phishing-aanvallen, wat helpt bij naleving van de BIO.
- **Beheer & technische specialisten**: Beheer van authenticatie is eenvoudiger met een centrale SSO-oplossing. Bijvoorbeeld, een systeembeheerder hoeft niet meer voor elke applicatie aparte inloggegevens te resetten.
- **Functioneel Beheer**: Met SSO hoeven medewerkers niet voor elke applicatie apart in te loggen, wat tijd bespaart en gebruikerservaring verbetert. Bijvoorbeeld, een sociaal werker die veldwerk doet, kan via één login veilig toegang krijgen tot meerdere gemeentelijke applicaties.
- **Projectmanagement**: Implementatie van MFA moet goed afgestemd worden met gebruikers. Een projectmanager kan zorgen dat MFA stapsgewijs wordt uitgerold en dat medewerkers goed geïnformeerd zijn over de impact.

2.3.2 Autorisatie

Autorisatie regelt welke rechten een gebruiker heeft binnen een systeem. Dit wordt meestal beheerd via:

- **Rolgebaseerd toegangsbeheer (RBAC)** – Toegang op basis van functies (bijv. alle medewerkers van Burgerzaken hebben dezelfde rechten).
- **Attribuutgebaseerd toegangsbeheer (ABAC)** – Toegang op basis van specifieke kenmerken (bijv. een tijdelijke medewerker krijgt beperkte toegang tot systemen en alleen tijdens kantooruren).

Voorbeelden per doelgroep

- **ICT-management**: Door RBAC en ABAC te implementeren, kan de gemeente beter voldoen aan de BIO en de AVG.
- **ICT-beheer & technische specialisten**: Toegangsbeheer wordt eenvoudiger en minder foutgevoelig. Bijvoorbeeld, een systeembeheerder kan rechten in bulk aanpassen bij functiewijzigingen.
- **Functioneel Beheer**: Automatisch rechtenbeheer voorkomt dat medewerkers handmatig rechten moeten aanvragen en lang moeten wachten op goedkeuring. Bijvoorbeeld, een nieuwe financieel medewerker krijgt direct toegang tot SAP op basis van zijn functie.
- **Projectmanagement binnen ICT**: Autorisatiebeheer speelt een grote rol bij nieuwe IT-implementaties. Bijvoorbeeld, bij de invoering van een nieuw zaaksysteem moet een projectmanager zorgen dat rechten correct worden ingesteld per afdeling.

2.3.3 Identiteitsbeheer

Identiteitsbeheer houdt zich bezig met het creëren, wijzigen en verwijderen van gebruikersaccounts. Dit wordt vaak gekoppeld aan HR-systemen en HR processen zodat toegangsrechten automatisch worden aangepast bij in- of uitdiensttreding of doorstroming binnen de organisatie.

Voorbeelden per doelgroep

- **Management**: Efficiënt identiteitsbeheer voorkomt dat oud-medewerkers onbedoeld toegang behouden tot gemeentelijke systemen.
- **Beheer & technische specialisten**: Door koppeling met HRM-systemen worden gebruikersrechten automatisch beheerd, wat fouten en beheerlast vermindert.
- **Functioneel Beheer**: Minder handmatige aanvragen voor accountwijzigingen, wat de doorlooptijd versnelt.
- **Projectmanagement**: Identiteitsbeheer moet goed worden afgestemd bij de implementatie van nieuwe applicaties om te zorgen dat gebruikers direct de juiste toegang krijgen.

2.3.4 Logging en monitoring

Logging en monitoring zorgen ervoor dat alle IAM-activiteiten worden geregistreerd en geanalyseerd. Dit helpt bij audits en detectie van verdachte activiteiten.

Voorbeelden per doelgroep

- **ICT-management**: Automatische rapportages tonen wie wanneer toegang had tot bepaalde systemen.
- **ICT-beheer & technische specialisten**: Security teams kunnen verdachte inlogpogingen sneller detecteren en actie ondernemen.
- **Functioneel Beheer**: Inzage in toegangslogs kan helpen bij het ondersteunen van audits en onderzoeken.
- **Projectmanagement binnen ICT**: IAM-monitoring moet worden opgenomen in de securitystrategie van nieuwe systemen.

3. IAM in de gemeentelijke context

Identity & Access Management (IAM) speelt een cruciale rol binnen gemeenten. Gemeenten werken met een breed scala aan gebruikers, uiteenlopende wettelijke verplichtingen en complexe IT-landschappen. IAM zorgt ervoor dat medewerkers, burgers, ketenpartners en leveranciers efficiënt en veilig toegang krijgen tot gemeentelijke systemen en gegevens. Dit hoofdstuk bespreekt de specifieke uitdagingen voor gemeenten en de manier waarop IAM gemeentelijke processen ondersteunt.

3.1 Specifieke uitdagingen en eisen voor gemeenten

3.1.1 Verschillende typen gebruikers en hun toegang

Binnen een gemeentelijke organisatie maken verschillende typen gebruikers gebruik van ICT-systemen. IAM moet ervoor zorgen dat elke groep op een veilige en efficiënte manier toegang krijgt tot de juiste applicaties en gegevens.

Verschillende gebruikersgroepen binnen een gemeente

1. **Ambtenaren** – Gemeentemedewerkers die dagelijks gebruikmaken van IT-systemen om hun werk uit te voeren, zoals het burgerzakenloket, sociaal domein of financiële administratie.
2. **Burgers** – Inwoners die via digitale loketten bijvoorbeeld vergunningen aanvragen, bezwaar maken of belastingzaken regelen.
3. **Ketenpartners** – Organisaties zoals politie, belastingdienst of zorginstellingen waarmee gegevens gedeeld moeten worden.
4. **Leveranciers en externe medewerkers** – Externe partijen die namens de gemeente werken en tijdelijke toegang tot systemen nodig hebben, zoals consultants of aannemers.

