Ekstern gjennomgang av Arbeids- og velferdsdirektoratets systematiske arbeid med internkontroll knyttet til IKT

Endelig rapport

Oppdragsgiver: Arbeids- og inkluderingsdepartementet (AID)

Utførende: KPMG AS

Dato: 26.06.2026

Sammendrag

Arbeids- og inkluderingsdepartementet (AID) har engasjert KPMG til å evaluere Arbeids- og velferdsdirektoratets arbeid med internkontroll knyttet til utvikling, drift og forvaltning av IKT. For en virksomhet der måloppnåelsen er tett integrert med IKT må internkontrollen ses som en del av virksomhetens helhetlige styringssystem, ikke som et separat spor. Dette ligger til grunn for KPMGs vurderinger og anbefalinger.

Direktoratet forvalter et samfunnskritisk oppdrag, der korrekt og sikker bruk av IKT er avgjørende for regelverksetterlevelse, pålitelig rapportering og tillit. Samtidig er IKT-porteføljen omfattende og kompleks, med over 550 systemer, rundt 120 produktteam, høy grad av egenutvikling og betydelig innslag av legacy-løsninger. Dette stiller høye krav til en helhetlig, operativ og risikobasert internkontroll.

KPMG vurderer samlet modenhet i internkontrollen til nivå 2 av 5 (delvis etablert). Nøkkelroller i direktoratet har via en spørreundersøkelse understøttet dette bildet, med en vurdert modenhet på 2,5. Samme vurdering er senere bekreftet av direktoratets ledelse. Krav og forventninger fra departement og regulatoriske føringer tilsier etter KPMGs vurdering nivå 4 (konsistent og operasjonalisert praksis). Direktoratet har via ledelsens tilbakemeldinger til KPMG og i interne strategiske beskrivelser sluttet seg til nivå 4 som direktoratets fremtidsambisjon.

De siste årene har direktoratet vært i en overgang fra en modell med høy grad av autonome produktteam til økt sentral styring. Det er særlig det siste året iverksatt flere viktige tiltak for å styrke internkontrollen. Tiltakene er relevante og nødvendige, men har foreløpig ikke hatt tid til å gi tilstrekkelig effekt i praksis. KPMGs vurdering er likevel at iverksatte tiltak i begrenset grad dekker våre anbefalinger. For å nå ambisjonsnivå 4 fra dagens nivå 2 kreves betydelig kompetanse innen endringsledelse og tverrfaglig samhandling. Etter KPMGs vurdering er det per i dag ikke etablert tilstrekkelige tiltak for å sikre slik kompetanse knyttet til internkontroll i toppledergruppen eller øvrige nøkkelroller. KPMG mener videre at sentrale rolle- og ansvarsforhold fortsatt er uavklarte ett år etter omorganiseringen som fant sted i mai 2025. Det er fortsatt ikke etablert tilstrekkelige mekanismer for styrt og tidsbunden oppfølging av avvik og revisjonsfunn, eller for å utnytte disse systematisk til læring og forbedret praksis.

KPMG vurderer at både direktoratet og AID nå står ved et veiskille. Uten tydeligere prioritering, styring og oppfølging av gjennomføring og effekt, er det risiko for at pågående tiltak ikke gir varig forbedring. Etter KPMGs vurdering må arbeidet forankres som et flerårig, helhetlig styrings- og endringsløp, med tydelige krav til prioritering, gjennomføring, oppfølging og rapportering.

Hovedfunn

- **Strategi, mål og ambisjoner**: Ambisjoner er definert, men ikke tilstrekkelig konkretisert eller konsekvent operasjonalisert i styringsmodellen. Manglende felles forståelse av alvor, risikotoleranse og tidskritikalitet reflekterer etter KPMGs vurdering svak felles prioritering og forankring vedrørende internkontroll i toppledergruppen, og er en sentral årsak til at svakheter har vedvart over tid.
- **Risikostyring**: Det mangler en tydelig prioritering av risikoer opp mot direktoratets strategiske mål, en omforent risikotoleranse og klar kommunikasjon av denne til linjen. Samhandlingen mellom risikoeiere, kravstillere og teknologimiljøer er svak, og teknologi- og produktteam er i begrenset grad involvert i forbedringsarbeidet. Risikovurderinger knyttet til etterlevelse av krav overlates i for stor grad til produktteamene. Dette indikerer manglende helhetlig prioritering og tydelig styringssignaler fra topplednernivå.
- **Styringsprinsipper og internkontroll**: Overordnet godt beskrevet, men lite operasjonalisert til konkrete, etterprøvbare kontrollkrav. Direktoratets egenutviklede plattform for utvikling, drift og kjøring av applikasjoner (kalt NAIS) utgjør et godt, men delvis uforløst, utgangspunkt for IKT-internkontrollen.
- **Organisering**: Svak operasjonalisering av ansvar i organisasjonen. Uklarheter i trelinjemodellen (god praksis for internkontroll) mellom de operative enhetene og støtte- og kontrollfunksjoner, særlig i andrelinjen, skaper ineffektivitet. Organisasjonen mangler et helhetlig compliance-program, herunder systematisk arbeid med forebygging og avdekking av økonomiske misligheter.
- **Opplæring og kommunikasjon**: Opplæringen knyttet til internkontroll har vært fragmentert. Et strukturert opplæringsløp er under implementering. Det er i dag betydelig usikkerhet på alle nivåer i organisasjonen om hva internkontroll faktisk innebærer i praksis. Det er et behov for å styrke dialogen med Riksrevisjonen gjennom mer strukturert involvering av teknologisk spisskompetanse og ledelse.
- **Etterlevelse**: Kontroller og avvikssystemer finnes, men etterlevelsen svekkes av manglende kontrollrammeverk, svak operasjonalisering og uklare ansvarsforhold. Dette gir rom for lokal praksis og fragmentert sporbarhet/dokumentasjon, med konsekvenser som svak prioritering, lang lukketid på avvik og utfordringer med konsistent rapportering på tvers av produktteam.
- **Rapportering**: Det er behov for å styrke ledelsesrapporteringen slik at den gir et helhetlig og risikobasert bilde av faktisk kontrollnivå og oppnådd risikoreduksjon. Dette krever konsolidering av styringsinformasjon på tvers av enheter, standardisering av KPIer og dashboards, samt systematisk utnyttelse og integrasjon av etterlevelsesdata – særlig fra teknologimiljøene – i den overordnede styringen.
- **Læring og forbedring**: Læring skjer i hovedsak lokalt og reaktivt. Systematiske forbedringssløyfer på tvers av organisasjonen er svakt utviklet, og gjentakende funn fra internrevisjonen og Riksrevisjonen viser manglende kultur og ansvar for lukking av avvik.

Samlet vurdering

KPMG vurderer at direktoratets internkontroll innen IKT samlet sett er på et **delvis etablert modenhetsnivå (nivå 2 av 5)**, mens krav og forventninger fra AID tilsier et nivå som forutsetter **full operasjonalisering og konsistent praksis (nivå 4)**. KPMG vurderer at dette i stor grad gjenspeiler manglende evne i toppledergruppen til å fungere som et samlet, tverrfunksjonelt lederteam for styring og utvikling av internkontroll i direktoratet, med tilstrekkelig kapasitet til å prioritere, beslutte og følge opp internkontroll på tvers av fag- og teknologimiljøer.

Det er særlig utfordringer knyttet til

- gjennomføringsevne,
- prioritering basert på risiko,
- konsistent etterlevelse på tvers av produktteam og
- styringsinformasjon og beslutningsgrunnlag.

Dette indikerer et betydelig gap mellom krav, ambisjon og faktisk praksis.

En gjennomgående observasjon er at ambisjonsnivået for internkontroll ikke er tilstrekkelig tydelig definert og operasjonalisert i styringsmodellen. Internkontroll fremstår som et område som konkurrerer med andre hensyn i en presset hverdag, noe som bidrar til ujevn prioritering, lang lukketid på avvik og fragmentert gjennomføring. Det er betydelig usikkerhet på tvers av nivåer og miljøer om hva internkontroll faktisk innebærer i praksis, og hvordan ansvar for risiko, krav, kontroller og oppfølging er fordelt.

KPMG vurderer at en sentral rotårsak til vedvarende svakheter er mangelfull samhandling mellom regulatoriske miljøer, styringsfunksjoner og teknologimiljøer, forsterket av svakt koordinert prioritering og oppfølging i toppledergruppen. God praksis for internkontroll er bygget opp etter trelinjemodellen, der tydelig rolle- og ansvarsdeling mellom drift (førstelinjen), risikostyring og etterlevelse (andrelinjen) samt uavhengig kontroll (tredjelinjen) er avgjørende. Selv om trelinjemodellen er kjent, er den i begrenset grad operasjonalisert i praksis. Manglende avklaringer av ansvar for risiko, krav, kontroller og oppfølging gir utydelighet, varierende praksis og ineffektiv ressursbruk. Særlig er andrelinjens rolle og oppgaver uklart definert og etterlevd.

KPMG konkluderer med at direktoratet står ved et veiskille. Våre anbefalinger er derfor rettet mot å tydeliggjøre ambisjonsnivå og risikotoleranse, styrke samhandling og rolleavklaringer, operasjonalisere trelinjemodellen, etablere risikobasert oppfølging av etterlevelse og utnytte NAIS og øvrige verktøy som integrerte deler av direktoratets helhetlige internkontrollsystem.

Hovedanbefalinger

Tiltaksområde 1: AID og direktoratets ambisjonsnivå, prioritering og oppfølging

KPMG anbefaler at AID, i tett dialog med direktoratet, videreutvikler og operasjonaliserer et tydelig og omforent ambisjonsnivå for internkontroll, basert på akseptabel risikotoleranse. Ambisjonsnivået bør kommuniseres eksplisitt og fungere som felles referanse for prioritering, gjennomføring og ledelsesoppfølging på tvers av styringsnivåer, fagområder, teknologimiljøer og porteføljestyring. Dette forutsetter at toppledergruppen samlet utøver tydelig lederskap i prioritering og oppfølging, og har tilstrekkelig kompetanse og kapasitet innen endringsledelse til å sikre faktisk gjennomføring og varig effekt.

KPMGs vurdering er at manglende felles forståelse av alvor, risikotoleranse og tidskritikalitet er en grunnleggende årsak til at svakheter i internkontrollen har vedvart over tid. Selv om oppmerksomheten rundt internkontroll har økt, blant annet som følge av alvorlige hendelser, revisjonsfunn og tydeligere forventninger fra AID, har forventningene historisk i begrenset grad vært operasjonalisert i en tydelig måltilstand. Konsekvensen er at internkontroll i praksis kan

konkurrere med andre hensyn i en presset hverdag, noe som bidrar til ujevn prioritering, lang lukketid på tiltak og fragmentert gjennomføring. Ambisjonsnivået bør derfor konkretisere hva direktoratet skal oppnå, hvilket modenhetsnivå som forventes over tid, hvilke risikoområder som er særlig kritiske, og hvordan risiko skal vurderes, prioriteres, aksepteres og eskaleres. Dette er nødvendig for at internkontroll skal bli en integrert del av ordinær styring, porteføljeprioritering og styringsdialogen mellom AID og direktoratet.

Gjennomgangen viser at Riksrevisjonen gjentatte ganger har påpekt vesentlige svakheter i internkontrollen, og at kritikken over tid har blitt tydeligere og mer systemorientert. Dialogen med Riksrevisjonen bør derfor styrkes gjennom mer strukturert involvering av teknologisk spisskompetanse og ledelse. Dette er særlig viktig for å tydeliggjøre hvordan plattformløsninger som NAIS understøtter tilgangsstyring, logging, endringshåndtering og revisjonsbevis, herunder gjennom innebygde og i stor grad preventive tekniske kontroller. En mer presis forklaring av disse kontrollene kan gi bedre grunnlag for vurdering av faktisk risiko, kontrollnivå og videre forbedringsarbeid.

Tiltaksområde 2: Kultur og kompetanse for tverrfaglig samhandling og endringsledelse

KPMG vurderer at utfordringene i samhandling i stor grad har sitt utspring i manglende tydelighet i prioritering, beslutning og oppfølging på toppledernivå. KPMG anbefaler at direktoratet styrker kulturen og kompetansen for tverrfaglig samhandling mellom regulatoriske miljøer, teknologimiljøer og styringsfunksjoner, og reduserer person- og initiativavhengig praksis. Direktoratets samfunnsoppdrag realiseres i skjæringspunktet mellom komplekst regelverk og et teknologisk komplekst IKT-landskap. Dette forutsetter modenhet i matriseorganisering, evne og kompetanse til å oversette juridiske, økonomiske og styringsmessige krav til praktisk og teknisk etterlevelse. KPMGs vurdering er at samhandlingen mellom regulatoriske miljøer, teknologimiljøer og styringsfunksjoner i dag i for stor grad er avhengig av enkeltpersoner, uformelle relasjoner og lokale initiativer. Mangelen på faste arenaer, tydelige mandater og felles arbeidsformer bidrar til ulik praksis, ineffektiv ressursbruk og økt risiko for feilprioriteringer. Dette forsterkes av at regulatoriske krav ikke alltid samordnes og oversettes tilstrekkelig før de adresseres mot produktteamene.

KPMGs vurdering er at teknologimiljøer og produktteam i dag i for liten grad involveres i forbedringsarbeidet som pågår. For å redusere denne risikoen bør direktoratet tydeliggjøre forventninger til samhandling og rolleutøvelse i matriseorganiseringen. Samhandlingen bør understøttes av faste, forpliktende arenaer og tydelige beslutnings- og eskaleringslinjer, slik at krav kan forstås, prioriteres og operasjonaliseres mer konsistent på tvers av fag, styring og teknologi.

Tiltaksområde 3: Helhetlig internkontroll, roller og ansvar

KPMG anbefaler at direktoratet videreutvikler og sikrer effektiv implementering av et helhetlig og operasjonelt internkontrollrammeverk, tydelig forankret som et lederansvar og integrert i ordinære styrings- og beslutningsprosesser. Internkontroll bør anvendes aktivt som et styringsverktøy for prioritering, ressursbruk og risikohåndtering – og ikke primært som dokumentasjon eller rapportering. For en virksomhet der IKT er en bærende del av oppgaveløsningen, er det etter KPMGs vurdering lite hensiktsmessig å skille mellom internkontroll knyttet til IKT og øvrig internkontroll.

KPMG anbefaler videre at direktoratet operasjonaliserer og konkretiserer trelinjemodellen i praksis, med tydelig avklaring av roller, ansvar og samspill mellom risikoeiere, kravstillere, produktteam og Teknologiavdelingen. Uklar ansvarsdeling og svake grenseflater er etter KPMGs vurdering blant de mest sentrale årsakene til manglende gjennomføring og vedvarende svakheter i internkontrollen, særlig innen IKT-utvikling, drift og forvaltning. Selv om trelinjemodellen formelt er kjent, er den i begrenset grad oversatt til praktiske forventninger i linjen. Manglende felles forståelse av hvem som har ansvar for å identifisere risiko, stille krav, utforme og implementere kontroller, dokumentere kontrollbevis og følge opp etterlevelse bidrar til uklart ansvar, varierende praksis og ineffektiv ressursbruk. Særlig fremstår andrelinjens operative rolle som utydelig, herunder ansvar for veiledning, påse-oppgaver, verifikasjon, eskalering og oppfølging. KPMG vurderer derfor at trelinjemodellen må operasjonaliseres i samspillet mellom fag, styring og teknologi, og ikke begrenses til formelle beskrivelser eller kontrollfunksjoner.

Mandatet for kvalitetsseksjonen bør tydeliggjøres hva gjelder ansvar for og egen rolle i helhetlig risikostyring. Det bør legge til rette for tydelig prioritering av risikoer opp mot direktoratets strategiske mål, tydelig og omforent risikotoleranse og kommunikasjon av dette til linjen. Seksjonen bør også tillegges ansvaret for å fange opp eksterne risikoer og trender som kan påvirke virksomheten fremover.

Ansvaret for et helhetlig compliance-program, herunder systematisk arbeid med forebygging og avdekking av økonomiske misligheter, bør plasseres tydelig og med en stiplet linje til arbeids- og velferdsdirektør. Slik direktoratet er organisert i dag er KPMGs anbefaling at det vil være naturlig å legge denne rollen til Juridisk avdeling.

Direktoratet bør samtidig gå fra en praksis preget av fragmentert dokumentasjon av etterlevelse til mer konsistent og risikobasert prioritering og oppfølging. Etterlevelsesarbeidet er i dag i for stor grad orientert mot registrering av status, og i for liten grad brukt aktivt til styring, prioritering og lukking av avvik basert på risiko og vesentlighet. Dette svekker ledelsens beslutningsgrunnlag og evnen til å målrette ressursinnsats der risikoen er størst. Styringssløyfene mellom produktteam, kravstiller og risikoeier bør derfor tydeliggjøres, med klare krav til eskalering, prioritering og ledelsesoppfølging.

Selv om det pågår relevante initiativer knyttet til videreutvikling av etterlevelsesverktøyet bør etterlevelsesinformasjon i større grad sammenstilles og brukes som ledelsesrettet styringsinformasjon, uten at verktøyet gjøres til et rent kontroll- eller avvikssystem. Dette innebærer blant annet at informasjon om manglende dokumentasjon, åpne restanser, risikoaksepter og vesentlighet bør brukes mer aktivt i prioritering, oppfølging og beslutninger.

NAIS bør inngå som et viktig virkemiddel i dette arbeidet. KPMG anbefaler at direktoratet etablerer tydelige og forpliktende styringsprosesser for bruk av NAIS, og utnytter plattformen som en bærende del av førstelinjens internkontroll. KPMG vurderer at NAIS representerer et svært godt teknisk utgangspunkt for robust og innebygd IKT-internkontroll, blant annet innen tilgangsstyring, logging, sporbarhet og endringshåndtering. Kontrollgevinsten realiseres imidlertid først når bruken av plattformen er standardisert, styrt og etterlevd på tvers av produktteam, og når dette inngår i direktoratets samlede internkontrollrammeverk. Tekniske tiltak er likevel ikke tilstrekkelige alene; effekten av NAIS forutsetter tydelig organisatorisk forankring, samspill med kravstillere og risikoeiere, og integrasjon i styrings- og rapporteringsprosesser.

Tiltaksområde 4: Systematiske lærings- og forbedringssløyfer

KPMG anbefaler at direktoratet etablerer forpliktende og systematiske lærings- og forbedringssløyfer basert på hendelser, revisjonsfunn, avvik og post mortem-rapporter. Formålet er å sikre at kjente svakheter ikke bare håndteres lokalt eller enkeltvis, men brukes som grunnlag for helhetlig forbedring av krav, kontroller, arbeidsprosesser, opplæring og styring på tvers av direktoratet.

KPMG vurderer at manglende systematisk læring er en vesentlig årsak til gjentakende funn og lang lukketid på tiltak. I dag håndteres hendelser og avvik i stor grad lokalt i enkeltmiljøer, og brukes i begrenset grad som grunnlag for strukturell forbedring på tvers av produktområder og fagmiljøer. Dette innebærer at læring i for stor grad blir person- og teamavhengig, og at likeartede svakheter kan oppstå flere steder uten at direktoratet samlet sett bygger tilstrekkelig modenhet.

Produktteamene arbeider i stor grad selvstendig, noe som gir fleksibilitet og lokal handlekraft. Samtidig innebærer denne arbeidsformen en risiko for at erfaringer, rotårsaker og korrigerende tiltak ikke deles systematisk på tvers. Direktoratet bør i større grad sikre at avvik og funn ikke bare registreres og lukkes, men også analyseres for rotårsak, følges opp med tydelig ansvar og frist, og vurderes i etterkant for å kontrollere om tiltakene faktisk har hatt ønsket effekt. KPMG observerer at det pågår initiativer som styrker håndtering av hendelser og avvik, men at disse i begrenset grad er samlet i en helhetlig og styrt forbedringssløyfe med tydelig ledelsesforankring.

Konsekvenser

Dersom dagens situasjon vedvarer, er det risiko for

- fortsatt gjentakende revisjonsfunn og svakheter i revisjonsbevis,
- redusert tillit til styringsinformasjon og rapportering,
- ineffektiv ressursbruk og vedvarende forbedringsarbeid uten tilstrekkelig effekt og
- økt risiko for feil, misligheter og manglende etterlevelse av regelverk.

Anbefalt videre oppfølging

KPMG anbefaler et tydelig skifte fra en fragmentert og reaktiv tilnærming til en mer helhetlig, styrt og risikobasert internkontroll. Det anbefales følgende prioritering:

1. Etablere et tydelig og forpliktende ambisjonsnivå

AID bør, i dialog med direktoratet, tydeliggjøre forventet nivå for internkontroll, inkludert risikotoleranse, prioriteringsprinsipper og krav til gjennomføring.

2. Styrke styring, ansvar og oppfølging

Styrke styring, ansvar og oppfølging, herunder etablere en mer samlet og forpliktende styringspraksis i toppledergruppen med tydelig ansvar for gjennomføring og effekt. Det bør etableres klarere ansvarslinjer og tydeligere krav til eskalering, prioritering og lukking av avvik.

3. Operasjonalisere internkontroll i praksis

Direktoratet må oversette krav til konkrete og etterprøvbare kontrollkrav som kan implementeres og følges opp i produktteam og teknologimiljøer.

4. Etablere risikobasert styring og rapportering

Informasjon om etterlevelse og risiko må i større grad brukes aktivt i ledelsesstyring og prioritering, med tydelig kobling mellom risiko, tiltak og oppfølging.

5. Sikre systematisk læring og forbedring

Det må etableres forpliktende mekanismer for læring fra hendelser, revisjonsfunn og avvik, slik at forbedring skjer på tvers av organisasjonen og ikke kun lokalt.

Implikasjoner for AIDs styring

AID har over tid gitt signaler om styrket internkontroll. Gjennomgangen indikerer at utfordringen i begrenset grad ligger i manglende krav, men i oppfølging av gjennomføring og effekt.

KPMG vurderer derfor at AIDs oppfølging fremover i større grad bør dreies mot

- tydeligere krav til dokumentert effekt av tiltak,
- mer konsekvent og utholdende oppfølging av gjennomføringsevne og
- tydeligere terskler og konsekvenser ved manglende forbedring.

Dette vil være avgjørende for å sikre varig forbedring i direktoratets internkontroll.

