DIGITAL IDENTITY SURVEY 2025

PRESENTATIE

14 April 2026

PvIB Platform voor InformatieBeveiliging

Introductie

Evert van Zanten

Voorzitter PvIB
Kwartiermaker PvIB SIG-IAM

Programma manager IB
Trusted Advisor IAM

Marcel Koers

Protiviti
Technology Consulting

SME Cyber Security & IAM
Qualified IT Auditor (RE)

De stand van zaken

Internet + TV Familie Daarom Odido Service Inloggen

Informatiepagina cyberincident Odido.

English version →

Het onderzoek loopt nog. Zodra er meer bekend is, updaten we deze pagina.
Laatst geüpdatet op 8 april 2026, 15.45 uur

De laatste updates.

8 april 2026, 15.45 uur

We waarschuwen voor een nieuwe phishingmail die lijkt a
gevraagd om een app-update te installeren via een extern
de link, download niets en verwijder de mail direct.

Goed om te weten: Wij vragen je nooit om de Odido App
van de Odido App gaan altijd via de Google Play Store of

Controleer ook altijd de afzender van een e-mail. Let niet
mailadres. Oplichters kunnen een naam gebruiken die bet

E-mails van Odido over dit onderwerp komen alleen van:

- info@mail.odido.nl
- _noreply@odido.nl

Let bij _noreply@odido.nl extra goed op dat ons adres be

NOS Nieuws • Dinsdag, 22:56

Bedrijf dat software levert voor patiëntendossiers aangevallen door hackers

Zorgleverancier ChipSoft is getroffen door een hack met gijzelsoftware.
meldt Z-Cert, het expertisecentrum voor digitale beveiliging in de zorg, i
vertrouwelijk bericht aan zorginstellingen. Dat bericht is in handen van
ChipSoft zegt niet te kunnen uitsluiten dat persoonsgegevens zijn ingez
gestolen.

NOS Nieuws • Gisteren, 08:48 • Aangepast gisteren, 14:36

Gegevens 200.000 leden Basic-Fit gelekt, ook bij Booking klantgegevens gestolen

Sportschoolketen Basic-Fit is getroffen door een hack. Daarbij zijn gegevens

TECHZINE HOME TOPARTIKELEN TOPICS INSIGHTS MEER NL

2MIN • SECURITY

Fout van AI-agent leidt tot datalek bij Meta

MELS DEES
20 mrt 2026, 13:49 CET

Meta heeft intern te maken gehad met een beveiligingsincident waarbij een AI-agent een rol speelde bij het tijdelijk toegankelijk maken van gevoelige gegevens. Volgens het bedrijf zijn er geen aanwijzingen dat de data daadwerkelijk is misbruikt.

KEUZE VAN DE REDACTIE

Hoe AI securityonderzoek van een niche tot een focus maakt

Net als quantum computing dwingt AI ons om cybersecurity te heroverwe...

Maar, waar staan we nu met deze opdracht?

Identity Is the New Perimeter: Why IAM Is the Frontline of Cybersecurity


Sudhakar Tiwari December 23, 2025

Introduction

Once upon a time, enterprise security was about defending the fortress. Firewalls and intrusion detection systems stood as gatekeepers, guarding the network perimeter. But in today's cloud-first, hybrid, and borderless world, that perimeter has dissolved. Employees work from anywhere, third parties connect to everything, and machines outnumber humans.

Attackers have noticed. Instead of battering down network doors, they simply steal or manipulate **identities**. In this reality, **Identity and Access Management (IAM) has become the true frontline of cybersecurity**.