Voorbeelden per doelgroep

- **Management**: IAM moet ervoor zorgen dat ketenpartners en externe partijen gecontroleerde en tijdelijke toegang krijgen. Een voorbeeld is een sociaal wijkteam dat toegang nodig heeft tot een cliëntvolgsysteem, maar alleen voor de duur van hun opdracht.
- **Beheer & technische specialisten**: Beheer moet geautomatiseerde workflows instellen waarmee externe medewerkers tijdelijk toegang krijgen en deze rechten automatisch vervallen na een bepaalde periode.
- **Functioneel Beheer**: Functioneel beheerders moeten ervoor zorgen dat gemeentelijke medewerkers toegang hebben tot de juiste systemen zonder ingewikkelde aanvragen. Een voorbeeld is dat een nieuwe medewerker bij Burgerzaken op dag één direct toegang heeft tot de BRP (Basisregistratie Personen).
- **Projectmanagement**: IAM-projecten moeten rekening houden met externe toegang. Een projectmanager moet bijvoorbeeld zorgen dat een leverancier veilig toegang krijgt tot een testomgeving zonder het risico dat productiegegevens worden gelekt.

3.1.2 Wet- en regelgeving (BIO, AVG, ENSIA, etc.)

IAM binnen gemeenten wordt sterk beïnvloed door wet- en regelgeving. Overheidsinstellingen moeten voldoen aan:

- **BIO (Baseline Informatiebeveiliging Overheid)** – Stelt normen voor informatiebeveiliging binnen gemeenten, waaronder IAM-beheer en toegangsbeheer.
- **AVG (Algemene Verordening Gegevensbescherming)** – Regelt hoe persoonsgegevens binnen gemeenten verwerkt en beschermd moeten worden, inclusief principes zoals minimale gegevensverwerking en rechten van betrokkenen.
- **ENSIA (Eenduidige Normatiek Single Information Audit)** – Gemeenten moeten jaarlijks verantwoording afleggen over hun informatiebeveiliging, inclusief IAM-processen, in lijn met de BIO en andere wetgeving.
- **Wpg (Wet politiegegevens)** – Beperkt de toegang en verwerking van politiegegevens binnen gemeentelijke diensten zoals BOA's en Veiligheid & Handhaving.
- **Wbni (Wet beveiliging netwerk- en informatiesystemen)** – Verplicht gemeenten om maatregelen te nemen tegen cyberdreigingen en meldplicht voor ernstige beveiligingsincidenten.
- **eIDAS (Electronic Identification, Authentication and Trust Services)** – Europese verordening die eisen stelt aan elektronische identificatie en vertrouwensdiensten, zoals DigiD en eHerkenning.
- **NIS2-richtlijn (Network and Information Security Directive 2)** – Verplicht gemeenten tot strengere cybersecuritymaatregelen, inclusief toegangsbeheer en incidentrespons.
- **Wet digitale overheid (Wdo)** – Regelt de standaarden voor digitale identificatie en veilige toegang tot gemeentelijke diensten, zoals DigiD en eHerkenning.
- **Archiefwet 2021 (in ontwikkeling)** – Regelt het beheer en de bewaartermijnen van digitale documenten, inclusief logbestanden en toegangslogs die relevant zijn voor IAM.
- **Wet Open Overheid (Woo)** – Bepaalt dat bepaalde gemeentelijke gegevens openbaar moeten zijn, waarbij IAM een rol speelt in het autoriseren van toegang tot informatie.
- **CIS Controls & ISO 27001/27002** (Niet verplicht, maar aanbevolen) – Internationale normen en best practices voor informatiebeveiliging en IAM-processen die vaak worden gebruikt binnen gemeenten.

Voorbeelden per doelgroep

- **Management**: IAM ondersteunt naleving van de AVG door 'least privilege'-toegang te garanderen. Een voorbeeld is dat een medewerker van het sociaal domein geen toegang heeft tot jeugdzorgdossiers als dit niet nodig is voor zijn functie.
- **Beheer & technische specialisten**: Logging en monitoring binnen IAM zijn essentieel om aan auditverplichtingen te voldoen. Beheerders moeten kunnen aantonen wie wanneer toegang had tot een systeem.
- **Functioneel Beheer**: IAM helpt bij het beperken van toegang tot privacygevoelige informatie. Bijvoorbeeld, een medewerker van de financiële afdeling mag alleen belastinggegevens inzien van inwoners waarvoor hij gemachtigd is.
- **Projectmanagement**: Bij de implementatie van een nieuw HRM-systeem moet een projectmanager zorgen dat IAM-oplossingen voldoen aan de BIO- en AVG-normen.

3.1.3 Integratie met basisregistraties en andere overheidsdiensten

IAM moet ervoor zorgen dat toegang tot deze systemen goed wordt beheerd en beveiligd.

Voorbeelden per doelgroep

- **Management**: IAM helpt bij het structureren van toegangsrechten tot basisregistraties en voorkomt dat medewerkers onterecht gegevens inzien. Bijvoorbeeld, een medewerker van Vergunningen heeft alleen leesrechten in de BRP, maar geen wijzigingsrechten.
- **Beheer & technische specialisten**: IAM koppelt interne gebruikersaccounts met landelijke registratiesystemen en zorgt dat toegang automatisch wordt beheerd op basis van rollen.
- **Functioneel Beheer**: IAM maakt het mogelijk om autorisaties in te richten per dienst. Bijvoorbeeld, een medewerker die mutaties in de BAG doorvoert, mag niet zomaar WOZ-gegevens aanpassen.
- **Projectmanagement**: Bij het opzetten van een nieuw zaaksysteem moet een projectmanager zorgen voor een correcte IAM-integratie met de BRP, zodat alleen bevoegde medewerkers persoonsgegevens kunnen inzien.

3.2 De rol van IAM in gemeentelijke processen

IAM ondersteunt drie belangrijke processen binnen gemeenten:

- Dienstverlening
- Beveiliging
- Compliance

3.2.1 Dienstverlening

Goede IAM-oplossingen zorgen ervoor dat burgers en bedrijven veilig en snel toegang krijgen tot gemeentelijke diensten, zoals het aanvragen van een paspoort of een vergunning.