I det videre arbeidet vil det ha stor betydning at både AID og direktoratet bygger oppunder de mange gode forutsetningene direktoratet har for å heve internkontrollen i tråd med beskrevet ambisjonsnivå. Som eksempel nevnes direktoratets egenutviklede plattform NAIS, som vurderes som et meget godt teknisk utgangspunkt for robust og innebygd IKT-internkontroll. Plattformen tilbyr standardiserte løsninger for blant annet tilgangsstyring, logging, endringshåndtering og sporbarhet, og gir et betydelig potensial for å redusere person- og kulturavhengig praksis. Kontrollgevinsten realiseres imidlertid først fullt ut når bruken av NAIS er tydelig styrt, standardisert og etterlevd på tvers av alle produktteam, og når plattformens kontrollmuligheter inngår i et helhetlig styrings- og oppfølgingsregime.

Innhold

1. Innledning og mandat

Dette oppdraget er gjennomført på bakgrunn av gjentatt kritikk av mangelfull internkontroll, særlig knyttet til IKT, i en virksomhet med høy kompleksitet og stor samfunnsmessig betydning. Formålet er å vurdere hvorvidt internkontrollen i tilstrekkelig grad sikrer etterlevelse av regelverk og pålitelig styrings- og regnskapsinformasjon, med utgangspunkt i krav fra Arbeids- og inkluderingsdepartementet. Vurderingen omfatter organisering, ansvar, prosesser og praksis knyttet til IKT-utvikling, drift og forvaltning, og legger til grunn at internkontroll må være helhetlig og integrert i virksomhetsstyringen.

1.1. Bakgrunn

Arbeids- og inkluderingsdepartementet (AID) har engasjert KPMG for å gjennomføre en ekstern evaluering av Arbeids- og velferdsdirektoratets (direktoratets) systematiske arbeid med internkontroll knyttet til utvikling, drift og forvaltning av etatens IKT-systemer.

Bakgrunnen for utlysningen er at direktoratet over tid har fått kritikk for manglende internkontroll i forbindelse med ulike gjennomganger og revisjoner av virksomhetens IKT-systemer. Dette kommer senest frem i Riksrevisjonens rapport om revisjon av statsregnskapet for 2024. Rapporten konkluderer med at Arbeids- og velferdsdirektoratet har betydelige svakheter i internkontrollen i databaser for alderspensjon, uføretrygd, avtalefestet pensjon og foreldrepenger, og at etablerte tilgangskontroller og logging ikke oppfyller kravene i økonomiregelverket. Riksrevisjonen har konkludert med at svakhetene har ført til at det ikke er mulig å innhente tilstrekkelig og hensiktsmessig revisjonsbevis i revisjonen av årsregnskapet til Arbeids- og velferdsetaten. Arbeids- og velferdsetaten har derfor fått revisjonsberetning med forbehold. Det er også avdekket at det har blitt utbetalt støtte til ortopediske hjelpemidler uten å kontrollere fakturaene, noe som ikke er i tråd med reglene for økonomistyring i staten og som kan ha ledet til feilaktig utbetaling av støtte etter folketrygdloven.

Arbeids- og velferdsdirektoratet er en stor organisasjon med et omfattende samfunnsoppdrag. Det stilles høye krav og forventninger til direktoratet fra myndigheter, befolkningen og arbeidsgivere til kvalitet, sikkerhet og tilgjengelighet. Det hersker tilsvarende lav toleranse for svakheter, feil og mangler. IKT-landskapet som driftes, utvikles og forvaltes er komplekst og har følgelig en høy iboende risiko for tekniske feil. Mangler i kontrollregimet kan blant annet øke risikoen for misligheter, resultere i feilrapportering og redusere tilliten til legitimiteten av regnskapstall.

Departementets tildelingsbrev fra 2025 vektlegger viktigheten av at direktoratet skal ha en forsvarlig internkontroll tilpasset risiko og vesentlighet og at denne skal være systematisk og integrert i styringen. I tildelingsbrevet for 2026 er det tydeligere beskrevet en eksplisitt forventning til at internkontrollen skal fungere i praksis, og at internkontrollen kobles tettere til IKT/digitalisering.

Arbeids- og velferdsdirektoratets årsrapport for 2025 beskriver internkontroll som et område med betydelige forbedringsmuligheter. Internkontrollen beskrives som svak på flere områder, særlig knyttet til IKT-systemer, herunder tilgangsstyring og logging samt kontroll av utbetalinger. Direktoratet har i 2025 eksplisitt løftet internkontroll som én av toppledelsens hovedprioriteringer. En rekke forbedringstiltak pågår.

1.2. Formål og mandat

Formålet med dette oppdraget har vært å gjennomføre en uavhengig og helhetlig vurdering av styrker og svakheter ved Arbeids- og velferdsdirektoratets internkontroll knyttet til utvikling, drift og forvaltning av etatens IKT-systemer. Evalueringen gir konkrete og prioriterte anbefalinger til forbedringstiltak, med særlig vekt på internkontrollens evne til å:

- **Sikre etterlevelse av lover og regler**: Dette innebærer at IKT-bruken må oppfylle relevante krav i økonomiregelverket, forvaltningsloven, personvernregelverket og øvrig gjeldende regelverk. Det omfatter kontroller for korrekt utbetaling av ytelser, lovmessig saksbehandling og betryggende informasjonssikkerhet.
- **Understøtte pålitelig styringsinformasjon og rapportering**: Internkontrollen skal bidra til korrekte regnskapsrapporter og beslutningsgrunnlag for ledelsen, og bidra til å redusere risikoen for feil og misligheter. Riksrevisjonen har påpekt at mangelfull styringsinformasjon, herunder fravær av loggdata i sentrale databaser, har svekket påliteligheten i rapporteringen.

Evalueringen belyser særlig tre fokusområder:

- **Organisering, roller og ansvar**: KPMG vurderer hvordan internkontrollarbeidet er organisert etter omorganiseringen, og om roller og ansvar er tydelig definert og forankret i den nye produktteam-strukturen. Dette inkluderer å vurdere om prinsippet om trelinjemodellen for internkontroll i direktoratet praktiseres tydelig og i tråd med god praksis – det vil si at produktteam (første linje), støttefunksjoner/internkontrollkoordinatorer (andre linje) og internrevisjon (tredje linje) sammen dekker kontrollbehovene. Det må avklares om internkontrollansvar er plassert riktig i organisasjonen og om ledelsen gir tydelig styring og prioritering av internkontrollarbeidet.
- **Etablerte systemer, rutiner og intern kommunikasjon**: KPMG kartlegger og vurderer direktoratets styringssystem for internkontroll, inkludert policyer, prosedyrer og verktøy. Viktige spørsmål er om retningslinjer og rutiner for internkontroll knyttet til IKT er oppdaterte, kjent og hensiktsmessige, og om de dekker kravene i regelverket og god praksis. Videre undersøkes om det er tilstrekkelig intern kommunikasjon og opplæring knyttet til internkontroll, slik at alle relevante medarbeidere kjenner sine kontrolloppgaver og rapporteringslinjer.
- **Løpende overvåking og evaluering**: Vi undersøker hvordan direktoratet følger opp og forbedrer internkontrollen over tid. Dette omfatter om det finnes nøkkeltall eller indikatorer for internkontroll som monitoreres av ledelsen, om rapporterte svakheter blir fanget opp og utbedret, og om det gjennomføres jevnlige evalueringer eller tester av kontroller. Riksrevisjonen har blant annet bemerket at direktoratet i begrenset grad hadde gjennomført etterkontroller av ekstraordinære utbetalinger (koronatiltak). Vi har vurdert om direktoratet nå har etablert mekanismer for kontinuerlig internkontrollovervåking, som periodiske ledelsesgjennomganger, internrevisjonsaktiviteter, risikoregistre eller lignende, og effektiviteten av disse.

AID har satt tydelige ambisjoner om å styrke direktoratets systematiske arbeid med internkontroll. Dette prosjektet gir en unik mulighet til å etablere robuste kontrollmekanismer og rutiner som sikrer at virksomheten opererer i tråd med samfunnets forventninger og krav. KPMGs mandat knytter seg spesifikt til direktoratets internkontroll knyttet til utvikling, drift og forvaltning av etatens IKT-systemer. For en virksomhet hvor utførelsen av samfunnsoppdraget i stor grad avhenger av velfungerende IKT-systemer vil det imidlertid ikke være hensiktsmessig å se internkontrollen knyttet til IKT som adskilt fra direktoratets helhetlige internkontrollsystem. Dette er et prinsipp KPMG også vektlegger i rapportens tiltaksanbefalinger og implementeringsplan.

Evalueringen kombinerer vurderinger av styringsstruktur, utforming og etterlevelse av kontrollprosedyrer, samt organisasjonskulturens betydning for internkontrollens effektivitet. Sluttproduktet vil være et solid beslutningsgrunnlag, bestående av tydelige og prioriterte anbefalinger til tiltak som styrker direktoratets internkontroll og sikrer etterlevelse av lover og regelverk, i tråd med både myndighetskrav og prinsipper for god praksis.

1.3. Avgrensninger og forutsetninger

Evalueringen er avgrenset til internkontroll innenfor Arbeids- og velferdsdirektoratet, og omfatter ikke internkontroll i øvrige deler av etaten (f.eks. fylker og Nav-kontorene i Arbeids- og tjenestelinjen). Forhold i enheter utenfor direktoratet eller forhold hos leverandører eller andre eksterne parter analyseres kun dersom de direkte påvirker eller har sammenheng med direktoratets internkontrolloppgaver eller systemer.

Videre avgrenses oppdraget tematisk til internkontroll knyttet til de to målene 1) etterlevelse og 2) pålitelig rapportering, og omfatter ikke målet om “målrettet og effektiv drift”. Dette betyr at vår evaluering ikke er lagt opp for å vurdere effektiviteten, måloppnåelsen eller økonomien i Arbeids- og velferdsdirektoratets IT-drift i seg selv. KPMG er imidlertid av den oppfatning at det er hensiktsmessig å innlemme slike hensyn der dette er nødvendig for å ivareta et helhetlig internkontrollsystem eller der gevinster knyttet til målrettet og effektiv drift kan høstes til liten tilleggskostnad eller -innsats.

Evalueringens rotårsaksanalyse omfatter definerte kritiske hendelser som følger KPMGs mandat, samt andre kritiske hendelser som kan ha betydning, basert på tilgjengeliggjort dokumentasjon og informasjon der dette foreligger. Vår rapport avgrenser seg til data beskrevet i kapittel 3 og 4. Det har ikke vært en del av KPMGs mandat å gjennomføre en fullstendig faktaundersøkelse av de kritiske hendelsene som er innlemmet i rotårsaksanalysen. KPMG har imidlertid kartlagt de kritiske hendelsene i den utstrekning som har vært nødvendig for å gjennomføre rotårsaksanalysen, deriblant relevant faktum knyttet til det systemtekniske, risikostyring og generell etterlevelse.

Denne rapporten er utarbeidet på bakgrunn av informasjonen som er gitt til KPMG og dokumentene som er gjort tilgjengelige. KPMG fraskriver seg ethvert ansvar for mulige feil eller utelatelser som følge av at KPMG har mottatt uriktige eller ufullstendige opplysninger eller dokumentasjon. KPMG kan ikke gjøres ansvarlig overfor tredjeparter.

1.4. Personvern og databeskyttelse

KPMG har behandlet personopplysninger i samsvar med gjeldende personvernlovgivning.

KPMG har ikke mottatt personopplysninger i særlig grad som del av vårt arbeid. Behandlingen av personopplysninger har vært begrenset til det som er nødvendig for å gjennomføre oppdraget, og har tatt utgangspunkt i mandatet gitt av departementet.

Innhentet dokumentasjon som inneholder personopplysninger slettes ved oppdragets avslutning.

1.5. Leserveiledning

I neste kapittel beskriver vi vår metode for datainnsamling og analyse, inkludert vurderingskriteriene for evalueringen. I kapittel tre presenterer vi sentrale faktiske forhold og pågående forbedringsaktiviteter i direktoratet. Dette omfatter blant annet direktoratets organisering, styrende dokumenter, internkontrollrammeverk, IKT-arkitektur, NAIS-plattformen og digitale verktøy til støtte for etterlevelse. I kapittel fire presenterer vi funn fra vår gjennomgang av kritiske hendelser og revisjonsfunn fra de siste årene, med særlig vekt på forhold avdekket av Riksrevisjonen. Kapittel tre og fire har til formål å skape et bredt og dekkende faktumsgrunnlag for videre analyser og vurderinger, og fremstår derfor detaljerte og omfattende.

I kapittel fem legger vi frem vår samlede vurdering av internkontrollen. Dette inkluderer en analyse av nåsituasjonen, vurderinger av modenhetsnivå innen 8 definerte områder, funn fra rotårsaksanalysen og en samlet vurdering av gap mellom krav, ambisjon og faktisk praksis. I kapittel seks presenterer vi våre anbefalte tiltak, strukturert etter fire tiltaksområder og fordelt på kortsiktige, mellomlange og langsiktige tiltak. Her gir vi også noen anbefalinger om veien videre. Sentrale vedlegg er samlet i kapittel syv.

2. Metode og gjennomføring

Vurderingen bygger på en kombinert metodisk tilnærming som inkluderer dokumentgjennomgang, intervjuer, spørreundersøkelse, analyser av kritiske hendelser og arbeidssamlinger for å gi et helhetlig og nyansert bilde av internkontrollen knyttet til IKT. Et etablert rammeverk med utgangspunkt i trelinjemodellen benyttes for å vurdere både utforming og faktisk etterlevelse av kontroller. Evalueringen gjennomføres ved å kombinere perspektivene fra en modenhetsvurdering og rotårsaksanalyse. Datagrunnlaget er bredt og sammensatt, og funn er triangulert på tvers av kilder. Tilnærmingen legger vekt på å identifisere styrker, svakheter og rotårsaker, med særlig fokus på forhold som påvirker etterlevelse av regelverk og pålitelig rapportering.

2.1. Innledning

I dette kapittelet redegjør vi for KPMGs metodiske tilnærming. Først beskriver vi kriterier for evalueringen, trelinjemodellen og det benyttede modenhetsrammeverket. Deretter beskriver vi våre metoder for datainnhenting og prosessen for gjennomføring av oppdraget.

2.2. Vurderingskriterier og begreper

KPMGs evaluering har lagt til grunn et modenhetsrammeverk for internkontroll som er forankret i Committee of Sponsoring Organization of the Treadway Commission (COSO) og Control Objectives for Information and Related Technology (COBIT), samt kravene i statens økonomiregelverk og Direktoratet for forvaltning og økonomistyrings (DFØ) krav til internkontroll i staten. Samlet utgjør dette evalueringskriteriene for oppdraget som sikrer at vurderingen er systematisk, helhetlig og forankret i god praksis.

2.2.1. DFØs definisjon av internkontroll for statlige virksomheter

I rapporten bruker KPMG DFØs definisjon av internkontroll. Denne bygger på COSOs internkontrolldefinisjon og kobler også internkontroll tett til økonomiregelverket i staten, særlig *Reglement for økonomistyring* § 14, men også og i andre lover og regelverk som forvaltningsloven, arbeidsmiljøloven, arkivloven og eForvaltningsforskriften. DFØ definerer internkontroll for statlige virksomheter slik:

«Internkontroll er alle systemer, rutiner og tiltak som skal gi rimelig sikkerhet for at virksomheter har:

- *målrettet og effektiv drift,*
- *at de etterlever lover og regler, og*
- *at de rapporterer på en pålitelig måte.»*

For statlige virksomheter understreker DFØ at

- *«internkontrollen er et lederansvar,*
- *internkontrollen skal være integrert i styringen,*
- *internkontrollen skal være dokumentert, og*
- *internkontrollen skal tilpasses virksomhetens risiko og egenart.»*

Internkontroll handler om å redusere risiko for feil, ineffektivitet, redusert måloppnåelse og lovbrudd. DFØ legger vekt på systemer, rutiner og tiltak – altså det praktiske og operative kontrollapparatet – men innholdet bygger på COSO.

2.2.2. Organisering av internkontrollarbeidet og god praksis

Trelinjemodellen (Three Lines Model) fra Institute of Internal Auditors[1] gir et helhetlig rammeverk for god virksomhetsstyring ved å tydeliggjøre roller, ansvar og samspill mellom departementet, ledelsen og uavhengig internrevisjon. Modellen legger vekt på effektiv samhandling på tvers av organisasjonen, klar ansvarsplassering for styring, risiko og etterlevelse, samt en balansert tilnærming der risikohåndtering understøtter både kontroll og måloppnåelse. Formålet er å styrke ansvarlighet, beslutningskvalitet og styringsevne i møte med et komplekst og endringspreget risikobilde. Modellen er ikke et lovkrav i staten, men regnes som en anerkjent og praktisk måte å organisere internkontrollarbeidet på både i Norge og internasjonalt.

Trelinjemodellen fordeler kontrollarbeidet i tre nivåer, definert som første, andre og tredje linje.

Første linje:

- Eier alle former for risiko i sine aktiviteter, herunder risiko for brudd på lovkrav og feilrapportering.
- Utarbeider rutiner tilpasset sine aktiviteter, i samsvar med overliggende styrende dokumenter.
- Gjennomfører førstelinjekontroller.
- God praksis: Hovedandelen av internkontrollaktiviteter ligger i førstelinjen.

Andre linje:

- Setter «spillereglene»: Utarbeider styrende dokumenter som gjelder på tvers av hele organisasjonen.
- Støtter og veileder første linje – bistår med å operasjonalisere styrende dokumenter i førstelinjen.
- Overvåker og følger opp etterlevelse (påse-ansvar): Sikrer gjennomføring av førstelinjekontroller og foretar stikkprøver.

Tredje linje:

- Gjennomfører uavhengig og objektiv vurdering av internkontroll, risikostyring og styringsprosesser på vegne av øverste ledelse.

Eksterne kontrollorganer som Riksrevisjonen kan ses som en slags **fjerde linje**, men regnes ikke som en del av virksomhetens interne kontrollsystem.

2.3. Rammeverk for modenhetsanalyse

Vi benytter et strukturert modenhetsrammeverk utviklet av KPMG som grunnlag for vurderingen av direktoratets systematiske arbeid med internkontroll knyttet til utvikling, drift og forvaltning av IKT-systemer. Rammeverket bygger på anerkjent god praksis fra KPMGs evalueringer av internkontrollsystemer, både nasjonalt og internasjonalt, og er utformet for å sikre en etterprøvbar og helhetlig vurdering. Vurderingen omfatter både hvordan internkontrollen er etablert og utformet (design), og i hvilken grad den fungerer effektivt i praksis (operativ etterlevelse og effekt).

[1] Three Lines Model - IIA

Rammeverket er forankret i prinsipper fra COSO og COBIT, samt krav og føringer i statens økonomiregelverk og relevante veiledere fra DFØ.

Modenhetsvurderingen har hatt tre hovedformål:

1. Å etablere et felles og operasjonelt bilde av nåsituasjonen for internkontroll knyttet til IKT-området, innenfor vurderingsmålene etterlevelse og pålitelig rapportering.
2. Å identifisere styrker og svakheter samt drivere for disse.
3. Å underbygge prioriterte anbefalinger ved å koble funn og forbedringsbehov til kriterier, modenhetsnivåer og underliggende datakilder.

Modenhetsvurderingen omfatter direktoratets internkontroll knyttet til IKT-området, herunder styring, prosesser, roller og praksis relatert til

- etterlevelse av lover og regler (særlig krav som påvirker IKT-bruken og internkontroll i IKT-systemer), og
- pålitelig økonomisk og annen rapportering, inkludert sporbarhet, dokumentasjon og kontrollmekanismer som understøtter revisjonsbevis.

Vurderingen er avgrenset til direktoratet og dets styrings- og gjennomføringsprosesser, men tar hensyn til relevante grenseflater der disse påvirker internkontrollens evne til å fungere i praksis.

KPMG har benyttet en femdelt modenhetsskala, der nivåene representerer en gradvis utvikling fra uformell og personavhengig praksis til integrert, målt og kontinuerlig forbedret internkontroll:

Nivå	Forklaring
Nivå 1 Ikke etablert	Internkontroll er svakt forankret i strategi og planer, med mål som ikke er operasjonalisert og få eller udokumenterte risikovurderinger. Styrende dokumenter, roller og ansvar er mangelfulle eller uklare, kontrollaktiviteter gjennomføres i stor grad ad hoc, og avvik håndteres lite systematisk. Noe rapportering forekommer, men brukes i begrenset grad til styring, og oppfølging av kontroller og funn er svak.
Nivå 2 Delvis etablert	Internkontroll er delvis forankret i strategi og planer, med enkelte mål operasjonalisert og kjent, men med begrenset systematikk i risikovurderinger og svak dokumentasjon. Styrende dokumenter, roller og styringsarenaer er delvis etablert, men ujevnt brukt og oppdatert, og kontrollaktiviteter gjennomføres i varierende grad. Rapportering skjer primært på mål og økonomi og brukes noe i styringen, men oppfølging, avvikshåndtering og tilbakemelding er begrenset.
Nivå 3 Etablert, men forbedringsbehov	Internkontroll er godt forankret i strategi, med sentrale mål operasjonalisert og kjent, og risikovurderinger er beskrevet og dokumentert, med involvering fra ledelse. Styrende dokumenter dekker de fleste prosesser, roller og ansvar er i hovedsak avklart, og det finnes etablerte arenaer for styring, med tydelige føringer, systematikk og utstrakt bruk av teknologi. Risikobaserte kontroller gjennomføres og følges opp, avvikssystem er delvis kjent, og rapportering på mål, økonomi og risiko brukes aktivt med oppfølging og tilbakemelding.

Nivå 4 Godt etablert	Internkontroll er sterkt forankret i strategi, med alle mål operasjonalisert og systematisk fulgt opp, og med etablerte systemer for risikovurdering og tiltak der effekt evalueres og lederinvolveringen er tydelig. Styrende dokumenter dekker alle sentrale prosesser, roller og ansvar er klart definert i tråd med trelinjemodellen, og styringsarenaer brukes aktivt til oppfølging og forbedring. Kontrollaktiviteter er planlagt og dokumentert, rapportering er integrert (inkl. compliance) med bruk av KPIer og dashboards, og styring, oppfølging og justering henger tett sammen.
Nivå 5 Fullt implementert og fungerer svært godt	Internkontroll er fullt integrert i virksomhetsstyringen og understøttes helhetlig av teknologi, med sanntidsdata, automatisert oppfølging og kontinuerlig evaluering av effekt. Styrende dokumenter, roller, kontroller og rapportering er digitalt tilgjengelige, aktivt brukt og dynamisk justert, der kontrollinjer spiller hverandre gode. Organisasjonen kjennetegnes av systematisk bruk av tilbakemeldinger, læring og teknologi til kontinuerlig forbedring av styring, risiko og etterlevelse.

