Identity Governance
Hvem har adgang til hvad - og hvorfor?

April 2026

Agenda

1. Regulatorisk pres
2. Problemstillingen
3. Hvad er Identity Governance?
4. Tilgangen

Compliance er ikke valgfrit

ISO 27001

International standard for informations-sikkerhed hvor Identity Governance er en central kontrol.

DORA

Digital Operational Resilience Act (DORA) stiller krav til styring af IT-adgange i finans-sektoren og hos leverandører.

GDPR

Stiller krav om beskyttelse af persondata og dokumentation af, hvem der har adgang.

NIS2

Pålægger bestyrelse og direktion ansvar for dokumenterbar risiko- og adgangsstyring. I kraft siden oktober 2024.

Interviewrunde

Utilstrækkelig adgangscertificering

”Kun syv ud af 160 systemer certificeres, og kun to gange årligt. Ledere forstår ikke rettighedskoderne.”

”Ingen automatisering, 140 systemer, og kontrol begrænset til om personen fortsat er ansat.”

Manglende sporbarhed

”Dokumentation i e-mails giver kun et snapshot-overblik.”

“Der er ingen fast eller veldefineret metode.”

Uforståelige rettighedsstrukturer

“Rettigheder tildeles ved ‘trial and error’.”

”System- og dataejere har ikke fuldt overblik eller forstår ikke opgaven.”

Strategiske perspektiver

“Organisationen forvalter intellektuel ejendom for mange milliarder.”

”Man skal kunne arbejde fra dag ét; det tager mindre end fem dage i dag.”

”En meget selvledende kultur gør det svært at indføre nye processer.”

Konklusioner: Manglende overblik udfordrer styring

01

Manuelle mails og regneark

Nye brugere oprettes via IT-support, ændringer gemmes i mails, overblikket holdes i regneark. Skalerer dårligt

02

Fejl og oprydning

Fejl opstår, opgaver trækker ud og dokumentation mangler. IT-afdelingen bruger tid på at rydde op fremfor at forbedre.

03

Viden forsvinder, når dokumentation mangler

Vigtig viden om adgange forsvinder, når medarbejdere stopper, fordi den sjældent er nedskrevet systematisk.

04

Persondata og adgang

GDPR kræver, at persondata er beskyttet, og at det kan dokumenteres, hvem der har haft adgang – og hvorfor.

05

Compliance-risiko

NIS2-direktivet kræver systematisk risiko- og adgangsstyring. Regneark er ikke velegnet til opgaven.