Voorbeelden per doelgroep

- **Management**: IAM helpt bij het verbeteren van digitale dienstverlening door burgers via DigiD veilig toegang te geven tot hun gegevens.
- **Beheer & technische specialisten**: IAM-systemen moeten stabiel en snel reageren, zodat inwoners soepel kunnen inloggen.
- **Functioneel Beheer**: IAM voorkomt dat burgers per ongeluk toegang krijgen tot verkeerde gegevens, bijvoorbeeld een woningdossier van een ander huishouden.
- **Projectmanagement**: IAM moet geïntegreerd worden bij de ontwikkeling van digitale loketten, bijvoorbeeld door koppelingen met eHerkenning voor ondernemers.

3.2.2 Beveiliging

IAM beschermt gemeentelijke systemen tegen cyberdreigingen, zoals phishing en datalekken.

Voorbeelden per doelgroep

- **Management**: IAM ondersteunt Zero Trust-beveiligingsstrategieën, waarbij gebruikers altijd opnieuw hun identiteit moeten bewijzen bij toegang tot gevoelige gegevens.
- **Beheer & technische specialisten**: IAM voorkomt dat gehackte accounts volledige toegang behouden door middel van adaptieve authenticatie (bijv. extra verificatie bij inloggen vanaf een onbekend IP-adres).
- **Functioneel Beheer**: Beheerders kunnen gebruikers snel blokkeren bij verdachte activiteiten.
- **Projectmanagement**: Beveiligingsaspecten van IAM moeten vanaf de start worden meegenomen in IT-projecten.

3.2.3 Compliance

IAM zorgt dat gemeenten voldoen aan wet- en regelgeving door controlemechanismen te automatiseren.

Voorbeelden per doelgroep

- **Management**: IAM genereert rapportages voor audits en externe controles.
- **Beheer & technische specialisten**: Logboeken worden automatisch bijgehouden om verdachte activiteiten te detecteren.
- **Functioneel Beheer**: Toegangscontroles kunnen periodiek worden gereviewd en aangepast.
- **Projectmanagement**: IAM-integraties moeten altijd voldoen aan wettelijke eisen zoals de AVG.

Als laatste ...

IAM is binnen gemeenten een essentieel fundament voor beveiliging, dienstverlening en compliance. Door slimme IAM-oplossingen te implementeren, kunnen gemeenten efficiënter en veiliger werken, terwijl ze voldoen aan alle wettelijke eisen.

4. De bouwstenen van een effectief IAM-beleid voor gemeenten

Een goed Identity & Access Management (IAM)-beleid binnen een gemeente zorgt ervoor dat de juiste mensen op het juiste moment toegang hebben tot de juiste systemen, zonder onnodige risico's. IAM is niet alleen een technisch vraagstuk, maar ook een organisatorische en procesmatige uitdaging. In dit hoofdstuk behandelen we de belangrijkste bouwstenen van een effectief IAM-beleid en hoe deze bijdragen aan een veilige en efficiënte gemeentelijke organisatie.

4.1 Identiteiten en lifecycle management (van in dienst tot uit dienst)

Identiteiten in een gemeente kunnen verschillende vormen aannemen: medewerkers, burgers, ketenpartners en leveranciers. Het beheren van deze identiteiten gedurende hun hele levenscyclus is een kernonderdeel van IAM.

De identiteitslevenscyclus binnen een gemeente

1. **Onboarding (nieuwe medewerkers en externen)**
    - Een medewerker start bij de gemeente en moet vanaf dag één toegang krijgen tot systemen zoals e-mail, zaaksystemen en HR-systemen.
    - Externe medewerkers (zoals consultants) krijgen beperkte, tijdelijke toegang.
2. **Wijzigingen tijdens de loopbaan**
    - Een medewerker krijgt een andere functie en moet toegang krijgen tot nieuwe applicaties, terwijl oude rechten automatisch worden ingetrokken.
    - Een projectleider heeft voor een tijdelijke periode extra rechten nodig voor een specifiek project.
3. **Offboarding (vertrek uit de organisatie)**
    - Wanneer een medewerker uit dienst gaat, moeten alle toegangsrechten direct worden ingetrokken om beveiligingsrisico's te voorkomen.
    - Accounts van leveranciers en ketenpartners worden automatisch gedeactiveerd zodra hun contract afloopt.

Voorbeelden per doelgroep

- **Management**: IAM ondersteunt het soepel onboarden van medewerkers, waardoor nieuwe medewerkers direct productief zijn en oud-medewerkers geen onterechte toegang behouden.
- **Beheer & technische specialisten**: Lifecycle management voorkomt 'orphaned accounts' (achtergebleven accounts van oud-medewerkers die een beveiligingsrisico vormen).
- **Functioneel Beheer**: Het IAM-systeem zorgt ervoor dat medewerkers die een nieuwe functie krijgen, automatisch de juiste toegangsrechten ontvangen.
- **Projectmanagement**: Projectmedewerkers krijgen tijdelijke projectgebonden rechten die na afloop automatisch vervallen.

4.2 Rollen en rechtenbeheer

Binnen een gemeente moet toegang tot systemen gebaseerd zijn op functionele rollen, zodat medewerkers alleen toegang krijgen tot informatie die ze echt nodig hebben.

Belangrijke principes van rollen en rechtenbeheer

- **Role-Based Access Control (RBAC)**: Toegangsrechten worden toegekend op basis van functies binnen de gemeente (bijv. een medewerker van de sociale dienst heeft andere rechten dan iemand van de financiële administratie).
- **Attribute-Based Access Control (ABAC)**: Toegangsrechten worden bepaald op basis van kenmerken zoals locatie of afdeling (bijv. alleen medewerkers op het gemeentehuis mogen bepaalde systemen inzien).
- **Least Privilege Principle**: Medewerkers krijgen alleen de minimale rechten die nodig zijn voor hun werk.