Direktoratet fikk i forbindelse med forberedelsene til spørreundersøkelsen anledning til å gi innspill til nivåbenevningen. Benevningen som fremstilt over er basert på tilbakemeldinger fra direktoratet for å lette tolkning og forståelse hos deres nøkkelpersoner. Innholdet i KPMGs rammeverk for modenhetsvurdering og nivåenes forhold til hverandre er uendret.

Modenhetsnivå settes basert på en samlet vurdering av design og operativ effekt, og med særskilt vekt på etterprøvbarhet og konsistens der dette er relevant for krav om internkontroll og revisjonsbevis.

2.4. Datagrunnlag

For dette oppdraget har KPMG benyttet en mixed method-tilnærming, med en kombinasjon av kvalitative og noe kvantitative data. Dette har muliggjort en kontinuerlig testing og triangulering av data for å sikre et solid datagrunnlag for våre vurderinger og anbefalinger. I det følgende gir vi en nærmere beskrivelse av hvordan vi har gjennomført evalueringen, deriblant

- Dokumentasjonsgjennomgang,
- semi-strukturerte intervjuer,
- spørreundersøkelse,
- gjennomgang av utvalgte kritiske hendelser, og
- arbeidssamlinger.

2.4.1. Dokumentasjonsgjennomgang

Aktuelle dokumenter og datakilder har blant annet omfattet (men er ikke begrenset til):

- Overordnede styringsdokumenter og retningslinjer
- Årsrapporter og relevante eksterne revisjonsrapporter
- Dokumentasjon av systemer, rutiner og interne prosesser
- Intern rapportering og annen relevant virksomhetsinformasjon
- Rapporter fra internrevisjon og Riksrevisjon

- Informasjon og dokumentasjon vedrørende pågående interne forbedringsprosjekter og -initiativer i direktoratet

2.4.2. Presentasjoner fra Arbeids- og velferdsdirektoratet

I de første ukene av KPMGs arbeid ble det avholdt en rekke presentasjonsmøter der utvalgt nøkkelpersonell hos direktoratet ga innføringer i direktoratets organisering, nøkkelprosesser og andre forhold av relevans for prosjektet:

- Direktoratets overordnede organisering
- Internrevisjonens organisering og arbeid
- Ytelsesavdelingens organisering og arbeid
- Teknologiavdelingens organisering og arbeid
- Juridisk avdelings organisering og arbeid
- Strategi og økonomi
- Økonomi- og styringsavdelingens organisering og arbeid

Disse presentasjonene satte KPMG i stand til raskt å sette seg inn i direktoratets kontekst og ramme, og har bidratt til det samlede datagrunnlaget evalueringen er basert på.

2.4.3. Intervjuer

I løpet av prosjektet har KPMG avholdt 38 intervjuer med 34 totalt respondenter. Intervjuer ble gjennomført med følgende aktørgrupper:

- Representanter fra AID: Ledelse, fag- og økonomiansvarlige
- Representanter fra Arbeids- og velferdsdirektoratet: Ledelse og fagansvarlige

Innen Arbeids- og velferdsdirektoratet har vi intervjuet følgende rolletyper:

- Avdelingsdirektør i Økonomi- og styringsavdelingen
- Avdelingsdirektører og ansatte i økonomi- og styringsavdelingen innen seksjonene for økonomisystemer, virksomhetsstyring og økonomi
- Ledere og ansatte i seksjonene for utvikling, digital sikkerhet, data og informasjonsforvaltning, organisasjon og styring samt overordnet ledelse i teknologiavdelingen
- Nøkkelpersoner i relevante fagområder
- Nøkkelpersoner på alle nivåer på tvers av organisasjonen innen utvikling, drift og forvaltning av etatens IKT-systemer
- Andre identifiserte nøkkelroller: HR, juridisk, sentrale roller knyttet til risikostyring, etterlevelse av lovverk, internrevisjon
- Tillitsvalgte

Det har vært metodisk viktig å sørge for at respondenter opplever at det er trygt å dele informasjon. Vi har informert respondenter innledningsvis om at vi ikke deler referater fra intervjuet med oppdragsgiver, og at vi ikke gjengir informasjon på en måte som gjør at det kan spores tilbake til respondenten. Vi følger videre rutiner for sikker oppbevaring og sletting av informasjon.

2.4.4. Spørreundersøkelse

I tillegg til intervju- og dokumentanalysen er det gjennomført en spørreundersøkelse rettet mot de samme ansatte i Arbeids- og velferdsdirektoratet som KPMG har avholdt intervju med. Undersøkelsen er benyttet for å:

- gi bredde i innsikt på tvers av roller og miljøer
- avdekke variasjoner i opplevd modenhet mellom områder, avdelinger og stillingsnivåer
- identifisere områder med særlig sprik mellom nåsituasjon og ønsket ambisjonsnivå
- styrke etterprøvbarheten i modenhetsbildet gjennom et bredt ansattperspektiv

Undersøkelsen er strukturert etter de samme hovedområdene som benyttes i modenhetsrammeverket. Spørsmålene måler opplevd modenhet på en skala fra 1 til 5 for nåsituasjon, og tilsvarende for fremtidsambisjon. Dette har muliggjort analyser av (a) gjennomsnitt og spredning per område, (b) forskjeller per spørsmål, og (c) identifikasjon av spørsmål med størst gap mellom nåtidsvurdering og ambisjon. Resultatene er analysert både på aggregert nivå og på detaljnivå for å avdekke interne variasjoner.

Spørreundersøkelsen er ikke brukt som eneste grunnlag for modenhetsnivå, men som et triangulerende datapunkt. Der undersøkelsen viser stor variasjon, er dette tolket som en indikasjon på ujevn operasjonalisering og forskjeller i praksis, og er brukt aktivt i dialog og verifisering opp mot øvrige kilder.

Undersøkelsen ble sendt ut til 32 personer og besvart av 23, som gir en svarprosent på 72 %. Undersøkelsen besto av totalt 43 spørsmål. I 39 av disse ble respondentene bedt om å ta stilling til i hvilken grad (på en skala fra 1 til 5) de vurderer påstandene som sanne eller usanne, basert på dagens situasjon og ønsket fremtidig nivå. Med ønsket fremtidig nivå menes hvilket modenhetsnivå organisasjonen bør ha på sikt (3-5 år frem i tid).

De resterende fire spørsmålene var åpne fritekstspørsmål. Disse omhandlet utviklingen de siste tre årene knyttet til implementering av internkontrolltiltak, opplæring, oppfølging av revisjonsfunn, samt vurdering av styrker ved dagens internkontroll på IKT-området.

Ytterligere omtale av undersøkelsens innretning og detaljert funn er redegjort i kapittel 8.6, nedenfor.

2.4.5. Gjennomgang av kritiske hendelser

En gjennomgang av utvalgte kritiske hendelser er en del av datagrunnlaget KPMGs evaluering baseres på. Gjennomgangen har til formål å informere og belyse KPMGs forståelse av IKT-internkontrollen i direktoratet samt å fungere som utgangspunkt for en rotårsaksanalyse.

Riksrevisjonen har gjentatte ganger de senere årene påpekt vesentlige svakheter i IKT-internkontrollen. Riksrevisjonen graderer alvorlighet i sine funn slik: “ikke tilfredsstillende” brukes ved svakheter i styring eller etterlevelse, “kritikkverdig” ved klare brudd eller mangler med vesentlige konsekvenser, og “sterkt kritikkverdig” ved alvorlige og systematiske svakheter som kan få store konsekvenser for samfunn eller enkeltpersoner.

KPMG har gjennomgått funnene fra Riksrevisjonen. KPMG har også gått gjennom kritiske funn i rapporter fra direktoratets Internrevisjon og et utvalg av post mortem-rapporter.

For rotårsaksanalysen har KPMG sett nærmere på hendelse i 2025 knyttet til feilrapportering om loggingsfeil / krav til tilgangskontroll og logging ikke oppfylt. KPMG har også gjennomgått mer i detalj hendelsen i 2024 knyttet til manglende kontroll av utbetaling, eks. for ortopedi. Disse hendelsene illustrerer slik KPMG ser det svakheter i ulike deler av IKT-internkontrollen. Gjennomgangene har bidratt til å vurdere:

- Faglig kvalitet og metodisk robusthet i utvalgte saker, med vekt på hvordan kontrollmekanismer er implementert og etterlevd
- Læringsverdi og modenhet i internkontrollsystemet, herunder hvordan erfaringer fra tidligere hendelser brukes til forbedring

Utvalget av saker er basert på følgende kriterier:

- Tema og variasjon, for å dekke ulike aspekter av IKT-styring og internkontroll
- Grad av oppfølging og estimert innvirkning, for å vurdere om tiltak har gitt ønsket effekt og læring er implementert

Gjennomgangen er basert på dokumentanalyse og intervjuer med nøkkelpersoner, og har gitt grunnlag for vurdering av:

- Om direktoratets internkontroll er tilpasset risiko og vesentlighet
- Om kontrollene fungerer effektivt i praksis, spesielt i lys av Riksrevisjonens kritikk av svakheter i kontrollmiljø, tilgangsstyring og rapportering

2.4.6. Arbeidssamlinger og -møter

I løpet av prosjektet har det blitt gjennomført tre arbeidssamlinger som del av prosjektets rotårsaksanalyse:

- Den første samlingen ble avholdt med det primære formål å identifisere potensielle rotårsaker til de hendelser som er innlemmet i rotårsaksanalysen. Som utgangspunkt for diskusjonen ble det presentert noen hovedfunn og -observasjoner fra spørreundersøkelsen, og KPMG delte om vårt perspektiv på internkontroll samt rotårsaksmetodikk. På bakgrunn av dette fikk deltakerne presentert en problemformulering som sammenfatter det rotårsaksanalysen skal besvare. Deretter sparret deltakerne om rotårsaker, først inndelt i grupper og deretter i plenum.
- Den andre samlingen ble innledet med en foreløpig sammenstilling av årsaksbildet som ble sparret frem under den første samlingen. Her fikk deltakerne inngi sine kommentarer og refleksjoner, og berede grunnen for å vurdere hvilke tiltak/anbefalinger som kan understøtte internkontrollen på en slik måte at tilsvarende hendelser eller forhold ikke gjentar seg i fremtiden. Deltakerne sparret om dette både gruppevis og i plenum.
- Den tredje samlingen var et arbeidsmøte som ble avholdt med deltakere fra prosjektets referansegruppe samt fungerende arbeids- og velferdsdirektør. Her delte KPMG den foreløpige modenhetsvurderingen av nåsituasjon samt fremtidsambisjoner slik disse fremgår av den avholdte spørreundersøkelsen. Ambisjonsnivået ble satt i kontekst av regulatoriske krav, eierforventninger og faktisk og ønsket modenhet hos andre sammenlignbare virksomheter. Deretter ble implikasjonene av de observerte gapene

diskutert i gruppen, blant annet sett i lys av de tiltak/anbefalinger som ble drøftet i samling 2 og prioriteringsrekkefølge.

Samtlige nøkkelpersoner som hadde møtt KPMG til intervju ble invitert til å delta i de to første samlingene. Den siste samlingen var forbeholdt ledernivå og bestod av deltakere fra prosjektets referansegruppe samt konstituert arbeids- og velferdsdirektør.

Arbeidssamlingene har generelt blitt benyttet til å sikre at rotårsaker og forslag til tiltak settes under debatt. Samlingene har blitt gjennomført som «åpne» i formen, med stor vekt på å samle inn nye tanker og innspill fra deltakerne. KPMG har derfor ikke presentert sin sammenstilling av rotårsaker eller tiltak i forkant av deltakernes egen sparring, og det har heller ikke blitt lagt føringer for utfallet utover beskrivelsen av metodisk prosess. En kommunisert avgrensning ved samlingene har vært at sparringene om både rotårsaker og tiltak skal begrenses til å løse problemformuleringen som har sin bakgrunn i hendelsene som er innlemmet i analysen. Det har ikke vært et mål at samlingene skal besvare spørsmål om årsaker eller tiltak knyttet til internkontroll i stort. Det er imidlertid i mange tilfeller nærliggende å se årsaker og tiltak knyttet til analysens problemformulering som relevante for internkontroll generelt. Videre er ikke rotårsakene eller tiltak/anbefalinger fra samlingene alene grunnlaget for KPMGs konklusjoner. I beskrivelsen av rotårsaker slik denne fremgår av rapportens kapittel 5 inngår både utfallet av samlingene og KPMGs egen vurdering.

2.5. Bruk av kunstig intelligens i arbeidet

KPMG har benyttet kunstig intelligens (KI) som et støtteverktøy i arbeidet med rapporten, i tråd med KPMGs etablerte prinsipper for ansvarlig bruk av KI ("Trusted AI"). Dette innebærer at bruk av KI er gjennomført med vekt på transparens, etterprøvbarhet, datasikkerhet og personvern.

KI er primært anvendt til å effektivisere analyse- og dokumentasjonsarbeid, herunder strukturering og oppsummering av informasjon. All bruk er gjort under faglig styring av KPMGs rådgivere, og KI-generert innhold er kvalitetssikret og validert før det er inkludert i leveransene.

KPMGs retningslinjer innebærer videre at bruk av KI på kundedata er underlagt klare krav til godkjenning og vurdering av dataklassifisering. Løsningene som er benyttet oppfyller gjeldende krav til datasikkerhet og personvern, herunder at data ikke benyttes til å trene underliggende modeller.

Samlet bidrar bruk av KI til økt effektivitet og kvalitet i arbeidet, samtidig som krav til forsvarlig og trygg håndtering av informasjon er ivaretatt.

2.6. Oppsummering av metode for modenhetsvurdering

Modenhetsvurderingen er gjennomført ved systematisk triangulering av de ulike datakildene beskrevet ovenfor.

Trianguleringen har vært brukt til å (1) avklare om funn er konsistente på tvers av kilder, (2) identifisere avvik mellom formell styring og faktisk praksis og (3) i den utstrekning datagrunnlaget har tillatt det, vurdere om modenhet varierer mellom miljøer.

Modenhetsvurderingen er gjennomført i to trinn:

1. **Delvurderinger per tema/område:** For hvert område er funn og evidens vurdert opp mot modenhetskriteriene, med eksplisitt vurdering av design og operativ effekt.
2. **Samlet vurdering:** Delvurderingene er konsolidert til en helhetlig modenhetsvurdering. I konsolideringen er det lagt vekt på områder som har størst betydning for måloppnåelse innen etterlevelse og pålitelig rapportering, samt områder der svakheter har høy risiko og/eller der svakheter går igjen over tid (for eksempel ved gjentakende revisjonsfunn).

Resultatet er et modenhetsbilde som beskriver både samlet nivå og hvor i styrings- og kontrollkjeden det er vesentlige gap: fra strategi og styringsmodell, via risiko og krav, til kontrollutførelse, rapportering og læring/forbedring.

3. Faktiske forhold og pågående forbedringsaktiviteter

Det er etablert overordnede føringer for internkontroll gjennom tildelingsbrev fra departementet og ansvarsdokumenter i direktoratet. Direktoratets IKT-arkitektur er sammensatt av standardiserte skytjenester, egenutviklede plattformsløsninger og eldre systemer. NAIS, direktoratets egenutviklede plattform for utvikling, drift og kjøring av applikasjoner har moderne kontroller som i stor grad støtter COBIT-målene om risikostyring, sikker drift og overvåking. Disse kontrollene er per rapporttidspunktet ikke formaliserte og brukes i varierende grad av produktteamene. Det er stor variasjon i hvordan avvik i etterlevelse av krav registreres, følges opp og lukkes, samt i hvilken grad erfaringer benyttes på tvers av produktteamene. I 2026 etablerte direktoratet et eget internkontrollprosjekt som jobber med de grunnleggende kravene som stilles til internkontroll som finnes i Økonomiregelverket (§14).

3.1. Innledning

For å støtte modenhets- og rotårsaksanalysen har KPMG kartlagt relevante faktiske forhold knyttet til direktoratet som organisasjon, IKT-arkitektur og digitale verktøy til støtte for etterlevelse av eksterne og interne krav. I det følgende redegjøres det for direktoratets kontekst, inkludert departementets oppfølging, organisering og rammeverk for internkontroll.

NAIS er den sentrale utviklings- og driftsplattformen som brukes av de fleste produktteamene. Vi har derfor inkludert tekniske dybdebeskrivelser av relevant funksjonalitet innebygd i NAIS i dag og planer for videreutvikling.

Til slutt har vi inkludert tre delkapitler med beskrivelser av data knyttet til etterlevelse og kvalitet: utdrag av data fra verktøyet Støtte til etterlevelse, oppsummering av observasjoner knyttet til post mortem-rapporter og oppsummering av relevante funn og trender i revisjoner gjennomført av direktoratets internrevisjon de senere årene.

3.2. Eksterne krav og forventninger

Det følger av *Reglement for økonomistyring i staten* (økonomireglementet) § 14 og *Bestemmelser om økonomistyring i staten* (bestemmelsene) punkt. 2.4 at direktoratet skal etablere en internkontroll. Virksomhetens ledelse har ansvaret for å påse at internkontrollen er tilpasset risiko og vesentlighet, at den fungerer på en tilfredsstillende måte og at den kan dokumenteres. Internkontrollen skal forhindre styringssvikt, feil og mangler og sikre at økonomistyringen er organisert på en forsvarlig måte og utføres i samsvar med gjeldende lover og regler, herunder at transaksjoner er i samsvar med underliggende forhold. Videre skal internkontrollen sikre effektiv ressursbruk, og at misligheter og økonomisk kriminalitet forebygges og avdekkes, jf. bestemmelsene 2.4 første ledd bokstav c, f og g.

Som beskrevet i kapittel 2 legger KPMGs evaluering til grunn et modenhetsrammeverk for internkontroll som er forankret i Committee of Sponsoring Organization of the Treadway Commission (COSO) og Control Objectives for Information and Related Technology (COBIT), samt kravene i statens økonomiregelverk og DFØs veiledning for hva de anser som god internkontroll i staten. **COSO** og **COBIT**, representerer samlet etablert **god praksis for internkontroll** som passer til oppdraget. Rammeverkene er utviklet av ledende fagmiljøer internasjonalt og benyttes bredt i både offentlig og privat sektor, herunder som grunnlag for statlige krav og veiledning.

COSO beskriver hvordan virksomheten som helhet skal styres og kontrolleres, og definerer internkontroll som en integrert styringsprosess som skal gi rimelig sikkerhet for måloppnåelse innen drift, rapportering og etterlevelse av lover og regler. Rammeverket vektlegger helhetlig styring, tydelige roller og ansvar, risikobasert tilnærming og sterk ledelsesforankring.

COBIT utfyller COSO ved å konkretisere god praksis for styring og kontroll av **IT og informasjonssystemer**, og beskriver hvordan IT skal understøtte virksomhetens mål og håndtere IT-relatert risiko. Samlet gir COSO og COBIT et strukturert, etterprøvbart og anerkjent grunnlag for vurdering av internkontroll, med overordnede prinsipper fra COSO og operativ konkretisering for IT-området gjennom COBIT.

I vår analyse legger vi også til grunn IIAs oppdaterte (Institute of Internal Auditors) trelinjemodell.

3.3. Departementets forventninger til og oppfølging av direktoratet

3.3.1. Innledning

Arbeids- og inkluderingsdepartementet har det overordnede ansvaret for arbeids- og velferdspolitikken i Norge. Departementet gir årlige mål og oppdrag til direktoratet i tildelingsbrev, og følger opp direktoratet gjennom etatsstyringsmøter og særmøter.

KPMG har gjort en analyse av tildelingsbrev samt referater fra etatsstyringsmøter og særmøter og sett på i hvilken grad IKT-internkontrollrammeverk har vært adressert og i hvilken grad hendelser er omtalt og brukt til å fremme endring.

Vurderingen er også gjort med bakgrunn i **DFØs *Veileder i etatsstyring*** som normativt vurderingsgrunnlag. Veilederen beskriver etatsstyring som **mål- og resultatstyring basert på risiko, vesentlighet, tillit og tydelig rollefordeling**. For en **stor, kompleks og publikumstett etat som Arbeids- og velferdsdirektoratet** innebærer dette særskilte krav til:

- Strategisk styring fremfor detaljstyring
- Klar grense mellom politisk ansvar og operativ gjennomføring
- Systematisk bruk av risiko- og evalueringsinformasjon

I det følgende oppsummerer vi våre funn og vurderinger.

3.3.2. Presentasjoner fra Arbeids- og velferdsdirektoratet

I de første ukene av KPMGs arbeid ble det avholdt en rekke presentasjonsmøter der utvalgt nøkkelpersonell hos direktoratet ga innføringer i direktoratets organisering, nøkkelprosesser og andre forhold av relevans for prosjektet:

- Internrevisjonens organisering og arbeid
- Ytelsesavdelingens organisering og arbeid
- Teknologiavdelingens organisering og arbeid
- Juridisk avdelings organisering og arbeid
- Strategi og økonomi
- Økonomi- og styringsavdelingens organisering og arbeid

Disse presentasjonene satte KPMG i stand til raskt å sette seg inn i direktoratets kontekst og ramme, og har bidratt til det samlede datagrunnlaget evalueringen er basert på.

3.3.3. Analyse av tildelingsbrev

KPMG har gjennomført en analyse av tildelingsbrev tilbake til 2014 og instrukser tilbake til 2019 fra regjeringen.no.

Det overordnede utviklingstrekket slik KPMG ser det er en bevegelse fra forventninger om grunnleggende etterlevelse og økonomikontroll til en mer helhetlig, risikobasert og systematisk styring av kvalitet, internkontroll, IKT og beredskap gjennom instruksene i stedet for i tildelingsbrevene.

Denne utviklingen akselererer særlig etter:

- EØS-saken (2019–2020)
- Pandemien
- Økt nasjonalt sikkerhets- og trusselbilde
- Økende digitalisering og automatisering av kjerneprosesser

Hovedtrekk: Blir hendelser omtalt og brukt til å fremme endring?

