identity stream

IdS IAM for virksomheter på Entra ID

Dokumenteier: Tore Olav Kristiansen, Produkteier IdS IAM

Status: Versjon 1.0

Versjonshistorikk

Dato	Versjon	Beskrivelse	Forfatter
01.11.2025	1.0	Første versjon av dokument	Tore Olav Kristiansen
09.11.2025	1.1	La til forord på kapitlet om risikofylte tilgangskombinasjoner.	Tore Olav Kristiansen

Innholdsfortegnelse

1 Sammendrag

EU skjerper nå kravene til digital robusthet og identitetsstyring gjennom nye reguleringer som **DORA** (Digital Operational Resilience Act) og **NIS2** (Network and Information Security Directive). Dette betyr at virksomheter – særlig innen finans – må kunne demonstrere full kontroll på hvem som har tilgang til hva, med omfattende revisjonsspor og styring. **Microsoft Entra ID** alene dekker kun det mest grunnleggende innen identitetsadministrasjon, og mangler en rekke funksjoner for å oppfylle disse skjerpede kravene. En organisasjon som kun bruker Entra ID må ty til manuelle rutiner og fragmenterte verktøy for å håndtere livssyklusen for identiteter – noe som øker risiko og arbeidsmengde, **uten** å gi samsvar med DORA og NIS2. Kort sagt tilfredsstiller ikke Entra ID alene de regulatoriske kravene, verken på **etterlevelse** eller **internkontroll**.

IdentityStream IdS IAM er utviklet nettopp for å fylle dette gapet. IdS IAM er en "**opinionated**" programvareløsning bygget på 13 års erfaring fra Norges mest regulerte sektor – finans. Løsningen kommer med innebygde beste praksiser og forhåndsdefinerte prosesser, slik at implementasjonen går raskt og effektivt i strengt regulerte miljøer. Dette står i kontrast til generiske IAM-løsninger som ofte krever tunge tilpasninger. IdS IAM muliggjør **rask utrulling** med lav driftsbelastning gjennom scriptet installasjon, sky-styrt konfigurasjon og gjenbruk av integrasjoner. Plattformen leveres dessuten med et bredt utvalg ferdige konnektorer (inkludert tett integrasjon med Entra ID) og det er minimal innsats for å lage nye. For virksomheten betyr dette at man kan ta i bruk IdS IAM langt raskere enn tradisjonelle IAM-løsninger – og begynne å høste gevinster nærmest umiddelbart.

Med IdS IAM får organisasjonen **helhetlig styring, sporbarhet og kontroll** over identiteter og tilganger, i en grad Entra ID ikke tilbyr. Løsningen fungerer som én sentral kilde til sannhet for alle identiteter, roller og tilganger i virksomheten. Dette gir konsistent policy-håndhevelse på tvers av systemer og avdelinger, uten siloer. **Revisjonsspor** er fullstendig: IdS IAM logger alle tilgangsendringer med kontekst og begrunnelse (f.eks. ny ansatt, rollebytte), slik at man i ettertid vet **hvem gjorde hva og hvorfor** – noe Entra ID ikke har støtte for. Ledere, sikkerhetsansvarlige og revisorer får dermed full innsikt i historikk og

endringer, noe som forenkler dokumentasjon av internkontroll og etterlevelse. IdS IAM har også innebygd **styring og kontrollmekanismer** som overgår Entra ID, eksempelvis mulighet for å definere og håndheve *Separation of Duties*-regler (SoD) for å forhindre risikofylte tilgangskombinasjoner. Alle brudd på SoD-policyer fanges opp og krever dokumentert godkjenning, med komplett loggføring for tilsyn og revisjon. Slik helhetlig kontroll fra IdS IAM sikrer at **alle uautoriserte eller uønskede tilganger** blir oppdaget.

Videre adresserer IdS IAM praktiske behov som Entra ID etterlater til manuell oppfølging. For eksempel har IdS IAM et rikt sett verktøy for lisensstyring og tilgangsadministrasjon som kan gi **betydelige kostnadsbesparelser og risikoreduksjon**. Entra ID tilbyr ingen enkel måte å identifisere ubrukt eller overflødig tilgang på; IdS derimot kan automatisk oppdage og stoppe uautoriserte tildelinger av dyre lisenser, velge rimeligste alternativ først, og vise nøyaktig hvem som bruker hvilke lisenser. Dette gir ledere og økonomiansvarlige kontroll på IT-kostnadene og eliminerer budsjett-overraskelser – samtidig som etterlevelse styrkes gjennom forebygging av ukontrollert tilgang. Et konkret eksempel: typisk vil *1–3 %* av de ansatte være i permisjon til enhver tid (i perioder opp mot 5 %). Med IdS IAM fanges slike fravær opp automatisk, og lisensene deres kan settes på pause eller omfordeles etter policy. Slik unngår man både unødige lisenskostnader og risikoen ved at brukere beholder tilganger de ikke trenger – en kontroll som må gjøres manuelt utenfor IdS IAM dersom man kun baserer seg på Entra ID.

Aller viktigst for målgruppen av IT- og sikkerhetsledere: IdS IAM er designet for **etterlevelse fra første stund**. Løsningen kommer "ut-av-boksen" med regelstyrte livssyklusprosesser (Joiner-Mover-Leaver) som sikrer at de rette personene godkjenner tilganger til riktig tid, at **alle endringer er dokumentert**, og at policyer automatisk blir håndhevet i hele organisasjonen. Dette gir umiddelbar effekt: mindre operasjonell risiko, færre avvik, og en mer strømlinjeformet etterlevelse av lovkrav enn det man oppnår med standardfunksjonaliteten i Entra ID. IdS IAM støtter også **distribuert ansvar** uten å miste sentral oversikt – linjeledere og systemeiere kan selv ta hånd om tilgangsforespørsler og revisjon innenfor rammer satt av sikkerhetsteamet, med full sporbarhet på tvers. Slik kombineres det beste av to verdener: lokal smidighet og sentral kontroll.

Flere virksomheter har allerede erfart fordelene av denne tilnærmingen. For eksempel innførte **Eika-alliansen** (en sammenslutning av norske sparebanker) en felles IdS IAM-plattform for alle medlemsbankene. Resultatet var en ensartet og helhetlig tilgangsstruktur på tvers av organisasjonene, med klare stordriftsfordeler: **lavere kostnader, bedre etterlevelse** og samtidig lokal fleksibilitet der det trengs. Lokale IT-ressurser som før var bundet opp i tilgangsadministrasjon, ble frigjort til mer verdiskapende arbeid – alt mens sikkerheten og kontrollen økte. Dette caset illustrerer hvordan IdS IAM muliggjør sentralisert styring uten byråkrati, noe som er vanskelig å oppnå med Entra ID alene.

Konklusjon: IdS IAM kompletterer Microsoft Entra ID ved å tilføre den avanserte identitetsstyringen, kontrollen og dokumentasjonen som moderne regulatoriske regimer krever. For virksomheter som må etterleve DORA, NIS2 og lignende, er IdS IAM et strategisk valg – en helhetlig IAM-plattform **skreddersydd for rask implementering i regulerte miljøer**, med betydelig bevismengde fra den norske finansnæringen. Den gir beslutningstakere trygghet for at identitetsforvaltningen er under kontroll, revisjonssikker, og kostnadseffektiv. Med IdS IAM på plass kan IT-ledere og sikkerhetsansvarlige være proaktive: de oppnår full oversikt og **etterlevelse by design**, i stedet for å lappe på begrensningene i Entra ID. Økonomisk kommer virksomheter bedre ut med IdS IAM, fordi plattformen leverer styring, revisjon og automatisering som lar virksomheter operere trygt og effektivt på et lavere og rimeligere Entra ID-tier uten å kompromittere sikkerhet eller etterlevelse. Kort oppsummert leverer IdentityStream IdS IAM en dokumentert, kontrollert og effektiv identitetsstyring som både styresmakter og virksomhetens ledelse vil forvente i årene som kommer – raskere og mer treffsikkert enn alternativer som krever større skreddersøm.

2 Innledning

EU skjerper kontinuerlig kravene til tilgangsstyring gjennom lover, forordninger og veiledere. Sist ut er DORA og NIS2. Nasjonale tilsyn følger opp med rapporteringskrav, uavhengige revisjoner og stedlige tilsyn.

Identity and Access Management (IAM) gjør det mulig å sikre at både mennesker og ikke-menneskelige enheter får riktig tilgang til riktig ressurs til riktig tid. En moden IAM-løsning er en nøkkelkomponent for etterlevelse av disse kravene.

IdS IAM er IdentityStream sin plattform for identitets- og tilgangsstyring, utviklet gjennom 13 år med kundedreven innovasjon i Norges mest regulerte sektor: finans.

Dette dokumentet introduserer IdentityStream IdS IAM og viser hvordan løsningen komplementerer Microsoft Entra ID.

3 IdS IAM modellen

IdS IAM har *systemtilkobling* som representerer et system. En systemtilkobling kan ha en *konnektor* som integrerer mot systemet. Systemtilkobling har omfattende systemspesifikk konfigurasjon for konnektoren mot systeminstansen. Den har også konfigurasjon for hvordan IdS IAM skal styre identitet og tilgang mot systemet. IdS IAM er prosessmotoren som disponerer systemtilkoblingene.

IdS IAM leveres med mange konnektortyper og det er lite arbeid å lage nye. Konnektortypen for Entra ID lar IdS IAM styre identitet og tilgang per leietaker i dette systemet. Det er sømløst for de som jobber i IdS IAM hvilke systemer en aksjon medfører operasjon mot.

IdS IAM lar virksomheten dele opp systemlandskapet sitt i *tjenester*. Hver tjeneste har en landingsside og omfattende konfigurasjonsmuligheter. *Tilgangsnivå* knyttet til tjeneste er en navngitt adgang til å utføre et sett aksjoner i systemet som tilgangsnivået er koblet mot. Hvert tilgangsnivå kan overstyre konfigurasjon fra tjenesten.

Tjeneste kan være koblet mot en systemtilkobling og kan overstyre innstillinger fra systemtilkoblingen.

Tilgangsnivåer kan være automatiske med obligatorisk systemtilkobling. De kan også være manuelle der tilgangsordre blir stoppet for manuell effektuering i systemet. Manuelle ordre brukes der virksomheten ikke har tilgjengelig integrasjon mot systemet. IdS IAM støtter forhåndsdefinerte malbaserte meldinger for videresending på e-post av manuelle ordre til ekstern part. Svar kommer direkte inn til ordren. Malene støtter å flette inn data om medarbeider, organisasjon og tilgang.

IdS IAM støtter registertjenester som bare registrer tilgang etter eventuell godkjenning, uten manuell operasjon. En tilgangseksport eller annen type effektuering på tidsplan, kan få tilgangene på plass på et senere tidspunkt. Det er også mulig å bare ha tilgangene i IAM som et oppslag. Det kan f.eks. være brukt på kredittfullmakter der en kun vil at medarbeider skal være klare over eget fullmaktsnivå og at utbetalingsfunksjon skal kunne detektere fullmaktsbrudd.

En og samme tjeneste kan ha tilgangsnivåer fra ulike systemtilkoblinger og av ulike typer.

Roller er pakker av tilgangsnivåer. Også roller har omfattende konfigurasjon.

Eierskap og oppdragsgrupper for IAM oppgaver er viktig konfigurasjon på tjeneste, tilgangsnivå og rolle. Godkjenning, revisjon og manuell utføring er eksempler på IAM oppgaver. Det modulære systemlandskapet gir virksomheten kontekst til å fordele IAM oppgaver ut i organisasjonen.

Entra ID har ikke en slik god oppdelingen av systemlandskapet og har heller ikke funksjon for manuelle tjenester eller registertjenester. En får dermed ikke fullstendig styring av identitet og tilgang. Som et eksempel kan vi bruke risikofylte tilgangskombinasjoner eller "Separation of duties" (SoD) som det heter på engelsk. Med IdS IAM kan du SoD-modellere at tilgang i et manuelt fagsystem, representert av en manuell tjeneste, ikke skal kunne kombineres med tilgang til et gitt SharePoint Online område, representert av et automatisk Entra ID tilgangsnivå. Det kan du ikke med Entra ID.

Entra ID har heller ikke tjenesteordremeldinger.

Tilordning av tilgang i IdS IAM er bygd opp rundt tre sentrale modeller for styring av identitet og tilgang.

3.1 RBAC (Role-Based Access Control)

Brukere får tilgang via roller. IdS IAM skiller mellom organisasjonsroller og funksjonsroller.

Organisasjonsroller er automatiske roller fra HR/organisasjonsstrukturen: Selskap, Avdeling, Kontorlokasjon, Ansettelsestype, Stilling og Leder. Organisasjonsrollene deler opp brukermassen og har innstillinger som utgjør kraftig regelstyrt tilgangskontroll som vi kommer tilbake til i PBAC (Policy-Based Access Control) seksjonen under.

Funksjonsroller er system- eller oppgaveorienterte. De velges som regel av leder siden det er leder og ikke HR som vet hva medarbeider skal jobbe med. Rolle-tilgangsnivå knytter et tilgangsnivå til en eller flere roller.

Tilgang gitt via rolle på denne måten kalles standardtilgang. Det er også mulig å gi en bruker et ekstra tilgangsnivå utover det brukeren får som standard via sine rollemedlemskap. Ekstra tilgang må gis via en rolle slik at medarbeider ikke drar med seg ekstra tilganger gitt i kontekst av en funksjon, ved endring til en annen funksjon.

3.1.1 Standardmodell for et menneske i IdS IAM

- Organisasjonsroller
    - 1 × selskap
    - 1 × ansettelsestype
    - 1 × stilling
    - 1 eller flere avdelinger
        - Avdelinger er hierarkiske; medlemskap arver oppover i hierarkiet.
        - Medarbeider kan ha ekstra avdelinger; disse arver også hierarki.
    - 0 eller flere kontorlokasjoner
        - Kontorlokasjon er ikke obligatorisk.
        - Kontorlokasjoner kan bygges hierarkisk
        - Kontorlokasjoner følger som regel avdeling, men kan overstyres per medarbeider.
        - Ekstra avdelinger gir medlemskap i tilhørende kontor(er) inkl. hierarki.
    - 0 eller flere lederroller

- Hvert selskap har en rolle med ledere for avdelinger i selskapet. Medlemskapet i denne blir automatisk bygget basert på avdelingshierarkiet.

- Funksjonsroller
  - 0 eller flere (leder velger som regel minst én).
  - Funksjonsroller kan være hierarkiske

3.2 ABAC (Attribute-Based Access Control)

IdS IAM kan tildele eller begrense tilgang basert på attributter som selskap, avdeling (hierarkisk), kontor, ansettelsestype og stilling. Rolle-tilgangsnivåer kan ha ekstra rollekrav eller unntatte roller.

Du kan for eksempel legge tilgangsnivået for 1 million i attesteringsfullmakt i en avdeling, sette lederrollen i selskapet som krav og deaktivere arv slik at bare lederen i den aktuelle avdelingen får tilgangen.

Du kan også for eksempel legge lisensen til Dynamics 365 i avdelingen Personmarked og sette ansettelsestypene Fast ansatt og Vikar som ekstra rollekrav slik at kun fast ansatte og vikarer i Personmarked automatisk får lisensen.

3.3 PBAC (Policy-Based Access Control) - Del og styr

IdS IAM har innstillinger på alle dimensjoner i den modulære modellen som i sum gir kraftig regelstyrt tilgangskontroll. Systemlandskap og brukermasse er distribuert ut modellen. Vi kan tillate oss en omskriving av det berømte uttrykket "splitt og hersk" for å beskrive fordelene modellen gir styring av identitet og tilgang: "del og styr".

3.3.1 Utvalgte regelinnstillinger i modellen

Rolle:

- Eiere, oppdragsgruppe og godkjenningsløp for medlemskap
- Godkjenning for selvbetjent aktivering (PAM)
- Tillatte tildelingstyper: aktiv og/eller selvbetjent
- Makstid for:
  - Aktiv tildeling av medlemskap
  - Selvbetjent tildeling av medlemskap (PAM)
  - Aktivering av selvbetjent tildelt medlemskap (PAM)
- Kan bestilles av leder
- Skal revideres av leder
- Begrensning av tilordning til brukere i avdeling (og underavdelinger)

Ansettelsestype:

- Maks antall dager arbeidsperiode
  - Står alltid tom for fast ansatte og konsulenter kan f.eks. settes til 365 dager.
- Opsjon for godkjenning ved aktivering av selvbetjente tilganger og roller

    - Den kan for eksempel være slått av for fast ansatte og slått på for eksterne medarbeidere
- Opsjoner for om ansettelsestypen tilordnes tilgang fra avdelinger:
    - Alltid
    - Aldri
    - La leder velge med «på» som standard
    - La leder velge med «av» som standard
- Opsjoner for om det skal opprettes postboks
- Opsjon for lisenstilgangsnivå som skal tilordnes som ekstra tilgang ved bestilling av postboks
    - Opsjonen er nyttig dersom Exchange lisens ikke tilordnes som standard
- Opsjoner for om det kreves mobiltelefoni

Selskap:

- Tilgangsansvarlige medarbeidere som kan erstatte eller hjelpe ledere for avdelinger i selskapet, med avdelingens IAM oppgaver.
- Permisjonsrolle som tilordnes medarbeidere i permisjon som et minimum av tilganger de skal ha i fraværsperioden.
- Stedfortrederrolle som tilordnes medarbeidere når ledere i selskapet legger de til som personlig stedfortreder eller tilgangsansvarlig på en av sine avdelinger
- Aktivering og tidsplan for periodisk leders tilgangsrevisjon for medarbeidere i selskapet
- Mulighet for å inkludere ansettelsesforhold i tilgangsrevisjon for å fjerne medarbeidere med identiteter og tilgang dersom de ikke lenger har aktiv arbeidsperiode.
- Regelsett for tilegning av ansvarssted til medarbeidere
- Exchange postbokskommandoer for innstillinger som må gjøres før, under og etter oppretting av postboks.
- Exchange postbokskommandoer skal kjøres etter aktivering og deaktivering av medarbeider.
- Mal og domener for oppretting av postboks
- Godkjenningsløp for bruk av selskapets avdelinger som en ekstra avdeling på medarbeider
- Har leder tillatelse til å endre arbeidsperiode for fast og/eller midlertidige medarbeidere

Avdeling:

- Tilgangsansvarlige medarbeidere som kan erstatte eller hjelpe leder med avdelingens IAM oppgaver.
- Standard kontorlokasjon for medarbeidere i avdelingen
- Aktivering og tidsplan for leders periodiske tilgangsrevisjon for medarbeidere i avdelingen. Dette overstyrer innstilling fra selskap.

Tjeneste:

- Eiere, oppdragsgruppe og godkjenningsløp for tilgang
- Godkjenning for selvbetjent aktivering (PAM)
- Tillatte tildelingstyper: aktiv og/eller selvbetjent
- Makstid for aktiv tildeling av tilgang og selvbetjent tildeling av tilgang (PAM)
- Makstid for aktivering av selvbetjent tildelt tilgang (PAM)
- Krev begrunnelse ved selvbetjent aktivering
- Begrensning av tilgangstilordning til selskap og ansettelsestype
- Tilgjengelighet for selvbetjent bestilling
- Tilgjengelighet for gjestebrukere
    - Gjester er typisk brukere fra andre virksomheter som har en identitet på infrastrukturen, men logger på med brukernavn og passord fra sitt eget selskap og gis tilgang til skybaserte tjenester.
- Tilgjengelighet for brukere som ikke skal ha pålogging til plattformen
    - Dette kan være renholds- og kantinepersonell.
- Tilgjengelig for medarbeidere uten tilgang til avdelingens fellesressurser
- Deling med andre leietakere i eventuell allianse
- Publisering til andre leietakere i alliansen
- Revideringsregler

Tilgangsnivå:

- Overstyring av innstillinger fra tjeneste
- Kan tilgang bestilles av leder
- Kan tilgang delegeres ved fravær
- Har tilgang personlig portefølje som må overføres ved avdelingsbytte og sluttføring.
- Gruppering av tilgangsnivå der medarbeider kan ha kun en tilgang innenfor hver gruppering

Leietaker:

- Konfigurasjon av varsling på sluttføring
- Konfigurasjon av slettingsprosess for brukere i systemer og postbokser
- Tillatt selvbetjent kontorlokasjon
- Kun ekstra tilgang skal godkjennes
- Tidsplan for rolleeiers revisjon

4 Tilgangsliste

IdS IAM tilgangslisten har full medarbeiderinformasjon og revisjonsinformasjon som inkluderer:

- Hvem bestilte og når
- Hvem godkjente og når
- Hvem utførte tilgangsendring og når
- Hvem utførte sist lederrevisjon og når
- Hvem fjernet og når tilgang ble fjernet (for historisk tilgang)
- Full sporing i form av saksgang lenket til tilgang som forklarer hvorfor tilgang ble gitt eller fjernet.

IdS IAM er en sentral autorativ kilde for hvilke tilganger som *skal* gis til brukere basert på definerte regler. Løsningen detekterer automatisk uregelmessigheter i tilgang mellom system og IAM

- Oppgaver tilordnes for å løse uregelmessigheter
- Samme mulighet er tilgjengelig for manuelle tjenester via import av tilgangslister eksportert fra systemet

Denne funksjonaliteten mangler Entra ID.

IdS IAM har enkel mulighet for å se historiske tilganger i tidsrom og på et tidspunkt. Dette mangler Entra ID. IdS IAM har også full historikk på endringer i regler.

Tilordning og fjerning av tilgang kan spores via saksgang som forklarer hvorfor endringen skjedde. Det kan være en endring i rollemedlemskap eller ekstra tilgang via registrering av ny medarbeider eller endring av avdeling for medarbeider. Denne funksjonaliteten mangler Entra ID.

Tilgangslisten til IdS IAM støtter utlisting av kostnad per avdeling, selskap og medarbeider. Dette kan brukes i internfakturering. Dette mangler Entra ID.

5 Medarbeiderliste og arbeidsperioder

IdS IAM har funksjonalitet for å se alle medarbeidere med brukerinformasjon i en brukervennlig liste med funksjoner for søk, sortering, filtrering, gruppering, rapportering og diagrammer. Det er mulig å slå på visning av historiske medarbeidere. Det er også funksjon for å vise hvilke medarbeidere som har hatt arbeidsforhold i et historisk tidsrom.

Entra ID har en enkel brukerutlisting og mangler helt muligheten til å se historiske arbeidsforhold.

6 Joiner, Mover and leaver (JML, livssyklus for brukere)

IdentityStream IdS IAM håndterer hele livssyklusen til medarbeidere gjennom automatiserte og regelstyrte prosesser. Fra registrering av nye ansatte og endringer underveis, til sluttføring når de fratrer, sørger løsningen for at tilganger og identiteter administreres effektivt, sikkert og konsistent i alle faser.

6.1 Overordnet funksjonalitet for registrering og endring

Den styrte **veiviseren** for registrering av nye medarbeidere og endring av eksisterende, er en nøkkelkomponent for livsyklusadministrasjon i IdS IAM.

Denne veiviseren leder HR-ansatte eller ledere gjennom en strukturert prosess for å opprette eller oppdatere en bruker, der relevante opplysninger (som personalia, ansettelsestype, start- og sluttdato, avdeling, stilling m.m.) fylles inn. Underveis **foreslår systemet automatisk riktige tilganger** basert på forhåndsdefinerte regler og roller – for eksempel kan standardtilganger avhenge av hvilken ansettelsestype eller avdeling man velger. **Nye systemer, roller og tilgangsnivåer blir umiddelbart tilgjengelige** i veiviseren så snart de er konfigurert med slike regler, uten behov for utvikling. Det betyr at hvis virksomheten legger til en ny applikasjon eller rolle og angir at den gjelder for f.eks. “Avdeling X” eller “Ansettelsestype Y”, vil veiviseren automatisk inkludere dette når en ny person med den avdelingen eller ansettelsestype registreres.

IdS IAM håndterer også **personendringer** sømløst. Når en ansatt bytter rolle eller avdeling, endrer stillingsprosent, får nytt navn osv., registreres dette som en **personendringssak**. Løsningen oppdaterer da automatisk tilganger etter de gjeldende retningslinjene: Tilganger som ikke lenger er relevante fjernes, og nye tilganger som trengs i den nye rollen blir tildelt – alt basert på de samme regelmotorene som ved nyansettelser. Hele prosessen er sporbar; IdS IAM **logger alle tilgangsendringer med kontekst** slik at man i ettertid kan se *hva* som ble endret *hvorfor*. For eksempel vil systemet dokumentere om en tilgang ble tildelt eller fjernet som følge av en nyregistrering, et avdelingsbytte eller en annen definert hendelse. Dette gir full oversikt og revisjonsspor over livssyklusen til hver medarbeider.

6.2 Brukeropplevelse og automatisering

Brukeropplevelsen i IdS IAM er designet for enkelhet og effektivitet, blant annet:

- **Enkel registrering:** HR eller bestiller (f.eks. linjeleder) kan registrere en ny medarbeider eller oppdatere en eksisterende via en enkel veiviser. Skjemaet er brukervennlig og logisk, og krever ingen teknisk kompetanse – man fyller kun inn nødvendige data og velger eventuelle tilleggsvalg (som ekstra systemtilganger utover standard).
- **Automatisk opprettelse av tilganger:** Når bestillingen sendes inn, tar IdS IAM over. **All kontoopprettelse og tilgangstildeling skjer automatisk i bakgrunnen.** Løsningen oppretter brukeren i relevante systemer (f.eks. Entra ID) og tildeler riktige grupper, lisenser og roller basert på personens stilling og avdeling. Eventuelle godkjenninger eller arbeidsflyter håndteres også automatisk. Bestiller trenger altså ikke å involvere IT direkte – IdS IAM sørger for at alt skjer korrekt og effektivt.
- **Fleksibel passordutsending:** IdS IAM kan automatisk lage et førstegangspassord eller påloggingskode for den nye brukeren og distribuere dette sikkert. Standardoppsettet er typisk at en **aktiveringslenke eller engangskode sendes til nærmeste leder**, slik at lederen kan overlevere sensitiv informasjon (som passord) personlig til den nyansatte på første arbeidsdag. For visse ansettelsestyper eller scenarioer kan man overstyre denne prosedyren: **passordet kan sendes direkte til medarbeideren via SMS på oppstartsdato** dersom det er mer hensiktsmessig (f.eks. ved remote onboarding). IdS IAM støtter tidsstyrt utsending, så meldingen kan planlegges til å gå ut akkurat når den trengs (f.eks. kl. 07:00 den dagen medarbeideren starter).
- **Håndtering av ekstra brukerkontoer:** Dersom den nye medarbeideren også blir ansvarlig for én eller flere **ekstra brukere eller systemkontoer** (f.eks. en driftsbruker eller systemadministrator

e.l.), kan IdS IAM automatisk sikre at påloggingsinformasjon for disse kontoene sendes til riktig ansvarshaver. I praksis betyr det at hvis en ansatt opprettes som eier/ansvarlig for en separat konto, vil systemet distribuere passord eller aktiveringslenke for denne kontoen til vedkommende (ikke til en felles innboks), slik at sikkerheten ivaretas og den ansatte har kontroll på alle sine ansvarskontoer.

- **Helautomatisk flyt med tilbakemeldinger:** Under hele prosessen holdes bestiller (og evt. andre involverte) informert gjennom automatiske varslinger. Når kontoen er klar og tilganger opprettet, får lederen beskjed. **Brukeropplevelsen fremstår som smidig og proaktiv**, der HR/leder kun trenger å initiere bestillingen – resten håndteres av systemet. Dette eliminerer mange manuelle oppfølgingspunkter, reduserer feil og sikrer at nye ansatte er produktive fra dag én.

6.3 Sluttføring av medarbeidere

Effektiv håndtering av **offboarding** er kritisk for sikkerhet og samsvar, og IdS IAM sørger for at ingenting faller mellom to stoler når en medarbeider slutter. Nedenfor beskrives hvordan løsningen støtter hele prosessen:

- **Planlagt sluttføring med karantene:** HR eller leder registrerer sluttdato for medarbeideren i IdS IAM så snart fratredelse er kjent.

  Sluttdatoen kan komme inn via HR import. Dersom sluttdatoen fra HR er siste arbeidsdag, vil denne bli satt umiddelbart til IdS IAM brukeren. Dersom sluttdatoen fra HR er siste dag med lønn, vil IdS IAM følge opp nærmeste leder på å få satt siste arbeidsdag på bruker. Det kan leder gjøre i samråd med medarbeideren. Siste dag med lønn blir satt som siste arbeidsdag i IdS IAM dersom leder ikke foretar seg noe innen et konfigurerbart antall dager før siste dag med lønn.