Voorbeelden per doelgroep

- **Management**: IAM voorkomt dat medewerkers willekeurig toegang krijgen tot gevoelige gegevens, zoals financiële of persoonsgegevens.
- **Beheer & technische specialisten**: IAM-systemen kunnen automatisch toegangsrechten aanpassen op basis van rolwijzigingen.
- **Functioneel Beheer**: Functiewijzigingen binnen een afdeling leiden automatisch tot aanpassingen in toegangsrechten.
- **Projectmanagement**: In tijdelijke projecten worden projectteams gevormd met specifieke toegangsniveaus, die na afloop worden ingetrokken.

4.3 Single Sign-On (SSO) en Multi-Factor Authenticatie (MFA)

Single Sign-On (SSO)

SSO stelt gebruikers in staat om met één set inloggegevens toegang te krijgen tot meerdere gemeentelijke applicaties. Dit vermindert de kans op zwakke wachtwoorden en verhoogt het gebruikersgemak.

Praktijkvoorbeeld:
Een medewerker van Burgerzaken logt in via een gemeentelijke portal en krijgt direct toegang tot BRP, het zaaksysteem en het DMS, zonder meerdere keren in te loggen.

Multi-Factor Authenticatie (MFA)

MFA voegt een extra beveiligingslaag toe door naast een wachtwoord een tweede verificatiestap te vereisen, zoals:

- Een SMS-code
- Een authenticator-app
- Een biometrische scan

Praktijkvoorbeeld:
Een ICT-beheerder die toegang nodig heeft tot een server, moet naast zijn wachtwoord ook een verificatiecode via een authenticator-app invoeren.

Voorbeelden per doelgroep

- **Management**: SSO verhoogt efficiëntie en MFA verkleint het risico op datalekken.
- **Beheer & technische specialisten**: IAM-systemen moeten integreren met SSO en MFA om gebruikerservaring en beveiliging te balanceren.
- **Functioneel Beheer**: SSO zorgt ervoor dat medewerkers minder vaak inlogproblemen ervaren.
- **Projectmanagement**: Bij de implementatie van nieuwe applicaties moet SSO en MFA standaard geïntegreerd worden.

4.4 Self-service en gebruikersbeheer

Een IAM-systeem moet medewerkers en burgers de mogelijkheid geven om zelf veelvoorkomende taken uit te voeren zonder tussenkomst van IT.

Voorbeelden van self-service mogelijkheden

- **Wachtwoord reset** – Medewerkers kunnen zelf hun wachtwoord herstellen via een beveiligde portal.
- **Aanvragen van toegang** – Medewerkers kunnen via een self-service portal toegang tot applicaties aanvragen, met goedkeuring door hun leidinggevende.

Praktijkvoorbeeld:
Een medewerker van de sociale dienst wil toegang tot een nieuw zaaksysteem. Via de IAM-portal vraagt hij deze toegang aan en na goedkeuring wordt dit automatisch verwerkt.

Voorbeelden per doelgroep

- **Management**: Self-service verlaagt de druk op IT-afdelingen en versnelt processen.
- **Beheer & technische specialisten**: IT hoeft minder handmatig toegang te verlenen en kan workflows automatiseren.
- **Functioneel Beheer**: Medewerkers krijgen sneller toegang tot systemen zonder lange wachttijden.
- **Projectmanagement**: Self-service portals maken onboarding van nieuwe projectmedewerkers efficiënter.

4.5 Auditing, logging en monitoring voor naleving en beveiliging

IAM-systemen moeten uitgebreide logging en monitoring ondersteunen om naleving van wetgeving en beveiligingseisen te waarborgen.

Belangrijke onderdelen van auditing en monitoring

- **Logging van inlogpogingen en toegang tot gevoelige gegevens.**
- **Detectie van afwijkend gedrag, zoals inloggen vanaf verdachte locaties.**
- **Regelmatige rapportages voor audits en ENSIA-verplichtingen.**

Praktijkvoorbeeld:

Een medewerker van de gemeente logt onverwachts in vanaf een IP-adres in het buitenland. Het IAM-systeem detecteert dit als verdacht en blokkeert automatisch de toegang totdat verificatie heeft plaatsgevonden.

Voorbeelden per doelgroep

- **Management**: IAM helpt bij het aantoonbaar voldoen aan regelgeving zoals de BIO en ENSIA.
- **Beheer & technische specialisten**: IT-afdelingen kunnen verdachte activiteiten proactief monitoren en ingrijpen.
- **Functioneel Beheer**: IAM geeft functioneel beheerders inzicht in wie welke gegevens heeft geraadpleegd.
- **Projectmanagement**: Nieuwe IT-systemen moeten voldoen aan logging- en auditvereisten.

Als laatste ...

Een effectief IAM-beleid binnen een gemeente bestaat uit meerdere bouwstenen die samen zorgen voor een veilige, efficiënte en compliant werkomgeving. Door IAM goed in te richten, kunnen gemeenten voldoen aan wet- en regelgeving, beveiligingsrisico's beperken en de digitale dienstverlening verbeteren.

5. Implementatieaanpak: hoe IAM succesvol invoeren in een gemeente

Een succesvolle implementatie van Identity & Access Management (IAM) binnen een gemeente vraagt om een gestructureerde aanpak. Dit hoofdstuk beschrijft de vijf essentiële stappen van het implementatieproces en geeft concrete voorbeelden van hoe verschillende doelgroepen—management, beheer & technische specialisten, functioneel beheer en projectmanagement—bijdragen aan een succesvolle invoering.

IAM is niet alleen een technisch project, maar een verandering in de manier waarop toegang en identiteit binnen de organisatie worden beheerd. Daarom is een integrale benadering essentieel, waarbij beleid, technologie en adoptie hand in hand gaan.