- Frem mot 2020: Hendelser omtales indirekte, ofte som avvik og brukes primært til å forklare hvorfor mål ikke nås, og til å begrunne ekstra tiltak eller ressurser.
- Lite eller ingen eksplisitt kobling til systemsvakheter, læring eller varig endring.
- Etter 2020: Hendelser brukes mer aktivt som læringsgrunnlag, styringsinformasjon og grunnlag for forbedring.

Tidsperioder	Overordnede utviklingstrekk	Hendelser
2014-2016: Grunnleggende kontroll og etterlevelse	• Fokus på: korrekt ytelsesforvaltning, saksbehandlingstid, økonomistyring og budsjettkontroll • Internkontroll omtales implisitt, knyttet til: «forsvarlig forvaltning», «god kvalitet» • IKT omtales primært som moderniseringsprosjekt, ikke som risikoområde	Lite eksplisitt - Hendelser som «avvik» – noe man håndterer
2017-2019: Mer eksplisitt styring og begynnende risikofokus	• Tydeligere kobling mellom: måloppnåelse, styringsdialog og rapportering • IKT løftes tydeligere frem som: kritisk muliggjører og eget styringsområde • IKT omtales i egne kapitler med fokus på modernisering, stabil drift, sammenheng mellom systemer og tjenestekvalitet • Krav om å varsle departementet ved vesentlige avvik og beredskap for endringer i arbeidsmarkedet	Lite eksplisitt – Overgangsfase - Hendelser som styringssignal og omtales som noe AID skal varsles om
2020-2021: Tydelig paradigmeskifte	• Internkontroll omtales som system, ledelsesansvar og kontinuerlig arbeid • Krav om læring av feil, oppfølging av avvik og styrking av kvalitet i ytelsesforvaltningen • Risiko, kvalitet og styring kobles eksplisitt sammen • IKT: Digital robusthet og beredskap blir tydeligere. Fokus på stabilitet, rask omstilling og evne til å håndtere stor belastning	Hendelser omtales eksplisitt både som faktiske hendelser (EØS, pandemi) og som noe virksomheten skal være forberedt på
2022-2024: Helhetlig internkontroll og kvalitetssystem	• Internkontroll omtales eksplisitt som helhetlig system og tett koblet til kvalitet • Krav om systematisk forbedring, oppfølging av Riksrevisjonen og dokumentert styring • IKT: Digitalisering + internkontroll sees i sammenheng. Fokus på informasjonssikkerhet, personvern og avhengigheter i verdikjeden	Krav om beredskap, øvelser, læring av hendelser Ikke bare «håndtere», men forbedre systemene etterpå
2025-2026: Modenhetsfase – internkontroll som kontinuerlig styring	• Internkontroll er eksplisitt omtalt som et eget utviklingsområde • Det forventes videreutvikling av helhetlig system for kvalitet og internkontroll, moden risikostyring og kobling mellom styring, læring og forbedring • IKT omtales som en del av nasjonal beredskap og kritisk for samfunnsfunksjoner • Forventning om robusthet, beredskap for alvorlige hendelser og evne til å opprettholde kritiske ytelser	Hendelser som kontinuerlig forbedringssløyfe. Det forventes ikke bare håndtering, men moden refleksjon, systematisk oppfølging og varige forbedringer

Figur 1 Trender - analyse av tildelingsbrev tilbake til 2014 og instrukser tilbake til 2019

3.3.4. Analyse av etatsstyringsmøter

KPMG har også gjennomført en analyse av mottatt dokumentasjon fra etatsstyringsmøter fra 2015 og til i dag. Vi har sett på trender over tid, spesielt knyttet til krav stilt av AID relatert til internkontroll, styring og kontroll og om hendelser (da spesifikt IKT-relaterte) er nevnt eller har ledet til endring i krav:

- Det er en tydelig bevegelse fra økonomisk og operativ styring til helhetlig risiko-, kvalitets- og internkontrollstyring. Dette skjer gradvis, men akselererer etter 2020.

- Før 2020 omtales internkontroll indirekte gjennom saksbehandlingstid, kvalitet og restanser. Etter NAV-/EØS-saken (2020–2021) blir internkontroll og etterlevelse løftet eksplisitt frem som et ledelsesansvar. Departementet etterspør i økende grad
  - systematikk i kvalitetsarbeid,
  - risikostyring som del av styringsdialogen og
  - oppfølging av svikt (feil lovanvendelse, feilutbetalinger og restanser)

Tidsperioder	Overordnede utviklingstrekk	Hendelser
2015-2017:	• Domineres av økonomi, produksjon, saksbehandlingstid, tiltaksnivå og effektivisering. • Internkontroll omtales indirekte som «måloppnåelse» og «kvalitet». • IKT omtales som moderniseringsløp (Arena, nye løsninger).	• Hendelser får liten plass. • Fokus primært på volum, drift, kapasitet og ressursbruk.
2018-2019:	• Mer struktur på digitaliseringsdialogen. • Styring av informasjonssikkerhet begynner å komme inn i styringsdialogen. • Mer vekt på risiko som begrep, men fortsatt lite integrert.	• Få hendelser brukt aktivt. • Enkelte omtaler av IKT-relaterte risikoer, men ikke systematisk.
2020-2021: Paradigmeskifte	• NAV-/EØS-saken, CV-saken og pandemi driver krav om systematikk, etterlevelse og internkontroll. • Risikokart og risikoarbeid blir sentrale styringsverktøy. • Kvalitet og lovanvendelse løftes som kritiske områder.	• EØS-/NAV-saken omtales eksplisitt og driver strukturelle endringskrav. • Personvern og rettssikkerhet blir tydelige kravområder. • Pandemien fører til skjerpede krav til robusthet, digital kapasitet og prioritering.
2022-2024: Modning	• Kraftig styrking av dialog om kvalitet, internkontroll, tilgangsstyring og etterlevelse. • IKT-modernisering kobles sterkere til risiko og beredskap. - Tilsyn (Datatilsynet m.fl.) brukes i styringsdialogen. • Fokus på helhetlig kvalitetssystem i NAV.	• Hendelser og tilsyn brukes aktivt: personvern, tilgangsstyring, gamle systemer, saksbehandlingssvikt. • Hendelser nasjonalt påvirker krav til beredskap og digital sikkerhet.
2025: Kontinuerlig modning	• Risikobasert internkontroll fremstår som fullt integrert styringspraksis. • Hendelser, øvelser og evaluering er rutinemessige styringspunkter. • Skytjenester og teknologiutvikling kobles til krav om styring, sikkerhet og modenhet.	• Hendelser forventes å inngå i læringssløyfer – ikke unntak, men en del av styringsmodellen. • IKT-sårbarheter (legacy, forsinkelser i modernisering) omtales som vedvarende risikoområder.

Figur 2 Trender - analyse av etatsstyringsmøter fra 2015 og til i dag

3.3.5. Analyse av særmøter

KPMG har gjennomført en analyse av særmøtereferater fra 2016 og til i dag. Det er en tydelig bevegelse fra plan- og økonomifokus til helhetlig, risikobasert og systematisk styring av kvalitet, internkontroll, IKT og beredskap.

Over tid ser vi:

- Internkontroll går fra implisitt forventning til eksplisitt og kontinuerlig ledelsesansvar (bl.a. knyttet til kvalitet/internkontroll som eget tiltaksområde og behov for internkontroll for å hindre “forvitring” av rutiner)
- IKT går fra moderniseringsløp til kritisk risikoområde (sikkerhet, personvern og beredskap; økt trusselbilde; behov for tilgangsstyring/logging)

- Hendelser omtales i økende grad som forventet del av risikobildet og brukes til læring og forbedring (øvelser/evaluering og oppfølging i ordinær styringsdialog)

Hovedtrekk: Blir hendelser omtalt og brukt til å fremme endring?

- Før 2020: Hendelser omtales relativt lite og brukes i begrenset grad til å drive varig endring; styringen domineres av plan/status/økonomi.
- 2021: Et tydeligere skifte – konkrete hendelser (personvern/sikkerhet) omtales eksplisitt og utløser oppfølging og endringsbehov.
- 2023–2025: Hendelser brukes mer systematisk som læring og styringsinformasjon (standarder/internkontroll, endret praksis etter dataangrep, øvelser → evaluering → oppfølging).

Tidsperioder	Overordnede utviklingstrekk	Hendelser
2016-2017:	• Fokus på økonomisk styringsinformasjon, effektivisering og grunnleggende kontroll • IKT omtales primært som moderniseringsprogram (prosjekt/leveranser) • Styring preges av plan, status, fremdrift og rammer	Hendelser omtales i liten grad; hovedvekt på status/plan og styringsgrunnlag
2018-2019:	• Mer strukturert dialog om digitalisering og tjenesteutvikling(• Etablering av format for periodisk rapportering og dialog om informasjonssikkerhet • Økt vekt på gjennomføringsstrategi og rammebetingelser	Hendelser omtales fortsatt begrenset; økt oppmerksomhet på risiko/rapportering (særlig innen informasjonssikkerhet)
2020-2021: Paradigmeskifte	• Etterlevelse, rettsgrunnlag og personvern løftes tydeligere inn i styringen (CV-/personvern-tematikk) • Risiko- og sårbarhetsvurderinger og etterlevelseskrav omtales eksplisitt i digital utvikling • Styringen preges av behov for robusthet og kontroll på hjemmelsgrunnlag	Hendelser/personvernbrudd og sikkerhetshendelser omtales eksplisitt og følges opp
2022-2024: Helhetlig internkontroll og kvalitetssystem	• Tillitsreform med tydelig balanse: handlingsrom vs. kvalitet, likebehandling og dokumentasjon • Internkontroll, kvalitet og oppfølging av svakheter/tilsyn kobles tettere sammen (bl.a. "kvalitet og internkontroll" som tiltaksområde; samt etterspørsel etter status vs ønsket nivå på etterlevelse) • Personvern, tilgangsstyring, logg og styring av sikkerhetsområdet får økt vekt	Hendelser og tilsyn brukes som styringsinformasjon; krav om beredskap, øvelser og læring (inkl. arbeid med sikkerhetslov/GNF Dataangrep mot departementenes felles IKT-plattform påvirker praksis
2025: Modenhetsfase – internkontroll som kontinuerlig styring	• Sikkerhet og beredskap integreres i ordinær styringsdialog (øvelser, evaluering, oppfølging) • Arbeid med GNF/skjermingsverdige verdier og kriterier/terskler i styring • Bestilling knyttet til skytjenester signaliserer styring av teknologivalg	Hendelser forstås som kontinuerlig forbedringssløyfe (øvelser/evaluering/oppfølging)

Figur 3 Trender - analyse av særmøtereferater fra 2016 og til i dag

3.3.6. Oppsummering

Gjennomgangen viser at Arbeids- og inkluderingsdepartementet (AID) over tid har tydeliggjort internkontroll, etterlevelse, risikostyring og hendelseshåndtering som ledelsesansvar og som en integrert del av styringen. Styringssignalene fremstår i hovedsak relevante og i tråd med god etatsstyring.

Samtidig viser dokumentasjonen at flere utfordringer innen internkontroll og etterlevelse har vedvart over tid, til tross for skjerpede krav og igangsatte tiltak. Dette gjelder særlig manglende helhet og ujevn praksis, lang lukketid på tiltak, svak læring av hendelser og begrenset dokumentert effekt av forbedringsarbeidet.

På denne bakgrunn vurderes det at AID i perioder kunne vært tettere på i oppfølgingen av direktoratet. Særlig gjelder dette der kjente svakheter og hendelser har gjentatt seg uten vesentlig eller varig forbedring. Behovet synes primært knyttet til mer konsekvent og utholdende oppfølging av gjennomføringsevne og effekt, snarere enn mer detaljstyring eller flere krav.

Dokumentasjonen indikerer videre at alvorlige eller gjentatte hendelser i begrenset grad er knyttet til tydelige styringsmessige konsekvenser eller klare terskler for skjerpet oppfølging. Samlet sett har AID styrt i riktig retning, men oppfølgingen kunne i enkelte faser vært mer eksplisitt og konsekvensorientert for å sikre varig forbedring.

3.4. Organisering av direktoratet

3.4.1. Overordnet om utvikling av organiseringen

Siden etableringen i 2006 har Arbeids- og velferdsdirektoratet gjennomgått flere omorganiseringer. Digitalisering har vært høyt prioritert, blant annet i utviklingen av digitale selvbetjeningsløsninger og i effektiviseringen av interne prosesser. De siste årene har direktoratet gjennomført en omfattende organisatorisk og digital transformasjon som blant annet har inkludert en stor omlegging av utvikling, drift og forvaltning av IKT-systemer.

I perioden 2012-2015 var direktoratets IKT-modernisering preget av store eksterne leverandørkontakter med høy grad av innleid spesialistkompetanse. IKT-utvikling var i stor grad prosjektbasert, med en klassisk bestiller- og utførermodell. IKT-utvikling ble gjennomført etter fossefallsmetoden med en lineær prosjektmodell der hver fase i stor grad må være ferdig før neste begynner. Store leverandører sto for betydelige deler av utviklingen. I perioden 2015-2017 konkluderte direktoratet med at avhengigheten av eksterne leverandører gav store utfordringer i form av liten intern teknologisk kontroll, utfordrende kunnskapsoverføring og høy kostnad. Direktoratet startet derfor arbeidet med å erstatte eksterne konsulenter med egne IKT-ansatte.

I 2016 innførte direktoratet tverrfaglige produktteam med egne ansatte (utviklere, drift, jurister etc.) med ende til ende-ansvar for produktet. Teamene ble gitt stor grad av autonomi med det formål å sikre rask og smidig utvikling. Man gikk bort fra den klassiske fossefallsmodellen og over til en agil og lean modell der man jobber i små iterasjoner (sprinter) med hyppige (del)leveranser.

I perioden 2016-2022 rekrutterte direktoratet bredt innen IKT-utvikling, drift og forvaltning og gikk gradvis fra en konsulentdominert IKT-utvikling til intern produktutvikling. Direktoratet har etter dette bygget kompetanse og kapasitet til å forestå utvikling, drift og forvaltning av hele sin IKT-portefølje.

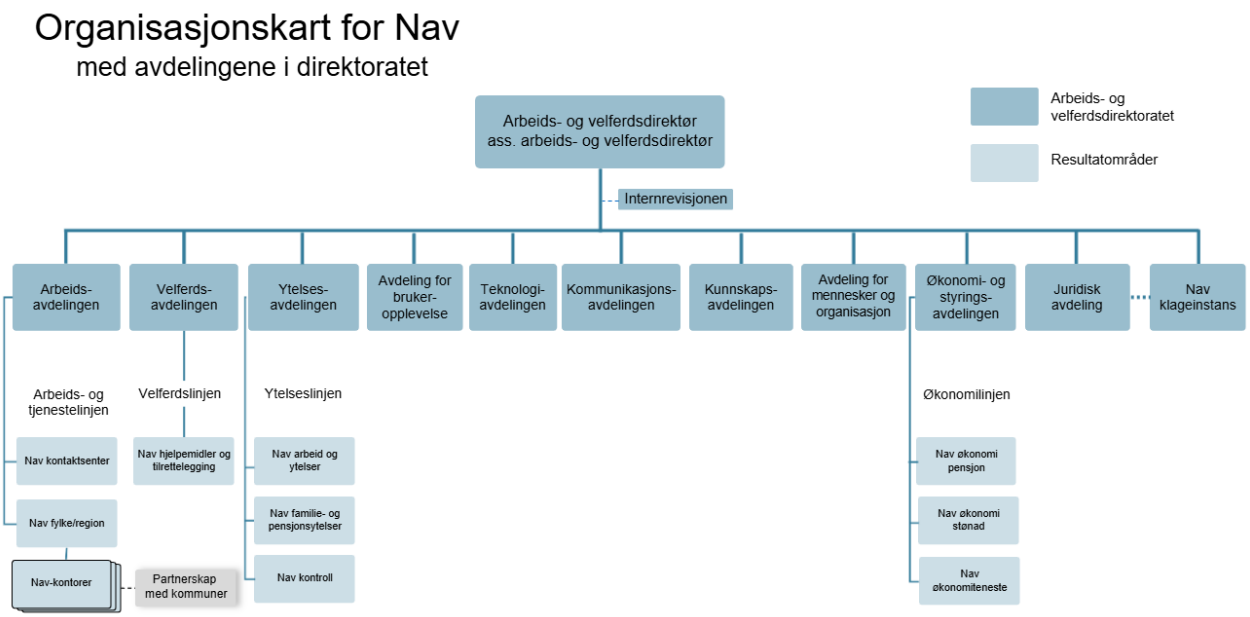
3.4.2. Større omorganisering i 2025

I mai 2025 gjennomgikk direktoratet en større omorganisering. Ifølge direktoratets årsrapport for 2025 var et overordnet mål å sikre et sterkt faglig og strategisk direktorat med bedre samhandling og bedre tjenester til brukerne. Det ble lagt vekt på å legge til rette for et mer tverrfaglig samarbeid mellom direktoratets rundt 1 800 ansatte.

- Direktoratet er organisert i avdelinger. Arbeidsavdelingen, Velferdsavdelingen, Ytelsesavdelingen og Økonomi- og styringsavdelingen (ØSA) har underliggende driftsenheter utenfor direktoratet som utfører etatens kjerneoppgaver. Ansvaret for underliggende driftsenheter innebærer et linjeansvar.
- Kvalitetsseksjonen i ØSA er ansvarlig for den grunnleggende internkontrollprosessen og tilhørende metoder og verktøy. Kvalitetsseksjonen har et særskilt ansvar for å sikre felles begrepsbruk, metodikk og opplæring på tvers av virksomheten. Kvalitetsseksjonens rolle

er å fastsette rammer og sikre felles forståelse, ikke å overta faglig påseansvar fra de øvrige enhetene med virksomhets- eller avdelingsovergripende ansvar.

- Direktørene for Avdeling for brukeropplevelse, Kunnskapsavdelingen, Kommunikasjonsavdelingen, Avdeling for mennesker og organisasjon, Teknologiavdelingen, Juridisk avdeling og Økonomi- og styringsavdelingen har ansvaret for felles-, støtte- og styringsfunksjoner som berører både etaten og direktoratet. Direktoratets klageinstans er organisert som en egen avdeling i direktoratet.
- De tre avdelingene Arbeidsavdelingen, Velferdsavdelingen og Ytelsesavdelingen har resultat- og fagansvar for sine ytelser og tjenester, herunder ansvaret for IKT-utvikling, drift og forvaltning av egne produkter. Det samme har Økonomi- og styringsavdelingen for utbetalingsløsningene til Nav.
- Direktørene skal løse enkeltoppdrag for, og representere arbeids- og velferdsdirektøren i, eksterne og interne fora.
- Juridisk avdeling er direktoratets felles juridiske enhet med en overgripende rolle knyttet til de juridiske funksjonene.
- Internrevisjonen har myndighet til å gjennomføre revisjoner i hele etaten, jf. forskrift om
- internrevisjon i Arbeids- og velferdsetaten.

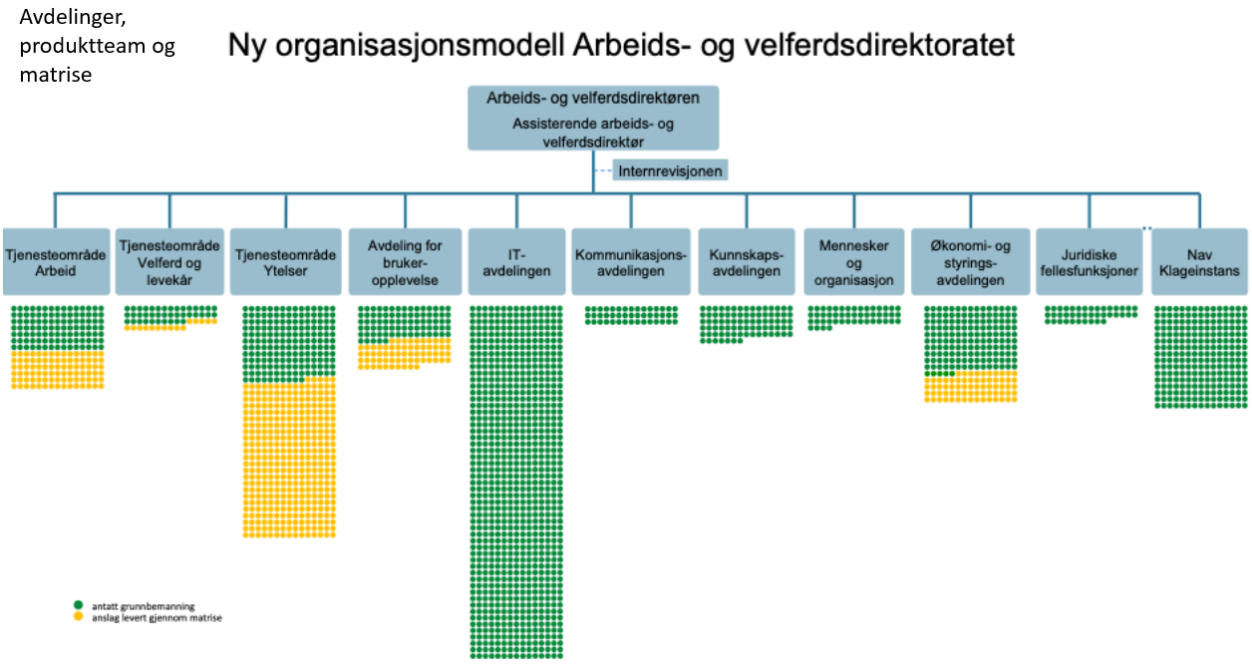


Figur 4 Arbeids- og velferdsdirektoratets organisering etter omorganiseringen i 2025. NB: Ny endring fra 1.4 - NKS en del av YTL

De tre avdelingene Arbeidsavdelingen, Velferdsavdelingen og Ytelsesavdelingen har etablert tverrfaglige lederteam med representanter da de ulike «støtte-avdelingene» med det formål å sikre tverrfaglig lederkompetanse og involvering – se figur 5.

Figur 5 Tverrfaglige lederteam

Direktoratet er organisert som matrise – se figur 6.