PvIB

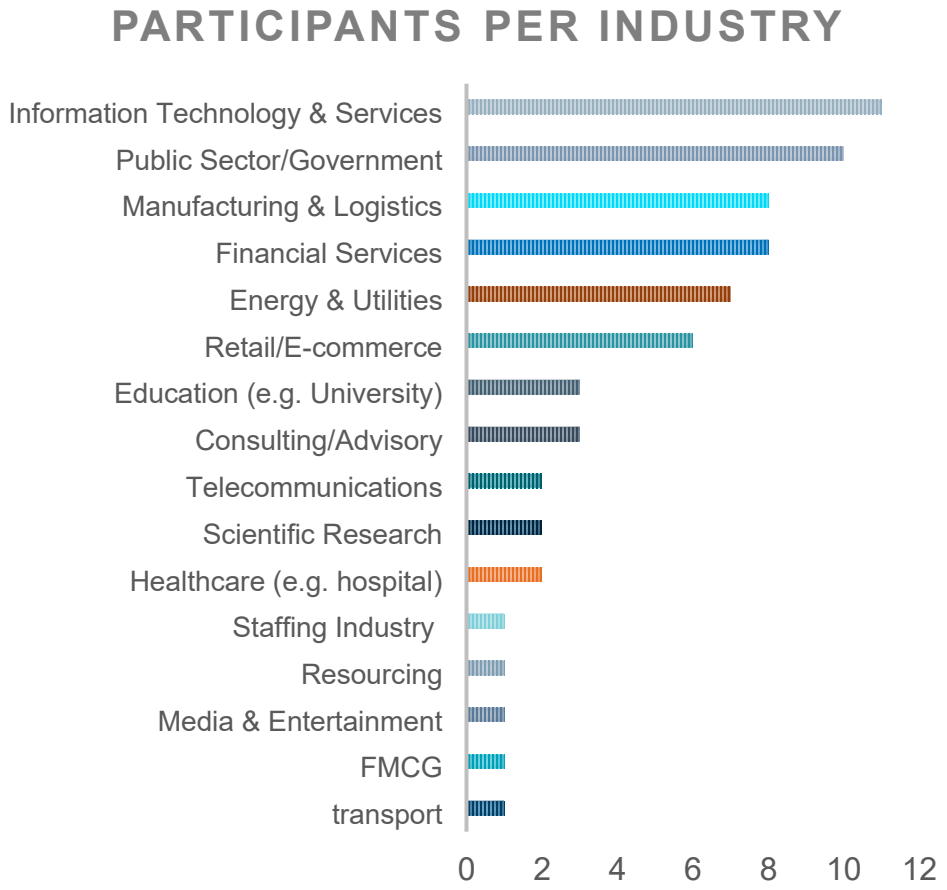
Digital Survey 2025

Inzicht in huidige staat van IAM, gebaseerd op praktijkervaring van professionals. Focus op:

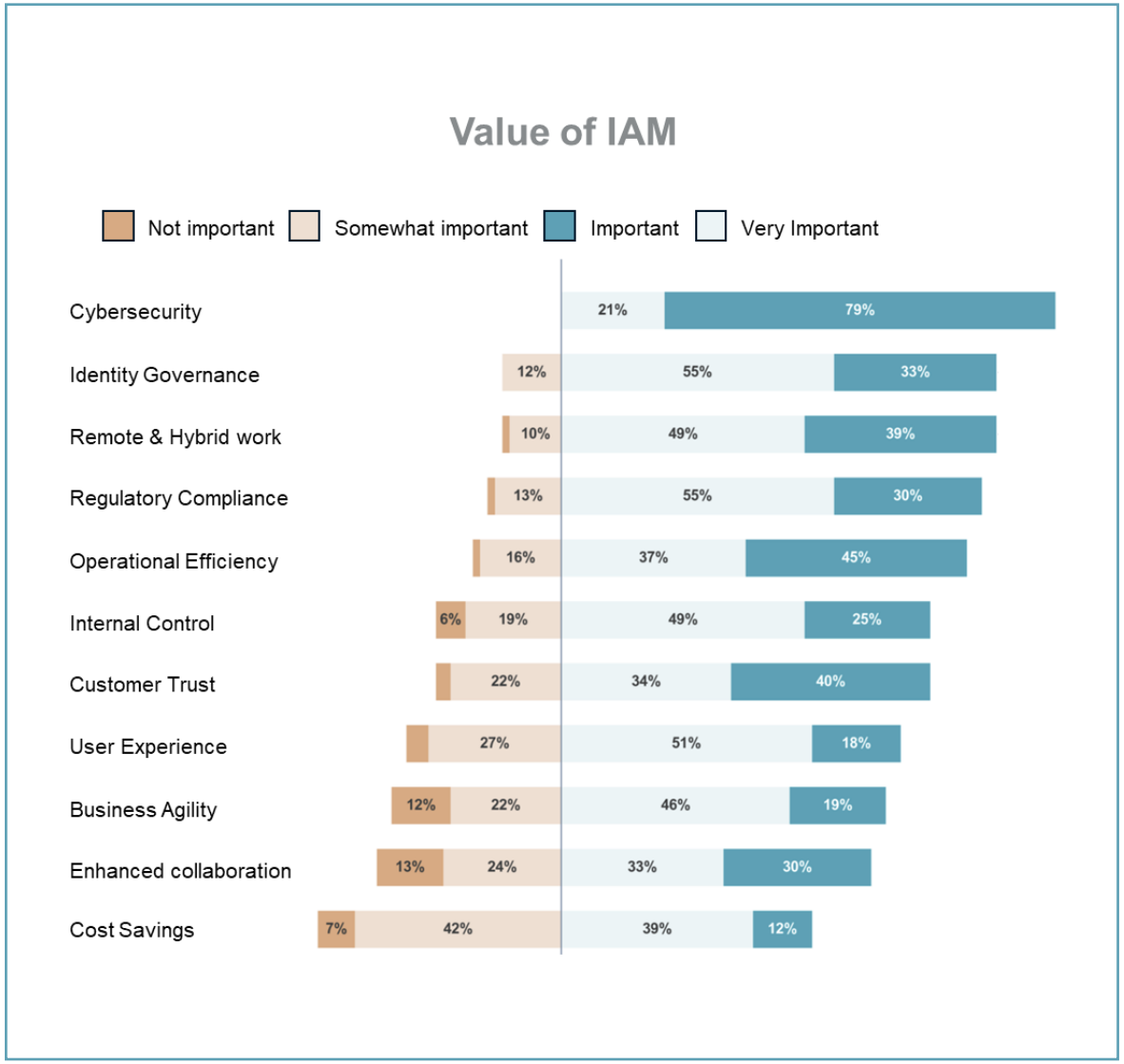
1. Value drivers voor IAM
2. Huidige IAM trends,
3. Volwassenheid gebruik van oplossingen en methoden
4. Implementatie uitdagingen

Over de deelnemers

1. 67 deelnemers uit diverse sectoren
2. Sterke vertegenwoordiging van risico managers, producteigenaren
3. Mix van industrieën en organisatietypen
4. Variatie in omvang en IAM-volwassenheid
5. Focus primair op workforce, deels ook CIAM



1. Value Drivers



Cybersecurity en governance gelden als belangrijkste drijfveren:

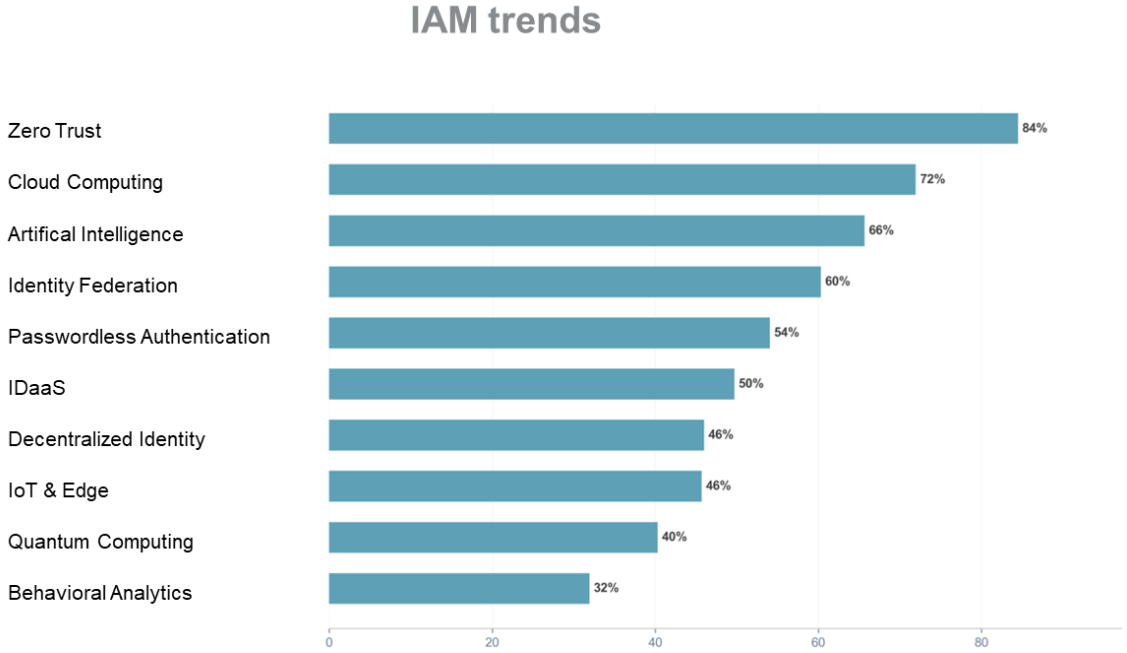
- IAM als fundament voor risicobeheersing
- Ondersteuning van audits en regelgeving (o.a. NIS2)

Toenemende focus op business enablement

- Ondersteunt hybride werken en snellere onboarding
- Verbetert efficiëntie en gebruikerservaring