5.1 Stapsgewijze aanpak

IAM-implementatie binnen een gemeente verloopt idealiter in vijf fasen:

- Huidige situatie in kaart brengen
- IAM-beleid en governance vaststellen
- Technologiekeuze en architectuur bepalen
- Gefaseerde implementatie en adoptie
- Doorlopende monitoring en optimalisatie

Fase 1: Huidige situatie in kaart brengen (IAM-assessment)

Voordat IAM verbeterd of geïmplementeerd kan worden, is het cruciaal om inzicht te krijgen in de bestaande situatie. Dit gebeurt door een IAM-assessment, waarin de volgende vragen worden beantwoord:

- Welke systemen en applicaties worden momenteel gebruikt?
- Hoe wordt toegang verleend en beheerd?
- Welke risico’s en beveiligingslekken zijn aanwezig?
- Hoe wordt authenticatie en autorisatie ingericht?

Praktijkvoorbeeld:

Tijdens een IAM-assessment bij een gemeente blijkt dat medewerkers die van functie wisselen vaak hun oude rechten behouden, waardoor ongewenste toegang ontstaat.

Wat wordt verwacht per doelgroep?

- **Management:** Faciliteert de assessment en stelt prioriteiten op basis van risico's en beleidsdoelen.
- **Beheer & technische specialisten:** Voeren technische analyses uit en identificeren kwetsbaarheden.
- **Functioneel Beheer:** Inventariseert wie toegang heeft tot welke systemen en controleert of dit overeenkomt met de werkelijke behoeften.
- **Projectmanagement:** Structureert het assessmentproces en bewaakt de voortgang.

Fase 2: IAM-beleid en governance vaststellen

IAM vereist duidelijke afspraken over wie verantwoordelijk is voor toegangsbeheer en hoe identiteiten binnen de organisatie worden beheerd.

Kernonderdelen van IAM-beleid:

- **Governance-model:** Wie beslist over toegang en welke goedkeuringsprocedures gelden?
- **Rollen en rechtenbeheer:** Hoe worden rollen gedefinieerd en toegewezen?
- **Beveiligingsstandaarden:** Hoe wordt voldaan aan BIO, AVG en ENSIA?
- **Account lifecycle management:** Hoe worden accounts aangemaakt, gewijzigd en afgesloten?

Praktijkvoorbeeld:

Een gemeente besluit dat alle toegang tot zaaksystemen voortaan via het ‘least privilege principle’ verloopt. Dit betekent dat medewerkers enkel toegang krijgen tot data die ze strikt nodig hebben voor hun functie.

Wat wordt verwacht per doelgroep?

- **Management:** Stelt beleid vast en zorgt voor mandaat en middelen.
- **Beheer & technische specialisten:** Vertalen beleid naar technische richtlijnen en configuraties.
- **Functioneel Beheer:** Definieert rollen en verantwoordelijkheden binnen de applicaties.
- **Projectmanagement:** Zorgt dat beleidsbeslissingen worden vastgelegd en geïmplementeerd binnen projecten.

Fase 3: Technologiekeuze en architectuur bepalen

IAM-oplossingen kunnen variëren van standaard cloudgebaseerde systemen tot op maat gemaakte on-premise oplossingen. Gemeenten moeten een oplossing kiezen die voldoet aan hun functionele en beveiligingsbehoeften.

Belangrijke keuzes:

- **Federated Identity vs. Local IAM:** Worden identiteiten centraal beheerd of per afdeling?
- **Single Sign-On (SSO) & Multi-Factor Authenticatie (MFA):** Welke authenticatiemethoden worden gehanteerd?
- **Integratie met andere systemen:** Hoe koppelt IAM met HR-systemen en basisregistraties?

Praktijkvoorbeeld:

Een gemeente kiest voor een hybride IAM-oplossing waarin medewerkers met hun gemeentelijke account via Single Sign-On toegang krijgen tot SaaS-applicaties zoals Microsoft 365 en interne zaaksystemen.

Wat wordt verwacht per doelgroep?

- **Management:** Zorgt voor budget en goedkeuring van de gekozen oplossing.
- **Beheer & technische specialisten:** Voeren technische analyses uit en testen de architectuur.
- **Functioneel Beheer:** Bepaalt welke applicaties en gebruikersgroepen IAM moeten integreren.
- **Projectmanagement:** Coördineert het selectietraject en bewaakt deadlines.

Fase 4: Gefaseerde implementatie en adoptie

Een 'big bang'-implementatie van IAM is vaak riskant. Een gefaseerde aanpak waarbij IAM eerst bij een beperkte groep gebruikers wordt geïntroduceerd, kan helpen om kinderziektes vroegtijdig op te lossen.

Gefaseerde implementatie kan bijvoorbeeld als volgt verlopen:

1. **Pilotfase:** IAM wordt getest bij een specifieke afdeling (bijvoorbeeld Burgerzaken).
2. **Uitrol bij interne medewerkers:** De nieuwe IAM-oplossing wordt breed uitgerold binnen de gemeente.
3. **Uitrol bij ketenpartners en leveranciers:** Externe toegang wordt volgens IAM-beleid ingeregeld.
4. **Optimalisatie:** Op basis van gebruikersfeedback worden verbeteringen doorgevoerd.

Praktijkvoorbeeld:

Een gemeente rolt IAM eerst uit voor de ICT-afdeling om kinderziektes op te sporen, voordat het systeem breder wordt ingezet.

Wat wordt verwacht per doelgroep?

- **Management:** Communiceert het belang van IAM binnen de organisatie.
- **Beheer & technische specialisten:** Beheren de technische uitrol en lossen problemen op.
- **Functioneel Beheer:** Ondersteunt gebruikers en traint medewerkers.
- **Projectmanagement:** Zorgt voor een strakke implementatieplanning en risicobeheer.

Fase 5: Doorlopende monitoring en optimalisatie

IAM is geen eenmalig project, maar een continu proces. Regelmatige audits en monitoring helpen om beveiligingsrisico's en compliance-issues te identificeren en aan te pakken.