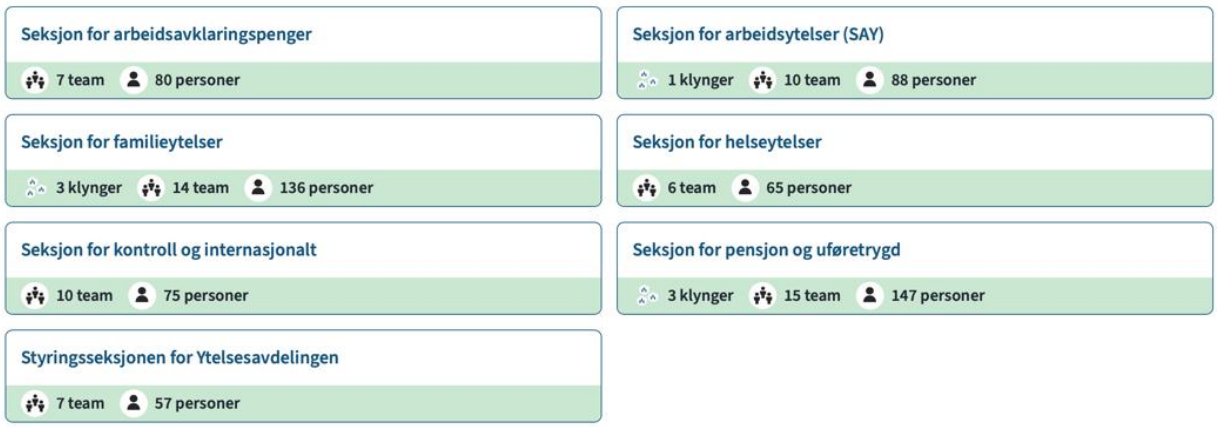


Figur 6 Matriseorganisering – grunnbemanning og ansatte fra andre avdelinger

Teknologiavdelingen samler alle IKT-medarbeidere og har per i dag rundt 800 ansatte. Disse kan også "lånes" ut til produktteam der all utvikling, drift og forvaltning innenfor avdelingene gjennomføres. Teknologiavdelingen skal utgjøre en strategisk kraft for utviklingen av direktoratet

og etaten i stort gjennom digitalisering gjennom å sette tydelig faglig retning samt utarbeide strategier, prinsipper og standarder på avdelingens ansvarsområder. Teknologiavdelingen skal i henhold til *Ansvarsdokumentet* fra mai 2025 «levere stabile, endringsdyktige, sikre og kostnadseffektive plattformer og verktøy, og kontinuerlig utvikle og forbedre arbeidsmåter, organisering og kompetanse. Avdelingen skal samarbeide tett med andre avdelinger i verdiøkende tilbakemeldingssløyfer».

En stor andel medarbeidere blir lånt ut til produktteam og har sitt faglige hjem der. Totalt er det i dag rundt 120 ulike produktteam, fordelt på disse fire avdelingene. Hvert produktteam er tverrfaglig sammensatt. Figur 7 eksemplifiserer dette for Ytelsesavdelingen:



Figur 7 Organisering i produktteam – tverrfaglig sammensatte team

3.5. Direktoratets internkontrollrammeverk

3.5.1. Innledning

I dette kapittelet beskriver vi faktum knyttet til status og pågående forbedringsarbeid med helhetlig internkontrollrammeverk i direktoratet, både arbeid knyttet til et helhetlig internkontrollrammeverk og IKT-internkontrollrammeverk for utvikling, drift og forvaltning av etatens IKT-systemer. For en virksomhet hvor utførelsen av samfunnsoppdraget i stor grad avhenger av en velfungerende IKT-ramme vil det ikke være hensiktsmessig å se internkontrollen knyttet til IKT som adskilt fra direktoratets helhetlige internkontrollsystem. Dette er et prinsipp KPMG også vil vektlegge i rapportens tiltaksanbefalinger og implementeringsplan.

Styrende dokumenter gir per i dag en overordnet beskrivelse av interne krav, roller, ansvar og prinsipper, og internkontroll er formelt integrert i lederansvaret. Direktoratet har etablert styringsdokumentasjon og føringer innen sentrale IKT-områder som sikkerhet, tilgangsstyring og endringshåndtering. Per mai 2026 har to nye styrende dokumenter nylig blitt godkjent av arbeids- og velferdsdirektør: *Retningslinje for internkontroll i Nav* v1.1 erstatter *Policy for internkontroll* fra 2008, og *Veileder internkontroll* er en nyopprettet operasjonalisering av denne. I tillegg er *Veileder for gjennomføring av internkontrollsprinter i Nav* godkjent og skal revideres i juni 2026. I delkapitlene 3.5.2-3.5.8 oppsummerer vi de viktigste punktene.

Direktoratet har i 2026 initiert flere forbedringsaktiviteter for å styrke kvalitet, internkontroll og risikostyring i virksomheten. Forbedringsaktivitetene omfatter både utvikling av felles styringsrammer og mer operative tiltak rettet mot prioriterte risikoområder. Arbeidet inngår i et

langsiktig løp som startet i 2024 for å sette kvalitet og internkontroll i et helhetlig system. Bakgrunnen er blant annet tidligere evalueringer av direktoratets kvalitetsarbeid, revisjonsmerknader knyttet til internkontroll og behovet for mer ensartet styring, dokumentasjon og oppfølging på tvers av etaten. Hovedaktivitetene er beskrevet i 3.5.6.

3.5.2. Virksomhetsstrategi – Nav 2030

KPMG observerer at virksomhetsstrategien ikke beskriver et ambisjonsnivå for internkontroll i direktoratet. KPMG observerer at internkontroll ikke er eksplisitt beskrevet i dokumentet *Virksomhetsstrategi – Nav 2030*. Operasjonaliseringen av Navs strategi skjer i treårige prioriteringer. Disse er under revisjon og nye treårige prioriteringer skal etter planen vedtas i juni 2026.

3.5.3. Mål- og disponeringsbrev

I *Mål- og disponeringsbrev 2025* til enhetene er inkludert seksjon «4 Krav til intern kontroll» med felles tekst for alle enheter som mottar mål- og disponeringsbrev. Kravene er skrevet på et overordnet nivå og ikke operasjonalisert i roller og ansvar per enhet.

Mål, krav og ansvar mht. internkontroll er i *Mål- og disponeringsbrev 2026*, f.eks. YA operative mål under ambisjon 4 «*Avdelingen har jobbet proaktivt, strukturert og helhetlig med personvern, internkontroll og sikkerhetsarbeidet*.»

Til ØSA er det gitt følgende mål fra arbeids- og velferdsdirektøren i «Etablerte rammer for helhetlig kvalitetsledelse og -styring i Nav». Målet har følgende indikatorer:

- Besluttet ambisjonsnivået for helhetlig kvalitetsledelse og kvalitetsstyring i Nav basert på anbefalingen fra BCG høsten 2024
- Gjennomført vedtatt plan for 2025 med å få på plass et system for helhetlig kvalitetsledelse og kvalitetsstyring
- Utviklet kvalitetsnettverket gjennom systematisk dialog om elementer, mekanismer, verktøy og innhold

ØSA-direktør har gitt tilsvarende mål til leder av seksjon for strategi og etatsstyring, som har ansvaret for å følge opp målet på vegne av ØSA-direktør med følgende indikatorer:

- Besluttet ambisjonsnivået for helhetlig kvalitetsledelse og kvalitetsstyring i Nav basert på anbefalingen fra BCG høsten 2024 og egen modenhetsvurdering.
- Gjennomført vedtatt plan for 2025 med å få på plass et system for helhetlig kvalitetsledelse og kvalitetsstyring.
- Utviklet kvalitetsnettverket gjennom systematisk dialog om elementer, mekanismer, verktøy og innhold.
- Inkludert temaet kvalitetsledelse og kvalitetsstyring i fremtidige møtearenaer for ledere på ulike nivåer for å sikre eierskap og etterlevelse.

3.5.4. Ansvar for etterlevelse

Direktoratet er underlagt strenge og sammensatte regulatoriske krav. Kraveiere sitter i ulike deler av organisasjonen. Kraveier for økonomireglementet er Økonomi- og styringsdirektør i direktoratet. Kraveier har ansvar for

- lovtolkning,
- utarbeiding av rundskriv og etterlevelseskrav,
- å svare ut spørsmål til krav og
- forvaltning av krav, herunder regelverksendringer.

Ansvar for lovtolkning og regelverk innebærer ansvar for å tolke eksisterende lov og forskrift på vegne av etaten, og sikre at denne er i tråd med lovgivers og departementets intensjoner. Det innebærer en instruksjonsmyndighet over alle enheter i etaten. Ansvaret vil være noe ulikt for generelle bestemmelser og for de ytelsesspesifikke bestemmelsene. Ansvaret innebærer å sikre at lovtolkningen gjenspeiles i rundskriv. Juridisk avdeling har ansvar for regelverk som ikke er opplistet og ansvarsplassert.

Ytelsesavdelingen, Arbeidsavdelingen og Velferdsavdelingen har ansvaret for etterlevelse av faglig regelverk knyttet til Navs ytelser og tjenester. Støtteavdelinger, som Mennesker og organisasjon og Økonomi- og styringsavdelingen, vil ha ansvar for prosesser og løsninger som er rettet mot interne, for eksempel virksomhetens oppgaver som arbeidsgiver og eiendomsforvaltning. Risikoeier skal gjennomgå produktteamenes dokumentasjon i etterlevelsesverktøyet, vurdere om krav og suksesskriterier er tilstrekkelig besvart, og ta stilling til eventuell gjenværende risiko.

I kapittel 3.8.3 om etterlevelsesverktøyet beskriver vi det digitale verktøyet direktoratet har utviklet for å sikre sporbarhet knyttet til etterlevelse på tvers av alle produktteam.

3.5.5. Ansvar for internkontroll

Ansvaret for internkontroll er plassert i avdelingene, og det er etablert styrings- og beslutningsarenaer på tvers av fag, teknologi og styring. *Ansvarsdokument for Arbeids- og velferdsdirektoratet* (ansvarsdokumentet) fra februar 2026 gir en overordnet beskrivelse av ansvar, ansvarsområder og oppgaver for direktører på nivå 1 i direktoratet (heretter kalt «direktørene»).

Om ansvaret til første- og andrelinjen i direktoratet

Ansvaret til første- og andrelinjen i direktoratet er beskrevet som følger:

3.2 Prinsipper for ansvar og fordeling av ansvarsområder

> *Alle avdelinger skal ha en oppdatert oversikt over egen organisering med tilhørende ansvarsbeskrivelser. Oversikten skal være beskrevet på Navet, som en del av Navs system for kvalitet og internkontroll.*

Virksomhetsstyring (utdrag): Tilpasse styring, oppfølging, internkontroll og forvaltning til risiko, vesentlighet og egenart

Kvalitet, internkontroll og risiko

- *Definere kvalitet innenfor eget ansvarsområde og sikre at leveranser holder rett kvalitet*
- *Følge opp og lære av avvik, revisjonsmerknader og tilsyn*
- *Sikre etterlevelse av lovkrav og retningslinjer*

- *Dokumentere nødvendig styring (styrende, gjennomførende og kontrollerende dokumenter) og forvalte styrende dokumenter på eget område*
- *Sørge for forsvarlig sikkerhet og gjennomføre nødvendig beredskapsarbeid, jf. kap. 3.5 Beredskapsansvar*
- *Sikre god informasjonsforvaltning*
- *Bruke risikostyring aktivt som styringsverktøy*
- *Iverksette nødvendige internkontrolltiltak*
- *Sikre og dokumentere systematisk HMS-arbeid [Ref194.2.9 Detaljert oversikt over ansvar for felles-, støtte- og styringsfunksjoner*

Økonomi- og styringsavdelingen: Etats- og virksomhetsstyring av Nav, herunder strategi, mål, budsjett, portefølje, virksomhetsarkitektur, gevinststyring, risikostyring, samt helhetlig system for kvalitet og internkontroll i Nav

Juridisk avdeling: Forvalte og videreutvikle internkontroll for personvern

Juridisk avdeling: Juridisk internkontroll og kvalitetskontroll

KPMGs observasjoner:

I intervjuene KPMG har gjennomført beskriver ansatte gjennomgående at rolle- og ansvarsforståelsen knyttet til internkontroll i første- og andrelinjen i praksis er uklar, særlig i grenseflatene mellom Teknologi, Økonomi- og styringsavdelingen og Juridisk. Særlig påpeker ansatte et andrelinjefunksjonen for internkontroll er lite operasjonalisert, med uklare forventninger til veiledning, påse-, verifikasjons- og eskaleringsansvar.

I ny *Veileder for internkontroll* som ble godkjent i mai 2026 er det inntatt beskrivelser av trelinjemodellen, med tydeliggjøring av roller og ansvar (se avsnitt 3.5.7). Internkontrollprosjektet har kommunisert til KPMG at prosessen for utarbeidelsen av Internkontroll-retningslinjen har bidratt til en meget stor grad av tydelighet på rolle og ansvar basert på responsen fra styringsmiljøene

Produktteamene

Det er etablert rundt 120 tverrfaglige produktteam som har ansvar for hele livsløpet til sine løsninger – utvikling, drift og forvaltning. Teamet har en ansvarlig leder i den formelle organisasjonsstrukturen, se eksempel i figur 6. Det gjennomføres kvalitetssikringer som er dokumentert i kvalitetssikringsrapportene fra internrevisjonen.

I intervjuene med KPMG fremgår det gjennomgående at produktteamene har betydelig frihet til å velge verktøy, arbeidsmetodikk og teknologier innenfor rammene av felles plattformer og overordnede prinsipper. Ansatte beskriver gjennomgående produktteamene som svært autonome og styringen i produktteamene som mål- og risikobasert, med korte planhorisonter (typisk 3 måneder), mens langsiktige veikart i mindre grad er formalisert. Produksjonssetting skjer med varierende frekvens avhengig av risiko. Noen produktteam setter i produksjon flere ganger daglig, mens andre gjør dette sjeldnere.

Ansvaret til tredjelinjen i direktoratet

Internrevisjonen, dvs. tredjelinjen i direktoratet, beskrives som følger:

> *Internrevisjonen i Nav er en objektiv bekreftelses- og rådgivningsfunksjon direkte underlagt arbeids- og velferdsdirektøren. Internrevisjonen styrker Navs evne til å skape, beskytte og opprettholde verdi ved å gi arbeids- og velferdsdirektøren og ledergruppen uavhengige, risikobaserte og objektive bekreftelser, råd, innsikt og fremtidsrettede vurderinger. Internrevisjonen har myndighet til å gjennomføre revisjoner i hele etaten, jf. forskrift om internrevisjon i Arbeids- og velferdsetaten.*

KPMGs observasjoner:

I intervjuene KPMG har gjennomført med internrevisjonen fremkommer det at internrevisjonen gjennomfører både regelmessige og ad hoc-møter med Riksrevisjonen. Det avholdes møter som beskrives som samhandlingsmøter der internrevisjonen sammen med Riksrevisjonen blant annet gjennomgår revisjonsplaner for kommende periode.

KPMG får forklart at internrevisjonens prioriteringer for en gitt revisjonsperiode vil hensynta de områder og formål Riksrevisjonen kommuniserer at planlegges, og at det i hovedsak vil innebære at internrevisjonen retter sine ressurser i andre retninger. Formålet er å dekke så mange områder som mulig gitt avdelingens ramme ved å hindre overlapp i dekning. I enkelte tilfeller vil internrevisjonen aktivt ønske å dekke områder som står på Riksrevisjonens plan.

Ansvar knyttet til lovtolkning og regelverk

Vedlegg 1 i ansvarsdokumentet beskriver ansvaret for lovtolkning og regelverk. Direktoratet forvalter rundt 70 ytelser i 54 ulike fagsystemer. Regelverket direktoratet forvalter er komplisert og krever mye skjønnsutøvelse. Tolkningsansvaret for de ulike regelverkene ligger hos definerte kraveiere. Kraveierne har ansvar for å

- tolke regelverket,
- publisere etterlevelseskrav,
- kvalitetssikre beskrivelser innenfor egne fagområder, og
- oppdatere kravene ved behov.

Økonomi- og styringsavdelingen har ansvaret for økonomiregelverket.

Av ansvarsdokumentet følger det videre at avdelingene i direktoratet har ansvar for etterlevelse av kravene til sine aktiviteter. Avdelingene har selv ansvar for å følge opp etterlevelse innenfor sine ansvarsområder. Kraveierne har ansvar for overordnet oppfølging innenfor sine lovtolkningsområder. Et konkret eksempel på slik oppfølging er ledelsens gjennomgang på personvern- og sikkerhetsområdet.

KPMGs observasjoner:

I intervjuer KPMG har gjennomført fremgår det at hvert produktteam skal dokumentere hvorvidt krav er oppfylt i etterlevelsesverktøyet (beskrevet i avsnitt 3.8.3). For nye applikasjoner er utgangspunktet at alle relevante krav skal dokumenteres i verktøyet før produksjonssetting. Når det er behov for personvernkonsekvensvurdering (PVK) gjennomføres denne som en del av samme dokumentasjonsløp. Digital PVK er integrert i Støtte til etterlevelse-verktøyet, og det er et

1:1-forhold mellom et etterlevelsesdokument og en eventuell PVK. Når denne er ferdigstilt av produktteamet skal etterlevelsesdokumentet sendes til risikoeier for godkjenning.

I intervjuene med KPMG beskriver ansatte i produktteamene høye etterlevelseskrav kombinert med tidspress. De beskriver videre at dette fører til mangelfull og ujevn kvalitet i dokumentasjon. Samspillet mellom jurister og teknologer beskrives av mange som krevende med lite gjenbruk av felles beslutninger noe de opplever som ineffektivt.

Vedlegg 2 i ansvarsdokumentet beskriver eksterne samhandlere og fordeling av koordineringsansvar. Økonomi- og styringsavdelingen (ØSA) har koordineringsansvaret for Riksrevisjonen. Direktoratet har etablert en egen rutine (fra 2023) for samhandling med Riksrevisjonen. Hver enkelt enhet er faglig ansvarlig i møtet med Riksrevisjonen, med ØSA som koordinator. Flere ansatte påpeker i intervjuer med KPMG at et sentralt forbedringsområde er svakheter i kommunikasjon og samhandling mellom ulike team som er i kontakt med Riksrevisjonen.

3.5.6. Styringsdokumentasjon og føringer innen sentrale IKT-områder

Direktoratet har etablert styringsdokumentasjon og føringer innen sentrale IKT-områder. Innen enkeltområder (f.eks. informasjonssikkerhet, tilgangsstyring og delvis endringshåndtering) finnes det etablerte og strukturerte krav gjennom standarder, retningslinjer og rutiner. Direktoratet har etablert krav og tiltak knyttet til logging, og KPMG har observert at logging inngår som et konkret kravområde i Støtte til etterlevelse. NAIS-plattformen inneholder også innebygde mekanismer som understøtter logging og sporbarhet (se avsnitt 3.7.2). Samtidig pågår det et arbeid med å strukturere dokumentasjonen. Gjennom intervjuer KPMG har gjennomført beskrives dagens situasjon som «work in progress». Det finnes omfattende dokumentasjon på Navet (se avsnitt 3.5.8), men flere peker på at struktur og tilgjengelighet gjør det krevende å få en samlet oversikt. Som del av det pågående forbedringsarbeidet foretar direktoratet nå en revisjon av risikometodikk og arbeid med retningslinjer og veiledere.

Direktoratet har etablert prosesser for risikostyring, og risiko inngår som en del av styringsdialogen med ledelsen. TryggNok (se avsnitt 3.8.2) benyttes som verktøy for dokumentasjon av risikovurderinger knyttet til digitale løsninger, basert på vurderinger av sannsynlighet og konsekvens. TryggNok dekker følgelig primært operative vurderinger på løsningsnivå. I intervjuer med produktteamene påpeker ansatte til KPMG at det ikke er etablerte dokumenterte prosesser for hvordan tiltak skal prioriteres og følges opp på en enhetlig måte etter at risiko er identifisert. Intervjuene KPMG har gjennomført med produktteam indikerer at oppfølgingen i stor grad håndteres lokalt i teamene.

I intervjuer med KPMG etterlyser en rekke ansatte i produktteamene tydeligere mekanismer for prioritering i en hektisk hverdag. De uttaler at kapasiteten er begrenset og det er vanskelig for produktteamene å avgjøre “hva som brenner mest”.

Intervjuer og revisjonsmerknader viser at praksis for oppfølging og bruk av logger varierer mellom miljøer og løsninger. Det er ikke fremlagt dokumentasjon som viser en standardisert og gjennomgående praksis for kontroll, analyse og oppfølging av logger på tvers av teamene.

3.5.7. Direktoratets internkontrollprosjekt

Direktoratet etablerte i 2026 et eget internkontrollprosjekt. Prosjektet jobber med de grunnleggende kravene som stilles til internkontroll som finnes i Økonomiregelverket (§ 14). Det betyr at prosjektet jobber med å forbedre den grunnleggende, generelle tilnærming til internkontroll i direktoratet for å sikre at denne blir enhetlig og helhetlig. I tillegg vil man jobbe med etterlevelse av de konkrete bestemmelsene knyttet til relevante prosesser og økonomisystem (som beskrevet i Bestemmelsene). Prosjektet består av fire leveransestrømmer, som illustrert i figuren nedenfor:

Figur 8 Leveransestrømmer i internkontrollprosjektet

Prosjektet må ses i sammenheng med det langsiktige arbeidet med å sette kvalitet og internkontroll i system. Bakgrunnen for prosjektet er blant annet anbefalingene fra tidligere gjennomganger av direktoratets kvalitetsarbeid, Riksrevisjonens merknader i revisjonen av 2024-regnskapet og Arbeids- og inkluderingsdepartementets ønske om en ekstern vurdering av direktoratets systematiske arbeid med internkontroll knyttet til utvikling, drift og forvaltning av etatens IKT-systemer. Revisjonsmerknadene gjaldt blant annet mangelfull dokumentasjon av endringer i databaser knyttet til utbetaling av pensjon, uføretrygd og foreldrepenger, samt svakheter på ortopediområdet og hjelpemiddelområdet.

Formålet med prosjektet er å bidra til at internkontrollen i direktoratet i større grad oppfyller kravene i økonomiregelverket, særlig knyttet til de grunnleggende styringsprinsippene og kravene til internkontroll. Prosjektet skal bidra til at relevante krav i økonomiregelverket forstås og omsettes til konkrete rutiner, kontrollaktiviteter og oppfølging i drift, produktutvikling og forvaltning av økonomisystemene. Arbeidet skal baseres på vurderinger av vesentlighet og risiko, og inngår i ambisjonen om at hele etaten skal opp på et strukturert nivå for kvalitet og internkontroll innen utgangen av 2027.