Resultaten zijn nog wisselend door gefragmenteerd landschap

2. IAM trends



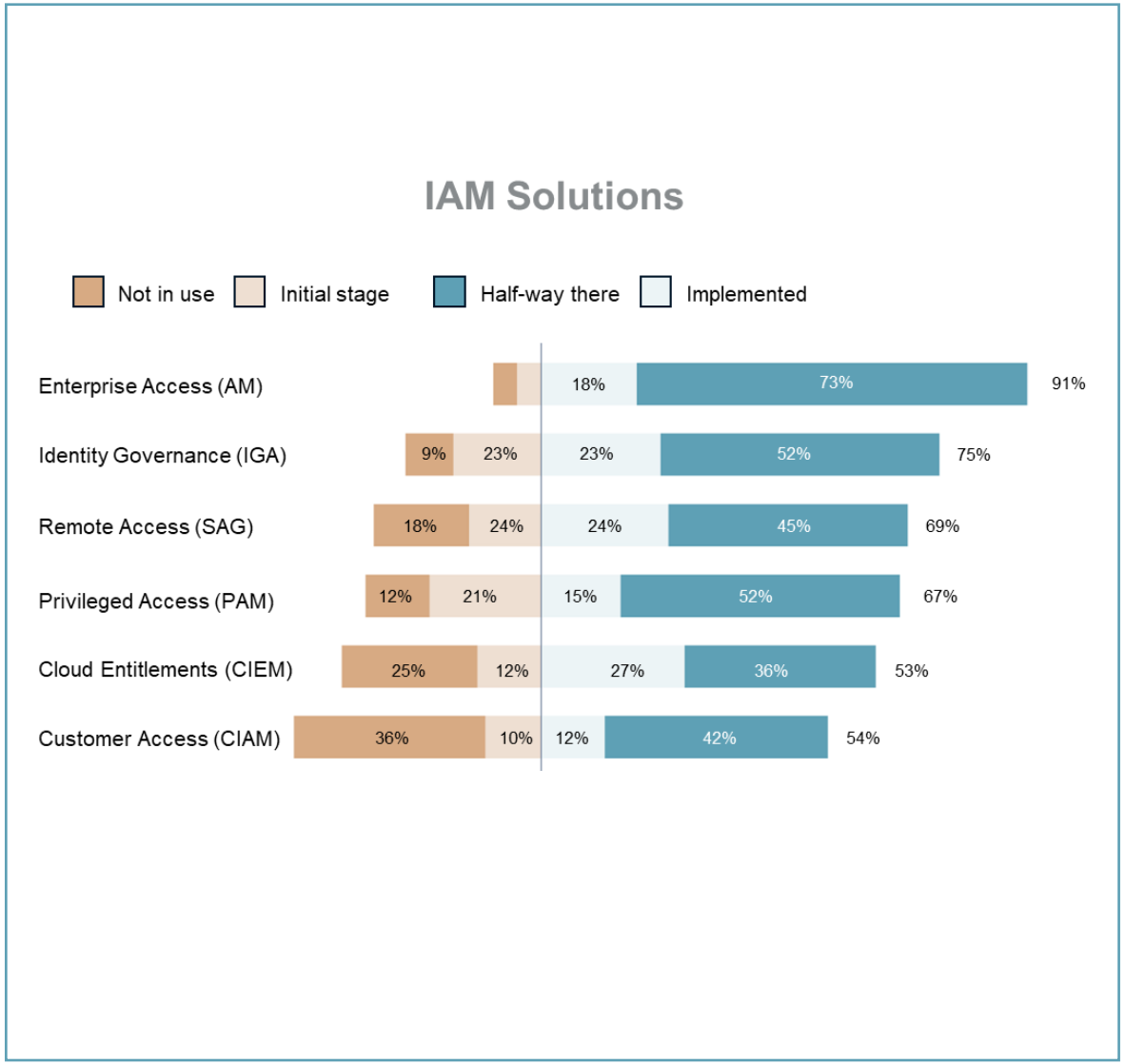
Gelet op de ranking:

- Zero Trust en cloud domineren het beeld
- Identity federation wordt breed toegepast
- Passwordless en IDaaS gelden als belangrijke modernisering drivers
- AI en decentralized identity zijn nog beperkt in praktijk

Aanvullend uit open responses:

- Management van non-human identities
- Interesse in ABAC/PBAC autorisatiestructuren