  Løsningen orkestrerer deretter sluttføringen tidsstyrt. På den ansattes siste arbeidsdag (sluttdato) vil IdS IAM automatisk deaktivere brukerkontoer i systemer og fjerne tilgang til tjenester flagget med umiddelbar fjerning. Umiddelbar fjerning er lurt å ha på automatiske tjenester som har kostnad eller høy risiko. Deretter iverksettes en definert **karantenetid** før endelig fjerning av all tilgang. Når fjerning av all tilgang er gjort, kan IdS IAM fjerne all tilgang i systemer som ikke administreres i IdS IAM. Dette kan brukes for en full opprydding i f.eks. Active Directory der bruker kan ha blitt lagt inn som medlem i grupper som ikke er registrert i IdS IAM. Etter nok en konfigurerbar karantenetid per system, slettes medarbeiderens brukere med opsjon per systemet. Karenstidene er nyttige fordi medarbeidere kan ombestemme seg om å slutte og fordi leder/HR kan ha satt feil sluttdato.

  For eksempel kan man konfigurere at en fratrådt konto i et system forblir deaktivert i 3 måneder før den slettes, eller at visse tilganger beholdes i inntil 365 dager for arkivformål før full fjerning.

  Slik **fjernes identitet og tilgang automatisk etter en kontrollert karanteneperiode**, i tråd med virksomhetens policy.

- **Varsling og oppgavefordeling:** IdS IAM lager en **sluttføringssak** knyttet til medarbeideren som slutter. Gjennom denne saken **varsles medarbeiderens leder og andre relevante parter**, og konkrete oppgaver tildeles til definerte roller for oppfølging. For eksempel vil lederen typisk få en oppgave om å samle inn utstyr eller overføre eventuelle porteføljer og ansvar den ansatte hadde. Tilsvarende kan IT-avdelingen eller fysisk sikkerhet få manuelle oppgaver om å fjerne tilganger til bygning (adgangskort). Sluttføringsoppgavene blir altså **fordelt ut i organisasjonen** der de hører

hjemme. Dermed sørger IdS IAM for at **alle nødvendige tiltak blir initiert og tilordnet noen**, slik at offboardingen ikke bare skjer teknisk, men også operasjonelt.

- **Oversikt og kontroll:** Ledere og administratorer har tilgang til **rapporter og oversikter over alle sluttføringsprosesser** – både åpne (pågående) og lukkede. I IdS IAM-portalen kan man enkelt se hvem som er i ferd med å slutte, hvilke tiltak som venter på utførelse, og hvilke saker som allerede er fullført. Dette gir ledelsen trygghet for at **ingen avslutninger blir glemt eller blir hengende**, noe som er avgjørende for både sikkerheten og for å oppfylle interne retningslinjer. Det komplette revisjonssporet viser i tillegg nøyaktig *hva* som ble fjernet *når*, og *hvem* som utførte oppgavene, slik at man i ettertid kan dokumentere at alle prosedyrer ble fulgt.
- **Hastesluttføring (øyeblikkelig sperring):** I ekstraordinære situasjoner der en ansatts tilganger må opphøre umiddelbart (for eksempel ved avskjed på grått papir eller sikkerhetsbrudd), har IdS IAM en egen **hastesluttføringsfunksjon**. Denne omgår den ordinære tidslinjen og iverksetter umiddelbar fjerning av tilganger. Med et klikk kan alle kontoer deaktiveres og tilgang sperres på tvers av samtlige systemer øyeblikkelig. Hastesluttføringen sørger for at virksomheten raskt kan nøytralisere sikkerhetsrisikoer, samtidig som det loggføres og senere kan inngå i den vanlige sluttføringsprosessen (f.eks. med oppgaver for etterarbeid som fortsatt må gjennomføres).

6.4 Sammenligning med Microsoft Entra ID

- **Grunnleggende JML-støtte i Entra ID:** Microsoft Entra ID (tidligere Azure AD) har enkelte innebygde funksjoner for identitetslivssyklus, men de er svært grunnleggende sammenlignet med IdS IAM. Entra ID kan for eksempel integreres med et HR-system for såkalt **HR-drevet provisjonering**, hvor nye brukerkontoer automatisk opprettes eller oppdateres basert på HR-data. Dette dekker det helt elementære – at en ny medarbeider får en konto i AD med riktige attributter. Microsoft har også nylig lansert **Lifecycle Workflows** som kan automatisere noen få rutineoppgaver i JML-syklusen (for eksempel å deaktivere kontoer ved sluttdato). Disse funksjonene forutsetter imidlertid dyre lisenser og må konfigureres av IT; de fokuserer primært på teknisk provisjonering og gir ikke noen veiviser eller forretningsprosess ut mot HR/leder.
- **Manglende livssyklusprosesser og saksflyt:** Entra ID mangler den helhetlige prosess-støtten som IdS IAM tilbyr for joiner/mover/leaver. Det finnes **ingen innebygd veiviser** eller selvbetjeningsportal der HR eller ledere kan registrere nyansettelser og endringer – vanligvis må dette løses via separate verktøy eller manuelle rutiner. Entra ID har heller **ingen saksbehandlings- eller oppgavesystem** knyttet til livssyklus-hendelser; for eksempel blir ikke en leder automatisk varslet gjennom Entra ID for å utføre oppgaver ved ansattes start eller slutt. I IdS IAM, derimot, blir hver hendelse fulgt av oppgaver og varslinger i systemet. Dessuten logger IdS alle tilgangsendringer med årsak (ny ansatt, rollebytte, osv.), mens Entra ID **mangler slik kontekstuell logging** – man kan i beste fall se *at* en endring skjedde, men ikke *hvorfor*.
- **Begrensninger i tilgangsbestilling og tilpasning:** En annen svakhet i Entra ID er manglende funksjonalitet for **tilgangsbestilling og tilpassede oppstartsoppsett**. Microsoft tilbyr riktignok Entitlement Management (Access Packages) for å gi brukere tilgang til grupper/applikasjoner via selvbetjening, men dette er ikke integrert med en JML-prosess slik IdS IAM sin veiviser er. I IdS IAM blir nye tjenester og roller automatisk tilgjengelige for riktig person basert på regler (f.eks. avdeling eller stilling), uten at administratorer manuelt må tildele grupper eller vedlikeholde dynamiske regler for hvert tilfelle. Entra ID alene krever ofte manuelt arbeid eller tilleggsscripting for å oppnå tilsvarende dynamikk, og gir ikke et samlet brukergrensesnitt hvor man kan bestille alt en ny ansatt trenger i én operasjon.

Oppsummering av Entra ID vs. IdS IAM: Kort oppsummert støtter Entra ID det mest nødvendige for å opprette og deaktivere kontoer, men **mangler mange av de livssyklus- og styringsfunksjonene** som IdS IAM leverer. For ledere og sikkerhetsansvarlige betyr dette mindre kontroll og innsikt. For eksempel har Entra ID ingen enkel måte å se en **historisk oversikt over tidligere ansatte** eller deres tilganger over tid – når en bruker slettes i Entra ID, forsvinner den fra den vanlige oversikten. IdS IAM, derimot, beholder historikk og gjør det mulig å rapportere på tidligere ansettelsesforhold og tilgangsendringer. Også fra et revisjonsperspektiv kommer Entra ID til kort: det finnes ingen ferdige rapporter eller dashbord for å følge opp pågående offboarding-oppgaver, lisensopprydding, permisjoner osv. Samlet sett må en organisasjon som kun bruker Entra ID, basere seg på manuelle prosesser og fragmenterte verktøy for å håndtere JML/RES-livssyklusen – noe som innebærer høyere risiko og merarbeid. Det vil heller ikke gi samsvar med de regulatoriske kravene i DORA og NIS2. IdentityStream IdS IAM er designet nettopp for å fylle disse hullene, ved å tilby en komplett, regelstyrt og dokumentert livssyklusprosess som sikrer at **ledelse, sikkerhetsansvarlige og IT-avdelingen har full kontroll** på alle identiteter gjennom hele ansettelsesforholdet med full revisjonshistorikk.

7 Godkjenningsløp (prosessmotor for godkjenning og saksgang)

IdS IAM tilbyr et fleksibelt og avansert **godkjenningsløp** for tilgangsstyring. Et godkjenningsløp er en konfigurert prosess som håndterer forespørsler om tilgang eller andre identitetsrelaterte tiltak gjennom definerte steg. Disse stegene kan være rene statusoverganger eller aktive godkjenninger, og de kan tilpasses i henhold til virksomhetens behov. Microsofts Entra ID Governance har på sin side bare en forenklet flyt for tilgangsforespørsler, uten mulighet for policy-styrt prosess med flere nivåer, parallelle godkjenninger eller skreddersøm – ofte ender man da med manuelle løp via IT og ujevn praksis. IdS IAM sin tilnærming fjerner disse begrensningene ved å tilby en komplett orkestrering av godkjenninger, regelverk og oppgaver. Nedenfor beskrives hvordan godkjenningsløpene fungerer, og hvordan de forankrer tilgangsbeslutninger i organisasjonen på en måte som overgår Entra ID Governance sin innebygde funksjonalitet.

7.1.1 Statussteg og godkjenningssteg

Et godkjenningsløp i IdS IAM er bygget opp av sekvensielle eller parallelle steg. **Statussteg** benyttes for å markere hendelser eller overganger i prosessen – for eksempel at en forespørsel er mottatt, under behandling, eller ferdigbehandlet. Disse stegene krever ingen godkjenning, men oppdaterer sakens status og kan utløse varsler eller automatiske aktiviteter før saken sendes videre til neste steg i prosessen. **Godkjenningssteg**, derimot, krever en aktiv beslutning fra en eller flere utpekte parter. I et godkjenningssteg sendes det ut en oppgave/forespørsel til godkjenner(e) om å vurdere og enten godkjenne eller avslå forespørselen. IdS IAM tillater konfigurasjon av flere slike godkjenningssteg i et løp, noe som betyr at man kan bygge flertrinns beslutningsprosesser (f.eks. første linjes godkjenning, deretter sikkerhetsgodkjenning, osv.) uten fast begrensning på antall steg.

En nøkkelfunksjon er at flere godkjenningssteg kan **kjøres parallelt**. Dette innebærer at ulike godkjenningsaksjoner kan utføres samtidig for å effektivisere prosessen. For eksempel kan en forespørsel om høy-privilegert tilgang konfigureres til å innhente godkjenning både fra nærmeste leder og fra systemeier parallelt. Begge mottar da godkjenningsoppgaven samtidig, og den samlede prosessen fullføres først når begge har tatt sin beslutning. Denne parallelliseringen bidrar til raskere beslutninger uten at man må vente på sekvensiell godkjenning. Det er også mulig å definere om parallelle godkjenninger skal være **uavhengige eller gjensidig avhengige** – for eksempel kan man kreve at *alle* parallelt utsendte godkjenningsoppgaver må godkjennes for at prosessen skal gå videre, eller man kan

akseptere at én av flere godkjennere godkjenner på vegne av en oppdragsgruppe. Slik fleksibilitet finnes ikke i Entra ID Entitlement Management, som kun støtter to sekvensielle godkjenningssteg uten parallelle løp.

7.1.2 Knytning til tilgangstildeling og bestillinger

Godkjenningsløpene i IdS IAM er tett integrert i hele tilgangsstyringsmodellen. De kan trigges av enhver hendelse som krever beslutning – f.eks. når en bruker ber om en ny tilgang via selvbetjening, ved tildeling av en rolle, når en bruker aktiverer sin selvbetjente tilgang (PAM) eller når en leder bestiller en tilgang for sin medarbeider. **Tilgangstildeling** kan derfor settes på hold i påvente av godkjenning, noe som sikrer at ingen uautoriserte tilganger effektueres uten nødvendige vedtak. Dette gjelder også *privilegert tilgang*-prosesser (inkl. PAP), slik at aktivering av høyere rettigheter kan kreve eksplisitt godkjenning fra forhåndsdefinerte ansvarlige. Systemet har f.eks. opsjon for godkjenning ved aktivering av selvbetjente administratortilganger (PAM); denne kan konfigureres differensiert – eksempelvis avslått for fast ansatte, men obligatorisk for eksterne konsulenter. Slik kan policyer håndheves i godkjenningsløpene.

Godkjenningsløpene er også knyttet opp mot **roller og tjenester** i IdS IAM-modellen. Hver *tjeneste* (applikasjon/system) eller *tilgangsnivå* kan ha definert en oppdragsgruppe eller eier som ansvarlig for godkjenninger. Dette betyr at dersom en bruker ber om en gitt tilgang, vil systemet automatisk vite hvem som skal godkjenne – det kan være en **rolle-eier**, en definert **systemeier** eller en **saksbehandlergruppe** (oppdragsgruppe) knyttet til den aktuelle ressursen. For eksempel: ved selvbetjent bestilling av en ny felles postkasse fyller brukeren ut et skjema med nødvendig info, og godkjenningen styres av et konfigurert godkjenningsløp – kanskje til en saksbehandler som vurderer behovet. Etter godkjenning opprettes så automatisk ressursen og tilganger tildeles i henhold til standarder, alt loggført i saken. Tilsvarende kan roller ha *rolle-eiere* som får godkjenne nye medlemmer i rollen før tilgangen effektueres.

En ekstra styrke ved IdS IAM er integrasjonen mot **support og manuelle rutiner**. Dersom en tilgang skal tildeles i et system som ikke er integrert automatisk, kan godkjenningsløpet inkludere et manuelt oppgavesteg: f.eks. at IT-support mottar en oppgave om å utføre tilgangen i systemet manuelt. Systemet sørger for at oppgaven rutes til riktig *oppdragsgruppe* og kan sende ut malbaserte e-poster med all nødvendig informasjon for å utføre endringen. Svar eller bekreftelse fra support kan registreres slik at arbeidsflyten fortsetter. Entra ID mangler slike muligheter for å inkludere manuelle aktiviteter i flyten – IdS IAM derimot kombinerer automatisering og menneskelig interaksjon sømløst i samme prosess.

7.1.3 Komplekse beslutningsflyter med betinget logikk

IdS IAM legger til rette for å bygge **komplekse beslutningsflyter** som speiler virksomhetens regler og unntak. Man kan involvere flere typer beslutningstakere i samme løp: **flere ledere**, eierroller og dedikerte oppdragsgrupper kan alle trekkes inn etter behov. For eksempel kan en tilgangsforespørsel først gå til brukerens nærmeste leder, og deretter automatisk videre til leder for divisjonen. Slike *flerledds-godkjenninger* sikrer at høyere risikobeslutninger går høyere opp i hierarkiet for godkjenning.

Eierroller (f.eks. applikasjonseiere, dataeiere) kan inngå i løpene slik at de godkjenner tilgang til “sine” systemer. Systemet utnytter konfigurasjonen av eierskap på ressursene, så disse stegene kommer automatisk inn der det er relevant. Alternativt kan man definere dedikerte **oppdragsgrupper** – en gruppe personer (avdeling, komité eller lignende) – som skal håndtere bestemte godkjenninger eller oppgaver. En oppdragsgruppe kan settes som godkjenner i et steg, enten med **en-til-mange** (førstemann til mølla kan godkjenne) eller **mange-til-mange** (flere må avgi godkjenning) oppsett, avhengig av kravet.

En særlig kraftig funksjon er muligheten for **betinget hopping** i flyten, altså at visse steg *skippes* eller *endres* basert på kriterier. IdS IAM bruker JSONPath-uttrykk for å definere slike betingelser på data fra skjema eller kontekst. Hvert steg kan ha en valgfri JSONPath-betingelse som evalueres mot

forespørselens data; dersom uttrykket evalueres til true, kan steget hoppes over eller en alternativ forgrening følges. For eksempel: om en bruker bestiller tilgang til en applikasjon og i skjemaet oppgir at vedkommende allerede har nødvendig lisens, kan et steg for lisensgodkjenning hoppes over automatisk. Eller som et annet eksempel, IdS IAM tillater at man **forbigår godkjenning for definerte sikre domener/partnere** – hvis en gjestebruker inviteres fra et forhåndsgodkjent domene, kan systemet registrere tilgangen uten ekstra godkjenning. Slik betinget logikk er helt konfigurérbar. JSONPath-bruken gjør det mulig å peke på ethvert felt i bestillingsskjemaet (eller andre data som f.eks. brukers type, avdeling, risikoklasse) for å styre flyten. Dette gir en enorm fleksibilitet til å modellere *"hvis X så gå til steg A, ellers hopp til steg B"*-scenarioer, alt innenfor det visuelle arbeidsflytoppsettet.

IdS IAM kan også inkludere **skjemabaserte steg** i selve flyten. Det vil si at et steg kan presentere et utfyllingsskjema til en ansvarlig person, slik at man henter inn supplerende informasjon som en del av beslutningsprosessen. For eksempel kan et godkjenningssteg for tilganger be systemeier spesifisere hvilken tilgangsprofil brukeren skal få (ved å velge i et skjema) før godkjenning gis, eller HR kan bli bedt om å fylle ut manglende opplysninger under en onboarding-prosess. Disse dataene kan deretter benyttes videre i godkjenningsprosessen. Entra ID's Entitlement Management har ingen tilsvarende mekanisme for å innhente ekstra data midt i flyten – IdS IAM's løsning sørger for at all nødvendig informasjon samles inn og vurderes før tilgangen tildeles.

7.1.4 Forankring i organisasjonens struktur

En av de største fordelene med IdS IAMs godkjenningsløp er at tilgangsbeslutninger **forankres i organisasjonens struktur**. Med det menes at beslutningene tas av de riktige personene i linjen eller i ansvarlige roller, og at prosessene automatisk reflekterer organisasjonskartet, delegasjoner og policyer.

Et sentralt element er integrasjonen med **lederhierarkiet**. IdS IAM har alltid et oppdatert hierarki av avdelinger og ledere tilgjengelig, og dette kan brukes direkte i godkjenningsløp. For eksempel kan tilgangsforespørsler på en tjeneste som standard rutes til brukerens nærmeste leder (hentet fra HR-organisasjonsdata). Men man kan konfigurere nivåstyring slik at bestemte typer forespørsler krever godkjenning på et høyere ledernivå. En *nivåstyrt* godkjenning kan fungere slik at: en mellomleder kan godkjenne vanlige tilganger for sine underordnede, men hvis tilgangen er klassifisert som høyrisiko kan den sendes inn i et helt annet godkjenningsløp. På den måten sikres det at beslutninger tas på riktig nivå i organisasjonen ut fra tilgangens sensitivitet eller kostnad. Dette prinsippet – at lederlinjen involveres proporsjonalt med risiko – oppfylles av IdS IAM's fleksible løp, mens Entra ID's standardflyt typisk kun involverer brukerens nærmeste leder (uten støtte for flernivå eskalering).

Videre forankres godkjenninger gjennom **roller og eierskap**. IdS IAM-modellen er bygget slik at hver tilgang (tilgangsnivå) kan knyttes til en *eierrolle* eller *systemeier*. Så når en tilgang bestilles, vet plattformen hvem i organisasjonen som "eier" denne tilgangen. Godkjenningsløpet kan automatisk sende en oppgave til denne rollen. Eksempelvis: tilgang til regnskapssystemet kan kreve godkjenning av økonomisjefen (som er definert som systemeier for regnskapstjenesten), uavhengig av hvem som bestiller. Dette forankrer beslutningen hos den som har det faglige ansvaret. Tilsvarende kan tilgang til sensitive fellesdata kreve godkjenning av en dataeier eller en person i en definert rolle for etterlevelse. IdS IAM's modulære modell med eierskap og oppdragsgrupper gjør det enkelt å fordele slike IAM-oppgaver ut i organisasjonen der de hører hjemme.

7.1.5 Sammenligning med Microsoft Entra ID (Entitlement Management)

Godkjenningsflyten i IdS IAM skiller seg markant fra – og overgår – godkjenningsflyten i Microsoft Entra ID's Entitlement Management. Tabellen under oppsummerer hovedforskjellene:

Funksjonalitet	IdS IAM	Entra ID Governance
Antall steg i flyt	Ubegrenset antall steg. Kan bygge komplekse sekvenser av status- og godkjenningssteg etter behov.	Maks 2 godkjenningssteg per forespørsel (to sekvensielle nivåer). Ingen dedikerte statussteg utover dette.
Parallelle godkjenninger	Støttet. Flere godkjenningsoppgaver kan utløses parallelt, og man kan kreve alle eller noen av dem fullført for å gå videre.	**Ikke støttet.** Godkjenninger håndteres sekvensielt (trinn 1 og så trinn 2).
Betinget logikk (skip/branch)	Støttet via JSONPath-regler på skjemadata og kontekst. Rett flyt kan velges basert på valgt tilgang. Flyten kan hoppe over steg eller endre forløp basert på verdier.	**Begrenset.** Ingen generell støtte for betinget hopping. Kun enkelte scenarioer som f.eks. å unnta godkjenning for interne brukere i visse tilfeller (hardkodet logikk for gjester vs interne).
Innhenting av ekstra data	Støttet. Skjemabaserte steg tillater å samle inn tilleggsinformasjon (f.eks. fra systemeier) underveis i flyten. Dataene kan brukes i videre beslutning og revisjon.	**Ikke støttet.** Godkjennere kan kun godkjenne/avslå; ingen mulighet til å fylle inn ekstra informasjon.
Integrasjon med organisasjonsstruktur	Full integrasjon. Automatisk oppslag av nærmeste leder, flernivå ledereskalering, involvering av rolle-/systemeiere og oppdragsgrupper basert på konfigurasjon. Godkjenning forankres i eksisterende struktur.	Begrenset. Kan typisk kun automatisk involvere nærmeste leder som første godkjenner. Ingen innebygd mekanisme for dynamisk valg av høyere leder eller eier basert på ressurs; krever manuell konfigurasjon av spesifikke godkjennere per access package.
Tilpassede sakstyper og oppgaver	Svært fleksibelt. Samme godkjenningsmotor brukes på tvers av ulike sakstyper (tilganger, onboarding, endringer mm.). Kan inkludere manuelle oppgaver til IT/support i flyten med sporing.	Smalt fokus. Kun beregnet på tilgangsforespørsler via access packages. Ingen støtte for HR-prosesser eller andre sakstyper. Ingen integrert oppgavehåndtering mot IT-support.
Livssyklus og sporing	Full sporbarhet på alle steg: hvem godkjente/avslo, når, og eventuelle kommentarer. Revisjonslogg knyttet til saken og til tilgangen. Kan vise komplett historikk for hele løpets levetid.	Grunnleggende sporbarhet (logg for godkjenning/avslag i access package-historikken), men ingen samlet saksvisning med alle statusendringer. Begrenset historikk per tilgang (fokuserer mest på aktive tildelinger).

Forklaring: Microsoft Entra ID Governance's Entitlement Management tilbyr kun en enkel to-trinns godkjenningsflyt for tilgangsforespørsler, rettet mot relativt enkle behov. IdS IAM på sin side leverer en

moden workflow-motor som er spesialtilpasset IAM-området. Dette inkluderer ubegrenset antall steg, parallelle løp og betinget logikk – noe som lar virksomheten modellere selv komplekse beslutningsprosesser uten å måtte ty til manuelle omveier. I tillegg er IdS IAM's løp sterkt **rolle- og kontekstbaserte**, ved at de automatisk trekker inn ledere, eiere eller grupper basert på hva slags tilgang eller sak det gjelder. Entra ID mangler denne tette koblingen mot organisasjonsmodellen og kan ikke på samme måte fordele ansvar ut i linjen.

Til syvende og sist sikrer IdS IAM's omfattende godkjenningsløp at riktige beslutningstagere er involvert til riktig tid, at alle betingelser og unntak håndteres konsistent, og at **policyer håndheves automatisk** i tråd med organisasjonens regler. Løsningen gir en revisjonsklar prosess med full oversikt over *hvem* som godkjente *hva* og *hvorfor*. For ledelsen og sikkerhetsansvarlige betyr dette forbedret kontroll, mindre risiko og bedre etterlevelse av regulatoriske krav – alt i en strømlinjeformet prosess som overgår det man oppnår med standardfunksjonaliteten i Microsoft Entra ID.

8 Tilgangsrevisjon i IdS IAM og sammenligning med Microsoft Entra Access Reviews

IdS IAM (Identity and Access Management) tilbyr et omfattende rammeverk for tilgangsrevisjon der flere interessentroller deltar i attestasjonsprosessen. Dette gjør at tilganger vurderes fra ulike perspektiver i organisasjonen for å sikre at hver bruker kun har nødvendige tilganger.

8.1 Flerdimensjonal tilgangsrevisjon i IdS IAM

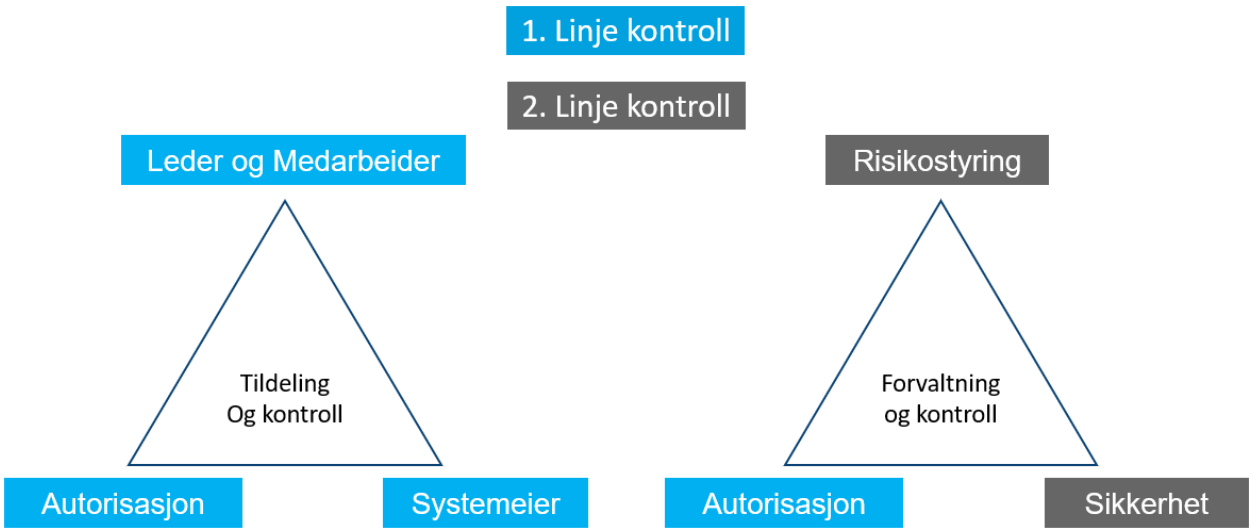
De viktigste revisjonstypene i IdS IAM inkluderer:

- **Leders revisjon:** Linjeledere får jevnlig i oppgave å gjennomgå sine ansattes tilganger. I en slik revisjon ser lederen over hver medarbeiders **roller**, eventuelle **ekstra tilganger** (tilganger utenom tildelte roller), oppdaterer status for **arbeidsforhold** (f.eks. om en medarbeider fortsatt er i sin stilling/prosjekt) og identifiserer **risikofylte kombinasjoner** av tilgang/rollemedlemsskap (SoD-konflikter). Hensikten er å sikre at ingen medarbeidere under deres ansvar har unødvendige eller uforenlige tilganger. Ledere kan attestere (godkjenne) eller tilbakekalle tilganger, roller, SoD-konflikter og arbeidsforhold direkte i denne prosessen, og de må signere en bekreftelse på at gjennomgangen er utført tilfredsstillende.
- **Systemeiers revisjon:** Ansvarlige systemeiere (applikasjons- eller tjenesteeiere) gjennomfører revisjon av tilgangene knyttet til sine systemer. Dette innebærer å verifisere bruken av **tilgangsnivåer i roller** og direkte **ekstra tilganger** for systemet. Systemeier sikrer at rettighetene som er inkludert i en rolle fortsatt er nødvendige og korrekt brukt, og at ingen brukere har høyere privilegier enn det som trengs på det aktuelle systemet. Denne gjennomgangen gir en spesialisert kontroll per applikasjon/tjeneste, der de som kjenner systemet best vurderer om tilgangene er riktige.
- **Rolleeiers revisjon:** Hver definert rolle i IdS IAM har typisk en rolleeier som jevnlig reviderer rollen. Rolleeiers revisjon setter søkelys på **rollemedlemmer** og de **tilgangsnivåer** rollen gir. Rolleeieren kontrollerer at de brukerne som er medlem av rollen, faktisk skal ha denne tilgangen (er autorisert ut fra sine oppgaver), og at innholdet i rollen (hvilke rettigheter den innebærer) fortsatt er gyldig og ikke medfører unødvendig høy tilgang. Dette bidrar til at roller forblir oppdatert og at ingen roller "glipper" og gir tilganger til feil personer.
- **Medarbeiders selvrevisjon:** IdS IAM støtter også at den enkelte **medarbeider selv** kan utføre periodisk revisjon av egne tilganger. Gjennom en selvrevisjon får ansatte oversikt over sine

tildelte roller og eventuelle ekstra tilganger, og kan bekrefte om de fortsatt har behov for dem. Dette øker bevisstheten hos hver ansatt rundt egne tilganger og gir en mulighet til å tilbakekalle tilgang de ikke lenger trenger. Selvrevisjon fungerer som et supplement til leder- og systemeierrevisjonene, ved at brukerne selv initierer første kontroll av sine tilganger før det eventuelt eskaleres til leder for bekreftelse.