Figur 9 Internkontrollprosjektets målbilde

Prosjektet ligger direkte under ØSA-direktør. Arbeidet gjøres i tett samarbeid med Kvalitetsseksjonen. Det er etablert en styringsgruppe med direktører fra sentrale avdelinger og en prosjektgruppe med representanter fra flere sentrale avdelinger, herunder Teknologiavdelingen, Ytelsesavdelingen, Velferdsavdelingen, Arbeidsavdelingen og ØSA. Internrevisjonen deltar i styringsgruppen.

Prosjektet består av flere leveransestrømmer. En egen leveransestrøm om økonomiregelverket skal bidra til bedre forståelse av kravene til internkontroll, blant annet gjennom tydeliggjøring av relevante krav, oppdatering av virksomhetsovergripende retningslinjer og rutiner, samt etablering av opplæringsprogram for ledere og relevante medarbeidere. Denne delen av prosjektet omfatter også tolkning av krav knyttet til relevante IT-systemer.

Prosjektet omfatter også en leveransestrøm for forbedret internkontroll, med et eget delspor knyttet til Teknologiavdelingen og produktutvikling. Her skal arbeidet blant annet bidra til å etablere og forbedre rutiner og kontrollaktiviteter knyttet til logging og oppfølging av logger, samt styrke dokumentasjon og praksis på områder som er relevante for etterlevelse av økonomiregelverket. I tillegg omfatter prosjektet egne spor for ortopediområdet samt ekstern evaluering og oppfølging av Riksrevisjonens IT-revisjoner for 2025 og 2026. Når det gjelder Riksrevisjonens IT-revisjoner, skal prosjektet blant annet bistå med å svare ut spørsmål fra Riksrevisjonen, følge opp identifiserte observasjoner og forberede organisasjonen på videre revisjon.

I tillegg opplyses det at internkontrollprosjektet har etablert et minimumskontrollrammeverk for økonomisystemer. Hensikten med kontrollrammeverket er å etablere et felles rammeverk for hvilke grunnleggende kontroller som skal vurderes og følges opp i tilknytning til digitale løsninger og økonomisystemer. Matrisen skal bidra til å systematisere kontrollarbeidet og støtte arbeidet med å videreutvikle internkontroll som også ivaretar kravene i økonomiregelverket.

Internkontrollprosjektet er dermed innrettet både mot å styrke forståelsen av økonomiregelverket på et overordnet nivå og mot å etablere mer konkrete kontrolltiltak og rutiner i de delene av virksomheten der etterlevelsesrisikoen vurderes som størst. Dokumentasjonen viser at prosjektet særlig skal bidra til tydeligere roller og ansvar, bedre opplæring, mer strukturert oppfølging av internkontroll og sterkere kobling mellom kravene i økonomiregelverket og den praktiske utøvelsen av internkontroll i drift, produktutvikling og forvaltning av IKT-systemer.

3.5.8. Ny retningslinje og veileder for internkontroll

Per mai 2026 har tre nye styrende dokumenter nylig blitt godkjent av arbeids- og velferdsdirektør:

- *Retningslinje for internkontroll i Nav*, v1.1: Nytt dokument som erstatter *Policy for internkontroll* fra 2008
- *Veileder internkontroll*
- *Veileder for gjennomføring av internkontrollsprinter i Nav* godkjent

Begge dokumentene eies av Økonomi- og styringsdirektør. Den nyetablerte kvalitetsseksjonen i Økonomi- og styringsavdelingen er ansvarlig for den grunnleggende internkontrollprosessen og tilhørende metoder og verktøy. I retningslinjen er det beskrevet at direktoratets tilnærming til internkontrollprosessen bygger på DFØs *Veileder for internkontroll i statlige virksomheter*. Det innebærer at direktoratet ser på internkontroll som en prosess som utføres løpende, og som skal

gi tilstrekkelig god kontroll, tilpasset direktoratets egenart, vesentlighet og risiko. Formålet med veilederen er å gi praktisk og anvendbar støtte til hvordan internkontroll skal forstås og utøves i direktoratet. Veilederen er ment som et oppslagsverktøy.

Veilederen beskriver blant annet trelinjemodellen, som fremstilt i figuren nedenfor:

- Første linje: Alle som utfører direktoratets oppgaver og eier risiko i den daglige driften
- Andre linje: Enheter med avdelings- eller etatsovergripende ansvar, som fastsetter premisser, støtter implementering og følger opp etterlevelse
- Tredje linje: Internrevisjonen, som gir uavhengig trygghet

Eksempel på hvordan det henger sammen

Når Økonomi- og styringsavdelingen (ØSA) utvikler nye styringsprinsipper, krav til risikovurdering eller internkontroll, f.eks. rutine for å gjennomføre årlige risikovurderinger, gjelder disse for hele Nav.

Førstelinjen, alle linjeledere og medarbeidere, bruker disse kravene til å håndtere risiko i egen drift. De må:

- gjennomføre risikovurderinger for sitt område
- etablere kontrollaktiviteter som oppfyller kravene
- dokumentere og følge opp tiltak
- rapportere status i styringsdialogen

Førstelinjen gjør dette fordi de eier risikoen, ikke fordi de tilhører en bestemt avdeling.

Andrelinjen, her: ØSA og eksempelvis Juridisk avdeling eller Teknologiavdelingen, utvikler og forvalter metodikk, krav og retningslinjer. De:

- setter standardene for hvordan risikovurdering og kontroll skal utføres
- gir støtte, opplæring og avklaringer
- risikobasert oppfølging av etterlevelse
- harmoniserer praksis på tvers av etaten

Tredjelinjen, Internrevisjonen, gjennomfører uavhengige, risikobaserte vurderinger om retningslinjene er fulgt, om risikostyringen fungerer godt nok og om styringssystemet bør forbedres.

Dette viser at tre-linjemodellen ikke handler om organisasjonskart, men om hvordan krav settes ett sted i Nav, brukes av andre deler av Nav, og kontrolleres uavhengig, for å sikre god styring og risikohåndtering i hele etaten.

Figur 10 Beskrivelse av trelinjemodellen hentet fra direktoratets «Veileder internkontroll»

Formålet med *Veileder for gjennomføring av internkontrollsprinter i Nav* er å gi en kortfattet, praktisk og operativ beskrivelse av hvordan internkontrollsprintene skal planlegges og gjennomføres. Veilederen er ment å være et sentralt virkemiddel for å operasjonalisere *Retningslinje for internkontroll* og bidra til at kravene til risikobasert, helhetlig og etterprøvbar internkontroll faktisk iverksettes i praksis. Sprintene skal gjennomføres med aktiv involvering av operative medarbeidere, fordi risiko oppstår og håndteres i den daglige utførelsen. Denne involveringen er avgjørende for å sikre riktig risikoforståelse, treffsikre kontrolltiltak og realistiske forbedringer.

3.5.9. Nytt felles dokumenthierarki

Som del av arbeidet med å styrke kvalitet, internkontroll og risikostyring i direktoratet er det etablert et felles dokumenthierarki og en felles struktur for styrende dokumenter i etaten. Hensikten er å

skape en mer enhetlig tilnærming til styring, tydeliggjøre sammenhengen mellom eksterne krav og interne føringer, og legge til rette for mer systematisk oppfølging av kvalitet, internkontroll og etterlevelse. Dokumenthierarkiet inngår som en sentral del av direktoratets system for kvalitet og internkontroll.

Figur 11 Dokumenthierarki

Hierarkiet er bygget opp i seks nivåer. De øverste nivåene omfatter eksterne krav og overordnede styringssignaler, herunder lover, forskrifter, myndighetskrav, departementale føringer, tildelingsbrev og instruks for virksomhets- og økonomistyring. De mellomliggende nivåene omfatter felles føringer, metode og malverk for ledelse, virksomhetsstyring og vesentlige funksjoner på tvers av etaten. De nederste nivåene retter seg mot den enkelte enhets behov for lokal virksomhetsstyring, internkontroll, risikostyring og praktisk støttemateriell.

Dokumenthierarkiet tydeliggjør samtidig et skille mellom det som skal etterleves i fellesskap i etaten, og det som kan tilpasses lokalt. Nivå I til IV representerer felles krav og føringer som skal være styrende for hele etaten. Nivå V og VI gir rom for at den enkelte enhet kan tilpasse styring, kvalitet og kontroll til eget ansvarsområde og etablere lokale verktøykasser der dette er nødvendig. Hierarkiet er dermed utformet for å kombinere felles styring med lokal tilpasning innenfor fastsatte rammer.

Som del av dette arbeidet er en retningslinje for utarbeidelse av styrende dokumenter under arbeid. Betegnelsen «policy» skal ikke lenger benyttes, og erstattes av «retningslinje». Retningslinjen for kvalitet, internkontroll og risikostyring er angitt som overordnet øvrige styrende dokumenter på området. Dokumentstrukturen skal tydeliggjøre både dokumentenes formål og den innbyrdes rangordenen mellom dem, og bidra til mer konsistent bruk av begreper og dokumenttyper på tvers av virksomheten.

I dokumentstrukturen skilles det også mellom styrende, gjennomførende og kontrollerende dokumentasjon. Gjennomførende dokumentasjon omfatter blant annet veiledere, prosessbeskrivelser, sjekklister, maler og opplæringsmateriell, mens kontrollerende

dokumentasjon omfatter dokumentasjon som skal verifisere at styrende dokumenter er fulgt, sikre sporbarhet og gi grunnlag for å avdekke avvik. Eksempler på slik dokumentasjon er etterlevelsesdokumentasjon, logger, rapporter, evalueringer og revisjoner.

Dokumenthierarkiet og den tilhørende dokumentstrukturen er dermed utformet som en del av direktoratets pågående forbedringsarbeid for kvalitet og internkontroll. Strukturen skal gi tydeligere rammer for hvordan krav og føringer skal forstås, omsettes og følges opp i virksomheten, og skal understøtte mer enhetlig styring og mer systematisk internkontroll på tvers av etaten.

3.5.10. Samhandling og involvering i internkontrollprosjektet

Et gjennomgående tema i KPMGs intervjuer med ansatte i Teknologiavdelingen er at involveringen av teknologimiljøene i arbeidet med å styrke internkontrollen per i dag oppfattes som mangelfull. Ansatte i Teknologiavdelingen uttaler til KPMG at det er en forutsetning for å lykkes at Teknologiavdelingen er tungt involvert i utviklingen av IKT-førstelinjekontrollene.

Et gjennomgående tema i KPMGs intervjuer med ansatte i Teknologiavdelingen har også vært at kravstillerne bør jobbe mer tverrfaglig og mer brukerrettet. Mange IKT-ansatte opplever at kravstillere i for stor grad kun tolker kravene, uten å sikre at de er forståelig beskrevet for IKT-ansatte som skal implementere kravene. Flere teknologiansatte opplever mangelfull dialog mellom kravstillere og IKT-ansatte og beskriver utilstrekkelig involvering. De ansatte etterlyser tydeligere operasjonalisering av regelverkskrav til konkrete, gjenbrukbare praksiser. Det fremheves også av ansatte i Teknologiavdelingen at der er et tydelig gap mellom teknologimiljøene og toppledelsen når det gjelder teknologiforståelse og prioritering.

Ansatte i Teknologiavdelingen fremhever viktigheten av at etterlevelse i størst mulig grad er innebygget i plattformer og fellesløsninger, og at avhengighet av manuelle rutiner i overgangssoner mellom gammel og ny teknologi reduseres. Ansatte beskriver IKT-internkontrollen i dag som krevende, spesielt i et landskap med mange produktteam (om lag 120) og stor grad av autonomi. En rekke IKT-ansatte beskriver at styringen og etterlevelsen historisk har vært person- og kulturavhengig, heller enn standardisert og dokumentert på tvers av produktteamene. Gjennomgående beskriver ansatte at Riksrevisjonens funn har vært en viktig driver for forbedringer, spesielt de siste årene, men at arbeidet i stor grad har vært reaktivt og ressurskrevende. Ansatte etterlyser tydelige retningslinjer som beskriver minimumskrav til internkontroll på tvers av alle produktteam og uttaler at det mangler felles metrikker og forventninger som gjør det mulig å styre og prioritere internkontrollaktiviteter riktig.

3.5.11. Kompetanse og opplæring innen internkontroll

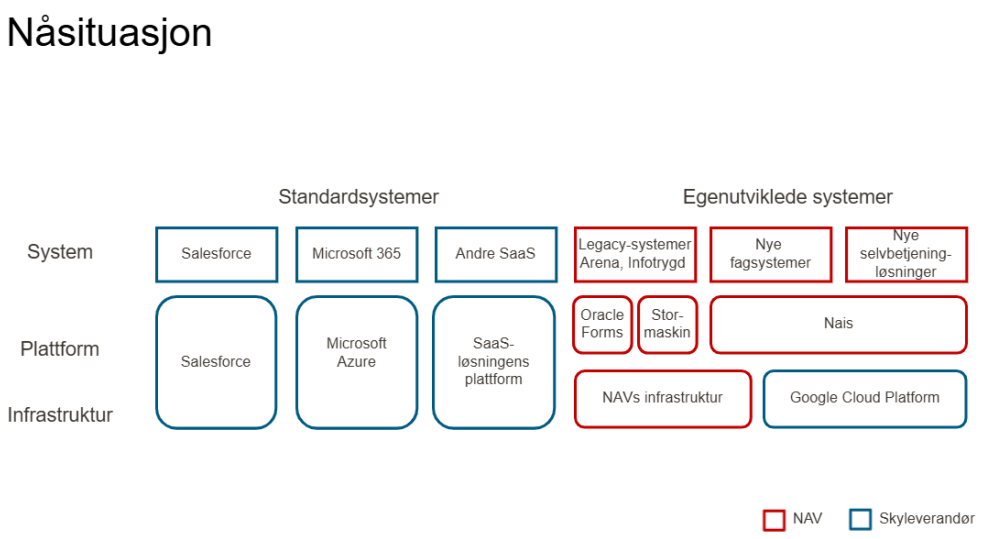
I intervjuene KPMG har gjennomført fremgår det tydelig at begrepet «internkontroll» ikke er et velkjent begrep for flere av de ansatte, på tvers av nivåer og enheter. Videre fremkommer det i intervjuene at det er et stort sprik i oppfatning av hva krav og forventninger til internkontroll innebærer i praksis, også på toppledernivå. Beskrivelsene av internkontroll slik de fremgår av COSO, COBIT, ISO og IIA er gjennomgående lite kjent blant ansatte i nøkkelroller med særskilt ansvar for internkontrollaktiviteter, også på ledernivå. Samtidig gjennomføres det en rekke aktiviteter i praksis, inkludert styrking av rutiner (ref. innebygget funksjonalitet i NAIS), uten at dette nødvendigvis forstås som internkontroll.

Det har det siste året vært økt oppmerksomhet rundt behovet for kompetanseheving innen internkontroll, økonomiregelverk og kvalitet. I intervjuene KPMG har gjennomført beskriver ansatte at opplæringen i liten grad fokuserer på læring fra kritiske hendelser, noe som bidrar til at kjente svakheter, særlig innen IT-kontroller, ofte vedvarer over tid.

Som del av det pågående Internkontrollprosjektet utarbeides det kompetansekrav og opplæringsprogram innen internkontroll for sentrale roller.

3.6. IKT-arkitektur

Direktoratets IKT-arkitektur er i dag sammensatt av standardiserte skytjenester, egenutviklede plattformsløsninger og eldre systemer som fortsatt driftes i virksomhetens egen infrastruktur. Direktoratet har under utvikling et eget system, Ardoq, for å holde oversikt over direktoratets applikasjoner og registre. Arkitekturen reflekterer en utvikling over tid, der nye løsninger i økende grad etableres i allmenn sky, samtidig som enkelte eldre systemer fortsatt er basert på tradisjonell teknologi. Dette innebærer at direktoratet forvalter en hybrid IKT-arkitektur med flere teknologiske generasjoner og driftsmodeller.



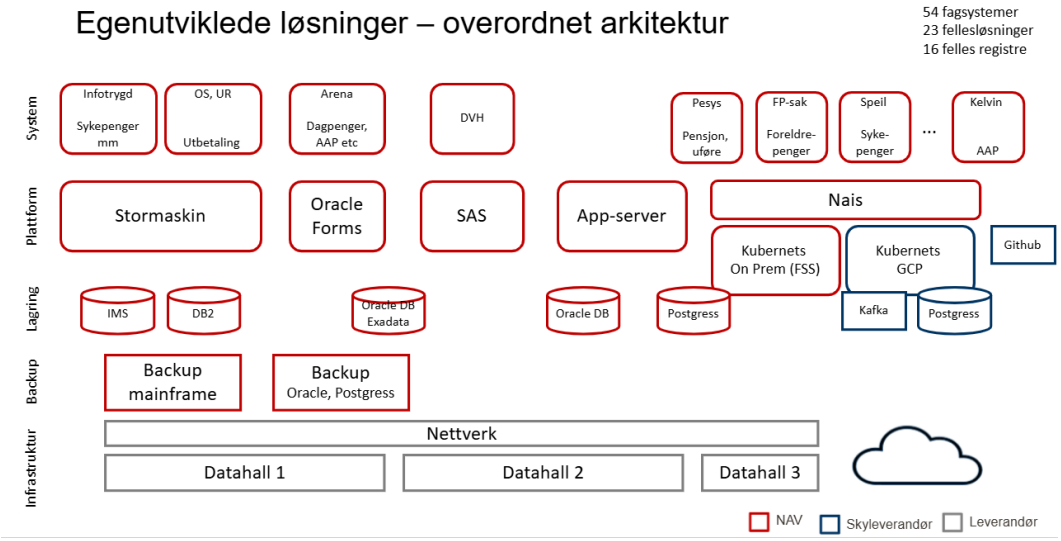
Figur 12 Nåsituasjon IKT-arkitektur

Arkitekturen kan overordnet forstås som lagdelt, bestående av systemer, plattformer og underliggende infrastruktur. På systemnivå inngår både standardiserte virksomhetsløsninger og egenutviklede systemer. Standardiserte løsninger leveres i hovedsak som skytjenester, blant annet Salesforce og Microsoft 365, og driftes av eksterne leverandører.

De egenutviklede løsningene omfatter både eldre fagsystemer og nyere skybaserte løsninger. Eldre systemer er fortsatt knyttet til teknologiplattformer som stormaskin og Oracle Forms og driftes i direktoratets egen infrastruktur. Nye løsninger utvikles i hovedsak for sky og bygger i stor grad på den egenutviklede plattformen NAIS, som inngår som en sentral komponent i moderniseringen av IKT-porteføljen.

På plattform- og infrastrukturnivå er løsningene fordelt på flere teknologiske lag og driftsmiljøer. Standardiserte løsninger er knyttet til plattformer og infrastruktur hos eksterne leverandører, mens

de egenutviklede løsningene er fordelt mellom interne miljøer og skybaserte plattformer. Dette innebærer at drift og forvaltning skjer på tvers av ulike teknologiske plattformer, databaser og leveransemodeller.



Figur 13 Nåsituasjon egenutviklede løsninger

Den totale porteføljen består av mer enn 550 ulike systemer, hvor de egenutviklede løsningene utgjør en vesentlig del. Porteføljen omfatter et stort antall fagsystemer utviklet og videreutviklet internt over tid, og innebærer at en betydelig del av direktoratets funksjonalitet både utvikles og forvaltes av virksomheten selv.

Disse løsningene er implementert på flere teknologiske plattformer, herunder stormaskin, Oracle Forms og NAIS, og er samtidig fordelt på ulike databaser og lagringsteknologier. Løsningene er også distribuert på tvers av datahaller og skymiljøer, noe som innebærer at både drift og forvaltning skjer innenfor ulike teknologiske og operasjonelle rammer.

I årsrapporten for 2025 beskrives porteføljen som svært kompleks og sammensatt, med utfordringer knyttet til legacy-systemer som fortsatt er i drift, herunder blant annet Infotrygd og Arena. Gjennom intervjuer og gjennomgått dokumentasjon fremkommer det at legacy-området er forbundet med vedvarende utfordringer, blant annet knyttet til krevende prioriteringer mellom utvikling av nye løsninger og arbeid med å erstatte eller bygge ned eksisterende systemer, samt begrenset tilgang på kompetanse innen eldre teknologier.

Dermed er direktoratet i et pågående moderniseringsarbeid, hvor en betydelig del av IKT-porteføljen er utviklet og forvaltes internt, støttet av høy teknologisk kompetanse og etablering av moderne plattformer som NAIS. Samtidig er porteføljen omfattende og kompleks, og inneholder fortsatt sentrale legacy-systemer som utgjør en kritisk del av virksomheten. Dette reflekteres også i etatens risikobilde, hvor legacy-området er vurdert som et område med vedvarende høy risiko.

3.7. Plattform for utvikling, drift og kjøring av applikasjoner (NAIS)

Direktoratet har utviklet en egen intern plattform for utvikling, drift og kjøring av applikasjoner, kalt NAIS. På direktoratets egne sider beskrives NAIS som en plattform laget for å gi «fart og flyt» til

utviklerne. Plattformen er i dag den sentrale utviklings- og driftsplattformen for nye digitale løsninger i direktoratet, og benyttes av de fleste fagområder. Enkelte eldre løsninger, som Arena, Infotrygd og stormaskinbaserte systemer, driftes fortsatt utenfor NAIS. Dette må ses i sammenheng med at NAIS i hovedsak er etablert som plattform for nyutvikling og videreutvikling av moderne applikasjoner, mens eldre legacy-systemer ofte bygger på teknologier og arkitekturer som ikke er direkte tilpasset drift på NAIS.

NAIS gir produktteamene et standardisert miljø for å utvikle, produksjonssette og drifte applikasjoner. Plattformen inneholder felles løsninger for blant annet kodehåndtering i Git, produksjonssetting, databaser, meldingsutveksling, logging, overvåking og tilgangsstyring. Dette bidrar til at mange grunnleggende krav til sikkerhet, drift og sporbarhet håndteres på en mer standardisert måte enn dersom hvert produktteam skulle etablert egne løsninger.

Bruk av NAIS er i prinsippet frivillig, men plattformen benyttes i praksis bredt fordi den gir produktteamene ferdige rammer og støttefunksjoner som forenkler utvikling og drift. Plattformen bidrar også til å redusere terskelen for å etterleve krav knyttet til logging, endringshåndtering, tilgangsstyring og sikkerhet. Samtidig bygger modellen på at produktteamene fortsatt har ansvar for egne applikasjoner og for å bruke plattformens funksjonalitet på riktig måte for å operasjonalisere etterlevelse av relevante lovkrav.

I det følgende beskrives den tekniske løsningen i større detalj.