3. Volwassenheid – gebruik van IAM oplossingen



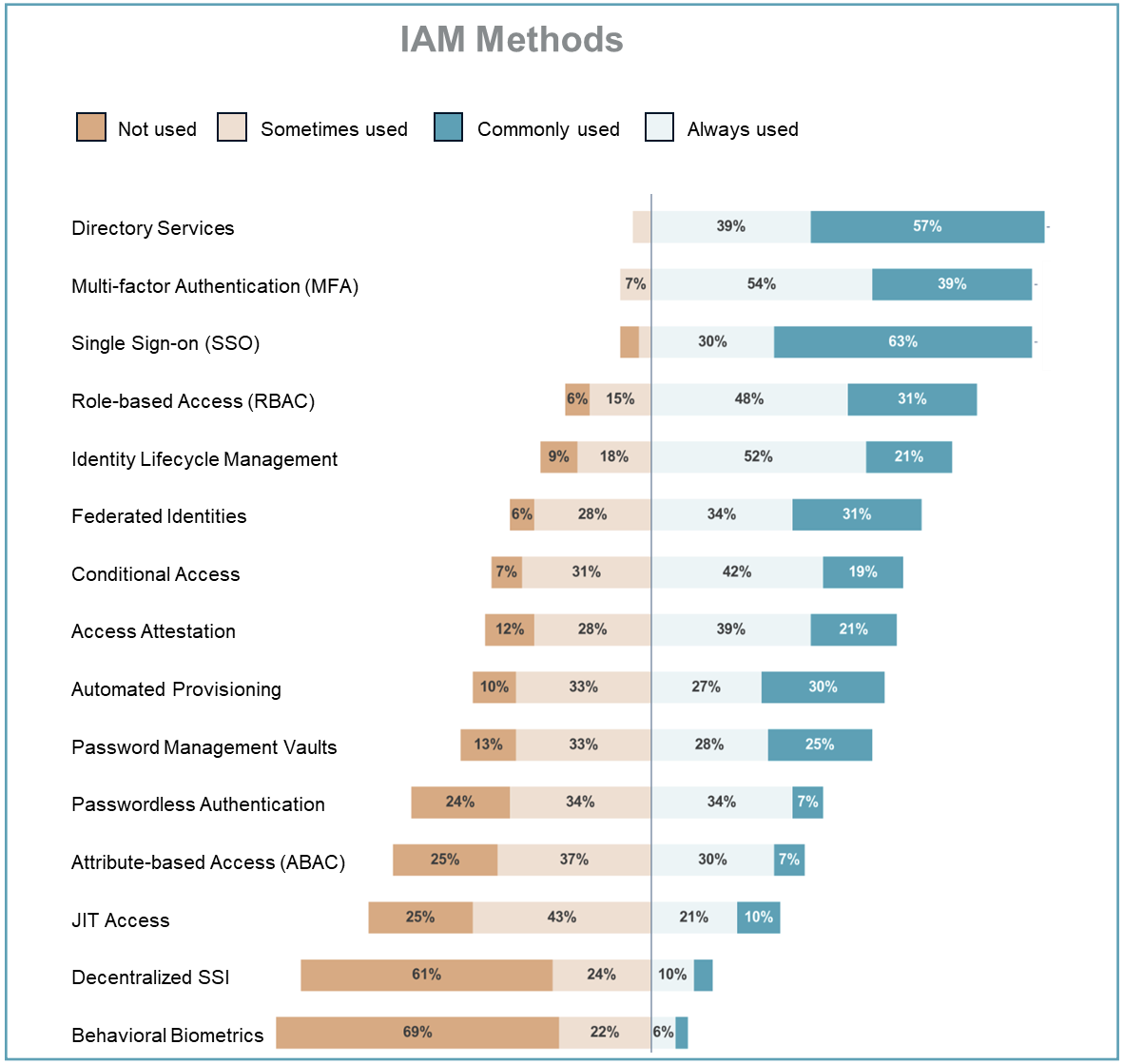
Op basis van de antwoorden van de respondenten:

- IAM landschappen zijn vaak een combinatie van AM, IGA, PAM en directory services
- Adoptie van governance oplossingen varieert per sector:
  - Regulated → governance & controls
  - Overig → onboarding & efficiency
- CIAM aanwezig bij externe gebruikers

Aanvullend uit open responses:

- Vaak hybride inrichting (cloud + on-prem)
- Federatie groeit in belang
- Automatisering nog niet consistent
- Legacy heeft grote invloed op inrichting