06

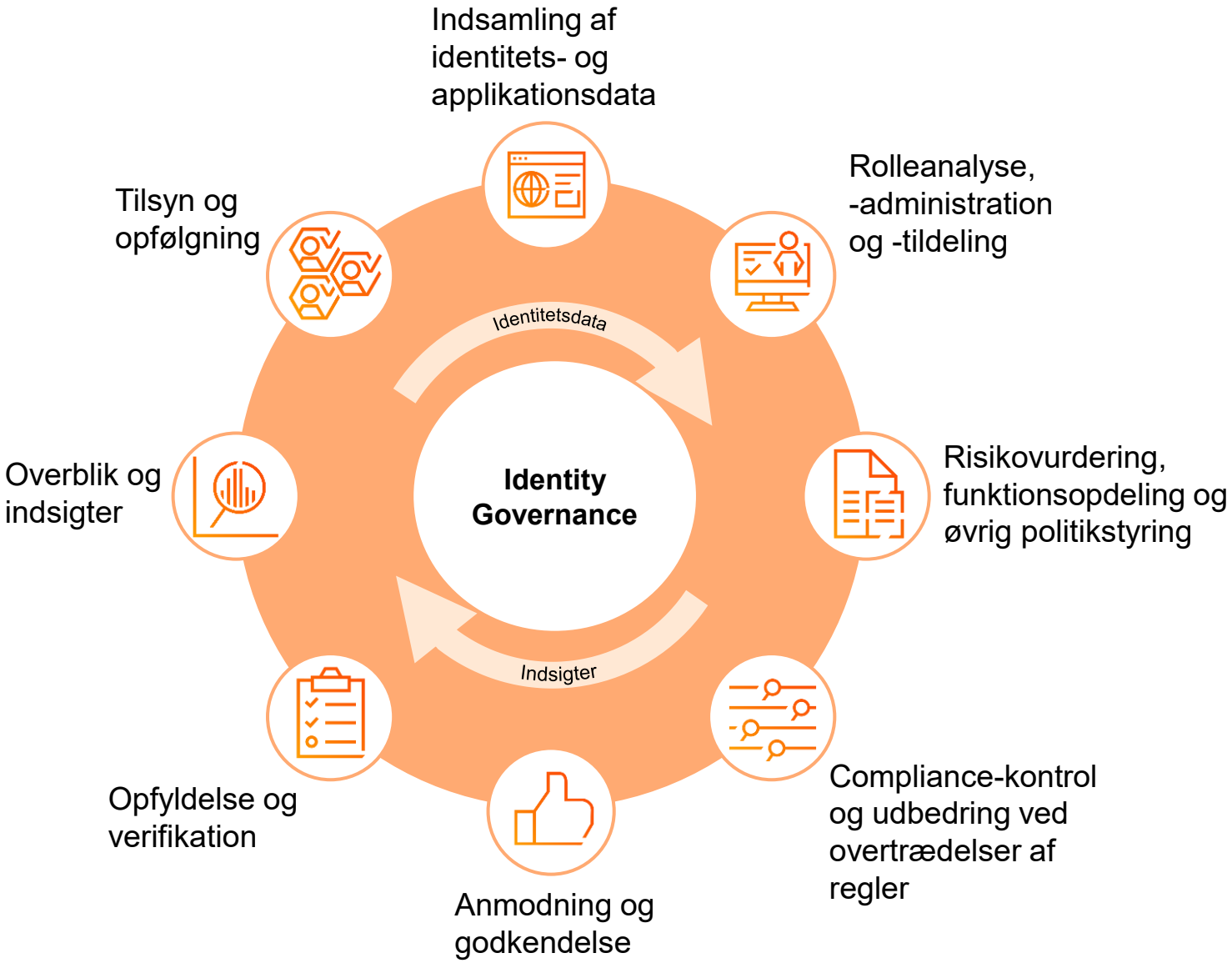
Manglende ledelsesoverblik

Organisationer, der ikke kan svare på adgangsspørgsmål, opererer med en risiko, de ikke har overblik over.

Hvad er Identity Governance?

Systemer der leverer konti og tilladelser

- Directory Service
- Cloud
- Økonomisystem
- Andre systemer



Reference: Model inspireret af OpenText

Tilgang - Fra start til drift

1. Analyse

- Kortlægning af systemer og adgange
- Analyse ift. regulativer, regler, ønsker, m.m.
- Risikovurdering og prioritering

2. Design

- Rollemodel, adgangs-politikker og governance-ramme
- Valg af IG-platform og driftmodel

3. Integration

- Konfiguration
- Kobling til HR, Active Directory og andre kilder
- Test af funktionalitet

4. Pilot

- Kontrolleret udrulning til pilotgruppe
- Test af livscyklus-flows, certificering og rapportering og funktions-opdeling

5. Fuld udrulning

- Trinvis udrulning til hele organisationen
- Change management
- Brugertræning hos ledere og systemejere

6. Drift og forbedring

- Løbende certificering og compliance-rapportering
- Drift og vedligehold

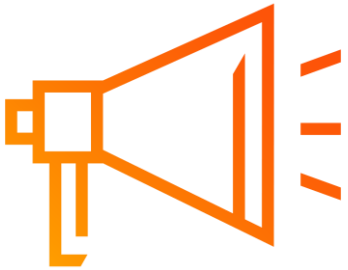
Tre greb til en succesfuld implementering

Grundig forberedelse

- Afklaring af mål, omfang og succeskriterier
- Kortlægning af systemer og nuværende arbejdsgange
- Tydelig rolle- og ansvarsfordeling samt afklaring af beslutningskompetencer

Tidlig og relevant involvering

- Aktiv inddragelse af ledere, systemejere og medarbejdere
- Involvering tidligt i processen
- Skabe engagement og ejerskab hos centrale medarbejdere



Målrettet kommunikation

- Klar kommunikation om formål, ændringer, og forventninger
- Tilpasset kommunikation til de forskellige medarbejdergrupper
- Løbende opdateringer der sikrer gennemsigtighed og fælles forståelse

FAQ

Vejledninger og begrebsafklaring

Nedenfor kan du finde mere information og vejledninger til specifikke funktioner.

- Hvad er en kontrolperson?
- Hvad er en tilsynsejer?
- Hvad er en detailrolle, systemrolle, jobfunktionsrolle i BAS?
- Hvordan fungerer tilsynsfunktionaliteten i BAS? (eLearning)
- Hvordan kan jeg se hvilke opgaver, der mangler at blive godkendt?
- Hvordan ændrer jeg visning i ledelsestilsynet, så jeg har fokus på medarbejdere eller jobfunktionsroller?
- Hvordan ændrer jeg visning i systemtilsynet, så jeg har fokus på specifikke roller?
- Hvordan behandler jeg flere linjer i tilsynet på én gang?
- Hvordan kan jeg få vist flere detaljer om rollerne i tilsynet?
- Hvor kan jeg finde mere detaljeret information om den enkelte rolle, f.eks. indhold og tildeling?

Eksempel på mail der synliggør lederens rolle og ansvar

Hej Kenneth

Det er blevet tid til at udføre ledelsestilsyn ift. autorisationskontrol

Du modtager denne mail, fordi du er anført som leder og personaleansvarlig. Du har derfor pligt til at forholde dig til og kontrollere, om de jobfunktionsroller dine medarbejdere har fået tildelt fortsat er relevante, samt fjerne dem der ikke længere er relevante, hvormed rettighederne fjernes. Selve kontrollen kommer til at foregå via et værktøj, der hedder NetIQ Identity Governance.

Som ansvarlig kontrolperson bedes du gennemføre tilsynet i løbet af 42 dage fra d.d. Når du har gennemført tilsynet, bliver dette sendt til tilsynsejer for endelig godkendelse.

Klik her for at gennemføre tilsynet.

Har du spørgsmål?

Tak for jeres tid –
Lad os fortsætte snakken

Martin Oldin
Phone: +45 5115 7920
Email: martin.oldin@pwc.com

Nicolai Glahn
Phone: +45 2528 2755
Email: nicolai.glahn@pwc.com