3.7.1. Teknologisk arkitektur og sikkerhetsmodell

NAIS er bygget som en felles plattform for moderne applikasjonsutvikling. Plattformen gjør det mulig å standardisere hvordan applikasjoner bygges, testes, settes i produksjon og driftes. For ledelsen er det sentrale at NAIS gir et felles teknisk rammeverk som kan bidra til mer ensartet praksis, bedre kontroll og tydeligere sporbarhet på tvers av produktteam.

Plattformen skiller mellom eldre interne driftsmiljøer og skybaserte løsninger. I skybaserte miljøer er utgangspunktet at applikasjoner ikke automatisk kan kommunisere med hverandre. Hver applikasjon må definere hvilke andre applikasjoner den skal kunne kommunisere med. Dette gir bedre kontroll med informasjonsflyt mellom systemer og reduserer risikoen for utilsiktet tilgang.

NAIS legger også til rette for at hvert produktteam har sitt eget avgrensede område i plattformen. Teamene kan utvikle og drifte egne applikasjoner innenfor definerte rammer, men har ikke ubegrenset tilgang til andre team sine løsninger eller til plattformen som helhet. Dette understøtter prinsippet om avgrensede rettigheter, rollebasert tilgangsstyring og tydeligere ansvarsdeling.

Plattformen tilbyr et avgrenset sett med standardiserte tjenester. Dette omfatter blant annet løsninger for kodeforvaltning, automatiserte bygg- og produksjonsløp, databaser og meldingsutveksling. Et bevisst smalt teknologispekter bidrar til stabilitet, forvaltbarhet og mer ensartet praksis. Det sentrale plattformteamet forvalter infrastrukturen og de felles plattformtjenestene, mens produktteamene har ansvar for applikasjonene de bygger og drifter på plattformen.

NAIS har også innebygde mekanismer som kan hindre at applikasjoner settes i produksjon dersom bestemte krav ikke er oppfylt. Dette kan for eksempel gjelde krav til hvordan applikasjoner skal kommunisere med andre løsninger, eller krav til at nødvendige konfigurasjoner er definert før

applikasjonen kan kjøres. På denne måten kan enkelte kontroller bygges inn i selve utviklings- og produksjonsløpet, fremfor å være avhengig av manuelle vurderinger i etterkant.

Endringer i applikasjoner skjer gjennom standardiserte arbeidsprosesser. Kode forvaltes i Git, og endringer dokumenteres gjennom kodehistorikk, pull-requests og sammenslåing av kode. Dette gir sporbarhet på hvem som har foreslått, gjennomgått og godkjent endringer, når endringene er gjort, og når de er satt i produksjon. Plattformen legger også til rette for kodegjennomgang, testing og automatiserte produksjonsløp, noe som bidrar til mer konsistent endringshåndtering.

Tilgangsstyring er en integrert del av NAIS. Tilganger til plattformen styres gjennom direktoratets sentrale løsninger for identitet og tilgang, og produktteamene får tilgang til sine egne områder basert på roller og rettigheter. Plattformen har også egne mekanismer for håndtering av passord, nøkler og andre sensitive tekniske verdier, slik at slike opplysninger ikke håndteres direkte i applikasjonskode eller på ustrukturerte måter.

NAIS samler også inn logger og overvåkingsdata fra applikasjonene. Dette gir produktteamene mulighet til å følge med på drift, oppdage feil og håndtere hendelser. Sentrale hendelser som produksjonssettinger, endringer i kapasitet, tilgangsforespørsler og enkelte databaseoperasjoner logges og kan brukes som revisjonsspor ved kontroll og etterprøving.

Samlet sett fungerer NAIS som et standardisert og kontrollert miljø for utvikling og drift av applikasjoner. Plattformen gir et godt utgangspunkt for å bygge inn kontroller i utviklings- og driftsprosessene, men forutsetter samtidig at produktteamene følger opp de kontrollene, loggene og varslene som plattformen tilgjengeliggjør.

3.7.2. Logging, sporbarhet og manuelle endringer

NAIS har omfattende logging på plattformnivå. Dette omfatter blant annet logger for innlogging, produksjonssetting, endringer i kapasitet og enkelte databaseoperasjoner. Slike logger gir grunnlag for å etterprøve hvem som har gjort hva, og når ulike handlinger er gjennomført.

Det er også utviklet egne løsninger for å samle og presentere informasjon om manuelle databaseendringer. Formålet er å gjøre det mulig for produktteamene å gjennomgå, bekrefte og dokumentere slike endringer i etterkant. Dette er særlig relevant der endringer gjøres utenfor applikasjonenes ordinære funksjonalitet.

Kontrollene knyttet til slike manuelle endringer er i hovedsak detekterende. Det betyr at de først og fremst synliggjør hva som har skjedd etter at en handling er utført, fremfor å kreve forhåndsgodkjenning før handlingen gjennomføres. Effekten av kontrollene avhenger derfor av at produktteamene faktisk gjennomgår loggene, vurderer eventuelle avvik og dokumenterer oppfølgingen.

Loggingen i NAIS må også ses i sammenheng med kodehistorikk og produksjonslogger. For kodeendringer vil Git gi sporbarhet på endringer i kildekode, mens plattformens logger gir informasjon om blant annet produksjonssettinger, driftsendringer og tilgangsbruk. Samlet kan dette gi et mer helhetlig revisjonsspor, forutsatt at informasjonen er tilgjengelig, strukturert og brukes aktivt i kontrollarbeidet.

Samlet gir loggingen i NAIS et viktig grunnlag for internkontroll, revisjonsspor og hendelseshåndtering. Samtidig forutsetter dette tydelige rutiner for hvem som skal følge opp loggene, hvor ofte dette skal gjøres, og hvordan eventuelle avvik skal dokumenteres og håndteres.

3.7.3. Tilgangsstyring

Tilgangsstyringen i NAIS er i stor grad basert på produktteamenes ansvar for egne applikasjoner. Teamene får tilgang til sine egne områder i plattformen, mens tilgang til andre områder er begrenset. Dette gir tydeligere avgrensning mellom teamene og reduserer risikoen for at brukere får bredere tilgang enn nødvendig.

Tilganger til databaser gis normalt tidsbegrenset gjennom egne verktøy. Det kan for eksempel gis tilgang for et kort tidsrom ved behov for feilretting eller analyse. Slike tilganger logges, slik at det i etterkant er mulig å se hvem som har hatt tilgang og når tilgangen ble benyttet.

Plattformen legger dermed til rette for god praksis, blant annet gjennom prinsipper om begrensede rettigheter, tidsavgrensede tilganger og sporbarhet. Samtidig sikrer ikke plattformen alene at alle team etablerer tilstrekkelige rutiner for kontroll rundt slike tilganger, for eksempel fire øyne-prinsipp eller særskilte prosesser for hastesituasjoner.

I intervjuer med KPMG er logging og revisjonsspor beskrevet som et krevende område. Selv om NAIS teknisk støtter omfattende logging, er det i praksis behov for å avklare nærmere hva som skal logges, hvem som har ansvar for oppfølgingen, og hvilke formål loggingen skal dekke. Det er også pekt på at kontekst kan gå tapt når krav oversettes fra regelverk til tekniske løsninger, og at dette kan skape ulike forståelser mellom juridiske miljøer, sikkerhetsmiljøer og utviklingsmiljøer.

3.7.4. Endringshåndtering og fire øyne-prinsipp

NAIS legger til rette for standardiserte prosesser for endringshåndtering. Endringer i applikasjoner håndteres som kodeendringer i Git, og gjennomføres gjennom etablerte prosesser for kodegjennomgang, godkjenning og produksjonssetting. Dette gir bedre sporbarhet enn mer manuelle og lokalt varierende prosesser.

Det er etablert fire øyne-prinsipp for kodeendringer og produksjonssetting. Dette innebærer at endringer normalt skal gjennomgås av mer enn én person før de settes i produksjon. I praksis understøttes dette blant annet gjennom pull requests, kodegjennomgang og regler for sammenslåing av kode. Det bidrar til å redusere risikoen for feil og uautoriserte endringer.

Kodehistorikk, godkjenninger og produksjonssettinger kan samlet gi et teknisk revisjonsspor som viser hvordan en endring har gått fra forslag til produksjon. Dette omfatter normalt informasjon om hvem som har gjort endringen, hvem som har gjennomgått den, hvilke tester som er kjørt, og når endringen er satt i produksjon. Slik sporbarhet er sentral for å kunne dokumentere etterlevelse av krav til endringskontroll.

I intervjuer med KPMG er det opplyst at slike regler har eksistert over tid, men at dokumentasjon og etterprøvbarhet tidligere har vært mer krevende. Flere intervjuobjekter har vist til at det i løpet av de siste 6–12 månedene er gjort forbedringer, blant annet som respons på tilbakemeldinger fra Riksrevisjonen. Tidligere måtte dokumentasjon i større grad hentes manuelt, for eksempel gjennom skjermbilder eller enkeltvise uttrekk. Det er nå etablert mer strømlinjeformede og automatiserte løsninger for å hente ut dokumentasjon og rapporter ved behov.

Dette gir bedre grunnlag for etterprøving av endringer og produksjonssettinger. Samtidig avhenger kontrollnivået av at teamene følger de etablerte prosessene og at relevante kontroller dokumenteres på en måte som kan etterprøves i etterkant.

3.7.5. Produksjonssetting

Utviklere har normalt ikke permanent tilgang til produksjonsmiljøer. Ved behov kan det gis tidsbegrenset tilgang. Tilganger forvaltes i stor grad av teamene selv, basert på hvem som faktisk arbeider i teamet og hvilke oppgaver som skal utføres.

Denne modellen gir fleksibilitet og støtter direktoratets arbeidsform med autonome produktteam. Samtidig reiser modellen spørsmål om rollefordeling, kontroll og uavhengighet, særlig der løsningene er relevante for økonomiregelverket eller underlagt revisjon.

Frekvensen på produksjonssetting varierer mellom team og løsninger. Noen team setter endringer i produksjon flere ganger daglig, mens andre gjør dette sjeldnere. Teamene vurderer selv risikoen ved endringene, og endringer med høyere risiko kan medføre strengere krav til testing, godkjenning og involvering av flere personer.

Produksjonssetting skjer gjennom standardiserte og i stor grad automatiserte løp. Ansatte i Teknologiavdelingen understreker i intervjuer med KPMG at slike løp kan bidra til at samme type kontroller gjennomføres likt fra gang til gang, for eksempel knyttet til bygging av applikasjon, testing, godkjenning og utrulling. Dette reduserer behovet for manuelle operasjoner og kan gi bedre konsistens i endringshåndteringen.

Automatisert testing og dokumentasjon er sentrale deler av produksjonssettingsprosessen. Mye dokumentasjon genereres gjennom verktøy, kodehistorikk og logger fra produksjonsløpet. Dette gir et bedre grunnlag for sporbarhet, men forutsetter at teamene har tilstrekkelig kompetanse og følger felles praksis for vurdering, testing og produksjonssetting.

3.7.6. Testing og overvåking

NAIS legger til rette for bruk av automatisert testing, kombinert med manuell testing der det er behov. Automatiserte tester kan bidra til å avdekke feil før endringer settes i produksjon, og kan redusere risikoen for at endringer påvirker eksisterende funksjonalitet negativt.

Testing inngår som en del av de standardiserte utviklings- og produksjonsløpene. Dette innebærer at testresultater, kodeendringer og produksjonssettinger i større grad kan ses i sammenheng. For kontrollformål kan dette gi bedre grunnlag for å dokumentere hvilke kontroller som er gjennomført før en endring ble satt i produksjon.

Overvåking av systemhelse, ytelse og automatiserte prosesser er også en sentral del av plattformen. Det er gjort forbedringer de siste årene for å redusere risikoen for at feil eller stopp i automatiserte prosesser ikke oppdages. Overvåkingen gir produktteamene bedre mulighet til å følge med på driften og reagere ved avvik.

Det påpekes av ansatte i intervjuer med KPMG at effekten samtidig avhenger av testing og overvåking av hvordan teamene bruker funksjonaliteten. Ansatte understreker at det må være tydelig hvem som følger opp varsler, hvilke terskler som utløser handling, og hvordan feil og avvik dokumenteres og håndteres.

3.7.7. Bruk og modenhet i organisasjonen

NAIS er bygget på et prinsipp om at produkt- og applikasjonsteamene har ansvar for egne løsninger, både når det gjelder utvikling og drift. Plattformmiljøet leverer felles verktøy, standarder og tjenester, men overtar ikke eierskapet til de enkelte applikasjonene eller kontrollene knyttet til dem.

Denne modellen gir høy grad av autonomi og legger til rette for effektiv utvikling. Samtidig stiller den betydelige krav til modenhet, kompetanse og kontrollforståelse i produktteamene. Plattformen gir gode tekniske rammer og innebygde kontrollmuligheter, men den praktiske internkontrollen avhenger av hvordan teamene bruker disse rammene, og hvordan ledelsen følger opp at praksis er tilstrekkelig ensartet på tvers av produktteam.

Samlet sett fremstår NAIS som et viktig virkemiddel for standardisering, sikkerhet og sporbarhet i direktoratets digitale utviklings- og driftsmiljø. Plattformen gir et godt grunnlag for å bygge internkontroll inn i utviklings- og driftsprosessene, men realisering av kontrollgevinsten forutsetter tydelige forventninger, felles praksis og systematisk oppfølging av hvordan plattformens kontrollmuligheter faktisk brukes.

3.7.8. Oppsummering

NAIS fremstår som et sentralt virkemiddel for å styrke direktoratets internkontroll på IKT-området. Plattformen standardiserer viktige prosesser knyttet til utvikling, drift, tilgangsstyring, logging, overvåking og produksjonssetting. Den bidrar også til redusert risiko gjennom automatisering, felles verktøy og økt sporbarhet. Bruk av Git, standardiserte endringsløp og logging av sentrale hendelser gir et bedre grunnlag for etterprøvbarhet og kontroll.

Plattformen legger til rette for at internkontroll i større grad kan bygges inn i de ordinære utviklings- og driftsprosessene. Samtidig viser intervjuene at det er viktig å skille mellom kontroller som håndheves direkte av plattformen, og kontroller som forutsetter aktiv bruk, konfigurasjon og oppfølging fra produktteamene. NAIS kan derfor understøtte god internkontroll, men erstatter ikke behovet for tydelige styringsprosesser, avklarte roller, dokumenterte krav og systematisk oppfølging fra ledelsen.

Flere av kontrollene som plattformen tilbyr, herunder logging, overvåking, tilgangsstyring og sikkerhetsrelaterte kontroller, gir et godt grunnlag for etterlevelse. Etterlevelsen kan likevel variere dersom kravene ikke er tilstrekkelig formaliserte, eller dersom oppfølgingen i produktteamene ikke er enhetlig. Dette gjelder særlig områder hvor plattformen tilgjengeliggjør kontrollmuligheter, men hvor teamene selv må ta stilling til hvordan kontrollene skal benyttes, følges opp og dokumenteres.

Intervjuene viser at det de siste 6–12 månedene er gjort forbedringer knyttet til dokumentasjon, etterprøvbarhet og automatiserte uttrekk av kontrollinformasjon, blant annet som respons på tilbakemeldinger fra Riksrevisjonen. Samtidig beskrives logging og revisjonsspor fortsatt som krevende områder, særlig når det gjelder å avklare hva som skal logges, hvem som skal følge opp, og hvordan loggene skal brukes som del av internkontrollen.

I intervjuer KPMG har gjennomført med ansatte i Teknologiavdelingen påpekes det at NAIS har høy betydning for direktoratets samlede kontrollmiljø på IKT-området og at plattformen kan fungere som en viktig pilar i internkontrollen, forutsatt at den understøttes av tydelige governance-

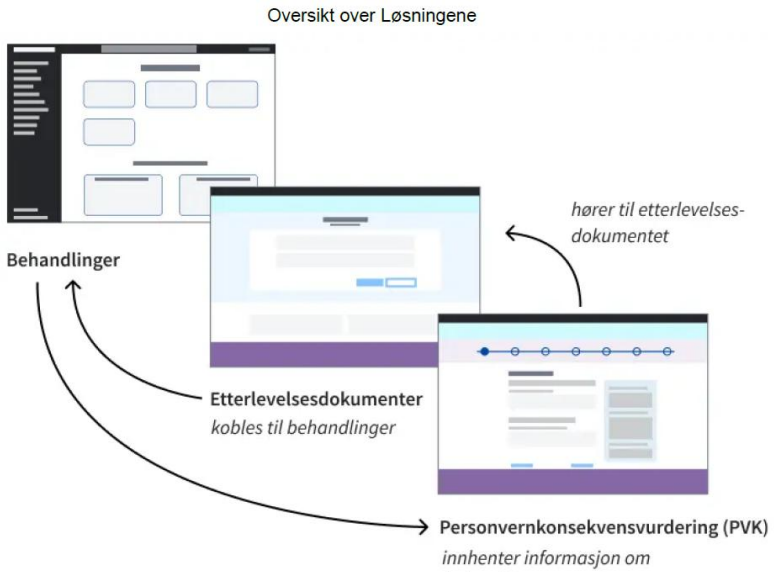
prosesser, klare krav til produktteamene og systematisk oppfølging av etterlevelse. Videre understreker ansatte i Teknologiavdelingen at sentrale risikoområder fremover vil være å sikre tilstrekkelig dokumentasjon, enhetlig praktisering av tilgangsstyring og aktiv analyse og oppfølging av logger og øvrige kontrollspor.

3.8. Digitale verktøy til støtte for etterlevelse av lovkrav og interne krav

Direktoratet har etablert systemstøtte for arbeidet med etterlevelse og risikovurdering i utvikling og forvaltning av digitale løsninger. De digitale verktøyene Behandlingskatalogen og Støtte til etterlevelse brukes til å dokumentere etterlevelse av regelverk og interne krav, mens TryggNok brukes til å dokumentere risikovurderinger relatert til informasjonssikkerhet for digitale løsninger. I tillegg er Digital PVK integrert i Støtte til etterlevelse og brukes i saker der det er behov for personvernkonsekvensvurdering. Samlet skal verktøyene bidra til å systematisere, standardisere og dokumentere både etterlevelse og risikovurderinger, og dermed gi et bedre grunnlag for internkontroll.

Behandlingskatalogen, Støtte til etterlevelse og Digital PVK er integrert med hverandre. Integrasjonen innebærer at etterlevelsesdokumentasjon kan kobles til registrerte behandlinger av personopplysninger i Behandlingskatalogen, og at personvernkonsekvensvurderinger kan gjennomføres som en utvidelse av etterlevelsesdokumentasjonen. TryggNok inngår ikke i den samme tekniske integrasjonen, men brukes parallelt i arbeidet med utvikling og forvaltning av digitale løsninger.

I forbindelse med utvikling av nye digitale løsninger og arbeid med etterlevelse av regelverk er verktøyene brukt i en arbeidsflyt der behandling av personopplysninger først registreres i Behandlingskatalogen. Som del av sårbarhetsvurderinger må teamene også gjennomføre verdivurdering og trusselmodelleringer (etterlevelseskrav informasjonssikkerhet). I saker som innebærer behandling av personopplysninger og der det er behov for personvernkonsekvensvurdering, inngår også Digital PVK i samme dokumentasjonsløp. Når det er sannsynlig at personvernrisikoen er høy så skal det gjennomføres en PVK.



Figur 14 Oversikt over digitale verktøy til støtte for etterlevelse

3.8.1. Behandlingskatalogen

Behandlingskatalogen ble tatt i bruk i 2020 og er direktoratets digitale protokoll over all behandling av personopplysninger som etaten i stort er ansvarlig for. Behandlingskatalogen er en intern systemløsning i direktoratet som benyttes for å dokumentere behandlingsaktiviteter knyttet til personopplysninger med formål om å etterleve personvernkrav. Gjelder all behandling av personopplysninger. Dette er en forpliktelse etter GDPR artikkel 30. Formålet med protokoll er å dokumentere ansvarlighet. Virksomheter skal kunne påvise at personvernregelverket etterleves. Art. 30 setter krav til hva en slik protokoll skal inneholde.

Løsningen fungerer som et sentralt register for registrering og oppfølging av behandlingsaktiviteter. En slik protokoll er en forutsetning for å kunne vite om behandlingsansvarlig følger personvernregelverket og den må holdes oppdatert. For hver aktivitet skal det angis formål, behandlingsgrunnlag, kategorier av personopplysninger, registrerte grupper, samt eventuelle databehandlere og utleveringer. Det skal videre fremgå om behandlingen innebærer bruk av helautomatiserte avgjørelser, profilering eller kunstig intelligens.

Behandlingskatalogen er strukturert i nivåer av behandlingsaktiviteter, og det stilles krav til at hver aktivitet har et klart definert formål og et gyldig behandlingsgrunnlag. Ansvar for registrering og oppdatering ligger hos fagansvarlige enheter i linjen. Juridiske fagmiljøer og personvernombudet har rådgivende roller.

Katalogen skal oppdateres ved etablering av nye behandlinger og ved endringer i eksisterende behandlinger. Løsningen legger til rette for internkontroll og dokumentasjon av etterlevelse, herunder mulighet for eksport av informasjon ved behov for innsyn. Behandlingskatalogen er et sentralt virkemiddel for å sikre strukturert og dokumentert håndtering av personopplysninger i direktoratet.

3.8.2. TryggNok

TryggNok er et verktøy direktoratet bruker for å dokumentere risikovurderinger og tilhørende beslutninger for digitale løsninger. Verktøyet brukes i arbeidet med informasjonssikkerhet, systemsikkerhet og personvern, og inngår i prosesser knyttet til utvikling, innføring, forvaltning og endring av IT-løsninger. Formålet er å registrere risikoer, dokumentere tiltak og understøtte beslutninger om videre håndtering av risiko.

Bruken av TryggNok er knyttet til hele livsløpet for digitale løsninger. Det gjennomføres risikovurderinger når nye løsninger etableres, og vurderingene oppdateres ved endringer som kan påvirke informasjonssikkerheten. Dette innebærer at verktøyet brukes både ved etablering av nye løsninger og ved senere endringer i løsning, organisering eller rammebetingelser.

TryggNok inngår i direktoratets arbeid med internkontroll og etterlevelse på IKT-området. Verktøyet brukes til å dokumentere at risikovurderinger er gjennomført, hvilke forhold som er vurdert, hvilke tiltak som er identifisert, og hvilke beslutninger som er tatt. Dokumentasjonen kan brukes som grunnlag for intern oppfølging, ledelsesbeslutninger og kontroll- og tilsynsformål.