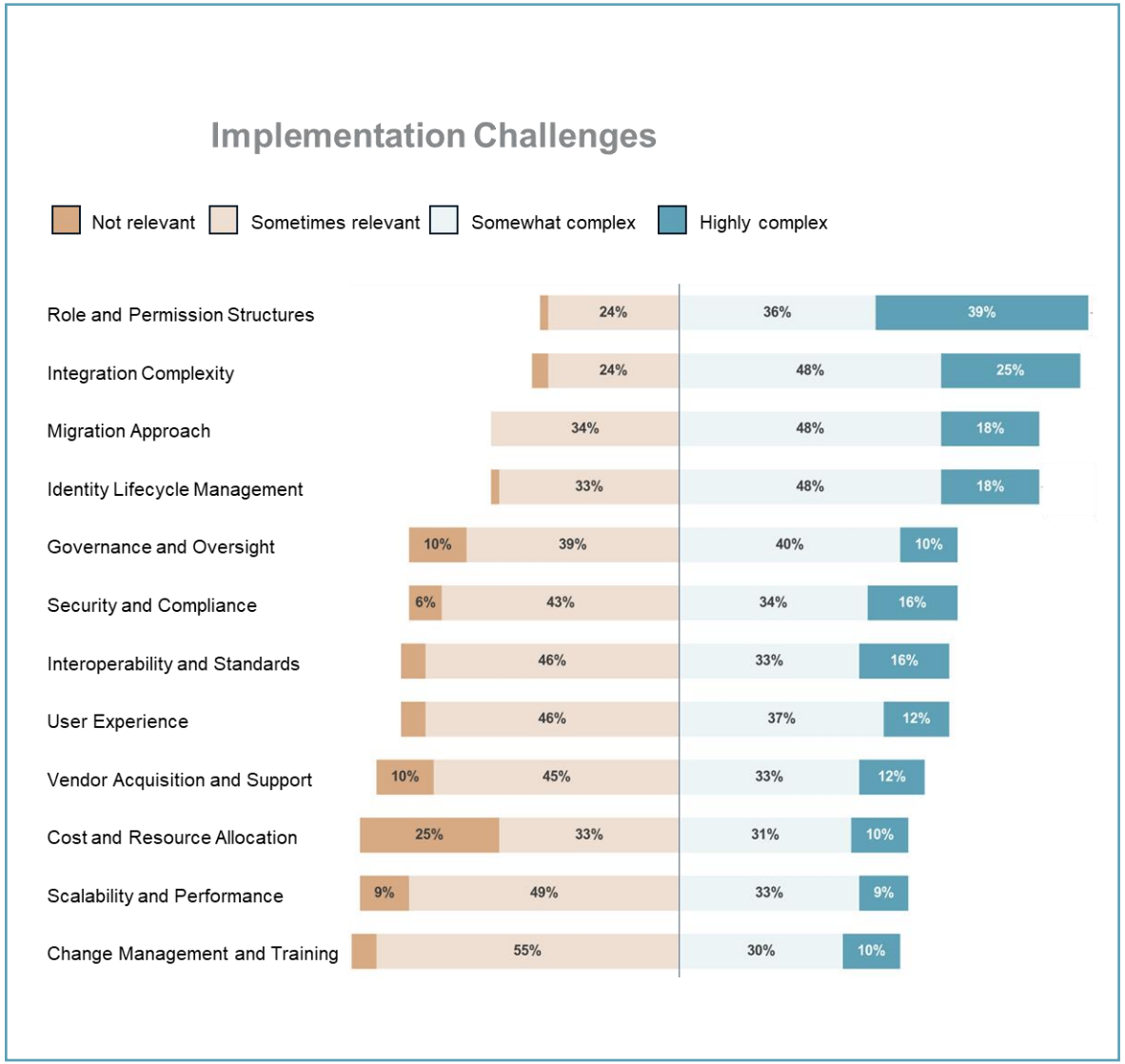
3. Volwassenheid – gebruik van IAM methoden



Gelet op de antwoorden van respondenten:

- Brede inzet van SSO en MFA
- Lifecycle management veel toegepast
- RBAC dominant model
- ABAC/PBAC beperkt toegepast
- JIT en conditional access selectief gebruikt

4. Implementatie uitdagingen



Gelet op de antwoorden van respondenten:

- Governance en ownership versnipperd
- Integratie met legacy en hybride omgevingen complex
- Rol- en autorisatiemodellen lastig schaalbaar
- Data kwaliteit en ontbreken van “single source of truth”
- Security en compliance blijven zwaar en complex

Aanvullend uit open responses:

- Veel handmatige stappen en uitzonderingen
- Fragmentatie van systemen en oplossingen
- Afhankelijkheid van vendors en interne capaciteit
- Uitdagingen rondom onboarding en user journeys

Ter afronding

Conclusies?