8.2 Revisjon som del av 1. linje kontroll, risikostyring og sikkerhet

Figur 1: Forenklet modell for tilgangsstyring og kontroll i IdS IAM. Første linje (blå trekant) involverer linjeledere, systemeiere, rolleeiere og brukere selv i daglig kontroll av tilganger (autorisasjon), mens andre linje (grå trekant) utgjøres av virksomhetens overordnede risikostyring og sikkerhetsfunksjon.



Tilgangsrevisjonene i IdS IAM inngår som en sentral del av **1. linjes kontroll** i virksomhetens internkontrollmodell. Førstelinjen er der hvor risikoer oppstår og skal håndteres i det daglige – her representert ved ledere og eiere som har ansvar for brukere og systemer. Gjennom de beskrevne revisjonsprosessene ivaretar disse aktørene et kontinuerlig ansvar for **risikostyring**: Ledere sørger for at ansatte ikke akkumulerer farlige tilgangskombinasjoner eller unødvendige rettigheter, mens system- og rolleeiere sikrer at deres respektive komponenter er riktig sikret. Denne **desentraliserte kontrollen** på førstelinjen fanger opp avvik tidlig og reduserer sannsynligheten for at feilaktige tilganger forblir uoppdaget.

Samtidig legger IdS IAM til rette for at **2. linje** (typisk risiko- og sikkerhetsfunksjoner sentralt i organisasjonen) kan overvåke og støtte førstelinjens tilgangsrevisjoner. All aktivitet i revisjonsprosessene loggføres og dokumenteres. Når en leder eller eier signerer en revisjon, utgjør det et formelt bevis på kontrollutførelsen. Disse dokumenterte revisjonene kan benyttes av sikkerhetsavdelingen og etterlevelse/risk managers for å føre tilsyn med at første linje faktisk gjennomfører kontroller i henhold til retningslinjene. Kombinasjonen av IdS IAM sine flerdimensjonale revisjoner og formell signering/dokumentasjon gjør at virksomheten oppfyller både interne krav til adgangskontroll og eksterne revisjonskrav.

8.3 Sammenligning med Microsoft Entra Access Reviews

Microsoft Entra ID tilbyr sin egen tilgangsrevisjonsfunksjonalitet gjennom **Access Reviews**. Dette er en del av Entra Identity Governance og dekker mange av de grunnleggende behovene for

attestasjonsprosesser. Nedenfor sammenlignes IdS IAM sin tilnærming med funksjonaliteten i Entra Access Reviews, med fokus på typer revisjoner, arbeidsflyt, dokumentasjon og eventuelle begrensninger.

8.3.1 Revisjonstyper og deltakere i Entra ID

Entra Access Reviews lar organisasjoner gjennomgå tilganger til grupper, applikasjoner og Azure-roller på en strukturert måte. Løsningen støtter flere **revisjonstyper** lignende de i IdS, men de konfigureres noe annerledes. Man kan sette opp periodiske attesteringskampanjer for medlemskap i sikkerhetsgrupper eller Microsoft 365-grupper, tilgang til applikasjoner, samt tildelinger til privilegerte roller i Entra ID. For hver slik kampanje defineres **hvem som skal revidere** tilgangen: typiske valg er brukerens **leder**, gruppens **eier(e)** (for grupper/Teams), applikasjonens **eier** (hvis definert) eller andre **spesifiserte personer/roller**, samt muligheten for **selvrevisjon** der brukerne attesterer sine egne tilganger. Man kan involvere for eksempel "Managers of users" (lederne) som første fase, deretter gruppeeiere som neste, og eventuelt en separat revisorgruppe (f.eks. i IT eller sikkerhet) som siste fase. Med andre ord støtter Entra Access Reviews mange av de samme deltakerrollene som IdS IAM – fra linjeledere og ressurseiere til brukerne selv – om enn innenfor rammen av sine egne kampanjer.

8.3.2 Arbeidsflyt og rapportering

Arbeidsflyten i Entra Access Reviews er **fleksibel innen gitte rammer**, men mindre modulær enn i IdS IAM. Microsoft tillater opptil tre sekvensielle **stadier** i en access review-kampanje. Dette betyr at man kan sette opp flerstegs attestasjonsprosesser (f.eks. først selvrevisjon, deretter leders gjennomgang, og til slutt en sikkerhetsansvarlig) for å oppnå flerdobbelt kontroll som ligner IdS' multidimensjonale revisjon. Man kan konfigurere om senere stadier skal se tidligere stadiers beslutninger eller ikke, og man kan filtrere hvem som går videre til neste steg (f.eks. bare de som ikke svarte eller som ble godkjent av forrige instans). Dette gir relativt gode muligheter til å etterligne IdS IAM sin arbeidsflyt innen en enkelt Entra-kampanje. Likevel er det noen begrensninger – **maksimalt tre steg** kan være en begrensning for veldig komplekse attestasjonsløp, og alle steg er knyttet til den aktuelle ressursen som revideres. IdS IAM på sin side kan kjøre separate, dedikerte revisjoner per rolle, system og lederområde kontinuerlig, mens Entra typisk krever oppsett av flere parallelle kampanjer for å dekke tilsvarende bredde.

Når det gjelder **rapportering**, leverer Entra Access Reviews grunnleggende statistikker og eksportmuligheter (f.eks. oversikt over hvem som ble fjernet eller fortsatt har tilgang etter en review). Resultatene av hver kjøring kan logges og lastes ned, og Entra ID Governance inkluderer et dashboard for å se status på gjennomførte og pågående attesteringsjobber. Dette dekker de **essensielle behov** for oversikt, men detaljert rapportering er relativt enkel. For eksempel kan man se hvem som ikke responderte innen fristen, og tilganger kan automatisk fjernes for de som ble benektet eller ikke svarte, med påfølgende loggføring. IdS IAM derimot kan ofte tilby rikere rapporter fordi revisjonene er en del av et helhetlig etterlevelsesrammeverk der alle beslutninger (signerte attester) lagres og kan kombineres i rapporter pr bruker, leder eller system over tid.

8.3.3 1. linje kontroll og dokumentasjon

Entra Access Reviews er i utgangspunktet et verktøy for **attestering** og kontroll, men Microsofts løsning omtaler ikke eksplisitt konseptet "første linje" vs "andre linje" kontroll slik IdS IAM-modellen gjør. I praksis kan man selvfølgelig bruke Access Reviews til førstelinjekontroll ved å involvere linjeledere og ressursansvarlige som attestanter. Mange av de samme spørsmålene adresseres – f.eks. "Trenger denne brukeren fortsatt tilgang til ressurs X?" – og lederne kan pålegges å bekrefte dette jevnlig. Forskjellen ligger i hvordan prosessen **forankres og dokumenteres**. Entra ID vil registrere utfallet av en access review (hvem godkjente/avviste hvilke tilganger, og hvilke ble fjernet automatisk), og dette kan tjene som dokumentasjon for revisjonsformål. Likevel er denne dokumentasjonen ofte **grunnleggende** – typisk i form av loggfiler eller eksporterte lister over gjennomganger. Det finnes ingen innebygd funksjon

for at en leder "signerer" et samlet attestasjonsskjema slik tilfellet er i IdS IAM; signeringen er implisitt gjennom at de har fullført oppgaven i systemet.

IdS IAM legger større vekt på at første linje aktivt **eier risikoen** knyttet til tilganger, noe som understøttes av funksjonalitet som signaturer og flerdimensjonal kontroll. Dokumentasjonen i IdS blir dermed mer **revisjonsvennlig** – man kan fremvise signerte attestasjonsrapporter per leder eller systemeier som bevis for internkontroll. I Microsoft Entra må man i større grad samle bevis manuelt (f.eks. ta ut rapporter fra hver access review eller samle Entra ID logger) for å demonstrere at kontroll er utført. Med andre ord adresserer begge løsninger første linjes kontrollbehov, men IdS IAM's rammeverk er mer spesifikt designet for å passe inn i et formelt kontroll- og risikooppfølgingssystem.

8.3.4 Svakheter i Entra Access Reviews sammenlignet med IdS IAM

Selv om Microsoft Entra Access Reviews gir mye nyttig funksjonalitet, finnes det noen **svakheter eller mangler** når vi sammenligner med det modulære, rollebaserte revisjonsrammeverket i IdS IAM. En klar begrensning er fraværet av innebygde **SoD-kontroller (Segregation of Duties)** og risikokombinasjons-sjekker. Entra ID Governance mangler avanserte funksjoner for å automatisk fange opp og varsle om risikofylte kombinasjoner av rettigheter under revisjon. I IdS IAM blir slike konflikter fremhevet for ledere (og potensielt blokkert), mens i Entra må man manuelt identifisere om en bruker har uheldige kombinasjoner av tilganger på tvers av systemer.

En annen forskjell er at Entra Access Reviews i stor grad er **ressursorientert** (man attesterer tilgang til en bestemt gruppe, app eller rolle om gangen), mens IdS IAM muliggjør **brukerorientert** revisjon (f.eks. at en leder attesterer alle tilganger for sine medarbeidere samlet). For å oppnå lignende brukerfokus i Entra må man koordinere flere access reviews for alle relevante ressurser eller benytte Entitlement Management for å gruppere tilganger, noe som øker kompleksiteten.

Oppsummert er Microsoft Entra Access Reviews et godt verktøy for basis tilgangsattestering i en Microsoft-sentrisk verden, men det kan **ikke uten videre erstatte** et fullverdig IAM-rammeverk som IdS IAM for virksomheter underlagt strenge krav som DORA og NIS2. IdS IAM's modulære og rollebaserte revisjonsfunksjoner gir dypere kontroll, større fleksibilitet og bedre integrasjon med virksomhetens risikostyring, mens Entra Access Reviews primært fokuserer på å løse kjernebehovene på en standardisert måte.

9 Fra sentralt til distribuert ansvar – styring med modulær modell

Tradisjonelt har tilganger blitt administrert sentralt av IT. IdentityStream legger til rette for en overgang fra sentral kontroll til **distribuert ansvar** i tilgangsstyringen med sin IAM. Den modulære, rollebaserte modellen i IdS IAM operasjonaliserer prinsippet *«del og styr»* ved å definere regler og ansvar granulært på systemlandskap og brukermasse. Dette betyr at virksomheten kan fordele oppgaver og myndighet utover i organisasjonen uten å miste oversikt eller sikkerhet. Resultatet er at linjeledere, systemeiere og andre domeneeksperter kan ta aktiv styring over tilganger – innenfor rammene av sentrale policyer og med full sporbarhet.

Eierskap på flere nivåer: IdS IAM introduserer tydelig **eierskap og ansvar på rolle-, tjeneste- og tilgangsnivå**. For hver rolle, applikasjon (tjeneste) og hvert tilgangsnivå kan man konfigurere hvem som "eier" den og hvem som skal behandle tilhørende forespørsler. Dette inkluderer å tilordne eiere for roller, systemeiere for applikasjoner/tjenester, samt dedikerte *oppdragsgrupper* (saksbehandlergrupper) som kan håndtere bestemte tilgangsforespørsler eller oppgaver. Slik får hver tilgang et definert ansvarspunkt distribuert ut i organisasjonen, noe som gir klar forvaltning og korte beslutningsveier. Eierskap og

oppdragsgrupper for slike IAM-oppgaver (godkjenning, revisjon, utførelse) er en sentral del av IdS-modellen, og gir nødvendig kontekst for å kunne fordele oppgaver ut til de rette personene.

Delegasjon i linjen: Den modulære modellen gjør det mulig å delegere myndighet videre nedover i organisasjonen. En avdelingsleder kan for eksempel utpeke *tilgangsansvarlige* for sine avdelinger, eller personlige stedfortredere, som kan bidra på lederens IAM-oppgaver på tvers av alle lederens avdelinger. Via slike stedfortredere og lokale tilgangsansvarlige sikrer IdS IAM at det alltid finnes noen på passende nivå som kan godkjenne tilgangsforespørsler, følge opp revisjoner eller utføre administrative tiltak – selv om leder er opptatt med annet. Dette avlaster IT og fordeler ansvaret til dem som har best kjennskap til teamets behov. I IdS IAM får stedfortredere de nødvendige rettighetene automatisk når de opprettes, og kan hjelpe eller erstatte leder for avdelingen i gitte perioder. Dermed bygges det inn en robust kontinuitet i tilgangsstyringen, uten at man er avhengig av sentrale administratorer i alle situasjoner.

Fordeling av IAM-oppgaver ut i organisasjonen: IdS IAM muliggjør at oppgaver innen tilgangsstyring håndteres av de rette funksjonene i linjen, i stedet for å kanaliseres gjennom IT-avdelingen. Dette omfatter flere typer oppgaver:

- **Godkjenninger nærmest kilden:** Når en bruker ber om en bestemt tilgang, vet IdS IAM automatisk hvem som skal godkjenne. Basert på konfigurasjonen rutes forespørselen til riktig ansvarlig – for eksempel nærmeste leder, definert systemeier eller en utpekt saksbehandlergruppe for den aktuelle ressursen. Løsningen støtter til og med flerleddede godkjenningsløp: en forespørsel kan gå til brukerens leder først, deretter automatisk eskalere til neste ledernivå, eller involvere en bestemt komité for høyrisiko-tilganger. Slike flertrinns prosesser sikrer at riktige beslutningstakere involveres på hvert steg, uten unødig forsinkelse. **Oppdragsgrupper** gjør det dessuten enkelt å tilordne godkjenninger eller manuelle oppgaver til en gruppe personer med riktig kompetanse, fremfor til enkeltindivider – dette gir fleksibilitet og avlaster nøkkelpersoner. All tilordning skjer automatisk basert på hvem som er satt som ansvarlig for den aktuelle rollen, tjenesten eller tilgangen, noe som eliminerer manuell triage av saker.
- **Periodisk tilgangsrevisjon i flere dimensjoner:** IdS IAM har et omfattende rammeverk for tilgangsrevisjon der flere interessentroller deltar samtidig. Linjeledere får jevnlig i oppgave å gjennomgå tilgangene til sine ansatte for å bekrefte at hver medarbeider kun har nødvendige tilganger. Samtidig kjører *systemeiers revisjoner* for at hver tjeneste sin eier kontrollerer bruken av sine tilgangsnivåer, og *rolleeieres revisjoner* for å sikre at roller inneholder riktige tilganger og at kun autoriserte personer er medlemmer av dem. IdS IAM kan dermed kjøre dedikerte attestasjonsrunder per lederområde, per system og per rolle, kontinuerlig og parallelt. Denne flerdimensjonale tilnærmingen sørger for at tilgangsrettigheter evalueres fra ulike perspektiver i organisasjonen, noe som øker sjansen for å fange opp avvik. Til og med den enkelte medarbeider kan involveres gjennom selvrevisjon av egne tilganger, som et ekstra kontrollnivå. Hele prosessen er støttet av elektroniske revisjonsrapporter – ansvarlig signerer digitalt på at gjennomgang er utført tilfredsstillende, og rapportene arkiveres som bevis på internkontroll. Dette sikrer at ingenting “faller mellom stolene”: hver tilgang blir periodisk sett på av noen som kjenner konteksten, uten at IT-avdelingen må initiere og gjennomføre alle revisjoner manuelt.
- **Manuell tilgangsutførelse uten IT-flaskehalser:** I mange organisasjoner er det tilganger som må legges til eller fjernes manuelt (for eksempel i systemer uten automatisert integrasjon). IdS IAM håndterer også dette på en distribuert måte. Hvis en tilgangsforespørsel ikke kan utføres helautomatisk, oppretter systemet en oppgave til riktig ansvarlig enhet for manuell utførelse. Dette kan være en oppdragsgruppe i IT-support, systemeieren selv eller en annen definert ansvarlig. Oppgaven inneholder all nødvendig informasjon (f.eks. hvilken bruker og hvilken

tilgang som skal endres), og IdS kan sende ut varsel (malbasert e-post) til de som skal utføre oppgaven. Når oppgaven er utført, registrerer de ansvarlige dette i IdS IAM, slik at arbeidsflyten fortsetter og blir fullført. Hele hendelsesforløpet loggføres og knyttes til saken og brukeren det gjelder, noe som gir full sporbarhet. **Poenget er at selv manuelle prosesser kan delegeres ut til de riktige teamene** i stedet for å hope seg opp hos et sentralt IT-team. IdS IAM har støtte for å inkludere manuelle aktiviteter direkte i arbeidsflyten, mens Microsoft Entra ID ikke har slike muligheter til å integrere manuelle oppgaver i sine forespørselsprosesser. Dermed slipper man at IT må involveres i hver eneste tilgangsendring – i stedet kan fageiere utføre sine deler av prosessen innenfor kontrollerte rammer.

Forankring i organisasjonsstrukturen: En nøkkelfaktor som muliggjør all denne delegeringen, er at IdS IAM er tett integrert med virksomhetens egen organisasjonsstruktur. Løsningen forstår selskapsstrukturen (selskaper, avdelinger, team) og **benytter lederhierarkiet aktivt** i tilgangsstyringen. For eksempel kan man aktivere periodisk lederrevisjon for alle ansatte i en avdeling – IdS IAM vil da automatisk tildele revisjonsoppgaver til riktig avdelingsleder med gitte mellomrom, uten manuell oppfølging. Tilsvarende knyttes applikasjonstilganger til definerte systemeiere i IdS; når noen bestiller en ny tilgang, vet systemet umiddelbart hvem i organisasjonen som "eier" den tilgangen og skal godkjenne. Godkjenningsprosesser og kontrolltiltak *forankres dermed i eksisterende struktur*, noe som sikrer at avgjørelser tas av dem som har formelt ansvar og innsikt. Microsoft Entra ID mangler denne tette koblingen til organisasjonsmodellen og kan **typisk bare automatisk involvere nærmeste leder** som godkjenner – den har ingen mekanisme for å dynamisk finne en høyere leder eller eier basert på ressursen, uten å legge opp spesialkonfigurasjoner per tilgangstilfelle. IdS IAM sin modell, derimot, støtter flernivå-eskalering og involvering av rolle- og systemeiere og utpekte grupper helt automatisk som del av arbeidsflyten. Dette **operasjonaliserer prinsippet "del og styr"** i praksis – ansvar og kontrollpunkter er delt ut i linjen, men alltid innenfor styrte rammer. Sikkerhet, revisjon og policyhåndhevelse blir ikke svekket av at flere deltar; tvert imot, de blir styrket ved at flere ledd bekrefter og dokumenterer at alt er i orden.

Kontrasten mot Microsoft Entra ID: Microsoft Entra ID tilbyr grunnleggende IAM-funksjonalitet, men **mangler mange av de desentraliseringsmulighetene IdS IAM har**. Entra ID fungerer primært som et sentralisert admin-verktøy: Oppgaver som revisjonskampanjer (Access Reviews) eller tilgangsbevilgning via Entitlement Management krever typisk oppsett og oppfølging fra en administrator eller global rolle. Man kan riktignok involvere en brukers leder i en godkjenning eller review i Entra, men plattformen har ingen like rik **fordeling av ansvarsnivåer**. For eksempel kan Entra ID per i dag ikke automatisk tilordne en systemeier som godkjenner basert på hvilken applikasjon det gjelder – dette måtte i så fall konfigureres manuelt for hvert enkelt access package eller gruppe. Løsningen støtter heller ikke flere parallelløp eller skreddersydde eskaleringsregler ut fra risiko; man står stort sett igjen med lineære, forhåndsdefinerte flyter (ofte maks to steg) og begrenset fleksibilitet. I praksis betyr det at **Entra ID krever mer sentral administrasjon og oppfølging** for å oppnå noe av det samme som IdS IAM gjør automatisk. Der IdS IAM kontinuerlig kjører separate revisjoner for hver avdeling, hvert system og hver rolle, må man i Entra gjerne sette opp flere parallelle "kampanjer" for å dekke tilsvarende bredde i kontrollen. Og mens IdS IAM kan fremvise signerte attestasjonsrapporter per leder eller systemeier som dokumentasjon på utført internkontroll, må man i Entra ID i stor grad samle bevis manuelt (for eksempel eksportere rapporter fra hver enkelt access review og sammenstille) for revisjonsformål. Kort sagt: **Entra ID mangler det organisatoriske innplasseringen av ansvar** som IdS IAM tilbyr, og kan derfor ikke fordele ansvar ut i linjen på samme måte. Dette gjør at mye av ansvaret forblir hos IT eller sentrale administratorer dersom man kun bruker Entra ID, med tilhørende risiko for flaskehalser og mindre lokalt eierskap til tilgangene.

Strategiske gevinster av distribuert styring: Evnen til å desentralisere tilgangsstyringen med IdS IAM gir betydelige fordeler for virksomheten. For det første øker **kontrollen og etterlevelsen**: Riktige beslutningstagere er involvert til riktig tid, alle endringer blir attestert av ansvarlige parter, og alt logges detaljert. Dette betyr mindre risiko for at uautoriserte tilganger vedvarer, og enklere demonstrasjon av internkontroll overfor revisorer og regulatoriske myndigheter. Samtidig oppnår man **bedre skalerbarhet og effektivitet**. Når linjeledere og systemeiere kan bestille, godkjenne og revidere tilganger for sine ansvarsområder, **frigjøres IT-avdelingen fra å være involvert i alle ledd**. IT kan fokusere på å tilrettelegge rammeverket og håndtere unntak, mens den daglige tilgangsstyringen går sin gang ute i organisasjonen. Dette gjør at modellen skalerer naturlig med virksomheten – om selskapet dobler antall ansatte eller systemer, fordeles også arbeidsmengden på flere ansvarlige i stedet for å hope seg opp sentralt. Viktigst av alt skjer alt dette **uten å svekke sikkerheten eller policyhåndhevelsen**: IdS IAM sørger for at policyer, rollemodell og godkjenningsregler gjelder likt overalt, uavhengig av hvem som utfører oppgaven. For toppledelsen og sikkerhetsansvarlige betyr dette en bedre balanse mellom kontroll og delegering: man får økt styring og etterlevelse uten å miste smidigheten i organisasjonen. Kort oppsummert leverer IdS IAM **"del og styr"**-prinsippet i praksis – virksomheten får det beste av to verdener: distribuert ansvar og sentralt overvåket sikkerhet. Dette er en **styringsmodell som overgår det man oppnår med standardfunksjonaliteten i Microsoft Entra ID** og gir et solid fundament for videre vekst og digital kontroll.

10 Helhetlig Ansvarsfunksjon i IdS IAM vs. Microsoft Entra ID

IdS IAM tilbyr en helhetlig **ansvarsfunksjon** som gir full oversikt og kontroll over hvem som har hvilket ansvar i organisasjonen. Løsningen samler **alle typer ansvar** en person kan ha – fra eierskap av systemtilganger og roller, til godkjenningsroller og stedfortrederfunksjoner – i ett grensesnitt. Dette gjør det mulig å enkelt se:

- **Individuell oversikt:** *Mitt ansvar*– hvilke ansvarsområder den påloggede brukeren selv har.
- **Lederoversikt:** *Dine medarbeideres ansvar* – hva en leder sine ansatte har av ansvar.
- **Totaloversikt:** *Ansvar (alle)* – ansvar for alle brukere og ressurser på tvers av hele leietakeren.
- **Kryss-organisatorisk:** *Brukeres ansvar* – ansvar brukere har på tvers av eventuelle flere tilkoblede leietakere.
- **Uregelmessigheter:** *Ansvarsuregelmessigheter* – systemidentifiserte avvik, f.eks. ansvar som ligger hos personer uten gyldig organisasjonstilknytning (sluttet, permisjon, etc.).

Dette gir en **aggregert visning** av ansvar på tvers av systemer og roller, med mulighet for filtrering på ansvarskategori og drill-down til den enkelte bruker for detaljert innsyn. Dersom en bruker flere av modulene på IdentityStream ServiceManager plattformen, får en også fordelen av aggregert visning på tvers av domener. Ansvarsobjektene er kategorisert etter type, eksempelvis: eierskap av tilgangsnivåer eller roller, medlem av oppdragsgrupper, dedikerte godkjennere i prosesser, ansvarlig bruker for tjenestekontoer eller gjestebrukere, stedfortreder for kollega, definert tilgangsansvarlig for en avdeling, systemeier/driftsansvarlig for en tjeneste, prosesseier, m.m. (flere av disse har også underkategorier, f.eks. primær og sekundær eier på tjeneste). Denne inndelingen gir klarhet i *hvilken type ansvar* den enkelte har, og legger til rette for målrettet oppfølging per kategori.

Ansvarsadministrasjon: IdS IAM lar utpekte brukere administrere og omfordele ansvar på en kontrollert måte. Et dedikert tilgangsnivå på IdS ServiceManager tjenesten kalt *"Ansvarsoverfører",* gir utvalgte brukere (f.eks. HR-personell eller andre uten fulle admin-rettigheter) mulighet til å igangsette overføring

av ansvar for hvem som helst i virksomheten. Også ledere (for sine underordnede), brukeren selv (for eget ansvar) eller administratorer kan initiere en ansvarsoverføring. Dette er en to-trinns prosess: Først velges hvilke ansvarsoppgaver som skal overføres fra person A til person B, og deretter involveres *eier av den aktuelle ressursen* for godkjenning. For eksempel må systemeier godkjenne at ansvar for "Tjeneste X" flyttes til en ny person – slik sikres det at riktig fagansvarlig har siste ordet. Dersom initiativtaker selv er eier av ressursen det gjelder, blir overføringen automatisk godkjent. (En administrator kan også overstyre eller godkjenne hvis nødvendig.) Denne innebygde arbeidsflyten gir kontrollert **ansvarsoverføring** ved f.eks. avdelingsbytter eller fratredelser, og forhindrer at kritiske eierskap blir stående igjen på personer som slutter.

Varsling og oppfølging: IdS IAM's ansvarsfunksjon inkluderer et varslingssystem som proaktivt alarmerer når ansvar må gjennomgås eller overtas av andre. Eksempler: Når en medarbeider får tildelt nytt ansvar via en overføring, får vedkommende (og dennes leder) et varsel. Ledere varsles også hvis en ansatt med ansvar slutter, går ut i permisjon eller flytter til en ny avdeling. Slik blir ledere minnet på å vurdere om ansvaret skal omfordeles. Disse varslene fungerer som *påminnelser* for å unngå at ansvarsområder faller mellom to stoler når organisasjonen endres.

Avvikshåndtering: Et annet viktig element er oversikten over *ansvarsuregelmessigheter*. IdS IAM identifiserer automatisk en rekke situasjoner som krever oppmerksomhet, for eksempel: tomme oppdragsgrupper (ingen medlemmer), saker som er tildelt personer som ikke lenger har gyldig rolle, tjenester eller roller uten utpekt eier, brukere i permisjon eller sluttede som fortsatt står oppført med ansvar, osv. Slike avvik flagges i systemet, og man kan ta affære ved å tildele ny ansvarshaver eller fjerne/avvikle det aktuelle ansvarsområdet. Denne kontinuerlige overvåkingen sikrer at ansvar alltid er plassert hos noen med gyldig tilknytning, noe som reduserer risiko (ingen "herreløse" kritiske oppgaver) og gjør det enklere å opprettholde etterlevelse.

10.1 Tilsvarende funksjonalitet i Microsoft Entra ID

Microsoft Entra ID tilbyr i utgangspunktet **ikke en samlet "ansvarsmodul"** tilsvarende den IdS IAM har. Entra ID fokuserer på identitets- og tilgangsstyring med funksjoner som gruppe- og applikasjonseierskap, men mangler en helhetlig oversikt over alle ansvarsroller pr. bruker. Enkelte elementer kan likevel sammenlignes:

- **Eierskap av objekter:** I Entra ID kan brukere oppføres som eiere av grupper, applikasjoner og enkelte andre ressurser. For eksempel har hver Microsoft 365-gruppe én eller flere eiere som kan administrere gruppen. Det anbefales alltid å ha minst to eiere per gruppe for å unngå at den blir "eierløs" hvis en person slutter. Entra ID har til og med en mekanisme som sender varsler hvis en gruppe står uten eier, slik at medlemmer kan påta seg rollen. Likevel finnes det ingen sentral visning som lister *alle* typer ansvar en person har (man må se gruppeeiere i én del av portalen, app-eiere i en annen, osv.).
- **Overføring av ansvar ved fratredelse:** Microsoft Entra ID har ikke en dedikert funksjon for "ansvarsoverføring" med arbeidsflyt og godkjenning. Når en ansatt med eierskap slutter, må administratorer eller ledere manuelt sikre at f.eks. grupper, tjenester eller prosesser fortsatt har en ansvarlig. Microsofts beste praksis er å identifisere om brukeren er eneste eier av noen grupper før man fjerner vedkommende, og i så fall tilordne en ny eier. Dette er imidlertid en manuell oppgave. Entra ID har nylig introdusert **Lifecycle Workflows** som kan automatisere visse offboarding-tiltak (f.eks. fjerne en bruker fra grupper, deaktivere konto, osv.), men å *fordele* eierskap eller godkjennerroller til andre personer skjer ikke automatisk – det må konfigureres via skripter eller administrativ oppfølging. Det finnes ingen rolle tilsvarende *"Ansvarsoverfører"* i Entra

ID; typisk vil slike endringer kreve en global administrator eller tilsvarende høye rettigheter, eller at man forhåndsdefinerer flere eiere per ressurs for å tåle frafall.