Belangrijke optimalisatiestrategieën:

- **Periodieke toegangsreviews:** Zijn alle rechten nog correct toegewezen?
- **Logging en monitoring:** Ongewone inlogpogingen en activiteiten detecteren.
- **Continuous Improvement:** IAM-processen aanpassen aan veranderende regelgeving en risico's.

Praktijkvoorbeeld:
Een gemeente ontdekt via logbestanden dat oud-medewerkers nog steeds toegang hebben tot bepaalde systemen. Dit leidt tot het verbeteren van het offboarding-proces.

Wat wordt er verwacht per doelgroep?

- **Management:** Evalueert de effectiviteit van IAM en stuurt bij waar nodig.
- **Beheer & technische specialisten:** Beheren de monitoringtools en rapporteren over beveiligingsincidenten.
- **Functioneel Beheer:** Controleert regelmatig of gebruikersrechten correct zijn ingesteld.
- **Projectmanagement:** Past lessen uit de implementatie toe op toekomstige IAM-gerelateerde projecten.

5.2 Praktische aandachtspunten en valkuilen

Een IAM-implementatie kent verschillende valkuilen die gemeenten moeten vermijden:

Veelvoorkomende valkuilen:

1. **Te weinig betrokkenheid van de business** – IAM is geen IT-feestje; alle afdelingen moeten meedenken.
2. **Verouderde rechtenstructuren overnemen** – Oude, ongecontroleerde toegangsrechten migreren zonder herziening leidt tot problemen.
3. **Onvoldoende aandacht voor adoptie** – Medewerkers moeten snappen waarom IAM belangrijk is en hoe ze ermee werken.

Praktische tips voor succes

- ✓ **Start met een kleine, afgebakende pilot** om lessen te trekken.
- ✓ **Betrek HR en Functioneel Beheer** vanaf het begin.
- ✓ **Monitor actief en voer periodieke toegangsreviews uit.**

Als laatste ...

Een succesvolle IAM-implementatie in een gemeente vraagt om een doordachte, gefaseerde aanpak waarin beleid, technologie en adoptie hand in hand gaan. Door IAM structureel in te richten, kunnen gemeenten hun beveiliging versterken en efficiënter werken.

6. Conclusie en aanbevelingen

IAM (Identity & Access Management) is een cruciaal onderdeel van de digitale strategie van een gemeente. Het draagt niet alleen bij aan een veilige en efficiënte IT-omgeving, maar ondersteunt ook de naleving van wet- en regelgeving, de samenwerking met ketenpartners en de digitale dienstverlening naar burgers. Dit hoofdstuk vat de belangrijkste inzichten samen, biedt best practices en geeft concrete aanbevelingen voor gemeenten die IAM willen professionaliseren.

6.1 Samenvatting van de belangrijkste inzichten

IAM binnen gemeenten kent specifieke uitdagingen en vereisten, zoals de diversiteit aan gebruikers (ambtenaren, burgers, ketenpartners, leveranciers), naleving van wet- en regelgeving (BIO, AVG, ENSIA), en de noodzaak van integratie met basisregistraties en andere overheidsdiensten.

De belangrijkste elementen van een effectief IAM-beleid zijn:

- **Identiteiten en lifecycle management**: Een gestroomlijnd proces van in-, door- en uitstroom van medewerkers.
- **Rollen en rechtenbeheer**: Strikte controle over wie toegang heeft tot welke systemen en data.
- **Single Sign-On (SSO) en Multi-Factor Authenticatie (MFA)**: Verhogen van gebruiksgemak en beveiliging.
- **Self-service en gebruikersbeheer**: Medewerkers en ketenpartners kunnen zelfstandig bepaalde toegang aanvragen of wijzigen.
- **Auditing, logging en monitoring**: Continue controle en naleving van beveiligingsregels.

De implementatie van IAM verloopt het beste via een stapsgewijze aanpak:

1. **Huidige situatie in kaart brengen (IAM-assessment)**
2. **IAM-beleid en governance vaststellen**
3. **Technologiekeuze en architectuur bepalen**
4. **Gefaseerde implementatie en adoptie**
5. **Doorlopende monitoring en optimalisatie**

IAM is geen eenmalig project, maar een continu proces dat periodieke evaluaties en optimalisaties vereist.

6.2 Best practices en tips voor gemeenten

1. Betrek alle belanghebbenden vanaf het begin

IAM raakt verschillende afdelingen: ICT, HR, functioneel beheer, security en het management. Door hen vanaf het begin te betrekken, zorg je voor draagvlak en een soepele implementatie.

Praktijkvoorbeeld:
Een gemeente startte een IAM-project zonder HR erbij te betrekken. Dit leidde tot problemen bij de onboarding van nieuwe medewerkers, omdat de accounts niet tijdig werden aangemaakt. Door HR als vaste partner in IAM op te nemen, werd dit probleem opgelost.

Tip: Organiseer een IAM-werkgroep waarin alle relevante afdelingen vertegenwoordigd zijn.

2. Begin met een kleine pilot en schaal gefaseerd op

Een stapsgewijze aanpak voorkomt dat een te grote, complexe uitrol leidt tot fouten en weerstand bij gebruikers.

Praktijkvoorbeeld:
Een gemeente startte de implementatie van een IAM-platform binnen de ICT-afdeling voordat het breder werd uitgerold. Hierdoor konden kinderziektes in de configuratie en adoptie worden aangepakt, waardoor de bredere uitrol soepeler verliep.

Tip: Kies een afgebakende groep, zoals de afdeling Burgerzaken, als pilot en verzamel feedback voordat je het systeem organisatiebreed uitrolt.

3. Voer periodieke toegangsreviews uit

Een IAM-systeem is slechts zo sterk als het beheer ervan. Zonder regelmatige controles kunnen oude accounts en ongewenste rechten blijven bestaan, wat een risico vormt.

Praktijkvoorbeeld:
Bij een audit bleek dat een oud-medewerker die twee jaar eerder was vertrokken, nog steeds toegang had tot de gemeentelijke financiële administratie. Dit leidde tot een aanscherping van het offboarding-proces en een automatische rechtencontrole bij functiewijzigingen.

Tip: Stel een beleid in waarbij elke zes maanden een toegangsreview wordt uitgevoerd, waarbij managers en systeembeheerders controleren of rechten nog correct zijn ingesteld.

4. Werk met het 'least privilege principle'

Gebruikers mogen alleen toegang krijgen tot systemen en data die strikt noodzakelijk zijn voor hun functie.

Praktijkvoorbeeld:
Een gemeente had een standaardprocedure waarbij alle nieuwe medewerkers toegang kregen tot alle gemeentelijke applicaties. Dit leidde tot onnodige risico's en datalekken. Door een strikter rollen- en rechtenbeheer in te voeren, werd ongewenste toegang beperkt.

Tip: Stel vast welke minimale rechten een gebruiker nodig heeft en geef niet standaard toegang tot alle systemen.

5. Zorg voor duidelijke communicatie en training

IAM is meer dan een technisch proces; het vraagt om gedragsverandering bij medewerkers. Zorg dat medewerkers begrijpen waarom IAM belangrijk is en hoe ze ermee moeten werken.

Praktijkvoorbeeld:
Een gemeente introduceerde MFA, maar kreeg veel weerstand van gebruikers die het als een extra drempel zagen. Door een communicatiecampagne op te zetten over de voordelen van MFA (zoals betere beveiliging en minder wachtwoordproblemen), werd de acceptatie verhoogd.

Tip: Organiseer korte trainingen of e-learningmodules waarin medewerkers leren hoe ze veilig met IAM omgaan.

6. Gebruik IAM als basis voor Zero Trust-beveiliging

Zero Trust is een beveiligingsmodel waarin geen enkele gebruiker of apparaat standaard wordt vertrouwd. IAM speelt hierin een sleutelrol door continu te controleren of de juiste personen toegang hebben tot de juiste bronnen.

Praktijkvoorbeeld:
Een gemeente implementeerde een Zero Trust-model waarin gebruikers niet automatisch toegang kregen tot interne netwerken, maar zich eerst via MFA en gedragsanalyses moesten verifiëren. Hierdoor werd het risico op cyberaanvallen aanzienlijk verminderd.

Tip: Maak IAM onderdeel van een bredere cybersecurity-strategie en implementeer principes zoals netwerksegmentatie en gedragsanalyses.

6.3 Call to action: hoe verder met IAM binnen jouw gemeente?

IAM is geen project met een einddatum, maar een doorlopend proces. Gemeenten die IAM serieus nemen, moeten IAM beschouwen als een strategisch onderdeel van hun digitale transformatie.

Concreet stappenplan voor gemeenten

- **Stap 1:** Vorm een IAM-werkgroep met vertegenwoordigers uit ICT, HR, functioneel beheer en security.
- **Stap 2:** Voer een IAM-assessment uit en breng risico's in kaart.
- **Stap 3:** Ontwikkel een IAM-beleidsdocument en zorg voor bestuurlijke goedkeuring.
- **Stap 4:** Kies een IAM-platform dat past bij de behoeften van de gemeente.
- **Stap 5:** Start met een pilot en leer van de implementatie voordat je breder uitrolt.
- **Stap 6:** Voer periodieke toegangsreviews en security-audits uit.
- **Stap 7:** Maak IAM onderdeel van een bredere cybersecurity-strategie.

IAM is een essentieel fundament voor een veilige, efficiënte en toekomstbestendige gemeente. Door nu actie te ondernemen en IAM structureel op te zetten, kunnen gemeenten zichzelf beschermen tegen cyberdreigingen en tegelijkertijd de digitale dienstverlening verbeteren.

7. Begrippenlijst

IAM (Identity & Access Management) kent veel technische en beleidsmatige termen. Hieronder volgt een uitgebreide lijst met definities en toelichting specifiek gericht op gemeenten.

A

Authenticatie
Authenticatie is het proces waarbij een gebruiker bewijst dat hij of zij is wie die zegt te zijn. Dit kan door middel van een wachtwoord, een pas, biometrie (zoals vingerafdruk of gezichtsherkenning) of Multi-Factor Authenticatie (MFA).
 Gemeentelijke context: Medewerkers loggen in op gemeentelijke applicaties met hun persoonlijke account, waarbij MFA wordt gebruikt om de toegang extra te beveiligen.

Autorisatie
Autorisatie bepaalt welke rechten en toegang een geauthenticeerde gebruiker krijgt binnen een systeem.
 Gemeentelijke context: Een medewerker van de afdeling Burgerzaken mag persoonsgegevens inzien, maar heeft geen rechten om belastinggegevens te wijzigen.

AVG (Algemene Verordening Gegevensbescherming)
Europese privacywetgeving die bepaalt hoe organisaties (waaronder gemeenten) persoonsgegevens mogen verwerken en beveiligen.
 Gemeentelijke context: Een gemeente moet ervoor zorgen dat alleen bevoegde medewerkers toegang hebben tot persoonsgegevens van burgers.

B

Beheerder (IAM-beheerder)
Een persoon of afdeling die verantwoordelijk is voor het inrichten, beheren en onderhouden van Identity & Access Management binnen de gemeente.
 Gemeentelijke context: De IAM-beheerder zorgt ervoor dat nieuwe medewerkers tijdig toegang krijgen tot de juiste systemen.

BIO (Baseline Informatiebeveiliging Overheid)
Een set beveiligingsrichtlijnen die overheidsorganisaties, waaronder gemeenten, moeten volgen om informatie veilig te houden.
 Gemeentelijke context: IAM moet voldoen aan de BIO-eisen, zoals het beperken van toegang op basis van rol en het regelmatig controleren van toegangsrechten.

Bronsysteem
Een systeem waarin de ‘bron’ van identiteiten en rollen wordt beheerd, zoals HR-systemen of het bevolkingsregister.
 Gemeentelijke context: Een HR-systeem registreert dat een nieuwe medewerker in dienst treedt en IAM verwerkt deze informatie automatisch door rechten toe te kennen.