- **Godkjenner- og stedfortrederroller:** I IdS IAM kan man eksplisitt definere godkjennere (f.eks. rolle-eier, systemeier eller oppdragsgruppe) som systemet automatisk vet skal involveres ved ulike forespørsler. Entra ID sin nærmeste parallell er **Entitlement Management** (tilgangspakker) hvor man kan sette opp godkjenningsflyt for tilgangsforespørsler. I slike tilfeller kan en forespørsel om tilgang sendes til en definert godkjenner (f.eks. gruppeeier). Men Entra ID mangler en generell oversikt over alle godkjenningsansvar – dette håndteres ad-hoc per tilgangspakke eller app. Når det gjelder stedfortredere, har ikke Entra ID noen standard funksjon for å utpeke en midlertidig erstatter for en ansatt (f.eks. ved ferie). Man kan oppnå lignende effekt ved å gi en annen person de nødvendige rolletildelingene midlertidig, men dette må gjøres manuelt og er ikke en innebygd, sporbart "stedfortreder" felt slik IdS IAM tilbyr.
- **Historikk og uregelmessigheter:** Entra ID lagrer **ikke historikk** om en brukers tilganger eller roller på en måte som er enkelt søkbar når brukeren er slettet. For eksempel, dersom en ansatt slettes i Entra ID, forsvinner vedkommende også fra de fleste oversikter, noe som gjør det vanskelig å ettertid se hva slags tilganger eller eierroller vedkommende hadde. IdS IAM beholder derimot historikken og kan vise hvem som hadde ansvar for hva, til hvilken tid. Videre finnes det i Entra ID ingen direkte parallell til IdS IAM sin "ansvarsuregelmessigheter"-modul. Entra ID tilbyr **Access Reviews** for jevnlig gjennomgang av tilganger (f.eks. kan ledere attestere om sine ansatte fortsatt skal ha visse gruppemedlemskap eller roller), og dette bidrar til å fange opp noen av de samme problemstillingene (som utdatert tilgang eller privilegier). Men Access Reviews er et mer generelt attestasjonsverktøy og dekker ikke alle typer ansvar (for eksempel vil den ikke automatisk oppdage at en bestemt applikasjon mangler en eier – slike ting må administratorer fange opp via separate rapporter). For grupper finnes det riktignok rapporter eller policy for "orphaned groups" i Microsoft 365 som nevnt, men igjen – dette er fragmenterte funksjoner og ikke en samlet, kategorioverskridende avviksoversikt slik IdS IAM leverer.

Oppsummert: Microsoft Entra ID har grunnleggende mekanismer for å tildele eiere til ressurser og for å gjennomføre periodiske tilgangsrevisjoner, men det mangler den helhetlige **ansvarsforvaltningen** som IdS IAM har. Det finnes ikke et enkelt dashboard der ledere kan se "hvilket ansvar hviler på mine ansatte" eller der en administrator kan filtrere ut alle systemer uten eier, etc.

10.2 Strategiske forretningsgevinster

Den omfattende ansvarsfunksjonaliteten i IdS IAM gir betydelige forretningsmessige fordeler:

- **Redusert operasjonell risiko:** Med klare eiere for alle systemer, roller og tilganger unngår man situasjoner der ingen føler ansvar. For eksempel forhindres "herreløse" grupper, kontoer eller applikasjoner som ellers kan utgjøre en sikkerhetsrisiko eller skape driftshindringer. IdS IAM sine mekanismer for å oppdage og rette opp manglende ansvarlige, sikrer kontinuerlig oppfølging og færre sikkerhetshull.
- **Effektiv håndtering av endringer:** Ved ansattes avgang eller interne omrokkeringer kan ansvar raskt og smidig overføres til nye personer ved hjelp av den innebygde to-trinns prosessen. Dette minsker sjansen for at viktige oppgaver faller bort i overgangsperioder. Automatiserte påminnelser til ledere (f.eks. når ansatte med ansvar slutter) gjør at man tidlig tar aksjon, noe som beskytter forretningen mot overraskelser. Sammenlignet med en ren Entra ID-tilnærming (hvor mye må følges opp manuelt), sparer dette tid og sikrer at *ingenting blir glemt* i en offboarding-prosess.

- **Bedre etterlevelse og revisjonsspor:** Det å kunne dokumentere *hvem som hadde ansvar for hva til enhver tid* er verdifullt for internkontroll og regulatorisk etterlevelse. IdS IAM loggfører alle endringer i ansvar, inkludert godkjenninger ved overføring, noe som gir et komplett revisjonsspor. Ledelsen og revisorer får innsikt i historikken – selv historiske data om tidligere ansatte beholdes for rapportering og revisjonsformål. Dette overgår Entra ID, der mye historikk går tapt ved sletting eller må gjenfinnes via logganalyse.
- **Økt ansvarliggjøring og tydelighet:** Når ansatte (og deres ledere) enkelt kan se hvilke ansvarsområder de er tilskrevet, øker bevisstheten rundt disse rollene. Det skaper en kultur der eierskap til systemer og prosesser er tydelig plassert. Dette fører igjen til raskere beslutninger og mer ansvarlig adferd – f.eks. en systemeier vet at det er deres plikt å godkjenne tilgangsforespørsler for "sitt" system, og kan følges opp på det. Slike klare ansvarsforhold er vanskeligere å oppnå med Entra IDs mer fragmenterte syn, der ansvar ofte implisitt ligger hos IT-avdelingen eller forsvinner i mengden.
- **Avlasting av IT og bedre delegasjon:** IdS IAM's modell legger til rette for at linjeledere og andre ikke-IT-ressurser kan ta aktiv del i identitetsstyringen. Ved å delegere ansvarsadministrasjon (gjennom roller som ansvarsoverførere, tilgangsansvarlige i avdelingene, etc.), fordeles arbeidet på flere hender. IT-avdelingen slipper å være flaskehals for hver lille justering av eierskap, og kan fokusere på overvåkning og støtte. Dette gir en mer skalerbar forvaltning av tilganger. Microsoft Entra ID alene tillater noe delegasjon via administrative roller og selvbetjening, men IdS IAM sin finmaskede ansvarsfordeling er designet for å *operasjonalisere* dette i stor skala på en trygg måte.

Kort oppsummert bidrar IdS IAM sin helhetlige ansvarsfunksjon til **bedre styring, sikrere drift og høyere effektivitet**. Når man sammenligner med standard Entra ID-funksjonalitet, blir det tydelig at en slik modul gir virksomheten et sterkere grep om "hvem som gjør hva" i det digitale økosystemet. Dette minimerer risiko og maksimerer kontinuitet – en strategisk gevinst for enhver organisasjon som tar identitetsforvaltning og sikkerhet på alvor.

11 Lisens- og kostnadsstyring

Effektiv lisenshåndtering og kontroll på IT-kostnader er essensielt for både IT-avdelingen og virksomhetens økonomiansvarlige. IdentityStream IdS IAM tilbyr en omfattende løsning for lisensstyring, som ikke bare forhindrer overforbruk av lisenser, men også gir innsikt i kostnadsbildet. Nedenfor gjennomgås hvordan IdS IAM håndterer lisenser og kostnader, og hvordan dette skiller seg fra Microsoft Entra ID.

11.1 Lisenshåndtering i IdS IAM

IdS IAM holder oversikt over antall tilgjengelige lisenser per **tjeneste** og per **tilgangsnivå** (f.eks. ulike lisensnivåer som *Basic* vs. *Premium* for en applikasjon). For hver tjeneste kan man konfigurere ett av tre håndteringsnivåer for lisensforbruk:

- **0 – Ingen håndtering:** Systemet begrenser ikke noe; lisensforbruk blir ikke overvåket utover ren telling.
- **1 – Varsle, men tillat overforbruk:** Systemet sender umiddelbart et varsel til systemeier og oppdragsgruppe når siste lisens blir brukt.

  Dersom tjenesten går over lisensgrensen oppretter IdS IAM en oppgave knyttet til den aktuelle

tjenesten for å følge opp anskaffelse av flere lisenser. På denne måten ivaretar systemet autorisert overforbruk ved å sikre at administratorer blir gjort oppmerksom på lisensoverskridelser uten å blokkere brukerens tilgang.

- **2 – Hindre overforbruk:** Systemet håndhever lisensgrensen strikt. Hvis en ny tilgang ville overskride tilgjengelig antall lisenser, vil IdS IAM automatisk blokkere tildelingen. Brukerens tilgangsforespørsel settes da i status **"Venter på lisens"**, og systemet oppdaterer diskusjonsloggen/kommentarfeltet på forespørselen med informasjon om at lisens mangler. Ellers gjelder de samme varslingene og oppgavehåndtering som i opsjon 1.

Denne flernivå-modellen gjør at virksomheter kan velge om de vil ha en myk tilnærming (kun varsling) eller en streng tilnærming (blokkering) til lisensstyring. Uansett nivå loggføres alltid lisensstatus, slik at man i etterkant kan se historikk på eventuelle forsøk på overforbruk og tiltak som er gjort.

11.2 Automatisk tilgangsnivå ved lisensmangel

En unik funksjon i IdS IAM er håndtering av **lisensoverløp**, altså tilfeller der primært ønsket lisensnivå ikke er tilgjengelig. Systemet kan da automatisk tildele et alternativt tilgangsnivå til brukeren dersom hovednivået er tomt for ledige lisenser. Dette fungerer som en *fallback* til et annet kostnadsnivå, f.eks. mer eller mindre omfattende lisensnivå for samme tjeneste. For eksempel, hvis en bruker ber om **Full** tilgang til et system, men det ikke finnes ledige **Full**-lisenser, kan IdS IAM i stedet tilby **Begrenset** tilgang (forutsatt at det er konfigurert som alternativ). Administratorer kan definere flere alternative nivåer i prioritert rekkefølge. På den måten unngår man at brukere står helt uten tilgang dersom topplisensen er oppbrukt – de får i stedet en begrenset tilgang som midlertidig løsning. Dette skjer automatisk og transparent, uten at administrator må gripe inn manuelt i hver enkelt sak. Fallback-mekanismen sikrer også at kostnadene optimaliseres ved at dyrere lisenser kun tildeles når de faktisk er tilgjengelige og nødvendige.

11.3 Visninger og innsikt i lisensbruk

IdS IAM gir rike **rapporter og dashbord** for å overvåke lisensbruken i organisasjonen. Administratorer kan inspisere hver tjeneste og se hvor mange brukere som har tilgang opp mot hvor mange lisenser som er kjøpt for både tjenesten og hvert tilgangsnivå. Disse oversiktene gjør det enkelt å identifisere tjenester der man nærmer seg (eller har overskredet) lisensgrensen. Det finnes blant annet et filter for **"Vis kun overforbruk av lisenser"**, som lar deg liste ut utelukkende de tjenestene/tilgangsnivåene hvor antall tildelte brukere overstiger lisensantallet – slik kan man raskt sette søkelys på avvik som krever oppfølging.

For hver rad i lisensoversikten (typisk en kombinasjon av tjeneste og lisensnivå) kan man dykke ned i detaljene. IdS IAM lar deg se **hvilke brukere** som har den aktuelle tilgangen, hvordan de har fått den (om det er via en rolle eller direkte tildelt ekstra tilgang), og eventuelt hvilke **roller** som inkluderer denne tilgangen. Dette gir full sporbarhet på hvem som "bruker opp" lisensene. I tillegg kan systemet identifisere **avvik** – for eksempel enkeltmedarbeidere som har uforholdsmessig høy lisenskostnad. Slike avvik vises tydelig i grensesnittet, og man kan følge lenker direkte fra rapporten for å utføre tiltak, for eksempel for å bestille fjerning av en unødvendig eller dyr lisens. Denne typen innsikt gjør det enklere å rydde opp i kostnadsdrivere og sikre at lisenser fordeles gunstig.

11.4 Kostnadsmodell for IT-tilganger

En sentral del av IdS IAM er en integrert **kostnadsmodell** som knytter økonomi opp mot tilganger. For hver tjeneste og hvert tilgangsnivå kan man registrere en pris (typisk en årlig kostnad per lisens). Når en ansatt får tildelt en tilgang, vet dermed systemet hvor mye denne tilgangen koster virksomheten. IdS IAM

summerer automatisk kostnaden per bruker ved å legge sammen prisen for alle den ansattes tilganger. Det samme gjøres på høyere nivåer: man får beregnet total **IT-kostnad per avdeling**, og helt opp til et aggregert beløp for hele organisasjonen. Denne funksjonaliteten muliggjør oversikt i **sanntid** over IT-kostnader knyttet til identiteter og tilganger.

Kostnadsdataene utnyttes i flere deler av løsningen. Blant annet vises de i **organisasjonskartet**, der ledere kan se årlig IT-kostnad for sin avdeling og hver medarbeider, med mulighet til å klikke seg ned i detaljer. (Se kapittelet om organisasjonskart for mer om hvordan IdS IAM visualiserer IT-kostnader i organisasjonsstrukturen.) Tilsvarende kan man i brukeroversikter se den totale lisenskostnaden per ansatt, og man har egne visninger som lister **distinkte tilganger med kostnad** – nyttig for å identifisere spesielt kostbare systemtilganger. Kostnadsmodellen støtter også gruppering av kostnader, slik at man kan tilrettelegge for **internfakturering** eller fordeling av IT-kostnader per kostnadssted. For eksempel kan man gruppere tjenester etter forretningsområde og generere rapporter for hvor mye hver avdeling skal belastes for sine ansattes lisenser.

Denne sammenstillingen av tilgang og pris gir virksomheten en faktabasert forståelse av IT-kostnadene. Ledelsen får direkte innsikt i hvilke tjenester som utgjør de største kostnadspostene, og kan enklere iverksette kostnadsoptimalisering. **Ubenyttede eller underutnyttede lisenser synliggjøres** tydelig, slik at de kan omfordeles eller termineres.

11.5 Sammenligning med Microsoft Entra ID

Microsoft Entra ID har svært begrenset innebygget funksjonalitet for lisensstyring sammenlignet med IdS IAM. Entra ID kan håndtere lisenstildeling på et grunnleggende nivå – administratorer kan tildele og fjerne lisenser for ulike skytjenester – men det finnes ingen finmasket kontroll slik IdS IAM tilbyr. Spesielt utmerker flere forskjeller seg:

- **Ingen blokkering ved lisensmangel:** Entra ID opererer i praksis med to tilnærminger: enten ingen sporing av lisensforbruk (manuell kontroll), eller at systemet registrerer at man har gått tom for lisenser, men likevel lar tildelingen skje (dvs. “varsle, men tillate”). Dersom man overskrider antall tilgjengelige lisenser i Entra/M365, blir brukeren markert som uten gyldig lisens i administrasjonsportalen, og administrator må i etterkant kjøpe flere lisenser eller frigjøre eksisterende. Det gis kanskje et varsel eller en indikasjon i portalen, men Entra ID stanser ikke automatisk nye tilganger selv om lisenskvoten er oppbrukt – systemet tillater overforbruk inntil administrator rydder opp. For eksempel har organisasjoner opplevd at gruppebasert lisensiering i Entra ID lot dem **overforbruke** noen lisenser uten å stanse nye brukere, hvor eneste indikasjon var en melding om at “X brukere trenger gyldige lisenser”. Noen automatisk e-postvarsel til ansvarlige uteblir også ofte i slike tilfeller, noe som gjør det lett å overse at man er over lisensgrensen. Entra ID mangler altså et nivå tilsvarende IdS IAMs “hindre overforbruk” som blokkerer tilgang ved lisensmangel.
- **Ingen støtte for lisensnivåer med fallback:** I Entra ID finnes det ikke noe konsept hvor systemet bytter til en alternativ lisensplan automatisk dersom primærplanen er tom. Hver lisens (f.eks. en Office 365 E3) behandles separat, og man har ikke mulighet til å konfigurere prioritert rekkefølge av flere lisensnivåer innen samme tjeneste. Dette betyr at dersom en ønsket lisens ikke er tilgjengelig, må administrator enten manuelt tildele en annen lisens eller brukeren får rett og slett ikke den aktuelle funksjonaliteten – det finnes ingen innebygget automatisert “degradering” eller oppgradering slik IdS IAM tilbyr.
- **Ingen kobling til økonomi eller kostnadsberegning:** Entra ID har ingen funksjonalitet for å legge inn lisenspriser eller beregne kostnad per bruker/avdeling basert på tildelte lisenser.

Microsoft 365-administrasjonsportalen gir kun oversikter over hvilke lisenser hver bruker har, men **ikke hva dette koster** virksomheten direkte. Økonomisk rapportering må gjøres ved siden av, typisk ved å eksportere lisenstabeller til Excel eller ved å bruke PowerShell/Graph API for å hente data og koble dem mot prisinformasjon manuelt. Det finnes PowerShell-skript og community-løsninger som kan lage kostnadsrapporter, men dette er ikke en del av standardfunksjonaliteten. For eksempel har Microsoft MVP-er laget skript som trekker ut lisensdata og lar en administrator legge inn pris per SKU for å generere rapporter med årlige kostnader per bruker og avdeling. Dette illustrerer at utenfor-boksen-løsninger må til for å oppnå noe IdS IAM har innebygget. Entra ID selv tilbyr **ingen rapportering** som viser lisenskostnader fordelt på organisasjonen (verken per avdeling, team eller bruker) i sine konsoller.

- **Manglende organisatorisk kontekst:** Fordi Entra ID ikke har kostnadsdata koblet til brukere, finnes det heller ingen visning som i IdS IAM hvor ledere kan gå inn og se IT-kostnad for sin avdeling eller team. Rapportering på lisenser i Entra er primært en teknisk oversikt for IT-administratorer (antall lisenser kjøpt vs. brukt totalt). Det er først når man eksporterer data til eksterne verktøy at man kan lage økonomiske fordelingsrapporter, og selv da krever det at man manuelt vedlikeholder informasjon om kostnadssted per bruker for å si hvilken avdeling en lisens skal belastes. Kort sagt mangler Entra ID den organisasjonsrapporteringen på lisenskost som IdS IAM har bygget inn.

Oppsummert: IdS IAM gir et langt rikere sett med verktøy for lisensstyring og kostnadskontroll enn det Microsoft Entra ID gjør. For ledere, sikkerhetsansvarlige og økonomiansvarlige betyr dette bedre kontroll på både etterlevelse og budsjett. Man unngår overraskelser knyttet til overforbruk fordi systemet kan stoppe uautoriserte tildelinger og foreslå rimeligere alternativer. Samtidig får man full oversikt over hvor IT-kostnadene oppstår og hvem som bruker dyre lisenser, alt innlemmet i virksomhetens organisasjonsstruktur og roller. Dette gjør det enklere å ta faktabaserte beslutninger, enten det er å kjøpe flere lisenser, reforhandle avtaler, eller omfordele kostnader internt for rettferdig budsjettallokering. IdS IAM sin helhetlige tilnærming til lisens- og kostnadsstyring kan dermed føre til både **reduserte kostnader og bedre etterlevelse**, i motsetning til Entra ID hvor mye av dette arbeidet må gjøres manuelt og uten støtte av verktøyene.

12 Risikofylte tilgangskombinasjoner (SoD) og risikotall

Her introduserer vi hvorfor “Risikofylte tilgangskombinasjoner (SoD) og risikotall” er kritisk for internkontroll – og hvordan IdS IAM operasjonaliserer dette i praksis.

I flere virksomheter har reelle innsiderangrep skjedd uten medvirkning fra andre. Fellesnevneren er at én medarbeider hadde tilstrekkelig brede tilganger til å utføre flere nøkkeloperasjoner som burde vært skilt av en SoD-regel.

Et konkret, anonymisert eksempel:

- Medarbeider A opprettet en “manuell kreditt” (operasjon X) og godkjente deretter samme transaksjon i regnskapet (operasjon Y). Begge operasjoner var tilgjengelige via ulike roller. Manglende SoD-regel gjorde at avviket ikke ble stoppet i bestilling eller oppdaget i tide.

For å forebygge slike situasjoner må virksomheten både definere konfliktregler (SoD) og kvantifisere risiko. IdS IAM muliggjør dette ved å gi risikotall til tjenester, tilgangsnivåer og roller, og ved å beregne en samlet risikoscore per person. Disse risikotallene er også et nyttig grunnlag i medarbeidersamtaler: de

kan brukes til å forklare hvorfor en medarbeider er "særlig betrodd", hvilke kompenserende kontroller som gjelder, og hvilke tiltak som kan redusere eksponeringen uten å hindre oppgaveløsning.

Her beskriver vi hvordan risikotall settes og summeres, hvordan SoD-definisjoner etableres, og hvordan overstyring og revisjon spores i IdS IAM.

12.1 Nåværende funksjonalitet

Risikotall på tjenester, tilgangsnivåer og roller: I IdentityStream IdS IAM kan alle tilgangsobjekter få et risikotall. Hver *tjeneste* (system/applikasjon) kan tildeles et risikonivå basert på hvor kritisk systemet er. Tilsvarende kan hvert *tilgangsnivå* (en konkret rettighet i et system) få et risikotall ut fra hvor sensitiv eller omfattende tilgangen er. Også *roller* – som er samlinger av tilgangsnivåer – kan ha et risikotall for å uttrykke den samlede risikoen rollen medfører. Disse risikoverdiene settes typisk av sikkerhetsansvarlige ut fra vurdering av konsekvensen dersom uvedkommende får den aktuelle tilgangen eller en på innsiden bruker tilgangen feil eller bevisst til egen vinning. Verdiene kan for eksempel reflektere om en tilgang gir mulighet til å utføre transaksjoner, lese sensitiv informasjon eller administrere systemer.

Summering per bruker: IdS IAM beregner en samlet *risikoscore per bruker* ved å summere risikotallene for alle tjenester, tilgangsnivåer og roller brukeren har. Summen gir et helhetsbilde av *brukerens risikoprofil* – altså hvor mye potensiell risiko vedkommende sine samlede tilganger utgjør for virksomheten. En person med mange høyrisiko-tilganger vil få en høyere samlet risikoscore enn en med bare lavrisikotilgang. Dette gjør det enkelt å identifisere enkeltbrukere som skiller seg ut med uforholdsmessig høy risiko.

Visning av risikopoeng i løsningen: IdS IAM presenterer risikoinformasjon tydelig flere steder i grensesnittet. I *organisasjonskartet* kan man slå på en visning som viser **årlig IT-kostnad og risiko** per avdeling og per medarbeider. Hver avdeling og ansatt får da opp sin aggregerte risikoscore ved siden av seg i organisasjonsstrukturen. Man kan klikke på disse verdiene for å se detaljer om *hva som bygger opp risikoen*, for eksempel hvilke tjenester og roller som ligger bak. Også i *brukeroversikter* og rapporter kan risikoscoren per person vises som en egen kolonne, slik at man kan sortere og filtrere brukere basert på risiko. Det finnes dessuten en egen **"Kalkulert risiko"**-visning der man kan fordype seg i en enkeltpersons risikoberegning. Her ser man hvilke konkrete tilganger og roller som bidrar til personens totale risikotall, noe som gir innsikt i *hvilke risikofaktorer* en bestemt bruker består av. Samlet gjør disse funksjonene det mulig for ledere og systemeiere å følge med på risikobildet i sine enheter, og for revisorer å få oversikt på tvers av hele organisasjonen.

Risikofylte tilgangskombinasjoner (SoD): IdS IAM har innebygd støtte for å definere *"Separation of Duties"*-regler, kalt risikofylte tilgangskombinasjoner (SoD). Dette innebærer at man kan definere to sett med tilganger som **ikke skal kunne innehas av samme bruker samtidig**. Når man oppretter en SoD-regel i IdS, angir man en **venstre side** og en **høyre side** – hver side består av ett eller flere tilgangsnivåer, tjenester eller roller. For eksempel kan venstre side være en rolle eller tilgang knyttet til *"Tilsagn"* (innvilgelse av lån), mens høyre side er en tilgang til *"Diskontering"* (bokføring av samme lån). Poenget er at ingen bruker skal ha begge deler samtidig, da det utgjør en uakseptabel risiko (f.eks. mulighet for å både initiere og godkjenne en sensitiv transaksjon).

- **Definisjon av SoD-regel:** Administrator definerer en tittel/beskrivelse for kombinasjonen og plukker hvilke tilganger som inngår på venstre og høyre side. Både enkelttilgangsnivåer, hele tjenester eller hele roller kan inkluderes. Man kan legge til flere elementer på hver side. Det er støtte for komplekse kombinasjoner – for eksempel at en *kombinasjon av to tilganger på venstre side* ikke skal kunne kombineres med en tredje tilgang på høyre side. Løsningen støtter altså mange-til-mange konflikter. SoD-regelen kan aktiveres eller deaktiveres etter behov.

- **Overstyring og saksbehandling:** Ofte vil det være behov for unntak – dvs. tilfeller der en medarbeider likevel må ha to konfliktfylte tilganger samtidig (f.eks. midlertidig i en liten organisasjon i forbindelse med ferieavvikling). IdS IAM har derfor funksjonalitet for *overstyring* av SoD-regler. Når man konfigurerer en risikofylt tilgangskombinasjon, kan man angi om overstyring er tillatt og om det *kreves* overstyring. Hvis en konflikt krever overstyring, håndteres dette via saksbehandling: IdS IAM oppdager at en bestilling eller eksisterende tilgang utløser en SoD-konflikt, og oppretter da en *forespørsel* som må godkjennes av en definert oppdragsgruppe eller ansvarlig part før tilgangen gis. Denne oppdragsgruppen for overstyring settes i selve SoD-definisjonen. Eksempel: En konflikt mellom tilgang A og B er markert som krever overstyring; dersom en bruker som allerede har A blir tildelt B, vil systemet opprette en sak som må godkjennes av f.eks. sikkerhetsansvarlig før tilgang B faktisk aktiveres. Godkjenningen dokumenterer *hvem som godkjente unntaket og hvorfor*, og unntaket loggføres.
- **Revisjonsspor og eksport:** IdS IAM logger alle forekomster av risikofylte tilgangskombinasjoner. I et eget *revisjonspanel* kan man se en oversikt over alle SoD-regler og hvorvidt de brytes, samt alle godkjente overstyringer (hvem som har fått unntak). Dette gir revisor full oversikt over hvilke brukere som sitter med risikofylte tilganger og på hvilket grunnlag det er godkjent. Løsningen tilbyr også eksport av disse dataene til Excel slik at man kan dokumentere SoD-etterlevelse og avvik for internrevisjon eller tilsynsmyndigheter. Revisjonsoversikten viser per SoD-regel, hvilke brukere som utløser konflikten og hvorfor, samt hvem som eventuelt har godkjent overstyring og tidspunkter.
- **Innsyn for revisor, leder og systemeier:** Tilgang til risikovurderingene er administrert i IdS IAM som tilgangsnivåer på IdS ServiceManager tjenesten. *Revisor* har innsyn i alle definerte risikofylt kombinasjoner og hvem som evt. bryter dem. Revisor kan administrere selve SoD-reglene (opprette, endre, deaktivere) og se alle overstyringer. *Ledere* i organisasjonen vil bli varslet og ha innsyn dersom ansatte i deres egen avdeling har en konfliktfylt kombinasjon – dette inngår også i ledernes periodiske tilgangsrevisjoner. En avdelingsleder kan dermed følge opp om det virkelig er nødvendig at en medarbeider har begge tilgangene, eller om en av dem skal fjernes.

Sammenligning med Entra ID: Microsoft Entra ID har ingen fullverdige funksjoner for risikovurdering slik IdS IAM tilbyr. Det finnes for eksempel ikke noe konsept for å tildele risikotall til tilganger eller å beregne en samlet risikopoengsum per person, så ledere kan ikke se et risikobilde per bruker slik de kan i IdS IAM. Entra ID har riktignok nylig fått noe grunnleggende støtte for **Separation of Duties (SoD)** gjennom Identity Governance-funksjonaliteten. Man kan nå konfigurere at en tilgangspakke er inkompatibel med en annen tilgangspakke eller med medlemskap i en bestemt sikkerhetsgruppe. Det innebærer at hvis en bruker allerede har tilgang *A* (eller tilhører den definerte gruppen), blir vedkommende automatisk forhindret fra å be om tilgang *B*. Dette bidrar til å unngå visse konfliktfylte tilgangskombinasjoner, men Entra ID mangler fortsatt de mer helhetlige SoD-mekanismene IdS IAM har. For eksempel finnes ingen mekanismer for overstyring med godkjenningsspor eller revisjonsvennlig logging av slike konfliktregler. IdS IAM har derimot hele denne funksjonaliteten integrert med saksbehandling og full sporbarhet, noe Entra ID ikke tilbyr.

12.2 Veikart: Planlagte utvidelser

IdS planlegger å utvide risikomodellen med *fem distinkte risikokategorier* som hver bidrar til en persons totale risikoprofil. De fem kategoriene som kommer, er:

1. **Transaksjonsrisiko:** Risiko knyttet til en brukers mulighet for å gjennomføre kritiske transaksjoner. Tilganger som gir rettighet til å initiere eller autorisere finansielle transaksjoner,

pengeoverføringer eller lignende vil typisk falle i denne kategorien. Jo større økonomiske verdier eller forpliktelser en bruker kan påvirke direkte, desto høyere transaksjonsrisiko.

2. **Informasjonsrisiko:** Risiko knyttet til tilganger på sensitiv informasjon. Dette reflekterer konsekvensene hvis konfidensiell informasjon kommer på avveie. Tilganger til personopplysninger, kundedata, helseopplysninger eller andre høygradert sensitive data bidrar til informasjonsrisiko. En ansatt med bred lesetilgang til interne dokumenter og databaser vil ha høy informasjonsrisiko.
3. **Administratorrisiko:** Risiko forbundet med administrativ eller privilegert tilgang. Dette inkluderer systemadministratorer, brukere med global admin-rolle, eller andre som kan endre sikkerhetsinnstillinger, opprette brukere eller tildele tilganger til andre. Slike "keys to the kingdom"-tilganger medfører stor risiko fordi de kan misbrukes til å omgå sikkerhetskontroller eller forårsake omfattende skade på systemer.
4. **Risikofylt tilgangskombinasjon:** Risiko som oppstår ved *kombinasjon* av tilganger som bryter SoD-regler. Selv om hver enkelt tilgang isolert sett kanskje ikke er kritisk, kan det å inneha visse tilganger samtidig utgjøre en stor fare. Denne kategorien fanger opp nettopp det – f.eks. hvis en person har både en tilgang som initierer utbetalinger og en som godkjenner utbetalinger. Systemet vil gi utslag på risikofylt kombinasjonsrisiko når en bruker innehar en definert konfliktkombinasjon.
5. **Instrueringsrisiko:** Risiko knyttet til muligheten for å instruere eller bestille handlinger som andre effektuerer. Det kan være å få gjennomført transaksjoner eller oppnå informasjonstilgang gjennom å instruere ansatte med tilganger. En kan også ha instrueringsmakt overfor to medarbeidere som til sammen utgjør en risikofylt tilgangskombinasjon.

Alle disse fem kategoriene vil for hver person *summeres* til en samlet risikoscore, samtidig som man kan se fordelingen på kategorinivå. Risiko per person blir altså mer detaljert: man får både totalsummen og innsikt i hvilke *typer* risiko som utgjør summen. I organisasjonskartet og rapporter vil man kunne få frem både total risiko og de underliggende kategoriverdiene per medarbeider. Dette gir mulighet for mer målrettet oppfølging – f.eks. kan man filtrere ut de med høy informasjonsrisiko spesielt, eller de med høy transaksjonsrisiko, alt etter fokus.

Maksimalverdier per kategori: I den nye modellen blir ikke bare summen viktig, men også *høyeste enkeltkategori* for en person. For eksempel vil en medarbeider som scorer moderat totalt sett, men har en spesielt høy administratorrisiko, kunne fremstå som et særskilt fokuspunkt. Løsningen vil derfor tydeliggjøre maksverdien per kategori for hver person. Dette kan presenteres grafisk (for eksempel ved at den aktuelle risikokategorien markeres spesielt dersom den overstiger visse terskler) eller i rapporter der man ser topp-risikoen for hver ansatt. Hensikten er å raskt identifisere om en person har et enkelt risikoområde som er kritisk høyt, selv om totalen kanskje drukner i gjennomsnittet.

Tilgang til risikoinformasjon: Innsynsmodellen utvides tilsvarende for de nye kategoriene. Revisorer vil ha full tilgang til alle kategorier for alle personer i organisasjonen, slik at de kan gjennomføre helhetlige risikovurderinger og etterlevelseskontroller. Ledere vil kunne se risikoprofilen for sine egne ansatte, fordelt på kategorier – på den måten kan en leder for eksempel oppdage at en av sine ansatte har høy transaksjonsrisiko og vurdere om dette er nødvendig eller bør reduseres. Systemeiere vil kunne se risikobildet for brukere av sine systemer: I praksis betyr det at når de gjør systemeierrevisjon, kan de i IdS IAM se hvilke risikoverdier (f.eks. informasjonsrisiko eller transaksjonsrisiko) som er knyttet til tilgangene på *deres* system. Dette gir systemeieren kontekst om hvor kritisk deres systemtilganger er i den større sammenheng.

Risikoberegning per person i stedet for per brukeridentitet: En viktig planlagt endring er at risiko skal knyttes til *personen*, ikke bare til én bruker-ID. I mange organisasjoner forekommer det at én fysisk person har flere brukerkontoer (f.eks. en ordinær konto og en adminkonto, eller kontoer i forskjellige domener). IdS IAM vil samkjøre risikovurderingen slik at hvis én person er ansvarlig for flere brukere/kontoer, så vil risiko fra alle disse samlet tilordnes personen. Dette gir et mer korrekt bilde – man ser *personens totale risiko* uavhengig av hvor mange påloggingsidentiteter vedkommende har. Det forhindrer at en person slipper under radaren bare fordi risikoen er fordelt på to kontoer. I praksis vil løsningen knytte brukeridentiteter til et personalia-register slik at all tilgang kan aggregeres pr. individ.

Samlet sett vil disse utvidelsene gi en langt rikere og mer finmasket oversikt over identitetsrisiko i virksomheten. IdS IAM utvikler seg fra å ha én dimensjon av risiko til å håndtere flere samtidige risikodimensjoner, noe som gir bedre beslutningsgrunnlag for både linjeledelse, systemeiere og revisjon. Dette gjør det mulig å målrette tiltak mot spesifikke risikoområder (for eksempel redusere administratorrettigheter eller forbedre SoD-etterlevelse) og oppfylle skjerpede krav til tilgangsstyring og internkontroll på en enda bedre måte.

13 IdS IAM vs. Microsoft Entra PIM/PAM

Både IdS IAM og Entra ID adresserer **PIM/PAM-funksjonalitet** (Privileged Identity/Access Management) – altså kontroll over høyrisiko identitet og tilgang. Strategisk sett har IdS IAM en bredere tilnærming til identitetsstyring, mens Entra PIM er en innebygd skytjeneste for å beskytte Microsoft-roller og -ressurser. Nedenfor sammenlignes funksjoner i IdS IAM opp mot tilsvarende i Entra PIM. Fokus er på viktige egenskaper som selvbetjent tilgang, tidsbegrenset tilgang, konfigurasjonsmuligheter, godkjenningsprosesser, rollestyring, tidslås og revisjon.

13.1 Selvbetjent tilgang og JIT-aktivering

En grunnleggende forskjell mellom IdS IAM og Entra PIM ligger i hvordan privilegerte roller tildeles og aktiveres:

- **IdS IAM – Aktiv vs. Selvbetjent tildeling:** I IdS IAM kan roller og tilganger gis som enten *aktive* eller *selvbetjente*. En **aktiv tildeling** betyr at brukeren får rollen umiddelbart og permanent (tilgang gjelder kontinuerlig, med mindre den fjernes manuelt). Derimot innebærer en **selvbetjent tildeling** at brukeren **må selv aktivere** ressursen ved behov før rettighetene trer i kraft. Ressursen ligger "på vent" inntil brukeren utløser den via selvbetjeningsportalen. Dette tilsvarer et *just-in-time*-prinsipp der ansatte kun bruker høyere privilegier når det trengs.
- **Microsoft Entra PIM – Permanent vs. Berettiget:** Entra PIM har en tilsvarende todeling. En **aktiv (permanent)** rolletildeling gir kontinuerlig tilgang, mens en **berettiget (eligible)** tildeling betyr at brukeren kun kan utøve rollen ved å **aktivere den on-demand**. I praksis vil en PIM-berettiget bruker logge inn i Azure/Entra PIM-portalen og "elevere" seg selv til rollen når oppgaver krever det. Tilgangen er altså ikke alltid aktiv, noe som reduserer unødvendige privilegier i hverdagen.

For sluttbrukeren betyr dette at IdS IAM og Entra PIM begge støtter selvbetjent, midlertidig **aktivering av admin-roller** ved behov – et viktig sikkerhetsprinsipp (just-in-time tilgang). Begge løsninger inkluderer å oppgi begrunnelse og passere sikkerhetskrav som MFA før aktivering. Begge løsninger støtter også godkjenning av aktivering.

IdS IAM integrerer denne funksjonen i sin brukerportal (f.eks. via menyvalget *"Selvbetjent tilgangsstyring"* i grensesnittet). Ansatte kan se hvilke roller og tilganger de **har tilgang til å aktivere**, og aktivere dem

med et par klikk. I Entra PIM skjer det samme gjennom Azure-portalen eller Microsoft MyAccess-portalen, der brukeren ser sine *berettigede* roller og kan aktivere dem etter behov. Begge løsninger oppnår formålet om å **minimere stående (konstant) privilegier** i organisasjonen, men IdS IAM gir denne opplevelsen i en helhetlig selvbetjeningsløsning som kan være mer tilpasset virksomhetens interne systemer.

13.2 PIM/PAM-konfigurasjon i IdS IAM – og hva som (ikke) finnes i Entra ID

IdS IAM har en modulær konfigurasjonsmodell der du setter PIM/PAM policy på **rolle og tjeneste** – med mulighet for å **overstyre** på **tilgangsnivå**. I tillegg kan regler styres etter **ansettelsestype** (fast, innleid, konsulent osv.). Entra ID (PIM) mangler begrepene *tjeneste* og *ansettelsestype* som førsteklasses nivåer; konfigurasjon gjøres primært per **rolle** (ev. per ressurs), med færre forretningsnære muligheter.

13.2.1 Nivåene i IdS IAM

- **Tjeneste-nivå:** Felles standarder for en tjeneste, med overstyring videre ned til individuelle tilgangsnivåer.
- **Tilgangsnivå (overstyring fra tjeneste):** Finjuster per konkret tilgang (kan være strengere eller mildere enn tjenesten).
- **Rolle:** Egen policy per rolle, uavhengig av tjenesteinnstillinger.
- **Ansettelsestype:** Policy etter brukerens tilknytning (f.eks. ekstern vs. fast ansatt).

Vurdering mot Entra ID: Entra PIM har ikke *tjeneste* og *ansettelsestype* som regel-scope. Du konfigurerer per rolle (og i noen tilfeller per ressurs). Dermed mangler PIM den forretningsnære plasseringen av regler som IdS IAM tilbyr, og den dynamiske styringen etter ansettelsestype må løses med omveier (egne grupper/roller, Conditional Access, eller prosessuelle retningslinjer).

13.2.2 Konfigurasjoner pr. nivå (IdS IAM) – med sammenligning mot Entra ID

1. **Makstid for aktiv- og selvbetjent tildeling** (dager, timer, minutter)
   Definerer hvor langt frem i tid du kan sette *utløp* når en ressurs tildeles – gjelder **all** tildeling (lederregistrering og selvbetjente bestillinger). Kan settes på tjeneste og overstyres ned på tilgangsnivå/rolle.

Entra ID: PIM støtter tidsavgrensede tildelinger (start/slutt), men konfigureres per rolle/ressurs – ikke som felles *tjeneste*policy som arves ned. Mangler dermed samme hierarkiske styring.

2. **Makstid for selvbetjent aktivering** (timer)
   Angir maks varighet for én aktivering (standard 24t). Kan settes sentralt og overstyres per tilgang/rolle.

Entra ID: PIM har *Maximum activation duration* per rolle. Mangler likevel IdS IAM sin modulære arv/overstyring via *tjeneste → tilgangsnivå*.

3. **Krav om begrunnelse ved selvbetjent aktivering**
   Slås på per tjeneste/tilgang/rolle; brukeren må oppgi årsak ved hver aktivering (med historikk for gjenbruk av begrunnelser).

Entra ID: PIM støtter krav om *justification* ved aktivering, men kun per rolle – ikke med arvede tjenestepolicyer.

4. **Godkjenning ved selvbetjent aktivering – styrt av ansettelsestype**
   Kan globalt slås på/av per **ansettelsestype** (f.eks. *på* for eksterne, *av* for faste). Standard er *av*.

Entra ID: PIM har godkjenning per rolle, men **mangler** ansettelsestype som egen policy-aksel.

5. **Finstyring av godkjenning per rolle og per tilgangsnivå**
   Som standard følges ansettelsestype-innstillingene. Du kan likevel **overstyre**:
   1. slå **av** godkjenning for en bestemt rolle/tilgang selv om den er *på* for ansettelsestypen,
   2. eller kreve **på** godkjenning for en rolle/tilgang selv om den er *av* for ansettelsestypen
   3. alternativt velge **ingen godkjenning, men varsling** til godkjennere når aktivering er gjort.

Entra ID: PIM tilbyr binær "krever/krever ikke godkjenning" per rolle og varsling til godkjennere, men har ikke samme **kombinasjon av arv + overstyring** på tvers av *tjeneste/tilgang/rolle/ansettelsestype*. Muligheten for kun varsling mangler i Entra ID.

6. **Tidslås (maks sammenhengende brukeraktivering pr. ansettelsestype)**
   Sikrer at brukere av en gitt **ansettelsestype** aldri kan holdes aktive utover X minutter i én omgang;

Entra ID: PIM har ikke *tidslås* knyttet til **ansettelsestype** som tverrgående begrensning.

13.2.3 Hvorfor IdS IAM konfigurasjonsmulighene betyr noe (strategisk vurdering)

- **Policy på riktig nivå:** IdS IAM lar sikkerhetspolicy *leve der forretningen lever* (tjenester og roller som brukerne forstår), og arves ned med presise overstyringer. Dette reduserer feilkonfigurasjon og gjør styringen mer forutsigbar for både IT og eiere av tjenestene.
- **Risikobasert differensiering:** Ansettelsestype som policy-aksel gir enkel differensiering (eksterne strengere enn faste) uten å multiplisere roller og grupper.
- **Driftseffektivitet og etterlevelse:** Krav om begrunnelse, tidslås og makstider driver *least privilege* i praksis og dokumenterer *hvem/hvorfor/hvor lenge* på en måte revisor forstår.

Konklusjon: Entra PIM dekker kjernen (tidsavgrensning, begrunnelse, godkjenning) – men **uten** IdS IAM sine nivåer (*tjeneste* og *ansettelsestype*) blir policyene mer "flate" og mindre forretningsnære. IdS IAM sin modulære modell gir derfor **mer treffsikker og brukervennlig** PIM/PAM-konfigurasjon i virksomheter på Entra ID.

13.3 Godkjenningsprosesser og arbeidsflyt

Et robust godkjenningsoppsett er avgjørende når brukere ber om eller aktiverer høye tilganger. **IdS IAM** utmerker seg ved å tilby konfigurerbare **godkjenningstyper** og flerstegs arbeidsflyter knyttet til både tildeling *og aktivering* av rolle og tilgang. Administrator kan definere et **godkjenningsløp** for selve medlemskapet i en rolle (f.eks. at en linjeleder eller applikasjonseier må godkjenne før noen får tildelt rollen). I tillegg kan man kreve **godkjenning ved selvbetjent aktivering** – f.eks. at hver gang en bruker

ønsker å aktivere en sensitiv rolle, må en sikkerhetsansvarlig godkjenne forespørselen først. IdS IAM støtter ulike godkjenningsmetoder: man kan angi at *rolle-eier*, *nærmeste leder* eller en dedikert *godkjenningsgruppe* skal motta forespørselen. Det er også mulig å sette opp flerstegs godkjenninger (for eksempel først leder, deretter sikkerhetsteam). Denne fleksibiliteten gjør at arbeidsflyten kan tilpasses virksomhetens interne kontrollkrav.

I **Entra PIM** er godkjenningsmulighetene mer begrenset. PIM lar deg **kreve godkjenning ved aktivering** av en privilegert rolle, men man kan typisk bare konfigurere **én gruppe av godkjennere** per rolle. **Godkjenningstyper** i PIM begrenser seg altså til "ingen godkjenning" (automatisk aktivering) eller "krever godkjenning av X personer".

Fra administrativt ståsted er poenget at begge systemer sikrer at kun autoriserte og verifiserte brukere får høye tilganger, men implementasjonen av godkjenningsprosessen er mer fleksibel i IdS IAM.

13.4 Innsyn, revisjon og etterlevelse

Både IdS IAM og Entra PIM logger alle aktiviteter for å muliggjøre inspeksjon og revisjon i etterkant. Entra PIM tilbyr et eget **revisjonslogg**-grensesnitt hvor man kan se hvem som aktiverte hvilke roller, når og hvorfor, samt om det ble godkjent og av hvem. Disse loggene kan lastes ned for intern eller ekstern revisjon.

IdS IAM har tilsvarende **revisjonsinnsyn**, enda mer omfattende fordi det samler data fra alle plattformer. Innen IdS IAM kan man gi revisorer og sikkerhetsansvarlige direkte tilgang til rapporter eller dashbord i portalen som viser *hvem som hadde hvilken tilgang når*. For eksempel kan få oversikt over alle aktiveringer som skjedde siste kvartal, med detaljer om varighet, godkjenner og brukerens begrunnelse. IdS IAM's **revisjonsrapporter** kan også inkludere tilganger utenfor Azure, slik at en intern revisor får et helhetlig bilde. Et annet fortrinn med IdS IAM er at man kan definere **kontroller** og attesteringer: f.eks. sette opp at alle ekstra tilganger skal gjennomgås av systemeier. Dermed fungerer IdS IAM som et verktøy for **etterlevelse** av regelverk (compliance) i vid forstand, ikke bare en systemlogg.

13.5 Konklusjon – helhetlig styring av privilegert tilgang

Sammenligningen viser at både IdS IAM og Microsoft Entra PIM oppfyller kjernebehovene for PIM/PAM: **just-in-time tilgang, tidsbegrensning, MFA, godkjenning og logging** for administratortilganger.

Microsoft Entra PIM er en spesialisert løsning for Azure-miljøet med dyp integrasjon i Microsofts økosystem. IdS IAM på sin side representerer en **mer helhetlig og fleksibel IAM-plattform** som ikke bare matcher PIM på funksjonalitet, men også utvider den. IdS IAM skinner spesielt når det gjelder:

- **Tilpassede arbeidsflyter og konfigurasjon av regler:** Granulær kontroll (f.eks. tidslås pr. ansatt-type, flerstegs godkjenning) utover det PIM tilbyr.
- **Brukervennlighet:** En konsolidert portal for alle selvbetjeningsbehov som senker terskelen for å be om tilgang riktig.
- **Tverrplattform dekning:** Mulighet til å styre tilgang på tvers av sky og lokale systemer, med Entra ID som én av mange integrasjoner (PIM dekker kun Azure).
- **Samlet oversikt:** Én sentral oversikt for alle roller og tilganger i virksomheten, som forenkler både administrasjon og revisjon.

For profesjonelle virksomheter er det klart at en løsning som IdS IAM gir et **strategisk løft**: den etablerer en konsistent, altomfattende styring av identitet og tilgang.

14 IdS IAM funksjoner som Entra ID mangler helt

Gjennom 13 år med kundedreven innovasjon, støttet av norsk finansnæring og forvaltet av IdentityStream sitt utviklingsteam, har IdS IAM fått en rekke unike funksjoner som dekker praktiske behov Entra ID ikke adresserer. Resultatet er en helhetlig og operativ IAM-plattform med funksjonalitet som strekker seg langt utover standard styring av identitet og tilgang. Dette kapitlet beskriver funksjoner som i dag mangler helt i Entra ID.

14.1 Signering av taushetserklæring

For å sikre konfidensialitet og integritet bør virksomheter kreve at medarbeidere signerer en digital taushetserklæring før tildeling av personlig passord og tilgang til systemer. Denne prosessen styrker virksomhetens forpliktelse til sikkerhet og etterlevelse av lover og forskrifter. Den sikrer også at medarbeiderne er fullt ut informerte om sitt ansvar og sine forpliktelser knyttet til håndtering av konfidensiell informasjon og bruk av IT-systemer.

Prosessen med digital signering av taushetserklæring er en integrert del av IdS IAM med automatikk og sperre mot utsending av passord. Løsningen er dermed både sikker og effektiv, og gir administratorer mulighet til å overvåke og administrere tilgangsrettigheter på en kontrollert måte. Systemet har funksjon for å sende signeringsforespørsel på nytt etter automatisk utsending ved registrering av ny medarbeider, og det er mulig å hente ut signeringslenken og sende kun denne.

Ledere har tilgang til taushetserklæringer for ansatte i sine avdelinger. Saksbehandlere har tilgang til alle signeringer. **IdS IAM fungerer som arkiv** for signerte taushetserklæringer. Administratorer kan ved behov overstyre standard prosedyre for passordutsendelse for å tilrettelegge for spesielle omstendigheter, uten å redusere sikkerhetsnivået.

14.1.1 Eksterne konsulenter: identitetssjekk er ofte fraværende – Bank ID løser dette

I praksis blir **identitetssjekk av eksterne konsulenter sjeldent gjort** når kontoer og tilganger settes opp. Dette er en betydelig risikofaktor: falsk identitet, forveksling av personer eller "deling" av kontoer kan gi uautoriserte tredjeparter tilgang til virksomhetens data.

Når en ekstern konsulent **signerer NDA elektronisk med Bank ID** (basert på personens nasjonale identitetsnummer/D-nummer), gjennomføres en **reell identitetssjekk**: kun den fysiske personen med dette NNIN kan autentisere seg og signere dokumentet. IdS IAM binder den signerte erklæringen til samme NNIN som brukes i onboarding, slik at virksomheten har bevis for at *riktig person* har akseptert vilkårene før tilganger gis.

Hvorfor er denne sjekken viktig?

- **Forebygger feilidentitet og misbruk:** Sikrer at tilgangen gis til riktig individ – ikke en kollega, stedfortreder eller innleid underleverandør.
- **Reduserer tredjepartsrisiko:** Eksterne aktører er ofte involvert i sensitive prosjekter; identitetsforankret NDA minimerer angrepsflaten.
- **Juridisk etterprøvbarhet:** Signert PAdES med verifiserbart tidsstempel og sertifikat gir dokumentert bevisverdi ved tvister.
- **Samsvar og ansvarlighet (accountability):** Underbygger virksomhetens krav til sikkerhet og personvern (minimering, sporbarhet og revisjon).
- **Klar rolleforståelse:** Konsulenten blir uttrykkelig informert om konfidensialitetskrav før noen tilgang gis.

Ved bruk av Bank ID-signering i IdS IAM valideres den signerte **PAdES-filen** og knyttes til onboarding-prosessen. Dette gir en effektiv, sporbar og etterprøvbar strøm hvor identiteten er kontrollert *før* passord og øvrige tilganger kan utleveres, gjelder både egne ansatte og eksterne konsulenter.

14.2 Bestilling av gjestebrukere

Streng M365-konfigurasjon som prioriterer sikkerhet (f.eks. at eiere ikke kan legge til gjester i Team, standard avskrudd ekstern deling i SharePoint, og behov for domenebegrensning) fører i praksis til at gjestehåndtering ender som en manuell IT-prosess: opprette gjest i ENTRA ID, legge vedkommende i Team-gruppen, åpne SharePoint-områdesamlingen for deling og sette riktige delingsgrenser. Dette gir merarbeid, risiko for feil og manglende sporbarhet over livssyklusen til gjestetilgangene.

IdS IAM adresserer dette ved å flytte «gjestereisen» fra uformelle manuelle løp til styrt bestilling med policy, tidsbegrensning, ansvar og revisjonsspor.

14.2.1 Slik fungerer gjestebrukerfunksjonen i IdS IAM

- **Bestilling med policy**
  Gjest kan bestilles (og forlenges) inntil en maksimaltid. Den er som standard **180 dager** og styrt av konfigurasjon. Sluttdato settes automatisk, og ansvarlig medarbeider varsles før utløp med mulighet til å forlenge for nye maks antall dager samarbeidsperiode.
- **Godkjenning og «sikre domener»**
  Løsningen kan kreve godkjenning, men også **forbigå godkjenning** for definerte sikre domener/partnere.
- **Automatisert etablering av tilgang**
  Ved godkjent bestilling opprettes gjesten i Entra ID og legges i riktig team/kanal; SharePoint-områdesamlingen åpnes for deling for eksisterende gjester, med mulighet for domenebegrensning.
- **Sentral styring av delingsinnstillinger**
  IdS kan styre SharePoint-deling og håndheve at ingen Team uten gjester har gjestedeling aktiv. Dette kjøres som en jobb på tidsplan («siste gjest ut slukker lyset»).
- **Varsling, forlengelse og avslutning**
  Ansvarlig medarbeider og alle eiere på team der gjesten er medlem, får varsel og mulighet til å forlenge før utløp av gjest. Ved utløp deaktiveres gjesten og alle tilganger fjernes. Når sluttføring er ferdigstilt, slettes gjesten i Entra ID. Det finnes også hastesluttføring som umiddelbart sletter gjesten.
- **Teknisk gjennomføring og etterlevelse**
  Automatiseringen bruker Graph API og CSOM med den eksisterende Entra ID systemtilkoblingen i IdS IAM.

14.2.2 Fordeler for virksomheten

- **Kontroll og etterlevelse:** Tidsbegrensning, ansvarlig eier, sporbarhet og planlagte «ryddeløp» reduserer risiko og støtter revisjonskrav.
- **Redusert manuelt arbeid:** IT slipper punkthåndtering i Entra ID/Teams/SharePoint; prosessen standardiseres.
- **Bedre brukeropplevelse med sikkerhetsnett:** Bestiller opplever smidig prosess (inkl. sikre domener), mens IdS håndhever delings- og livssyklussikkerhet i bakgrunnen.

14.3 Bestilling av fellespostkasse

Fellespostkasser er kritiske for team, funksjoner og kundedialog, men i Microsofts standardverktøy finnes det ikke en styrt bestillingsprosess med godkjenning, navnestandarder, rollebaserte tilganger og livssyklus. Resultatet blir ofte manuelle løp via IT og ujevn praksis: ulikt navn og format, feil tilgangsnivå (Full Access/Send As), manglende eierskap og svak sporbarhet. IdS IAM løser dette ved å flytte hele «fellespostkasse-reisen» inn i en policy-styrt bestillingstjeneste med eierskap, tilgangsnivåer og automatikk – på tvers av Exchange Online, hybrid og on-prem.

14.3.1 Slik fungerer funksjonen i IdS IAM

- **Styrt bestilling med godkjenning:** Bestiller fyller ut et strukturert skjema (tittel, ønsket eier(e), begrunnelse, selskap hvis flere i leietaker m.m.).
- **Godkjenning** konfigureres via godkjenningsløp. En saksbehandler kan f.eks. være godkjenner.
- **Automatisert etablering:** Ved godkjenning opprettes fellespostkassen og nødvendige sikkerhetsgrupper etter virksomhetens standarder. Arkivfunksjonen kan slås på som del av prosessen.
- **Tilgangsnivå som styringspunkt:** Tilgang håndteres via ett eller to **tilgangsnivåer** i tjenesten:
    - **Full Access** (lese/endre)
    - **Send As** (sende som postkassen)
      Løsningen kan bruke **én** gruppe for begge (forenkling), eller **to** separate grupper for granularitet – alt styrt av konfigurasjon.
- **Eierskap og selvbetjent medlemskap:** Bestilte **eiere** settes som ansvarlige og kan etterpå administrere medlemskap i tilgangsnivå(ene) uten å gå via IT.
- **Livssyklus og endringer:** Eierskifte, navneendring og avvikling kjøres via samme tjeneste, med sporbarhet og revisjonsvennlige logger.