C

Compliance
Het voldoen aan wet- en regelgeving en interne beleidsregels rondom informatiebeveiliging en toegangsbeheer.
 Gemeentelijke context: Een gemeente moet kunnen aantonen dat alleen geautoriseerde medewerkers toegang hebben tot vertrouwelijke gegevens.

Context-based access
Een autorisatiemodel waarbij toegang wordt verleend op basis van de context, zoals locatie, apparaat of tijdstip.
 Gemeentelijke context: Een medewerker die buiten de gemeentelijke netwerken inlogt, moet verplicht MFA gebruiken.

D

Directory Service
Een digitale database waarin identiteiten en toegangsrechten worden opgeslagen en beheerd, zoals Microsoft Active Directory.
 Gemeentelijke context: Active Directory beheert de accounts en toegangsrechten van alle medewerkers binnen de gemeente.

E

ENSIA (Eenduidige Normatiek Single Information Audit)
Een auditproces waarmee gemeenten verantwoording afleggen over informatiebeveiliging en gegevensverwerking.
 Gemeentelijke context: ENSIA-audits controleren of de gemeente voldoet aan IAM-standaarden zoals periodieke toegangscontroles.

F

Federated Identity
Een methode waarbij gebruikers één digitale identiteit kunnen gebruiken om toegang te krijgen tot meerdere systemen of organisaties zonder aparte inloggegevens per dienst. Dit wordt mogelijk gemaakt door vertrouwensrelaties tussen identiteitsproviders en serviceproviders.
 Gemeentelijke context: Federated Identity kan gemeenten helpen om externe partners, zoals ketenpartners en leveranciers, veilige en efficiënte toegang te geven tot gemeentelijke systemen zonder dat er aparte accounts hoeven te worden aangemaakt. Dit verhoogt gebruiksgemak en veiligheid, mits goed beheerd binnen IAM-richtlijnen.

I

IAM (Identity & Access Management)
Het geheel aan processen, technologieën en beleidsmaatregelen waarmee identiteiten worden beheerd en toegang wordt geregeld.

 Gemeentelijke context: IAM zorgt ervoor dat een gemeenteambtenaar die bij Burgerzaken werkt, alleen toegang heeft tot relevante applicaties en niet tot financiële systemen.

Identiteitsbeheer
Het proces waarbij gebruikers en hun kenmerken (zoals naam, functie, afdeling en toegangsrechten) worden vastgelegd en beheerd.
 Gemeentelijke context: Zodra een nieuwe medewerker in dienst komt, wordt automatisch een account aangemaakt en gekoppeld aan de juiste rol.

ISO 27001
Een internationale norm voor informatiebeveiliging waarmee organisaties (waaronder gemeenten) hun beveiligingsbeleid kunnen certificeren.
 Gemeentelijke context: Gemeenten hanteren ISO 27001 als basis voor hun informatiebeveiligingsbeleid.

L

Least Privilege Principle
Een beveiligingsprincipe waarbij gebruikers alleen de minimale rechten krijgen die nodig zijn om hun werk te doen.
 Gemeentelijke context: Een medewerker van de gemeente mag enkel documenten bewerken die relevant zijn voor zijn functie en niet automatisch toegang krijgen tot alle documenten.

Logging & monitoring
Het continu registreren en analyseren van activiteiten binnen een IT-omgeving om misbruik en afwijkend gedrag op te sporen.
 Gemeentelijke context: Gemeentelijke systemen houden bij wie toegang heeft gehad tot persoonsgegevens, zodat verdachte activiteiten kunnen worden onderzocht.

M

Multi-Factor Authenticatie (MFA)
Een beveiligingsmethode waarbij een gebruiker twee of meer verificatiestappen moet doorlopen, zoals een wachtwoord én een SMS-code.
 Gemeentelijke context: Medewerkers moeten naast hun wachtwoord een code uit een authenticator-app invoeren om toegang te krijgen tot gevoelige applicaties.

R

RBAC (Role-Based Access Control)
Een autorisatiemodel waarbij gebruikers rechten krijgen op basis van hun rol in de organisatie.
 Gemeentelijke context: Een medewerker van de afdeling Belastingen krijgt automatisch toegang tot belastingsoftware, maar niet tot burgerlijke stand-systemen.

S

Self-service portaal
Een platform waar gebruikers zelfstandig hun wachtwoord kunnen resetten of toegang kunnen aanvragen zonder tussenkomst van een beheerder.
 Gemeentelijke context: Een medewerker kan via het self-service portaal toegang aanvragen tot een specifieke applicatie, waarna zijn manager dit goedkeurt.

Single Sign-On (SSO)
Een technologie waarmee gebruikers slechts één keer hoeven in te loggen om toegang te krijgen tot meerdere applicaties.
 Gemeentelijke context: Een ambtenaar logt in op het gemeentelijk netwerk en krijgt direct toegang tot alle benodigde systemen zonder opnieuw in te loggen.

T

Toegangsbeheer
Het proces van het verlenen, wijzigen en intrekken van rechten op IT-systemen.
 Gemeentelijke context: Als een medewerker overstapt naar een andere afdeling, worden zijn toegangsrechten automatisch aangepast.

Two-Factor Authentication (2FA)
Een verificatiemethode waarbij een gebruiker naast een wachtwoord een extra factor moet gebruiken, zoals een eenmalige code via SMS.
 Gemeentelijke context: Gemeenten eisen dat medewerkers 2FA gebruiken om in te loggen op systemen met gevoelige informatie.

Z

Zero Trust Security
Een beveiligingsmodel waarin geen enkele gebruiker of apparaat standaard wordt vertrouwd, en alle toegang constant moet worden geverifieerd.
 Gemeentelijke context: Een gemeente past Zero Trust toe door ervoor te zorgen dat medewerkers die buiten het netwerk werken altijd MFA moeten gebruiken en dat toegang wordt beperkt op basis van locatie en apparaat.