14.3.2 Fordeler for virksomheten

- **Standardisert kvalitet:** Lik navngivning, rette tilganger og korrekt konfigurasjon hver gang – uten manuelle avvik.
- **Færre henvendelser til IT:** Eiere kan selv administrere medlemmer på tilgangsnivå.
    - Digitaliseringen flytter aksjon til behov og effektiviserer.
- **Revisjonsklar prosess:** Godkjenning, eierskap, metadata og logg gir sporbarhet for internkontroll og tilsyn.
- **Fleksibel plattformstøtte:** Samme bestillingsopplevelse dekker Exchange Online, hybrid og on-premises.

14.4 Midlertidig tilgangspass (TAP) for to-faktor autentisering

Når en medarbeider (ofte ekstern/konsulent) skal onboardes utenfor virksomhetens nett, eller når noen har mistet/byttet telefon og mangler Microsoft Authenticator, stopper innloggingen opp. Entra ID tilbyr *Temporary Access Pass* (TAP) for å løse påloggingen, men i praksis mangler det en **styrt prosess** med godkjenning, målrettet utsending (SMS/e-post), språkmaler, livssyklus og sporbarhet. Resultatet blir ofte manuell håndtering på servicedesk-nivå, varierende praksis og svake revisjonsspor.

14.4.1 Slik fungerer funksjonen i IdS IAM

- **Bestilling og godkjenning**
  Tjenestesiden «Midlertidig tilgangspass» automatiserer bestilling av TAP for leder ved onboarding og lar servicedesk bestille TAP for gjenoppretting. Bestillingen kan kreve godkjenning og knyttes til et definert **tilgangsnivå** (f.eks. «Ekstern pålogging»).
- **Automatisk utstedelse av TAP**
  IdS IAM oppretter et **engangspassord** (Temporary Access Pass) i Entra ID med tidsbegrensning og engangsbruk. Utløp settes iht. policy.
- **Styrte meldingsløp (SMS/e-post)**
  Utsending skjer automatisk via forhåndsdefinerte **tjenesteordre-meldinger** på ulike kanaler:
  - **SMS**: sender innloggingsnavn/UPN.
  - **E-post**: sender selve tilgangspasset, lenke til sikkerhetsinformasjon (for å registrere ny påloggingsmetode) og intern brukerveiledning.
    Malene er språkstyrte og kan tilpasses per kanal.
- **Fletting av variabler**
  Meldingsmalene fletter inn dynamiske felter, bl.a.:
  [TemporaryAccessPass] (engangskoden), [TemporaryAccessPassExpirationDate], [FirstName] og UPN.
  Eksempel: *«Hei [FirstName], et tidsbegrenset, midlertidig passord er opprettet for deg. Passordet er: [TemporaryAccessPass] … Passordet kan brukes én gang og utløper [TemporaryAccessPassExpirationDate].»*
- **Sikker bruk og opprydding**
  Når brukeren logger inn med TAP og registrerer ny Authenticator-metode, markeres TAP som brukt/utløpt; IdS IAM **logger hendelsen**. Ubrukte koder utløper automatisk.

14.4.2 Fordeler for virksomheten

- **Automatisk** utstedelse av TAP ved **onboarding**.
- **Null ventetid ved gjenoppretting** – sikker, styrt gjenoppretting uten manuell «akutt» bistand.
- **Standardisert og revisjonsklar prosess** – godkjenning, språkmaler, logging og automatisk utløp.
- **Bedre brukeropplevelse** – riktig informasjon i riktig kanal: UPN på SMS, TAP på e-post, med tydelige steg videre.
- **Komplement til Entra ID** – IdS IAM gjør TAP operativt i linjen med policy, meldingsflyt og eierskap – ikke bare som en teknisk funksjon.

14.5 Permisjon (policy-styrt tilgangsstyring ved fravær)

Medarbeidere på permisjon skal ha **minimum nødvendige tilganger** av hensyn til både **sikkerhet (least-privilege)** og **kost (lisenser/kapasitet)**. I praksis mangler Entra ID en helhetlig prosess for å registrere permisjon, planlegge tiltak før/under/etter perioden, og automatisk justere tilganger på tvers av systemer.

IdS IAM løser dette med en styrt, tidslinjestyrt prosess fra HR til leder/IT, med revisjonsspor.

Hvor mange er typisk i permisjon? I en «normal» kunnskapsbedrift vil ofte **omtrent 1–3 %** av arbeidsstokken være i permisjon til enhver tid (barsel, utdanning, permisjoner m.m.). I perioder/virksomheter med høy barselandel kan dette ligge **opp mot 3–5 %**. Riktig håndtering gir merkbare lisensbesparelser og reduserer risiko.

14.5.1 Slik fungerer funksjonen i IdS IAM

- **Registrering**
  HR finner medarbeideren, setter **start- og sluttdato** og registrerer permisjonsperioden.
- **Før oppstart**
  14 dager før permisjonen starter varsles leder. Har medarbeider **portefølje/ansvar**, bes lederen overføre denne til en annen medarbeider.
- **Ved oppstart av permisjon**
  Etter **siste arbeidsdag** fjernes alle tilganger som ikke skal gjelde i permisjon. Medarbeider beholdes kun med tilganger via selskap og eventuell **permisjonsrolle**. **Systembrukere** for tjenester med støtte for dette **deaktiveres** i permisjonsperioden.
- **Før planlagt retur**
  30 dager før slutt varsles leder om å bekrefte/endre retur og behov. **14 dager før** slutt opprettes automatisk en **personendring** for å gjeninnføre tilganger iht. gjeldende roller og ekstra tilganger medarbeider hadde før permisjon. Leder varsles samtidig om å justere tilganger etter faktisk behov. Permisjonslisten lenker alle sakene i flyten og kan vise historikk etter slutt.

14.5.2 Operativ «least-privilege»

Medarbeidere på permisjon **trenger normalt ikke** de samme rettighetene som før fraværet. Å la full tilgang stå uberørt bryter med **least-privilege** og øker angrepsflaten. IdS IAM håndhever minstetilgang under permisjon, og gjeninnfører kun nødvendige tilganger ved retur – med leder i loopen og med revisjonsspor.

14.5.3 Fordeler for virksomheten

- **Sikkerhet:** Praktisk gjennomført **least-privilege** i hele permisjonsperioden; systembrukere kan deaktiveres.
- **Kostnad: Lisens- og kapasitetsbesparelser** ved å parkere/ta ned tilganger mens 1–3 % (ofte opp til 5 %) av arbeidsstokken er i permisjon.
- **Etterlevelse og revisjon:** Tidfestede varsler, oppgaver og logg før/under/etter permisjon gir **sporbarhet**.
- **Forutsigbar drift:** Automatikk for porteføljeoverføring, tilgangsfjerning og retur reduserer manuell oppfølging og feil.

Kort sagt: Permisjonsfunksjonen i IdS IAM reduserer risiko og kost – og gjør samtidig at HR, leder og IT har en felles, styrt prosess for hele permisjonslivssyklusen.

14.6 Lås opp konto og resett passord via kollega

Når en medarbeider blir låst ute (for mange feilede forsøk) eller glemmer passordet sitt, stopper arbeidet. Klassisk løsning er å kontakte IT—som skaper kø, ventetid og kost. **IdS IAM** lar virksomheten delegere

trygge, avgrensede handlinger til kolleger eller ansvarlige, slik at brukeren kommer raskt i gang igjen uten å omgå sikkerhetskrav.

14.6.1 Slik fungerer det i IdS IAM

- **To selvbetjente handlinger i "Mine funksjoner" → Selvbetjening**
    1. **Lås opp brukerkonto for en kollega** – kollega søker opp bruker (navn, ident/innloggingsnavn) og låser opp med ett klikk. Av sikkerhetshensyn kan en konto kun låses opp **én gang per døgn** av en kollega. IT kan også begrense at funksjonen bare er tilgjengelig for kolleger **i samme avdeling**.
    2. **Resett glemt passord for en kollega** – kollega søker opp bruker og utløser passord-resett. **Nytt passord sendes på SMS** til mobilnummeret som er registrert på medarbeideren. Også her kan IT begrense funksjonen til samme avdeling.
- **Ansvarlig-tilgang for "egne" brukere**
  Medarbeidere kan i tillegg selv resette passord for **brukere de er ansvarlig for** (f.eks. ekstra brukere til drift/testing) – uten å gå via servicedesk.
- **Kontekst og kontroll før utføring**
  Skjermbildet viser tydelig **hvem** som låses opp/tilbakestilles, tilhørende **avdeling** og **leder** før handlingen bekreftes. Dette reduserer feil og øker sporbarhet.
- **Sikker utsending av legitimasjon**
  Ved passordreset sendes det midlertidige passordet **som SMS** til brukerens registrerte mobil, ikke til kollegaen som initierte handlingen.

14.6.2 Styring og begrensninger (policy)

- **Avdelingsavgrensning:** Kan konfigureres slik at kun kolleger **i samme avdeling** kan låse opp/resette.
- **Frekvensbegrensning:** Lås-opp via kollega kan gjøres **maks én gang per døgn** per konto.
- **Ansvarlig-modell:** Egen policy for at ansvarlig medarbeider kan hjelpe **tilknyttede ekstra brukere** (drift/test).

14.6.3 Typiske brukstilfeller

- **Låst konto ved feiltasting:** Kolleger i teamet hjelper på sekunder – ingen serviceticket.
- **Glemt passord før kundemøte:** Kollega initierer reset; brukeren får SMS umiddelbart og kan logge inn.
- **Drifts- og testbrukere:** Ansvarlig utvikler/driftsressurs kan selv resette passord for sine ekstra brukere.

14.6.4 Fordeler for virksomheten

- **Rask gjenoppretting:** Minutter i stedet for timer – uten å belaste servicedesk.
- **Bedre sikkerhet i praksis:** SMS direkte til bruker, avdelingsavgrensning og døgnbegrensning reduserer misbruk.
- **Forankret i linjen:** Team hjelper egne kolleger/ansvarsbrukere – med tydelig kontekst før utføring.

Kort sagt: IdS IAM gjør passordhjelp og konto-opplåsing **selvbetjent, rask og sikker** – med kontrollert delegering til kolleger og ansvarlige, og uten at sensitivt passord deles med andre.

14.7 Meldingspanel for utsending av SMS og mail

Endringer, driftsavvik og utrulling av nye sikkerhetstiltak må kommuniseres raskt, men tradisjonelle fordelingslister blir fort utdaterte og treffer feil. Meldingspanelet utnytter **IdS IAM-modellen** (roller, tjenester og tilgangsnivåer) til å sende **presise meldinger til akkurat de som bruker et system eller har en gitt tilgang**. Det reduserer støy («alle ansatte»-eposter), øker etterlevelse ved endring, og gir sporbarhet.

Eksempler:

- Varsle **alle som har tilgang til et bestemt system** om en planlagt endring.
- Sende til **alle i IRT** (Incident Response Team), **alle fast ansatte**, eller alle i **Privatmarked Storkunder** – uten manuelt vedlikehold av lister.

14.7.1 Slik fungerer funksjonen i IdS IAM

- **Velg kanal:** E-post eller SMS.
- **Velg mottakere dynamisk:** Plukk målgruppen basert på **Rolle**, **Tjeneste** eller **Tilgangsnivå**. Du kan filtrere, kombinere og supplere med **enkeltmottakere** (telefon/e-post) hentet fra personregisteret. Du kan også skrive inn egne.
- **Skriv og send:**
  - **SMS:** kortmelding; støtte for **utsatt utsending** (praktisk f.eks. når et passord skal gå ut **07:00 i morgen**, men ikke før).
  - **E-post:** emne, prioritet (Lav/Medium/Høy), **To/Cc/Bcc**, og **vedlegg**.
  - **Koder/fletting:** bruk variabler (f.eks. navn, brukernavn) der det er relevant.
- **Sporbarhet:** Valgfritt kan meldingstekst og utsending **lagres på saken** for revisjon og etterkontroll.

14.7.2 Fordeler for virksomheten

- **Treffsikker kommunikasjon:** Alltid riktig målgruppe – fordi den styres av faktisk **tilgang** i IdS IAM, ikke statiske lister.
- **Rask respons ved hendelser:** Umiddelbar utsending til alle brukere av et rammet system.
- **Mindre støy, bedre etterlevelse:** Riktige personer får riktige instrukser; færre «masseutsendinger».
- **Sikker praksis: SMS med utsatt utsending** støtter tidskritiske scenarier (passord/engangskoder) uten å kompromittere tidspunkt.
- **Revisjonsklarhet:** Hvem fikk hva, når, og på hvilket grunnlag – dokumentert i saken.

Kort sagt: Meldingspanelet gjør identitets- og tilgangsdata operativt for kommunikasjon – raskt, presist og etterprøvbart.

14.8 Organisasjonskart (tilgjengelighet, kontakt og innsikt direkte i IdS IAM)

Medarbeidere trenger raskt å finne ut **hvem som gjør hva**, **hvem som er tilgjengelig nå**, og **hvordan de kontakter rett person/avdeling**. Klassiske intranett-sider og statiske org-PDF-er blir raskt utdaterte, og de mangler kobling til faktisk **tilgangs- og kostnadsdata**. IdS IAM sitt Organisasjonskart gjør organisasjonsstrukturen operativ: oppdatert, søkbar, og koblet til tilgangsmodell, kostnad og risiko.

14.8.1 Slik fungerer Organisasjonskartet

- **Tilgjengelig for alle medarbeidere**
  Alle kan slå opp en avdeling eller en spesifikk medarbeider og se:
  - **Teams-tilstedeværelse (presence)** for å vurdere om vedkommende er tilgjengelig eller se hvem som er tilgjengelig i en avdeling.
  - **Kontaktinformasjon** (telefon, e-post) og **funksjon/rolle**.
  - **Avdelingsinformasjon** som **leder**, **kontoradresse** og nøkkeldata.
- **Finn meg / filtrer**
  Hurtigfiltre for medarbeider og avdeling gjør det enkelt å navigere i store organisasjoner. Allianser med flere leietakere lar deg også raskt bytte leietaker til en annen du har tilgang til.
- **Drill-down i avdelinger**
  Se liste over medarbeidere, underenheter og relevante detaljer direkte i kortvisningen.

14.8.2 Innsiktsvisninger for de med tilgang

Brukere med utvidede rettigheter kan aktivere to ekstra lag med innsikt:

- **Vis tilgangsnivåer**
  Viser hvilke **tilgangsnivåer** som er bygget inn i organisasjonstreet – nyttig for å forstå hvilke fellesressurser som er tilgjengelig for alle i avdeling.
- **Vis årlig IT-kostnad og risiko**
  Viser **årlig IT-kostnad** og **risikoscore** både per avdeling og per medarbeider. Hver verdi lenker videre til detaljer som forklarer **hva som bygger kostnad/risiko** (tjenester, lisenser, kritikalitet m.m.), slik at ledere og eiere kan ta informerte beslutninger.

14.8.3 Typiske bruksområder

- **Hverdagsbruk:** Finn riktig kontakt på sekunder, se om de er tilgjengelige i Teams, ring eller send e-post direkte.
- **Ledelse/forvaltning:** Forstå hvilke tilganger som finnes i avdelingen, identifiser avvik som f.eks. enkeltmedarbeidere med høy lisenskostnad. Følg lenker for å ta aksjon ved f.eks. å bestille fjerning av en dyr lisens.
- **Kost/kontroll:** Se avdelingskostnad, identifiser «tunge» lisenser/tilganger og vurder optimaliseringstiltak.

14.8.4 Fordeler for virksomheten

- **Raskere samarbeid:** Alle finner rett person og ser tilgjengelighet med én gang.
- **Bedre styring:** Synlighet for **tilgangsnivåer** i samme flate som organisasjonsdata gir god oversikt.

- **Kostnad og risiko på kontekst:** Ledere får **live-innsikt** i IT-kostnad og risiko på egen avdeling/medarbeidere – med sporbar drill-down.
- **Alltid oppdatert:** Data trekkes fra IdS IAM og viser faktisk status, ikke statiske dokumenter.

Kort sagt: Organisasjonskartet gjør struktur, mennesker, tilganger, kost og risiko tilgjengelig i én og samme flate – for effektivt samarbeid i linjen og faktabasert styring for ledere.

14.9 Kjøring av konfigurerbare Exchange kommandoer i IAM prosesser

Entra ID tilbyr ikke en måte å kjøre målrettede Exchange-kommandoer på som del av **Joiner/Mover/Leaver** og andre IAM-flyter. I praksis trengs ofte presise Exchange-endringer (mailbokser, autosvar, kalenderrettigheter, arkiv, skjuling i adressebok osv.) i **riktig rekkefølge og kontekst**—og dette varierer mellom Online, hybrid og on-premise. IdS IAM støtter alle tre driftsmodeller og kobler Exchange-automatisering direkte inn i IAM-prosessene, med moderne autentisering, rettighetsstyring og mulighet til å **begrense hvilke PowerShell-kommandoer som er tillatt** på systemnivå (white-liste).

14.9.1 Slik fungerer funksjonen i IdS IAM

- **Støtte for Online, hybrid og on-prem**
  Integrasjonen kan settes opp mot online, hybrid eller on-prem Exchange.
- **Sikker tilkobling og minstemulige rettigheter**
  Tilgang gis via dedikerte roller (f.eks. *Recipient Management* eller skreddersydd rolle) og moderne auth (sertifikat/client secret). Du kan også **hviteliste** kommandoer som kan kjøres fra IdS.
- **Kommandoer knyttet til IAM-hendelser**
  IdS lar deg konfigurere kommandoer som kjøres **før/under/etter opprettelse**, ved **deaktivering/aktivering**, **tilordning/fjerning av tilgangsnivå**, og **før sletting**. Hver blokk kjører i riktig steg med støtte for variabler (f.eks. {mail}, {sAMAccountName}, {0}, $[x-CurrentPrimarySmtp]).

14.9.2 Eksempel A – Medarbeider som slutter

Mål: Oppretting av postboks og bevare kundedialog når noen slutter. Kunden skal få svar og kunne nå teamet som overtar.
Løsning i IdS IAM:

1. **Før oppretting** (fjern medarbeiders e-postadresse fra fellespostkasse med autosvar):
   Set-RemoteMailbox -Identity Sluttet_i_Acme -EmailAddresses @{remove="$[x-CurrentPrimarySmtp]"}
2. **Oppretting** (opprett mailboks med arkiv):
   Enable-RemoteMailbox -Alias "{sAMAccountName}" -PrimarySmtpAddress "{mail}" -RemoteRoutingAddress "{mailAddressUserName}.{sAMAccountName}@identitystream.mail.onmicrosoft.com"

   Set-RemoteMailbox -EmailAddresses @{add="{mailAddressUserName}.{sAMAccountName}@identitystream.mail.onmicrosoft.com"}

   Enable-RemoteMailbox -Archive
3. **Etter oppretting** (språk/datoformat):
   Set-MailboxRegionalConfiguration -Identity {0} -Language nb-no -DateFormat dd.MM.yyyy

4. **Ved deaktivering** (skjul/frihold adresse og gi til fellepostkasse, retention til Exchange Online):
   Set-RemoteMailbox -HiddenFromAddressListsEnabled $true

   Disable-RemoteMailbox -Confirm:$false

   Set-RemoteMailbox -Identity Sluttet_i_Acme -EmailAddresses @{add="$[x-CurrentPrimarySmtp]"}

   $(msExchExtensionAttribute20=Retention)
5. **Ved re-aktivering** (tilbakeføring):
   Set-RemoteMailbox -HiddenFromAddressListsEnabled $false

   $(msExchExtensionAttribute20=$null)
6. **Før sletting i IdP** (rydd på fellespostkasse):
   Set-RemoteMailbox -Identity Sluttet_i_Acme -EmailAddresses @{remove="$[x-CurrentPrimarySmtp]"}

I interimperioden ligger **fraværsmeldingen som autosvar på fellespostkassen** som overtar e-postadressen, til IdP-sletting er gjennomført. Dette er et praksiseksempel på hvordan Exchange-kommandoer kan bindes til **IAM-flyt**.

14.9.3 Eksempel B – Bookingfunksjon med kalenderrettigheter til alle

Mål: En sentral bookingrolle skal kunne legge inn avtaler i alles kalendere; unntak styres via tilgangsnivå.

Løsning i IdS IAM (etter opprettelse):
Add-MailboxFolderPermission -Identity {0}:\$CalendarName -User Role-Calender-Access-Acme -AccessRights Owner

Ved tilordning av tilgangsnivå "Ikke kalenderinnsyn" (for HR/Sikkerhet):

Set-MailboxFolderPermission -Identity {0}:\$CalendarName -User default -AccessRights AvailabilityOnly

Set-MailboxFolderPermission -Identity {0}:\$CalendarName -User Role-Calender-Access-Acme -AccessRights AvailabilityOnly

Koblingen mellom **tilgangsnivå** i IdS og Exchange-rettigheter gir finmasket, policybasert styring uten manuelt etterarbeid.

14.9.4 Hvorfor dette er unikt vs. Entra ID

- **Prosessnær automasjon:** Kommandoer kjører *i* IAM-flyten (J/M/L, aktivering/deaktivering, tildeling av tilgangsnivå).
- **Driftsmodeller dekket:** Samme mønster fungerer i **on-prem, hybrid og EXO**—med moderne auth og anbefalte roller.
- **Sikkerhet & etterlevelse:** Mulighet til å **begrense hvilke PS-kommandoer** som kan brukes, revisjonsspor og feilhåndtering.

14.9.5 Fordeler for virksomheten

- **Mindre manuelt arbeid:** IT slipper "håndsveiving" i Exchange Admin/PowerShell ved hver endring.
- **Bedre kundeopplevelse ved Leaver:** Fraværslogikk og adressehåndtering gjør at kunder når rett team—ingen tapt dialog eller kunde-«churn».
- **Kvalitet og konsistens:** Standardiserte språk-/dato-innstillinger, arkiv, skjuling i adressebok og retention kjøres likt hver gang.
- **Sikker praksis:** Least-privilege på kalenderdata og tydelig separasjon av hvem som kan gjøre hva (roller/tilgangsnivåer).
- **Fleksibilitet:** Én konfigurasjon lar deg rulle ut virksomhetsspesifikke variasjoner uten kodeendring.

Kort sagt: IdS IAM gjør Exchange-administrasjon til en **policy-styrt del av identitetsprosessene**, ikke en separat manuell jobb—noe Entra ID i dag ikke tilbyr.

14.10Agentmodus for systemtilkoblinger (sikker bro til interne systemer)

Mange virksomheter har systemer bak brannmur/on-prem som ikke kan eksponeres ut. Entra ID tilbyr ingen generell, sikker «innsiden-til-utsiden» oppsett for IAM-prosesser. **IdS IAM agentmodus** løser dette ved å la en lettvekts **agent** kjøre **inne** i nettverket og gjennomføre oppgaver på vegne av IdS IAM, uten å åpne innkommende porter. All kommunikasjon er **kryptert og klient-sertifikatverifisert**, slik at bare autoriserte parter kan utveksle oppdrag.

14.10.1 Slik fungerer agentmodusen

- To driftsmoduser
  - **Listen mode:** Agenten lytter på en angitt port (f.eks. 8443). IdS IAM kobler til for å sende kommandoer.
  - **Polling mode:** Agenten **ringer ut** til IdS IAM og henter oppdrag. Krever ingen eksponert port inn til kundenettet.
- Installasjon på minutter
- Samme agent kan gjenbrukes av flere **systemtilkoblinger** i samme leietaker.

14.10.2 Hva agenten muliggjør i praksis

- **On-prem/hybrid-støtte i IAM-flyt:** Kjør PowerShell/CLI mot interne plattformer (f.eks. **Exchange on-prem/hybrid**, fil-/AD-operasjoner, lokale API-er) som en del av **Joiner/Movers/Leaver** og tjenestebestillinger – uten å eksponere dem ut.
- **Robusthet:** Flere **AgentPollingUris** kan legges inn for høyere tilgjengelighet; listen/polling kan byttes pr. tilkobling.
- **Streng sikkerhet:** Gjensidig TLS med klient-sertifikater for både identitet og transportkryptering. Konfigurasjon styres sentralt i IdS.

14.10.3 Hvorfor dette er unikt vs. Entra ID

- **Prosessnær utførelse inne i kundens miljø:** Entra ID mangler en generell, styrt agent for interne handlinger i IAM-prosesser. IdS IAM gir dette som en standard kapasitet.

- **Ingen åpne porter i polling-modus:** Tryggere nettarkitektur—agenten ringer ut, IdS IAM gir oppdrag.
- **Sertifikatbasert null-tillit:** Gjensidig verifisering, sporbarhet og enkel rotasjon av nøkler.

14.10.4 Fordeler for virksomheten

- **Sikker tilkobling til alt som er «på innsiden»** – uten ny infrastruktur eller eksponering.
- **Rask utrulling og lav drift:** Scriptet installering, sky-styrt konfigurasjon og enkel gjenbruk mellom tilkoblinger.
- **Konsistente IAM-prosesser på tvers av plattformer:** Online, hybrid og on-prem oppfører seg likt – samme policy, samme flyt.
- **Revisjonsklarhet:** Hvem kjørte hva, hvor, og når – koblet til IdS-sak og tilkobling.

Kort sagt: Agentmodusen gjør IdS IAM til en **fullverdig bro** mellom skyens IAM-prosesser og interne systemer – sikkert, standardisert og uten friksjon.

14.11 HR-skjema (utvidbare HR-felter per ansettelsestype)

Standard HR-registre dekker sjelden all informasjon virksomheten faktisk trenger i **Joiner/Mover**-løpene: ekstra felt for vikarer, lærlinger, eksterne, spesielle godkjenninger, uniform/sted/turnus – ofte forskjellig **per ansettelsestype**. Entra ID har ingen innebygd måte å utvide HR-skjemaet, styre visning/tilgang og gjøre dataene operasjonelle i IAM-prosessene. **IdS IAM HR-skjema** løser dette med en skjemabygger som knyttes til ansettelsestyper og er tett integrert i Joiner/Mover – med rollebasert innsyn.

14.11.1 Slik fungerer HR-skjema i IdS IAM

- **Skjemabygger (drag-and-drop)**
  Opprett HR-tjenesten, legg til nytt skjema og bygg feltene ved å dra inn komponenter; definer spørsmål og svaralternativer etc.
- **Knyttes til ansettelsestyper**
  Velg hvilken **ansettelsestype** som skal bruke skjemaet (f.eks. Ansatt, Vikar, Konsulent). Da dukker HR-skjemaet automatisk opp i **Registrer** og **Endre medarbeider** for riktig målgruppe.
- **Del av Joiner/Mover**
  Skjemaet inngår i J/M-løp: leder/HR fyller inn felter når nyansatt registreres eller når arbeidsforhold endres. Feltverdier kan **sendes til** og **hentes fra** tilkoblede systemer der det er konfigurert, slik at HR-data blir en del av systemintegrasjonen.
- **Rollebasert visning av HR-data**
  I “Alle brukere” kan de med tilgang slå på visning av **HR-data.**

14.11.2 Hvorfor dette er unikt vs. Entra ID

- **Utvidelse per ansettelsestype:** Skreddersy feltene for ulike arbeidsforhold – ikke ett “one-size-fits-all” skjema.
- **Operasjonelt i IAM-prosesser:** HR-felt blir styringsdata i **Joiner/Mover**, ikke bare fritekst.
- **Sikret innsyn:** HR-data synlig kun for HR-roller og nærmeste leder – direkte i IdS IAM.

14.11.3 Fordeler for virksomheten

- **Raskere og riktigere J/M:** Skjema tilpasset kontekst gir færre avklaringer og mindre manuell etterarbeid.
- **Én kilde – færre feil:** Data kan utveksles med HR-/fagsystemer; mindre dobbeltregistrering.
- **Bedre styring og etterlevelse** gjennom sporbarhet og konsekvent bruk per ansettelsestype.
- **Sikkerhet og personvern:** Rollekontroll på visning av HR-data (HR og leder)

Kort sagt: HR-skjema lar virksomheten modellere HR-informasjon**, sikker og prosessnær** – akkurat der den trengs for å styre tilgang og arbeidsflyt i Joiner/Mover.

14.12IdentityMap og Role mining

Over tid akkumuleres «ekstra tilganger» (ad-hoc rettigheter) ved siden av de standardiserte rollene i rollebaserte IAM. Det gir avvik fra standarden, skaper kompleksitet i revisjon og gjør det vanskelig å onboarde nye systemer uten å lage flere spesialtilfeller. IdentityMap + role mining i IdS IAM adresserer dette ved å **visualisere hele tilgangslandskapet som en graf** (brukere ⇄ roller ⇄ tjenester/tilgangsnivåer ⇄ systemer) og bruke **algoritmer** til å foreslå bedre rollefordelinger og avdekke overflødige/risikable tilganger. Grafdatabaser er spesielt egnet til dette fordi de modellerer relasjoner, mønstre og avhengigheter langt mer uttrykksfullt enn tabeller.

14.12.1 Slik fungerer IdentityMap i IdS IAM

- **Grafmodell av IAM-relasjoner**
  IdentityMap projiserer IdS IAM-data til en graf: sirkler for brukere, roller, tjenester/tilgangsnivåer og systemressurser; lenker for «har rolle», «gir tilgang», «bruker system», «kost/risiko». Dette gir en **interaktiv oversikt** over hvem som har hva og hvorfor.
- **Sanntidsnær visualisering og drill-down**
  Fra org → avdeling → rolle → tilgangsnivå kan du zoome inn på avvik (f.eks. personer som har overflødig ekstra tilgang) og følge lenker videre til detaljene. Visualiseringen er utviklet nettopp for å forstå **komplekse sammenhenger i IAM**.
- **GRC-lag**
  IdentityMap kan vise **kostnad og risiko** i samme kart (SoD-bruddindikatorer, kritikalitet og lisenskost). Dermed ser eiere ikke bare *hvem* som har tilgang, men også *hva det koster og risikoen*.

14.12.2 Slik fungerer Role mining i IdS IAM

- **Startpunkt 1 – Standardisere «ekstra tilgang»:**
  Kjør role mining mot dagens **ekstra tilganger** opp mot eksisterende roller og medlemmer. Systemet analyserer mønstre (grupper av brukere som ofte har samme ekstra tilganger) og foreslår tilganger som kan legges inn i eksisterende roller.
- **Startpunkt 2 – Onboarde nytt system som «ekstra tilgang»:**
  Legg all tilgang fra et nytt system inn som **ekstra tilgang** først. Kjør så role mining for å **mappe til eksisterende roller**. Dette gir verdi raskt uten å designe alt på forhånd for å få en standardisert rollemodell.

- **Algoritme og validering:**
  Role Mining bruker Jaccard index for å finne kandidater for å legge tilganger inn i rolle. Forslagene **simuleres** før endring: antall berørte brukere og forventet reduksjon i ekstra tilganger.

14.12.3 Typiske bruksområder

- **Rydde «spagetti» av ekstra tilganger:** Få dem inn i få, gode roller.
- **Rask integrasjon av nytt fagsystem:** Start som ekstra tilgang → role mining → inn i standardroller.
- **Revisjonsforberedelser:** Visualiser SoD-konflikter, «hvem har hva og hvorfor» og pek videre til evidens.

14.12.4 Hvorfor dette er unikt vs. Entra ID

- **Grafbasert innsikt + mining, tett integrert i IAM-flyt:** Entra ID mangler innebygd grafvisualisering og domene-tilpasset role mining for å optimalisere rollemodellen over tid. IdentityMap kombinerer **visualisering** og **algoritmer** i samme verktøy — og resultatet kan publiseres direkte som IdS-roller/tilgangsnivåer.
- **GRC i kontekst:** Kost/risiko vises sammen med tilgangsrelasjoner, ikke i en separat rapport.

14.12.5 Fordeler for virksomheten

- **Mer standardisert tilgangsmodell:** Mindre «ekstra tilgang», færre unntak og lavere revisjonsbyrde.
- **Bedre sikkerhet (least-privilege):** Mining-forslagene er designet for å *redusere* over-provisjonering og avdekke risikable kombinasjoner.
- **Raskere utrulling av nye systemer:** Start enkelt, standardiser datadrevet etter hvert.
- **Felles situasjonsbilde:** Ledere, eiere og sikkerhet ser **samme kart** med roller, tilganger, kost og risiko — og kan handle direkte fra innsikten.

Kort sagt: IdentityMap + role mining gjør rolleforvaltning **datadrevet**: du *ser* relasjonene, *finner* mønstrene og *operasjonaliserer* forbedringene i IdS IAM — noe tradisjonell Entra-funksjonalitet ikke dekker i dag.

14.13IdS OfficeHoursManager (standardisert medarbeidertilgjengelighet)

Kunder og kolleger må vite **når** og **hvordan** de kan kontakte medarbeidere – fysisk, digitalt eller på telefon. Uten et felles rammeverk blir åpningstider og kanaler uensartet, vanskelig å vedlikeholde og lite egnet for integrasjoner (f.eks. booking). OfficeHoursManager lar virksomheten **standardisere og styre kontortid** sentralt, samtidig som lokale behov ivaretas. Kontortid kan **arves** fra kontorlokasjon/avdeling og **overstyres** per medarbeider ved behov.

14.13.1 Slik fungerer OfficeHoursManager i IdS IAM

- **Modellforankret tilordning:** IdS IAM-modellen med **selskap** → **avdeling** → **kontor** brukes til å tilordne **standard lokasjon**, **kontortid** og **tilgjengelige kanaler** (fysisk/digitalt/telefon). Standardiserte tider konfigureres én gang og arves til medarbeidere i organisasjonstreet.

- **Standard, ingen eller egendefinert:** For hver medarbeider kan man velge **Ingen kontortid**, **Standard kontortid** (arvet), eller **Egendefinert** (kombinasjon av felles/persontider). Validert på tvers av lokasjoner for å hindre overlapp/konflikt.
- **Rolle-/tilgangsstyrt administrasjon:** IdS OfficeHoursManager er en tjeneste i IdS IAM med tilgangsnivåer som lar virksomheten styre hvordan de vil sette administrasjon av kontortid ut i organisasjonen:
    - **Administrator for kontortid** – gir tilgang til å administrere felles kontortider og tilordning av disse til brukere og kontorer.
    - **Egendefinert kontortid** – Gir bruker tilgang til å sette/redigere sin egen kontortid og tilgjengelighet.
    - **Redaktør for kontorlokasjoners kontortid** – Gir tilgang til å redigere kontortid for kontorlokasjoner.
    - **Redaktør for kontortid til sine medarbeidere** – Dette er en lederfunksjon som gir tilgang til å opprette/redigere "personlig" kontortid og tilgjengelighet for seg selv og sine medarbeidere.
    - **Bruker med kontortid i eksternt system** – Brukere med denne tilgangen vil få kontortid oppdatert i eksterne systemer som støtter kontortid (kan legges på avdeling med fast ansatt som ekstra rollekrav f.eks.).
- **Eksponering til eksterne systemer:** Kontortid og kontorlokasjoner kan **synkroniseres** ut ved å skru på flaggene **Overfør kontortid** og **Overfør kontorlokasjoner** på relevante systemtilkoblinger; støttes bl.a. for Dynamics-integrasjoner. Man kan også trigge **manuell oppdatering** for alle og enkeltmedarbeidere ved behov.
- **IAM-integrasjoner og automasjon:** Kontortid kommer automatisk i **Joiner/Mover**-prosessene og styrer **tilgjengelighet** i eksterne booking-/kundesystemer. Det finnes også innstilling for **automatisk fjerning av tilgang** i perioder (f.eks. før sluttføring/permisjon/avdelingsbytte) slik at ressurser ikke kan bookes feil.
- **Operativ innsikt:** Listevisninger støtter **kolonnegruppering** (f.eks. per kontorlokasjon) for rask innsikt og kontroll.

14.13.2 Hvorfor dette er unikt vs. Entra ID

- **Modellkobling:** Utnytter **innplassering i selskap/avdeling/kontor** og IdS IAM-modellen til å **tilordne standard tilgjengelighet** – noe Entra ID ikke tilbyr.
- **Integrert synk:** Innebygd mekanisme for å **overføre kontortid og kontorlokasjoner** til eksterne systemer, med manuell/planlagt oppdatering.
- **Styrt overstyring og validering:** Sentral standard + lokal fleksibilitet med validering som gjør at virksomheten unngår overlapp/feil.

14.13.3 Fordeler for virksomheten

- **Konsistent kundeopplevelse:** Like regler for åpningstider og kanaler – færre feilmeldinger, mindre støy.
- **Effektiv drift:** Én sentral kilde som mates inn i CRM/booking; mindre manuelt vedlikehold.

- **Styring i IAM-prosessene:** Kontortid blir **førsteklasses data** i Joiner/Mover/Leaver og kan styre tilgang/tilgjengelighet automatisk (inkl. sperrer rundt slutt/permisjon/flytt).
- **Transparens:** Enkle oversikter for ledere/administratorer; gruppering gir rask innsikt per sted/avdeling.

Kort sagt: IdS OfficeHoursManager standardiserer **hvem som er tilgjengelig, hvor, når og hvordan** – ved å bruke IdS IAM-modellen til å tilordne lokasjon, kontortid og kanaler, med sikker overstyring og synk til eksterne systemer.

14.14 Selvbetjent bestilling av tilgang

Brukere forventer å kunne be om tilgang **selv**, uten å vente på manuell saksbehandling – samtidig må virksomheten beholde **kontroll, godkjenning og policy-håndheving**. IdS IAM leverer selvbetjent bestilling som er tett koblet til **tilgangsnivåer**, **godkjenningsløp** og de samme **policyene** som gjelder for lederbestilling. Resultatet er kortere ventetid for brukerne og forutsigbar styring for eiere/IT.

14.14.1 Slik fungerer det i IdS IAM

- **Aktiveres per tilgangsnivå**
  Eiere kan slå på selvbetjening **for hvert enkelt tilgangsnivå** i en tjeneste. Bare de nivåene som er åpnet, blir synlige for sluttbruker.
- **To sammenflettede godkjenningsløp**
  Tjenesten har et eget **godkjenningsløp for selvbetjent bestilling** (standard: **Kun leder**). Når dette er godkjent, kjører de **ordinære godkjenningene for tilgangsnivået** (f.eks. systemeier). Med andre ord: **selvbetjent-løpet** settes **foran** det vanlige løpet – begge må passeres før tilgang tildeles. Det er selvfølgelig også mulig å fjerne godkjenning helt slik at medarbeidere kan bestille tilgang til distribusjonslisten for bedriftsidrettslaget etc.
- **Én inngang for brukeren: "Bestill tilgang"**
  Fra forsiden søker brukeren opp funksjonen **Bestill tilgang** og får en **søkbar liste** over tilgangsnivåer som kan bestilles. Listen viser bl.a. tjeneste, tittel, beskrivelse – og **status**:
  - *Tilgangen innehas* (allerede på plass)
  - *Tilgang bestilt* (sak pågår)
  - *Bestill tilgang* (kan bestilles)
- **Status og sporbarhet**
  Hver bestilling oppretter en **sak** som følger godkjenningsløpene til ferdig tildeling. Bruker og leder kan følge status fortløpende.
- **Policy og styring** (samme regler som for lederbestilling)
  Begrensninger på **selskap**, **ansettelsestype** og **avdeling** (IdS IAM-modellen/PBAC) håndheves likt – brukeren kan kun be om det vedkommende **er kvalifisert** til å motta. Dette gir konsistente beslutninger uansett hvem som initierer bestillingen.

14.14.2 Hvorfor dette skiller seg fra Entra ID alene

Entra ID tilbyr selvbetjening for **Entra-objekter** i Governance modulen.

IdS IAM leverer dette uten ekstra kostnad og utvider til **hvilket som helst system** som er integrert i IdS (on-prem, hybrid, SaaS), med **per-tilgangsnivå-aktivering**, **doble/flettede godkjenningsløp**, og

policyhåndheving fra IdS-modellen – i samme tjenestekatalog og saksløp.

14.14.3 Fordeler for virksomheten

- **Raskere tilgang – med kontroll:** Brukeren initierer selv; leder/systemeier godkjenner etter standard.
- **Konsekvent etterlevelse:** Samme policyer (selskap/ansettelsestype/avdeling) som ved lederbestilling – færre feil og avvik.
- **Lavere belastning på IT:** Eiere styrer hvilke nivåer som er selvbetjente; IdS håndterer sak, godkjenning og tildeling.
- **Transparens og revisjon:** Status per bestilling, komplett historikk og dokumentert beslutningsgrunnlag.

Kort sagt: IdS IAM gir virksomheten en moden, policy-styrt **selvbetjeningsopplevelse** som reduserer ventetid for brukere – uten å kompromittere godkjenning, kontroll eller etterlevelse.

14.15Integrasjon med HR system

For å få **korrekt tilgang ved riktig tidspunkt** må IAM ha pålitelig HR-data om hvem som starter, flytter og slutter (JML/RES), samt hvor de hører hjemme organisatorisk. I praksis finnes HR-data i mange systemer – ofte flere på samme tid – og strukturen varierer. IdS IAM leverer en **standardisert HR-importmotor** som håndterer flere kilder parallelt, bygger hele **organisasjonstreet med ledere og lokasjoner**, og driver **JML-automatisering** – direkte inn i IAM-prosessene.

For selskaper uten HR system, kan HR oppgavene knyttet til registrering, endring og sluttføring utføres direkte i IdS IAM.

14.15.1 Hva løsningen gjør

- **Støtter mange HR-systemer** ut av boksen (bl.a. **Bluegarden Paga**, **Aditro Personec**, **4human Evolution**, **Simployer**, **Zalaris**, **SD Worx**, **HLO, CatalystOne**) – samt en **standard fil-/API-profil** som kan brukes når et HR-system kan konfigureres til å eksportere på vårt format.
- **Kjører flere importer per leietaker** med ulike tidsplaner (cron), slik at f.eks. konsern, datterselskap, team og konsulentregistre kan oppdateres med forskjellig frekvens og datakilde. (Planlegging/TimerJobs og per-import schedule).
- **Bygger organisasjonen**: avdelingshierarki med **ledere**, **kontorlokasjoner** (adresse) og **stillinger** – og håndterer divisjons/forskyvningsregler når organisasjonsstrukturen endres.
- **JML/RES**: **Registrering** av **Joiners**, **Endring** for **Movers**, og **Sluttføring** for **Leavers** med riktig effektuering i identitets- og tilgangsmodellen.
- **Datavalidering og kvalitet**: Importen **validerer** og kan avdekke avvik (for eksempel medarbeidere som fortsatt får lønn etter slutt og sluttførte avdelingsledere).
- **Skrive tilbake** til HR: Felt som HR ikke er master for kan returneres til HR for konsistens. (f.eks. innloggingsnavn, e-post og jobbtelefon).

14.15.2 Oppsett

- **Felles konfig og timerjobs**: Alle HR-importer ligger under leietakers jobber med egne **elementer per kilde** (Standard, Paga, Simployer, 4human, Zalaris/SD Worx m.fl.). **Cron-uttrykk** styrer når hver import kjører. Det finnes throttling for å håndtere feilscenario f.eks. på hvor mange Joiners, Movers og Leavers det kan være per import. Det kan også settes på maks antall brukere og avdelingsfiltre for prosessering. Dette er nyttig ved igangsetting for å unngå å kjøre hele datasettet på en gang.
- **Avdelings-forskyvning**: Når HR-strukturen ikke passer, kan du definere **divisjons-/nivåsubstitusjon** (eks. flytte avdelinger ett nivå opp).
- **Ekstra attributter**: Mulighet til å sette ekstra identitets-attributter (f.eks. extensionAttributes) som del av importen – med kultur/format/regex-kontroll.

14.15.3 Enkel integrasjon av nye HR systemer

For å integrere et nytt HR-system trengs **kun selve uthentingen** (adapteren). Importmotoren spør etter data den trenger underveis (organisasjoner, ansatte, ansettelsesforhold osv.) og tar seg av resten: mapping, validering og oppretting/endring i IdS IAM. Dette reduserer tid-til-verdi betydelig ved nye kilder.

14.15.4 Mangel i Entra ID

Entra ID tilbyr ikke en **generell HR-importmotor** som kan:

- kjøre **flere** HR-kilder parallelt i samme leietaker,
- **bygge/transformere** komplett org-hierarki med ledere, lokasjoner og stillinger,
- **validere** og **berike** HR-data med egendefinerte regler,
- **skrive tilbake** HR-støttedata (innloggingsnavn/e-post/telefon) og
- eksponere dette som førstklassedata inn i **IAM-prosessene** (JML/RES) på tvers av alle tjenester.

IdS IAM gjør dette til **standard funksjonalitet** med én motor og enhetlig konfig – og bruker resultatet direkte i tilgangsmodell, roller og godkjenningsløp.

14.15.5 Effekter for virksomheten

- **Rett tilgang og identitetsattributter med en gang**: HR er kilden; IdS IAM operasjonaliserer JML uten manuelle prosesser – og hindrer «spøkelsesbrukere».
- **Enkle integrasjonsprosjekter**: Standardprofil + «kun uthenting» ved nye kilder senker kost/tid.
- **Bedre etterlevelse og sporbarhet**: Full revisjon av hva som kom fra HR, hva som ble endret og hvorfor – pr. kjøring.
- **Konsistent organisasjonsdata**: Ledere/avdelinger/lokasjoner i IdS blir én sannhet for tilgang, godkjenning og rapporter.

Kort sagt: IdS IAM sin HR-import løfter HR-data til en **styrt, validerende og flerkilde-kapabel motor** som bygger organisasjon og driver JML – en kapasitet Entra ID ikke har som ferdig, helhetlig funksjon.

14.16Mine tilganger og fullmakter

I IdS IAM får medarbeider en søkbar oversikt og sine tilganger og fullmakter på tvers av hele systemlandskapet. En slik helhetlig oversikt mangler i Entra ID.

14.17Fremtidig avdelingsendring

Når en medarbeider skal bytte avdeling, bør påtroppende leder få bestilt riktige tilganger **i forkant** slik at dette er klart til oppstart. Avtroppende leder bør vurdere overføring av ansvar og porteføljer. Uten en styrt prosess blir det lett hull i tilganger første dag, til i ansvar og porteføljer, dobbeltilganger i overgangsperioden og dårlig sporbarhet. IdS IAM løser dette med en egen **fremtidig avdelingsendring** som kobler varsling, oppgaver og automatikk inn i Mover-løpet.

14.17.1 Slik fungerer funksjonen i IdS IAM

- **Registrer endringen én gang – med effekt på dato**
  HR/leder søker opp medarbeider, velger **ny avdeling** og **endringsdato**, og huker eventuelt av at personen **tiltrer som leder** i ny avdeling.
- **Arbeidsliste over planlagte endringer**
  Alle planlagte avdelingsendringer ligger i en **oversikt** med kolonner for fra- og til-avdeling, dato, om vedkommende skal tiltre som leder, koblet henvendelse **til ny leder**, og status. Det er også mulighet for å avbryte avdelingsendringen og historikk kan vises ved behov.
- **Varsling og oppgaver settes i gang med én gang**
  Når endringen registreres, **varsles både påtroppende og avtroppende leder**. Det opprettes en **sak til ny leder** med lenke til endring av medarbeideren, slik at tilganger og eventuelle forberedelser kan bestilles i tide.
- **Bestill tilganger før første dag – styrt av IdS-modellen**
  Veiledningen til ny leder beskriver å bestille **IT-utstyr, funksjonsroller og eventuelle ekstra tilganger** før oppstart; dette reduserer risiko for at medarbeideren mangler noe dag 1. IdS IAM styrer også at **eksisterende tilganger** ikke blir med videre hvis de ikke er relevante, i tråd med least-privilege.
- **Automatisk effektuering på endringsdato**
  På dato flyttes medarbeider **automatisk** til ny avdeling selv uten HR integrasjon. N**y leder** settes og andre org-attributter oppdateres i samme operasjon. Eventuelle porteføljer/relasjoner håndteres iht. virksomhetens prosess (avtroppende leder får oppgaven på forhånd via saken).
- **Tiltre som leder**: Hvis medarbeideren skal bli leder for ny avdeling, kan dette settes allerede ved registrering, slik at org-ansvar og senere godkjenninger havner riktig fra dag 1.

14.17.2 Mangler i Entra ID

Entra ID har ikke en helhetlig **planleggings- og oppgaveflyt for avdelingsbytte** som:

- registrerer *fremtidig* org-endring,
- varsler ny/avtroppende leder med **lenket sak**,
- og **effektuerer** selve avdelingsendringen automatisk på dato – samtidig som avtroppende og påtroppende leder får en styrt bestillingsprosess for nødvendige tilgangsendringer. IdS IAM leverer dette som standard del av Mover, tett koblet til **org-hierarki, lederlinje, tjenester/tilgangsnivåer og godkjenningsløp**.

14.17.3 Fordeler for virksomheten

- **Medarbeider operativ dag 1:** Ny leder får oppgaven tidlig og kan bestille alt før oppstart.

- **Mindre risiko og støy:** Relevante tilganger bestilles på forhånd; irrelevante blir ikke "med på lasset".
- **Null manuelt "husk å utføre på dagen":** Selve org-flyttingen skjer automatisk på dato, med sporbarhet.
- **Forankret i linjen:** Varsler og oppgaver går til riktige ledere – ikke til IT-køen.

Kort sagt: Fremtidig avdelingsendring gjør Mover-prosessen forutsigbar: varsler sendes når de skal, bestillingene skjer i forkant, og flyttingen **effektueres automatisk** på riktig dato. Det er en praktisk funksjon Entra ID ikke tilbyr.

14.18Kompetanse

Mange tilganger bør bare gis når medarbeideren har **dokumentert kompetanse** (opplæring, sertifisering og sikkerhetskurs). Uten en styrt mekanisme ender man med manuelle kontrollspørsmål og varierende praksis. IdS IAM lar deg **modellere kompetansekrav som en del av tilgangsstyringen**, koblet til både tjenester og konkrete tilgangsnivåer – med gyldighet, dokumentasjonskrav og automatisert (eller låst) håndheving.

14.18.1 Slik fungerer det i IdS IAM

- Opprett en **opplæringstjeneste** som administrerer **kurs og kompetanse** (medarbeider med kurs)**.** Kompetanse kobles som krav til andre tjenester/tilgangsnivåer.
- Kurs registreres omtrent som et tilgangsnivå, men har feltene:
  – **Må dokumenteres?** (krever opplasting/vedlegg)
  – **Gyldighetsrom (måneder)** (automatisk utløp/fornyelse)
  – **Overstyringstype for krav** = *Automatisk* / *Manuell* / *Låst*
  Automatisk tildeler tilgang uten å vente på kompetansekravet blir oppfylt. *Manuell* krever godkjenning dersom tilgangen skal gis uten at kompetansekravet er oppfylt. *Låst* blokkerer tilgangen til kravet er oppfylt uten mulighet for manuell overstyring.
- Fra kursbildet velger du **Tilgangsnivåer som krever [kurs]** og/eller **Tjenester som krever [kurs]**. Når dette er lagret, håndhever IdS kravet ved bestilling og vedlikehold av tilgang.
- Under "Mine funksjoner" finnes oversikter for **roller med kompetansekrav**, **medarbeideres kompetanse** og **kompetansemangler** (for ledere og andre med innsyn).
- Krav kan håndheves med **godkjenningsløp** – f.eks. *Selvbekreftelse* av kursdeltagelse med stegtypen "Den som skal få tilgangen", eventuelt ekstra ledersteg. E-postinvitasjon inneholder lenke til bekreftelse i ServiceManager; etter bekreftelse tildeles tilgangen automatisk.

14.18.2 Eksempel

Etasjeansvarlig krever kurs i brannsikkerhet. Når leder legger inn tilgang "Etasjeansvarlig", får medarbeideren e-post: "Bekreft at du har tatt kurset …". Ved bekreftelse (eller vedlagt dokumentasjon hvis påkrevd) godkjennes henvendelsen og tilgangen aktiveres. Kravet kan settes til å **utløpe** (f.eks. 24 mnd) – da må kurset fornyes før rollen beholdes.

14.18.3 Mangler i Entra ID

Entra ID har ikke en egen **opplæringstjeneste** eller en modell for **kompetanse som krav** med gyldighet/dokumentasjonskrav knyttet direkte til tilgangsnivåer. Du kan riktignok bygge manuelle godkjenninger i access packages, men du får ikke:

- kurs som førsteklasses objekter med **utløp**, **dokumentasjon** og **overstyringstype**
- **avhengigheter** fra kurs → tilgangsnivå/tjeneste
- standardiserte **oversikter over kompetansemangler** i linjen.

14.18.4 Fordeler for virksomheten

- **Etterlevelse i praksis:** Tilganger gis først når **krav er oppfylt** – dokumentert, sporbart og klart for revisjon.
- **Automatisk fornyelse/avvikling: Gyldighetsrom** sikrer at utløpte kurs trigger fornyelse, ellers faller tilgangen/graden tilbake iht. policy.
- **Mindre manuelt arbeid:** *Automatisk* eller *låst* håndheving reduserer saksbehandling og feil.
- **Transparens for ledere:** Oversikter for **kompetansekrav** og **mangler** gjør det lett å lukke gap før revisjon.

Kort sagt: IdS IAM gjør kompetanse til en **del av tilgangsmodellen** – ikke en e-post ved siden av. Krav defineres én gang, kobles til tilgangsnivåer og håndheves konsekvent med gyldighet, dokumentasjon og arbeidsflyt.

14.19Ekstern prosessering i webhooks

Ikke alle oppgaver bør eller kan utføres av IAM-plattformen selv. Ofte finnes det **fagteam, mikrotjenester eller scripts** som allerede gjør jobben best (DNS-endringer, oppdatering i fagsystemer, dokumentgenerering, osv.). Med **webhooks** kan IdS IAM sende bestillingen trygt til et eksternt endepunkt, **vente på svaret**, og **logge resultatet inn i saken** – uten skreddersøm inne i IdS. Dette gir raskere utrulling, mindre låsing, og ryddig ansvarslinje mellom IAM og de som eier prosessen.

14.19.1 Slik fungerer webhooks i IdS IAM

- **Slå på webhook per tjeneste**
  I tjenesteinnstillingene velger du *webhook* og fyller en **startkonfigurasjon**. IdS støtter **signering**, **egendefinerte HTTP-headers**, **properties** (JSON-datafelt i body) og **querystring-parametre** – med mulighet for **kryptering** av sensitive verdier.
- **Sikkerhet by design**
  Verdier merket encrypted="true" lagres kryptert og vises aldri ukryptert. Endrer du **URL** må krypterte felt legges inn på nytt (hard sikkerhetsgaranti).

Webhook-requests kan **signeres** med HTTP Signature; IdS legger en Signature-header (med keyId) som mottaker kan verifisere. Eksempler og verifiseringssnutt finnes for flere språk tilgjengelig i GitHub.

- **Krav til mottaker (robust drift)**
  1. Endpoint må **utføre operasjonen** og returnere **HTTP 200 OK** når bestillingen er akseptert/utført.
  2. Mottaker må være **idempotent** (tåle re-forsøk).
  3. Ved feil skal den **ikke** svare 200; IdS setter saken i **«venter på ekstern part»**. Systemet **forsøker på ny automatisk**. Detaljer om feilen kan sees på saken i IdS IAM.
- **Skjema → data i request**
  Felter fra bestillingsskjemaet kan mappes inn i **body** (properties), **querystring** og til og med i

URL. UI-en tilbyr praktisk "**Koder**"-innsetting av felt fra IdS IAM modellen (f.eks. UPN, Department, egendefinerte felter).

- **Asynkron kjøring og sporbarhet**
  IdS sender til webhook **asynkront** via jobb i tidsplan. Saken viser status **"Venter på utføring av ekstern part"** til svar kommer, og responsen legges i saken. Korrelasjons-ID anbefales; for Azure Functions kan **Invocation Id** slås opp i **Application Insights**. Det finnes direkte lenke fra sak til jobb for å se detaljert kjørestatus.

14.19.2 Designmønster

1. **Bygg skjema** i IdS med feltene du trenger.
2. **Konfigurer webhook**: URL, headers, signering, hvilke felt som sendes (body/query).
3. **(Valgfritt)** Kjør bestilling gjennom **godkjenningsløp** før utsendelse.
4. **Prosesser eksternt** og svar **200 OK** med korrelasjons-ID.
5. **Logg og etterprøv**: se responsen i saken, følg jobben i Hangfire/Insights.

14.19.3 Hva dette gir virksomheten

- **Modulær arkitektur**: bruk eksisterende scripts/tjenester uten å "bygge inn alt i IAM".
- **Sikker integrasjon**: krypterte konfig-verdier + **HTTP-signatur** på alle kall.
- **Rask utrulling**: ny prosess = nytt skjema + enkel webhook-konfig, ikke ny konnektor.
- **Sporbarhet i én sak**: IdS viser status, lagrer respons, og lenker til jobb-/telemetri.
- **Feiltoleranse**: idempotenskrav, tydelig feilstatus og automatisk/manuell nye forsøk.

Kort sagt: Webhooks gjør IdS IAM til en **orkestrator**: du beholder styring, godkjenning og sporbarhet i IdS – mens **selve jobben** utføres av riktig eksternt system, sikkert signert og med full innsikt i hva som skjedde.

15 GRC og administrative tjenester støttet av IdS IAM

Forrester påpeker at **GRC** (Governance, Risk and Compliance) og **IAM/IGA** har et **symbiotisk forhold** der samlet innsats gir større gevinst enn om de opererer hver for seg. Når retningslinjer for risikohåndtering og etterlevelse definert av GRC knyttes direkte til identitetsforvaltningen, kan riktige **tilgangsrettigheter** tildeles og fjernes i tråd med policy – støttet av automatiserte prosesser som revisjonsrunder og **separation of duties**-kontroller for å forhindre rollekonflikter. En slik felles IAM-plattform gir et **felles datagrunnlag** (*"single source of truth"*) for roller, tilganger og kontrollmekanismer i hele virksomheten. Dette skaper konsistente prosesser, bedre oversikt og reduserer risiko for feil eller uregelmessigheter. Forrester understreker dessuten at regelverksetterlevelse ofte er en hoveddriver for investering i IAM – mange virksomheter anskaffer identitetsstyringsverktøy først etter å ha fått avvik i revisjon. Ved å **integrere GRC og IAM** fra starten av unngår man slike «panikktiltak» i etterkant; i stedet bygges etterlevelse og risikokontroll inn proaktivt. **Resultatet** er en lavere risikoprofil, mer strømlinjeformet etterlevelse av krav, samt styrket styring og kontroll – fordi GRC-teamets policyer automatisk omsettes i praksis gjennom IAM-systemets livssyklusprosesser og tilgangskontroller, i én helhetlig og sikkerhetsstyrt plattform.

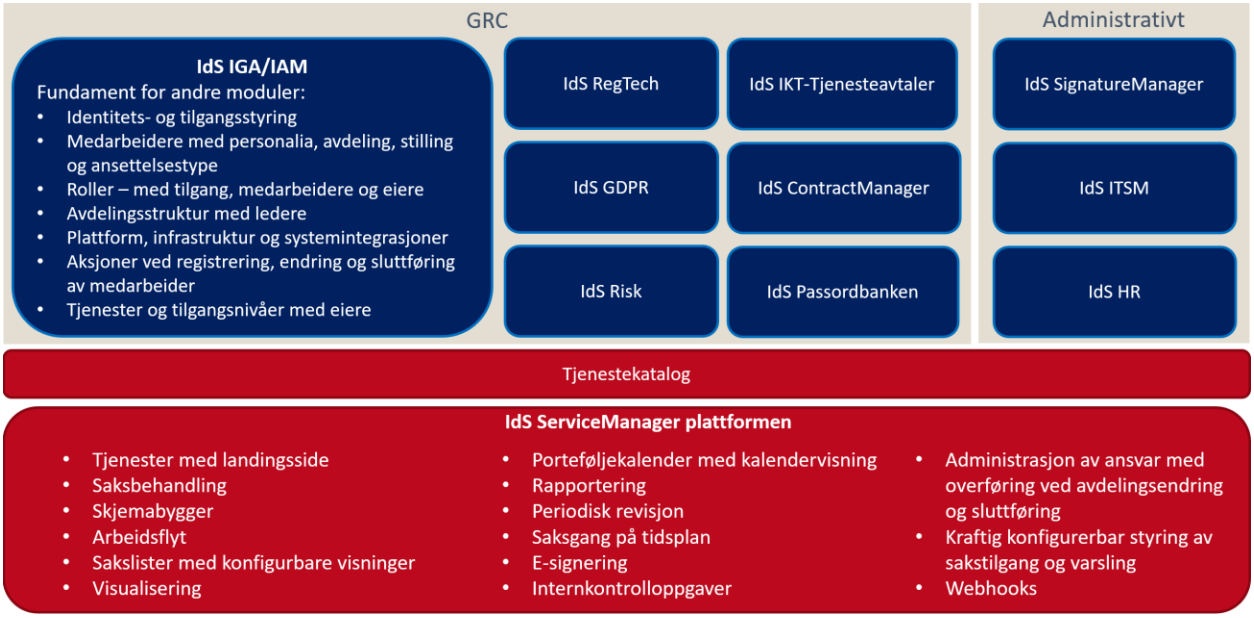
15.1 IdS IAM som fundament for styring og kontroll

IdentityStream IdS IAM danner et solid fundament for virksomhetens styring, risiko og etterlevelse (GRC) samt ulike administrative støttefunksjoner. Hele IdentityStream-økosystemet er bygget rundt identitets- og tilgangsmodellen i IdS IAM, noe som betyr at **alle moduler deler samme autoritative identitetsgrunnlag**. Dette gir *én samlet løsning* med innebygget støtte for GRC og administrative tjenester. IdS IAM fungerer som en **sentral kilde til sannhet** for hvem som er hvem i organisasjonen, hva deres rolle er, hvem de rapporterer til, og hvilke tilganger de har. På denne måte kan tverrfaglige moduler hente sine tilgangsregler og autorisasjoner direkte fra IAM-modellen, i stedet for å operere med isolerte siloer av varierende datakvalitet.

Strategiske fordeler: Ved å la GRC- og administrative systemer bygge på IdS IAM oppnår man:

- **Helhetlig sikkerhet:** Felles identitetsmodell sikrer at tilgangsstyring er konsistent på tvers av *alle* moduler. Bare autoriserte personer får innsyn i sensitive saker, og dette styres sentralt via definerte roller, lederhierarki og tilgangsnivå. Sikkerhetsnivået blir høyt og enhetlig fordi samme policyer gjelder overalt.
- **Innebygd kontroll og sporbarhet:** Alle endringer – om det er nye tilganger, endring av eierskap for en kontrakt, registrering av en risiko, eller opprettelse av en HR-sak – logges med kontekst i IdS IAM. Det finnes et komplett revisjonsspor knyttet til identiteten og hendelsen, slik at man i ettertid kan se *hva* som skjedde og *hvorfor*. Dette gir full oversikt for revisjon og etterlevelse.
- **Dynamikk og automatisering:** Siden modulene bruker IdS IAM som motor, kan rettigheter og ansvar *automatisk* justeres ved organisasjonsendringer. Når en ansatt bytter avdeling eller rolle, vil systemet automatisk oppdatere både IT-tilganger **og** tilhørende rettigheter i GRC- og administrative moduler – uten manuelt merarbeid. Dette gir en dynamisk løsning der tilgangene alltid er tilpasset organisasjonens til enhver tid gjeldende struktur.

Figuren under viser samspillet der alle moduler bygger på IdS ServiceManager plattformen og de øvrige modulene kan bygge videre på datagrunnlaget fra IdS IAM modulen.



15.2 Automatiske innsyn og dynamiske rettigheter gjennom IAM-modellen

En kjernefunksjon i IdS IAM er utnyttelsen av **lederhierarkiet og rollekonseptet** for å styre rettigheter. Fordi IdS IAM forstår virksomhetens organisasjonskart – inkludert avdelinger, team og hvem som leder hvem – kan denne strukturen benyttes til å tildele innsyn og oppgaver automatisk. For eksempel kan en avdelingsleder per definisjon ha en form for eierskap til det som foregår i sin avdeling, konfigurerbart per innsynsområde på tjenester som Hendelsesdatabasen. Ledere kan automatisk få tilordnet oppgaver som godkjenning av tilganger, gjennomgang av risikoer, eller oppfølging av hendelser for medarbeiderne og avdelingene de har ansvar for. Dette skjer uten at IT-avdelingen manuelt må administrere tilgangene – IAM-modellen sørger for forankring i eksisterende struktur, slik at beslutninger tas av dem som har formelt ansvar og innsikt.

Denne **rolle- og hierarkiforankringen** forsterker verdien i modulene på to måter: For det første øker det **lokalt eierskap og ansvarliggjøring**. Linjeledere og utpekte eiere tar aktiv stilling til risikoer, kontrakter og hendelser innenfor sitt område, noe som skaper en sterk ansvarskultur. For det andre sikrer det **kontinuitet og oppdatert tilgang**: IdS IAM sin ansvarsmodul passer på at alle oppgaver og eierskap alltid er knyttet til noen med gyldig tilknytning. Hvis en nøkkelperson slutter eller flytter på seg, trigges en kontrollert overføring av ansvar. Systemet vil for eksempel kreve at en avtroppende medarbeider får overført ansvaret til en annen, godkjent av riktig nivå i organisasjonen. Ledere blir også proaktivt varslet hvis en ansatt med ansvar skal slutte eller gå i permisjon, slik at de kan omfordele oppgaver i tide. Summen av dette er at ingen kritiske saker, kontrakter eller risikoer havner i et ingenmannsland – ansvaret er alltid plassert hos en gjeldende rolle/person, noe som reduserer risiko betydelig og gjør det enklere å opprettholde samsvar.

15.3 Unik posisjon kontra Microsoft Entra ID

Det er verdt å merke seg at **Microsoft Entra ID** – til tross for sin utbredelse som identitetsplattform – ikke tilbyr noe tilsvarende helhetlig økosystem som IdentityStream. Entra ID fokuserer primært på basis identitets- og tilgangsstyring og har ikke innebygde GRC eller administrative tjenester, For eksempel finnes ingen mekanisme i Entra ID som automatisk gir avdelingsleder innsyn i en sikkerhetshendelse, eller som overfører eierskap ved fratredelse – dette måtte i så fall løses manuelt eller via tredjepart. Kort sagt: **Ingen direkte sammenligning finnes i Entra ID** – IdentityStream sin integrerte tilnærming gir en betydelig strategisk fordel i markedet.

Denne strategiske fordelen viser seg i praksis som **mer effektiv styring og bedre etterlevelse**.

15.4 Risiko vs. gevinst ved integrert IAM–GRC

Å integrere IAM med GRC- og administrative løsninger kan reise enkelte spørsmål rundt sikkerhet. Et mulig ankepunkt er at en så tett integrasjon betyr at **mye ansvar samles i ett system** – dersom IdS IAM-plattformen skulle kompromitteres, kan man frykte bredere konsekvenser siden den har nøkkelroller i både tilgangsstyring og etterlevelsesprosesser. Det er også viktig å håndtere tilgangskonfigurasjonene nøye, slik at ikke kombinasjonen av data fører til utilsiktet innsyn (f.eks. at en leder får se en personalsak han ikke burde se).

Mitigering av risiko: IdentityStream har adressert disse hensynene gjennom streng tilgangskontroll og rolleavgrensning i systemet. Hver modul bygger på prinsipper som minste privilegium og fire-øyne-godkjenning på kritiske operasjoner. Det betyr at selv om modulene er integrert, har brukerne kun den tilgangen de skal ha, og sensitive endringer krever involvering av to parter eller ekstra godkjenning. Testing, logging og overvåking er gjennomgripende, slik at uregelmessigheter kan oppdages raskt. På den måten beholder man fordelene ved en felles plattform uten å ofre sikkerhet.

Konklusjon – betydelig gevinst: Fordelene ved å la IAM være navet som GRC og administrasjonsmoduler spinner rundt, **oppveier klart de potensielle risikoene**. Den integrerte modellen gir bedre sporbarhet, sterkere ansvarliggjøring av ansatte og ledere, og et rikere datagrunnlag for regelverksetterlevelse og rapportering enn silo-løsninger gjør. Man unngår manuelle mellomledd og "skyggesystemer", og alt knyttes tilbake til en felles identitetsplattform. I praksis betyr det færre feil, høyere effektivitet, lavere driftskostnader og en felles sikkerhetsmodell som er *innebygd* i alle tjenestene. For en virksomhet med strenge krav til kontroll og fleksibilitet, vil en IdS IAM-støttet løsning for GRC og administrasjon dermed gi et robust konkurransefortrinn – **en helhetlig styring hvor rett person til rett tid har rett tilgang og ansvar**.

16 Alliance-Tenant og Standardisering i IdS IAM

Alliance-tenancy i IdentityStream ServiceManager-plattformen innebærer at flere organisasjoner (leietakere) kan operere som en samlet allianse innen én felles IAM-løsning. Hver virksomhet beholder sin egen **leietaker** (tenant) i løsningen, men de er satt opp til å stole på hverandre under et felles styringsregime. Dette muliggjør tett samarbeid på tvers av selvstendige enheter som deler **identitets- og tilgangsstyring**. For eksempel kan sentrale funksjoner hos en alliansepartner få nødvendige tilganger i andre medlemsvirksomheter på en kontrollert måte, takket være denne delte tilliten. Alliance-tenancy skaper dermed et tryggere fellesskap av leietakere, der **standardiserte regler og prosesser** for identitetstilgang gjelder på tvers av alle deltakerne. Resultatet er en koordinert administrasjon av brukere, roller og rettigheter som *fungerer på tvers av virksomhetsgrenser uten å kompromisse sikkerhet*.

16.1 Mal-leietakere og felles oppsett for tilgangsstyring

En kjerneidé i alliansemodellen er bruken av **mal-leietakere** – også kalt *"standardbanker"* i bankallianser. Disse fungerer som et felles oppsett av roller, tjenester, tilgangsnivåer og risikoregler (SoD) som alle medlemmene i alliansen skal følge. IdentityStream har utviklet en løsning der en eller flere mal-leietakere inneholder det autoritative oppsettet for tilgangsstyring. Roller, grupper, applikasjoner og regler defineres én gang i malen og synkroniseres deretter ut til leietakerne i alliansen.

Dette betyr at hvis alliansen gjennomfører en endring – f.eks. innfører en ny rolle eller justerer en risikoregel – vil endringen propageres konsistent til alle medlemsenheter. Den sentrale malen utgjør et **"lager" av standardkonfigurasjoner** som kontinuerlig forbedres og distribueres til alle banker eller organisasjoner. Hvert medlem får et identisk grunnoppsett for IAM, noe som sikrer en **ensartet tilgangsstruktur** i hele alliansen. Alliansestøtten i IdS gjør også at man kan delegere administrasjon på tvers: eksempelvis kan alliansen sitt sentrale IT-team få umiddelbar tilgang til lokale systemer i hver av leietakerne i alliansen.

Denne malbaserte modellen er sporbar og transparent, noe som forenkler både internkontroll og tilsyn fra myndigheter.

Det er viktig å merke seg at **lokal fleksibilitet** fortsatt ivaretas. Hver enkelt leietaker kan supplere med egne, lokale roller eller tilganger der det er særbehov. Slik kan en virksomhet legge til spesialtilganger for sine egne systemer, uten å bryte ut av den standardiserte strukturen alliansen har satt. Hver enkelt leietaker kan også velge bort deler av oppsettet fra standarden. Summen av dette er en harmonisert tilgangsmodell på tvers av alle enheter i konsernet eller bankalliansen.

16.2 Gevinster ved standardisering gjennom alliansemodellen

Den malbaserte allianse-tenancy modellen i IdS IAM gir en rekke forretningsgevinster for konsern og samarbeidsallianser:

- **Skalerbarhet og ensartet tilgangsstruktur:** Når alle enheter er satt opp likt, blir det mye lettere å skalere opp eller endre organisasjonen uten friksjon. Nye applikasjoner og systemer kan sømløst rulles ut i eksisterende infrastruktur for alle medlemmer samtidig. Organisasjoner kan dermed vokse og omstille seg uten større forstyrrelser. Et konkret eksempel fra Eika Alliansen er at alle ~50 lokalbankene nå er likt utstyrt med de *samme systemene og rollestrukturene*, noe som gir store fortrinn ved at support og IT-støtte kan standardiseres og gå raskere. Plattformen støtter også at Eikas sentrale kundesenter kan administrere svært mange ansatte parallelt og likevel beholde full kontroll over tilganger på tvers av alle banker.
- **Redusert administrasjonsbyrde og kostnad:** Standardisering og integrasjoner eliminerer mye manuelt arbeid og dobbeltregistrering, noe som gir direkte kostnadsbesparelser.

  I Eika alliansen måtte tidligere hver bank bruke ressurser på egen tilgangsadministrasjon og support, gjerne med ulik praksis. Med felles IAM-plattform slipper man denne *fragmenteringen*. Eikas caset viser at ved å sentralisere identitetsstyringen har de lokale IT-ressursene fått frigjort betydelig tid – koordinering og rutineoppgaver er kraftig redusert, og man anslår store samlede gevinster i form av sparte timer. Ansatte i IT og brukerstøtte kan nå fokusere mer på strategiske, verdiskapende aktiviteter fremfor repetitive oppgaver.
- **Konsistent sikkerhet og revisjonsklarhet:** Når alle enheter følger samme sikkerhetsmodell, blir det enklere å holde oversikt og oppfylle regulatoriske krav.

16.3 Dele ressurser

Utgangspunkt. Hver IdS IAM-leietaker er en separat sikkerhetssilo, også når den inngår i en allianse. Alliansemodus åpner for kontrollert deling – ikke sammensmelting – av ressurser på tvers av leietakere.

16.3.1 Prinsipper

- **Isolasjon først:** Tjenester og roller forblir per leietaker.
- **Minste privilegium:** Del bare det som er nødvendig, og bare med utvalgte leietakere.
- **Transparent styring:** Alle delingsbeslutninger er sporbare, reverserbare og kan revideres.

16.3.2 Delingsmåter

IdS IAM støtter to komplementære modeller for deling i alliansemodus:

1. **Tillate eksterne brukere per tjeneste/rolle**
   Leietaker A kan gi brukere fra leietaker B medlemskap i A's tjenester og roller.
   - **Sikt/innsyn:** B ser ikke A's tjenestekatalog eller roller; A eksponerer kun selve tilordningen til eksterne brukere.
   - **Delingskontroll**: A kan begrense hvilke leietakere sine brukere som gis tilgang til tjeneste (tillatelsesliste). Uten begrensning kan alle i alliansen gis tilgang.
   - **Brukstilfelle:** Rask, målrettet tilgang uten å publisere katalogobjekter.
2. **Publisere en tjeneste til andre leietakere**
   Leietaker A kan gjøre en tjeneste synlig i andre leietakeres katalog (lister, relaterte tjenester, søk m.m.).
   - **Innbygging:** Mottakende leietaker kan bygge tjenesten inn i egne roller og tilordne den som ekstra tilgang til egne brukere.

- **Synlighetskontroll:** A kan begrense hvilke leietakere som ser tjenesten (tillatelsesliste). Uten begrensning blir den synlig for alle i alliansen.

16.3.3 Gjesteoverføring (guest access transfer)

For delte tjenester kan A aktivere **overføring til gjest**:
Når en bruker i B får tilgang til en tjeneste i A, gis tilgangen i stedet til en korresponderende **gjestebruker** i A. Dette kan f.eks. brukes i scenarioer der A og B har hver sin leietaker i Entra ID og brukere i B har fått opprettet gjestebruker i A samt at A har en del Entra ID tjenester i IdS IAM som brukere i B skal ha tilgang til.

- **Effekt for ledere:** Tilordningen fremstår som en vanlig tilgang til egen medarbeider i B; det er «gjennomsiktig» at en gjest i A mottar den faktiske tilgangen.
- **Fordel:** Forenkler livssyklus i A og sikrer at alle rettigheter i tjenestens hjemleietaker er knyttet til lokale (gjeste-)objekter.

16.3.4 Roller som oppdragsgrupper på tvers

Leietaker i alliansemodus kan tillate at **egne roller** brukes som **oppdragsgrupper** i andre leietakere. Dette er nyttig når en sentral leietaker (fellesfunksjoner) definerer standardroller som andre leietakere kan referere til på sine tjenester.

- **Fordel:** Reduserer duplisering, sikrer konsistente definisjoner og forenkler delegert forvaltning.

16.3.5 Styring og etterlevelse

- **Godkjenning:** Konfigurer tydelige godkjenningsflyter for inter-leietaker tilordninger og publisering.
- **Revisjon:** Alle delingshendelser og tilordninger logges per leietaker og kan eksporteres for etterlevelse.
- **Livssyklus:** Tilgang følger kildens ansettelses- og rolleendringer; opphør i én leietaker utløser automatisk rydding i den andre.
- **Dataegenskaper:** Delingsmekanismer endrer ikke dataenes domene; data behandles i tjenestens hjemleietaker.

16.3.6 Når velge hva?

- **Trenger du rask tilgang uten katalogsynlighet?**
  Bruk *eksterne brukere per tjeneste/rolle*.
- **Vil du gjenbruke tjenester i andres katalog og roller?**
  Publiser tjenesten, eventuelt med *gjesteoverføring*.
- **Ønsker du standardisering av tilgangsgrupper på tvers?**
  Bruk *roller som oppdragsgrupper* fra en sentral leietaker.

Kort oppsummert: Alliansemodus beholder sikkerhetssiloene, men gir presise, revisjonsvennlige koblinger mellom dem – fra enkel tilordning, via publisering med gjesteoverføring, til felles oppdragsgrupper.

16.4 Delt Microsoft Entra ID med Administrative Units

Alliansemodellen strekker seg også til integrasjonen mot **Microsoft Entra ID**. IdS IAM kan orkestrere en løsning der flere leietakere i alliansen **deler én felles Entra ID leietaker**, men avgrenser tilganger og administrasjon via Microsoft konseptet *Administrative Units (AU – Microsoft Entra-funksjon for delegering*

av administrasjon). En AU i Entra ID er et logisk container-objekt som grupperer brukere, grupper og enheter, og lar administratorer få delegert kontroll kun over den definerte delen av organisasjonen. Med IdS IAM kan man ha én felles Entra ID for en hel allianse, men likevel gi hver leietaker sine egne administratorroller som bare har effekt innenfor sin tildelte **AU**. Dermed oppnås en silo-effekt internt: hver leietaker har kun tilgang til sine egne brukere og ressurser, selv om de teknisk ligger i samme Entra ID leietaker. I praksis får hver leietaker kontroll over egne ressurser i Microsoft 365-miljøet sitt – men slipper å ha en separat Entra ID. Fra et sikkerhetsperspektiv er dette gunstig: man har færre leietaker å forvalte (reduserer kompleksitet og angrepsflate), samtidig som *prinsippet om minste privilegium* opprettholdes ved at hver leietaker bare kan endre det som angår egen virksomhet. Administrasjonsmessig forenkles også hverdagen, fordi nye brukere, grupper eller rettelser som gjøres via IdS IAM automatisk havner under korrekt AU. IdentityStream har laget dype integrasjoner med Entra ID nettopp for slike scenarioer – å automatisere oppgaver i skyen der standard Microsoft 365 ikke strekker til. For en allianse betyr dette **bedre sikkerhet og enklere forvaltning**: Felles Entra ID gir enhetlig policyhåndhevelse og synlighet, mens AUs sørger for nødvendig isolasjon mellom medlemmene.

16.5 Ulikheter fra Microsoft Entra ID alene

Det er verdt å understreke hvordan denne alliance-tenancy modellen skiller seg fra å bruke Microsoft Entra ID på konvensjonelt vis uten et verktøy som IdS IAM. Entra ID er i utgangspunktet laget for én enkelt virksomhet. Har man flere juridisk adskilte virksomheter, finnes det ingen innebygd mekanisme i Entra ID for *malbasert distribusjon* av oppsett mellom dem – hver må tradisjonelt sett administrere sine egne grupper, applikasjoner og roller manuelt. Det er ingen støtte for et "alliansehierarki" hvor man kan gjenbruke strukturer på tvers på en strukturert måte. I praksis må hver virksomhet bygge opp sine IAM-objekter selv, eller man må ty til skripting og tredjepartsverktøy for å holde flere Entra ID leietakere synkronisert.

Selv om Microsoft de senere år har innført enkelte funksjoner for **multitenant management** (som Azure Lighthouse, Cross-tenant Sync, etc.), er det fortsatt langt unna den helhetlige alliansemodellen IdS tilbyr. For eksempel, om man via Entra prøver å samle flere selskaper i én tenant uten et IAM-lag, vil man typisk slite med manglende rolleisolasjon og ingen automatisk måte å distribuere felles oppsett. Hver bedrift risikerer å måtte gjøre samme jobb om igjen – definere de samme gruppene, tildele rettigheter til de samme applikasjonene – i hver sin silo. Det finnes ingen **strukturert gjenbruk** eller felles sikkerhetsmodell ut-av-boksen i Entra ID som kan sammenlignes med mal-leietaker i IdS IAM. Alliance-tenancy lukker dette gapet ved å tilby et styringslag oppå Entra ID som orkestrerer en felles sikkerhetsarkitektur på tvers. Forskjellen kan oppsummeres slik: Med standard Entra ID er man overlatt til fragmentert administrasjon per leietaker, mens med IdentityStream får man *én felles plattform* der standarder settes sentralt og automatisk slår gjennom hos alle.

Konklusjon: Alliance-tenancy og standardisering i IdS IAM representerer et viktig konkurransefortrinn for virksomheter med mange enheter, enten det er konsern, sparebank-allianser eller andre samarbeidende grupper. Det gir mulighet til å **styre identitets- og tilgangsforvaltning på en helhetlig måte**, med klare stordriftsfordeler: lik struktur, mindre kostnad, bedre etterlevelse og samtidig lokal fleksibilitet. I en tid der digitale trusler øker og regulatoriske krav strammes inn, kan en slik modell gjøre hele forskjellen for å holde kontroll og kostnader nede – effektivt, sikkert og skalerbart – på tvers av en mangfoldig organisasjon.

17 IdS IAM – et strategisk valg for moderne tilgangsstyring

IdentityStream IdS IAM kompletterer Microsoft Entra ID ved å levere den avanserte identitetsstyringen, kontrollen og dokumentasjonen som moderne regulativer forventer. Som helhetlig IAM-plattform

skreddersydd for strenge krav, gir IdS IAM virksomheten full oversikt, automatisert etterlevelse og bedre kostnadskontroll – uten behov for å oppgradere til dyreste Entra-lisensnivå. Tabellen under oppsummerer noen sentrale forskjeller og fordelene IdS IAM tilfører sammenlignet med Entra ID alene:

Område	IdentityStream IdS IAM	Microsoft Entra ID
Regulatorisk etterlevelse	Oppfyller krav i DORA, NIS2 m.fl. med full **kontroll på tilganger** og dokumentasjon. Bygger inn etterlevelse *by design*.	Dekker kun **grunnleggende** identitetsadministrasjon. Mangler funksjoner for komplett internkontroll; krever manuelle tiltak for å oppnå samsvar.
Livssyklus & automasjon	**Automatiserte livssyklusprosesser** (Joiner-Mover-Leaver) og arbeidsflyt ut-av-boksen som sikrer riktige godkjenninger til rett tid. Rask utrulling med ferdige integrasjoner og beste praksis-prosesser.	Ingen innebygde IAM-prosesser for livssyklus. **Manuelle rutiner** og skript må brukes for å administrere tilganger over tid. Implementering av avansert styring krever eksterne verktøy eller tilpasninger.
Sporbarhet & kontroll	**Fullt revisjonsspor** for alle tilgangsendringer med kontekst og begrunnelser. Støtte for *Separation of Duties* (SoD) regler som forhindrer risikofylte tilgangskombinasjoner og fanger opp brudd automatisk. Sentral kilde til sannhet for identiteter gir konsistent policy-håndhevelse.	**Begrenset logging** – mangler kontekst og begrunnelser for endringer. Begrenset SoD-kontroll; potensielle rollekonflikter må oppdages manuelt. Policy-håndhevelse fragmentert på tvers av systemer uten et felles IAM-verktøy.
Lisens- og kostnadsstyring	**Automatisk lisensstyring** identifiserer ubrukt/overflødig tilgang og stopper uautoriserte lisens-tildelinger. Kan sette lisenser på pause ved permisjoner etc. for å kutte kostnader. Gir ledelsen oversikt over hvem som bruker dyre lisenser.	**Ingen lisensoptimering:** Har ingen funksjonalitet for å oppdage ubrukte lisenser eller optimalisere lisensforbruk. Ubrukte eller kostbare tilganger må følges opp manuelt uten støtteverktøy, med risiko for unødige kostnader.
Implementering & integrasjon	Leveres med **bredt utvalg konnektorer**, inkl. tett integrasjon med Entra ID, og minimal innsats for å lage nye. "Opinionated" standarder og beste praksiser gir rask implementering og lav driftsbelastning.	**Standard Entra ID** er primært en identitetsplattform; utvidet IAM-funksjonalitet krever separat implementering (f.eks. Entra ID Governance P2 eller tredjepart). Mer *skreddersøm* trengs for tilsvarende funksjoner.

Som tabellen illustrerer, leverer IdS IAM et rikere sett med identitetsstyringsfunksjoner enn det Entra ID alene tilbyr. For en virksomhet betyr dette at man kan oppnå sterkere sikkerhet og etterlevelse, samt effektiviseringsgevinster og kostnadsbesparelser, **uten** å måtte ty til manuelle kontrollrutiner eller dyre oppgraderinger. En slik helhetlig plattform gir beslutningstakere trygghet for at identitets- og tilgangsforvaltningen er under kontroll, revisjonssikker og fremtidsrettet. Avslutningsvis står IdS IAM frem

som et strategisk godt valg for organisasjoner som ønsker å ligge i forkant av både sikkerhetskrav og regulatoriske krav – et valg som muliggjør proaktiv styring fremfor reaktiv brannslukking.