Vurderingene i TryggNok bygger på en strukturert metodikk for sannsynlighet og konsekvens. Konsekvens vurderes med utgangspunkt i virkninger for brukere, ansatte og virksomheten. Dette

innebærer at risiko ved digitale løsninger vurderes både ut fra tekniske forhold og ut fra mulige virkninger for tjenesteleveranse, personvern, arbeidsforhold, omdømme og måloppnåelse.

Verktøyet brukes også som støtte i den praktiske gjennomføringen av risikovurderinger. Det benyttes i risikoworkshoper og i oppfølgingen av identifiserte forhold. TryggNok legger til rette for å registrere risikoer, beskrive tiltak, følge opp status og oversende vurderinger til risikoeier for beslutning. Verktøyet fungerer dermed både som dokumentasjonsløsning og som støtte i arbeidsprosessen rundt risikovurderingene.

Temaene som behandles i risikovurderinger knyttet til TryggNok omfatter blant annet tilgangsstyring, autentisering, logging, beskyttelse av sensitive opplysninger, avhengigheter mellom systemer og tjenester, risiko for uautoriserte endringer, utilgjengelighet og svindel. Bruken av verktøyet er dermed knyttet til både sikkerhetsmessige og etterlevelsesmessige forhold ved direktoratets digitale løsninger.

3.8.3. Etterlevelsesverktøyet

Etterlevelsesverktøyet Støtte til etterlevelse ble produksjonssatt høsten 2022 og er direktoratets digitale verktøy for å dokumentere etterlevelse av generelt regelverk og interne krav. Verktøyet erstatter tidligere Excel-baserte løsninger for etterlevelsesdokumentasjon. I løsningen er relevante krav strukturert som etterlevelseskrav og gruppert etter tema. Kravene omfatter både krav som følger av lov og forskrift og krav som følger av interne føringer og standarder. Kraveierne har ansvar for å tolke regelverket, publisere krav og oppdatere disse ved behov. Kraveiere sitter i ulike deler av organisasjonen. Kraveier for økonomireglementet er Økonomi- og styringsdirektør i direktoratet.

Verktøyet brukes til å opprette og vedlikeholde etterlevelsesdokumenter for ulike aktiviteter, løsninger eller produkter. Når et etterlevelsesdokument opprettes, registreres blant annet navn, beskrivelse, egenskaper som styrer hvilke krav som blir relevante, hvilken avdeling og seksjon som er ansvarlig og hvem som er risikoeier. Dersom aktiviteten innebærer behandling av personopplysninger, skal minst én behandling i Behandlingskatalogen knyttes til dokumentet. Ett etterlevelsesdokument kan være knyttet til flere behandlinger.

Hvert produktteam skal dokumentere hvorvidt de enkelte kravene er oppfylt. Det er opp til produktteamet å organisere hvem som besvarer de ulike kravene i verktøyet. Hvert krav består av ett eller flere suksesskriterier, og for hvert kriterium skal det tas stilling til om det er oppfylt, ikke oppfylt eller ikke relevant. Enkelte krav inneholder et stort antall underpunkter, og et krav vil først fremstå som oppfylt når alle relevante underpunkter er besvart og oppfylt. Verktøyet skiller ikke mellom krav etter alvorlighetsgrad eller konsekvens. Dette innebærer at ulike typer krav behandles innenfor samme dokumentasjonsstruktur, uten innebygd differensiering av vesentlighet.

KPMG fikk presentert en demonstrasjon av verktøyet. Per tidspunktet for evalueringen (15. april 2026) inneholder verktøyet 91 krav, hvorav 15 er knyttet til økonomiregelverket. Kravene er fordelt på ulike temaer, og i økonomitemaet inngår blant annet krav til dokumentasjon, historikk, toveis sporing, totrinnskontroll, avstemming mellom fag og økonomi og sikkerhet i økonomisystemet. Det er kraveier som utformer kravtekst og suksesskriterier i løsningen. For nye applikasjoner er utgangspunktet at alle relevante krav skal dokumenteres i verktøyet før produksjonssetting.

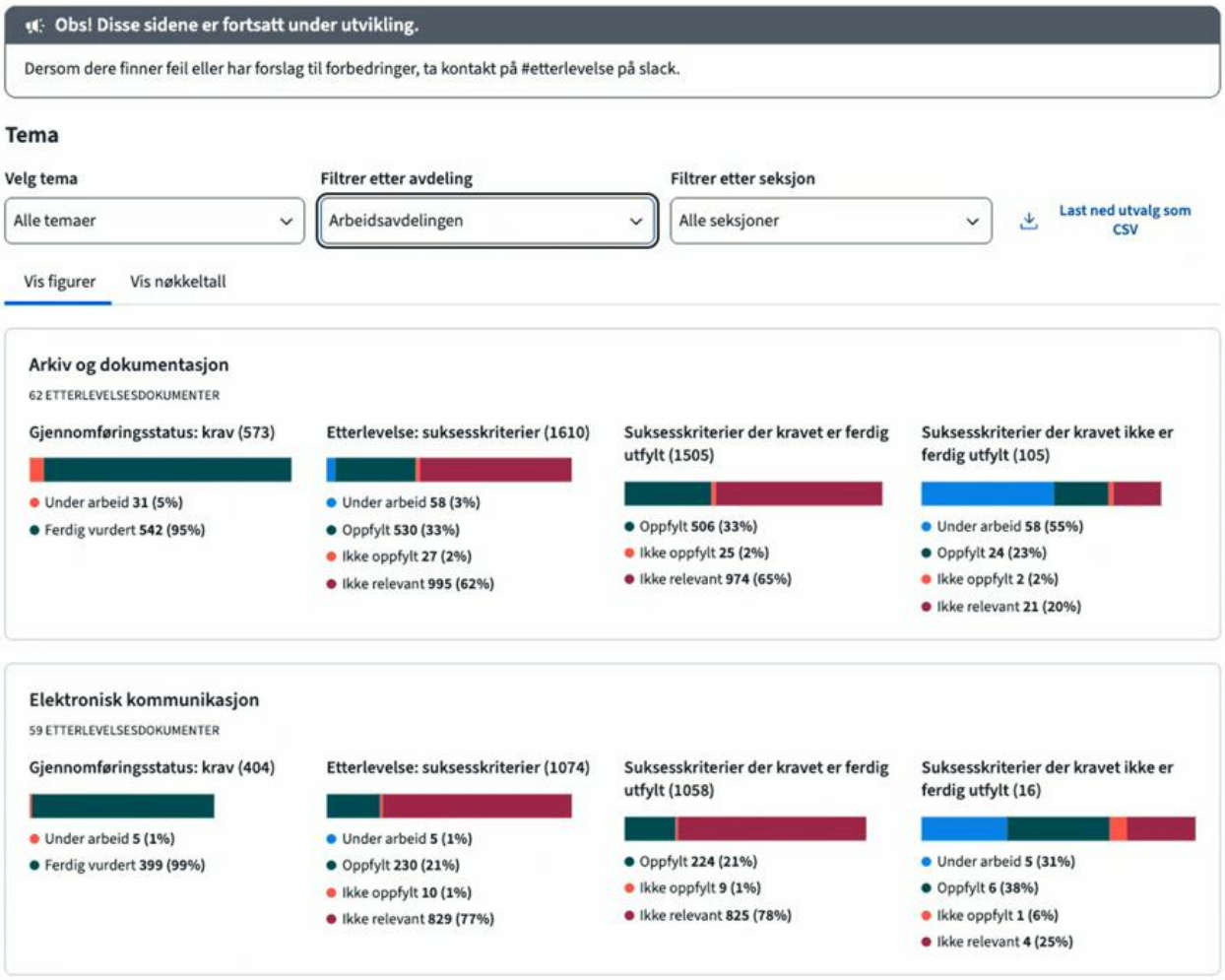
Når det er behov for personvernkonsekvensvurdering (PVK) gjennomføres denne som en del av samme dokumentasjonsløp. Digital PVK er integrert i Støtte til etterlevelse-verktøyet, og det er et 1:1-forhold mellom et etterlevelsesdokument og en eventuell PVK. Når det er ferdigstilt av produktteamet skal etterlevelsesdokumentet sendes til risikoeier for godkjenning.

Risikoeier har en sentral rolle i etterlevelsesprosessen. I praksis innebærer rollen at risikoeier skal gjennomgå produktteamenes dokumentasjon i etterlevelsesverktøyet, vurdere om krav og suksesskriterier er tilstrekkelig besvart, og ta stilling til eventuell gjenværende risiko. Risikoeier skal dermed bidra til at risiko knyttet til manglende eller delvis etterlevelse blir vurdert, akseptert eller fulgt opp i linjen. I intervjuer med KPMG fremkommer det imidlertid at det fortsatt er uklart hvordan risikoeierrollen utøves i praksis, herunder hvor grundig risikoeier gjennomgår produktteamenes vurderinger i etterlevelsesverktøyet (for eksempel når et produktteam har svart «Ikke Oppfylt» på et krav), hvordan risiko aksepteres eller eskaleres, og i hvilken grad dette skjer etter en standardisert prosess på tvers av avdelinger og produktteam. Det fremkommer også i intervjuer med KPMG at det er uklart hvordan informasjon fra etterlevelsesverktøyet rapporteres videre oppover i styringslinjen, og hvordan samlet etterlevelsesstatus benyttes som grunnlag for prioritering og oppfølging.

Intervjuene KPMG har gjennomført som del av evalueringen viser også at det ikke er etablert en systematisk praksis der kravstiller følger opp team som har registrert at et krav ikke er oppfylt. Videre kommer det gjennomgående frem i intervjuene at verktøyet per i dag er innrettet mot dokumentasjon av status. Oppfølging og videre veiledning beror i stor grad på den enkelte kraveier, det enkelte produktteam og den generelle styringslinjen.

Direktoratet har også et pågående arbeid med videreutvikling av verktøyet, blant annet gjennom etablering av dashboards og rapporteringsløsninger som gir mer presis og samlet oversikt over etterlevelse av krav og suksesskriterier på tvers av avdelinger og produktteam. Formålet med dette arbeidet er å styrke analyse- og oppfølgingsgrunnlaget, slik at risikoeiere og ledelse får bedre innsikt i hvilke krav som er oppfylt, hvilke som ikke er oppfylt, og hvor det foreligger manglende etterlevelse. Samtidig legger løsningen til rette for å tydeliggjøre hvilke krav som vurderes som ikke relevante, noe som kan bidra til mer ensartet rapportering av etterlevelsesstatus på tvers av organisasjonen.

I møte avholdt 12. mai 2026 fikk KPMG en utvidet demonstrasjon av Verktøy for etterlevelse og informasjon om pågående forbedringsarbeid, inkludert utvikling av nye dashboard etc. for å støtte analyse og rapportering. KPMG ba om dokumentasjon knyttet til det videre forbedringsarbeidet og avventer mottak av denne.



Figur 15 Dashboard – status på etterlevelse for hele direktoratet

3.8.4. Avviksverktøy

Direktoratet har egne verktøy (applikasjoner) for ulike former for avvik bl.a. innen:

- HMS
- Personvern
- Informasjonssikkerhet
- Tilgangsstyring og hendelseshåndtering
- Funn fra internrevisjoner

Avvikssystemet blir brukt for alle overnevnte punkter utenom funn fra internrevisjoner. Her benyttes TeamMate+ til registrering og oppfølging av funn og tiltak knyttet etter internrevisjoner. Tiltak etter revisjoner fra Riksrevisjonen blir også registrert og fulgt opp i TeamMate+.

Ulike avvikssystemer og -prosesser er etablert og i aktiv bruk, særlig innen informasjonssikkerhet og personvern. Det pågår arbeid med en mer helhetlig tilnærming til avvikshåndtering på tvers av direktoratet. Kvalitetsseksjonen i ØSA har flere pågående initiativ knyttet til «sentraliserte mekanismer» på dette området, f.eks. etablering av en retningslinje for avvikshåndtering.

3.8.5. Oppsummering

Direktoratet har tatt i bruk flere digitale løsninger for å støtte arbeidet med personvern, etterlevelse og risikovurdering i utvikling og forvaltning av digitale løsninger. Behandlingskatalogen, Støtte til etterlevelse, Digital PVK, TryggNok og avvikssystemer dekker ulike deler av dette arbeidet og bidrar samlet til bedre struktur, mer dokumentasjon og økt sporbarhet.

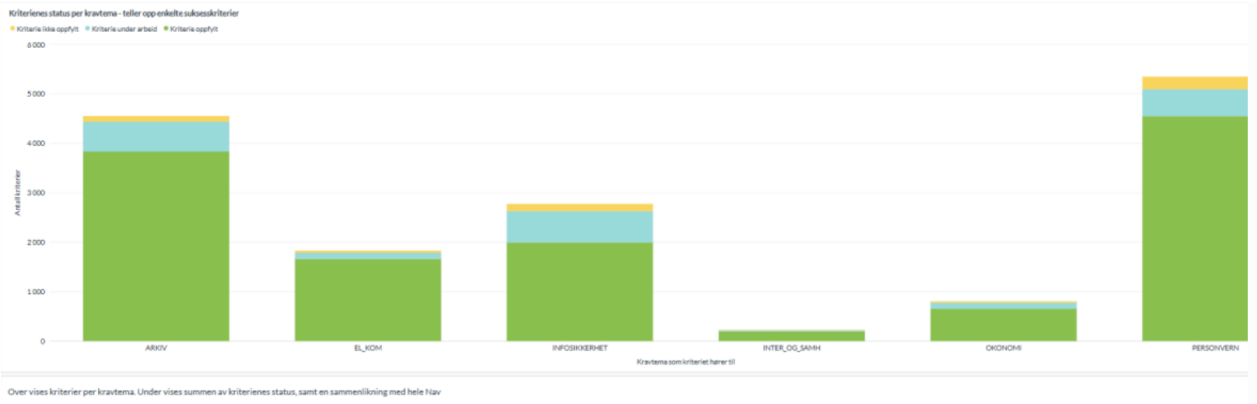
Gjennomgangen viser samtidig at verktøyene i hovedsak er innrettet mot å registrere og synliggjøre status, mens den videre oppfølgingen i mindre grad ser ut til å være standardisert.

Det fremgår også av intervjuene at det ikke er etablert en fast prosess for systematisk oppfølging av krav som ikke er oppfyllt mellom risikoeiere, kravstillere og produktteamene. I tillegg er kravene ikke differensiert etter vesentlighet, alvorlighetsgrad eller konsekvens. Dette innebærer at ulike typer krav behandles innenfor samme dokumentasjonslogikk, uten en innebygd prioritering av hvilke forhold som bør følges opp først eller tettest.

Samlet sett vurderes det som positivt at direktoratet har etablert digital systemstøtte på dette området. Verktøyene legger til rette for mer samlet dokumentasjon og bedre oversikt enn tidligere. Gjennomgangen tyder samtidig på at nytteverdien av verktøyene i stor grad vil avhenge av hvordan informasjonen brukes i den videre styringen, og at det fortsatt er et forbedringsbehov knyttet til operasjonalisering, prioritering og systematisk oppfølging av identifiserte avvik og risikoer.

3.9. Observasjoner knyttet til data i etterlevelsesverktøyet

KPMG har mottatt data som viser nåsituasjonen i etterlevelsesverktøyet. Figuren nedenfor viser status per 12. mai 2026 på tvers av om lag 120 produktteam, og er et uttrekk direktoratet selv mener gir et dekkende bilde av etterlevelse. Figuren viser andel relevante suksesskriterier som er oppfylt, under arbeid eller ikke oppfylt. I figuren er grønn benyttet for kriterier som er oppfylt, blå for kriterier som er under arbeid, og gul for kriterier som ikke er oppfylt.



Figur 16 Samlet etterlevelse i direktoratet etter direktoratets egen vurdering

KPMG observerer at enkelte krav i etterlevelsesverktøyet er formulert på et overordnet nivå. I intervjuer med ansatte i produktteamene fremkommer det at det i stor grad overlates til produktteamene å vurdere om kravene er relevante for deres løsning og i hvilken grad kravene er

oppfylt. Dette innebærer at hvert produktteam selv må vurdere relevans og etterlevelse av krav og tilhørende suksesskriterier. I intervjuer med KPMG er det fremhevet at dette kan være tidkrevende, og at ansatte i produktteamene etterlyser at kravstiller i større grad operasjonaliserer kravene og bidrar til å vurdere hvordan kravene treffer ulike produkter, løsninger og team.

KPMG observerer videre at enkelte krav og kontrollområder kan være relevante på tvers av flere regelverk. Tilgangsstyring er et eksempel på et kontrollområde som kan understøtte etterlevelse av personvernregelverket, økonomiregelverket, sikkerhetskrav og interne styringskrav. Dette innebærer ikke at gjeldende regelverkskrav kan reduseres, men at det kan være behov for tydeligere operasjonalisering av hvordan kravene skal etterleves og dokumenteres i praksis. Dersom slike krav registreres og følges opp isolert innenfor hvert enkelt tema, kan produktteamene måtte dokumentere samme eller nært beslektede kontroller flere steder i verktøyet. I intervjuer er det pekt på at dette kan være tidkrevende og lite effektivt, særlig der kravene ikke er tilstrekkelig operasjonalisert.

Intervjuene viser videre at etterlevelsesansvaret, særlig innen IKT, kan fremstå som uklart og fragmentert. Når vurderinger og oppfølging i stor grad skjer i de enkelte produktteamene kan det være krevende å etablere en samlet oversikt over risikobildet og prioriteringer på tvers av områder. Det er også pekt på manglende mekanismer for beslutningsmyndighet og fremdrift der risikoer og avvik går på tvers av organisatoriske enheter.

Krav og suksesskriterier som vurderes som «ikke relevant» inngår ikke i grafen ovenfor. Figuren viser derfor status for krav og kriterier som produktteamene selv har vurdert som relevante.

KPMG observerer at løsningen per i dag ikke skiller mellom krav etter alvorlighetsgrad, risiko eller konsekvens. Alle krav vektes dermed likt i fremstillingen, uavhengig av om kravet gjelder forhold med høy betydning for eksempelvis sikkerhet, økonomistyring eller personvern. I intervjuer med KPMG er det fremhevet at dette kan gi et forenklet bilde av faktisk etterlevelsesrisiko, ettersom manglende oppfyllelse av ett kritisk krav kan ha større betydning enn manglende oppfyllelse av flere mindre vesentlige krav.

Figuren viser status på ett tidspunkt og gir ikke alene informasjon om utvikling over tid. Den viser dermed ikke hvor lenge krav eller suksesskriterier har vært under arbeid, om identifiserte avvik er under lukking, eller aldersprofilen på åpne avvik. KPMG er kjent med at godkjenning og versjonering nå er etablert i verktøyet, og at dette kan bidra til bedre historikk og oppfølging fremover. Slik status fremstilles i gjeldende versjon, kan team som har påbegynt dokumentasjon, men ikke ferdigstilt denne, fremstå med lavere etterlevelse enn det som nødvendigvis er tilfelle.

Figuren viser videre betydelig variasjon mellom temaområdene i antall suksesskriterier. Personvern, arkiv og informasjonssikkerhet har et høyt antall kriterier sammenlignet med enkelte andre områder, mens økonomi og internkontroll/styring har et lavere volum. Dette innebærer at samlet etterlevelsesstatus i stor grad påvirkes av temaområder med mange kriterier, og at figuren i mindre grad synliggjør relativ vesentlighet eller kritikalitet mellom områdene. En høy andel oppfylte kriterier innen et stort temaområde kan derfor dominere totalbildet, selv om åpne avvik innen et mindre temaområde kan være mer vesentlige ut fra risiko eller konsekvens.

KPMG observerer at det nye dashboardet, som fortsatt er under utvikling, synliggjør en betydelig andel krav og suksesskriterier som er markert som «ikke relevant». Dette kan indikere at kravene enten ikke er tilstrekkelig presist målrettet mot ulike typer løsninger og at kravstrukturen bør deles opp eller differensieres ytterligere. Det kan også være uttrykk for ulik praksis i teamenes vurdering og bruk av verktøyet. En høy andel «ikke relevant» er ikke nødvendigvis en svakhet i seg selv, men kan påvirke hvor presist dashboardet gir uttrykk for faktisk etterlevelsesstatus. Dersom mange krav vurderes som ikke relevante, blir det viktig at begrunnelsene er dokumenterte og at praksis er enhetlig på tvers av team.

3.10. Observasjoner knyttet til post mortem-rapporter

Direktoratet benytter post mortem-rapporter i forbindelse med enkelte hendelser innen IKT-utvikling og drift. I direktoratets kontekst er dette etterfølgende hendelsesgjennomganger som skal bidra til å dokumentere hva som har skjedd, hvordan hendelsen ble håndtert, hvilke konsekvenser hendelsen hadde, og hvilke lærings- og forbedringspunkter som bør følges opp. Slike rapporter brukes normalt for å identifisere underliggende årsaker og systemsvakheter, uten at formålet er å plassere skyld hos enkeltpersoner eller team.

KPMG har mottatt dokumentet *Tips til mal for oppbygging*, som beskriver anbefalt oppbygging av post mortem-rapporter. Dokumentet angir at en post mortem blant annet bør inneholde oppsummering av hendelsen, bakgrunn, beskrivelse av feilen, hvordan problemet ble oppdaget, påvirkning på Nav, sluttbrukere eller andre, respons, gjenoppretting, tidslinje, rotårsak, læring og tiltak. Dokumentet fremhever også at målet er læring og forbedring, og at fokus skal være på hendelsen og ikke person. Videre fremgår det at post mortem ideelt sett bør gjennomføres innen 24-48 timer etter at hendelsen er løst, og ikke senere enn fem virkedager, slik at viktige detaljer ikke går tapt.

Dokumentet gir dermed en anbefalt struktur for hva en post mortem-rapport bør inneholde. I intervjuer med ansatte i Teknologiavdelingen fremkommer det at det det ikke er etablert en obligatorisk mal eller formalisert prosess for når post mortem-rapporter skal utarbeides, hvem som skal godkjenne dem, hvordan tiltak skal følges opp, eller hvordan læring skal deles på tvers av organisasjonen.

KPMG har etterspurt eksempler på representative post mortem-rapporter i direktoratet, samt eventuelle trendanalyser av hendelser. Direktoratet har oversendt et utvalg post mortem-rapporter, men KPMG har ikke mottatt trendanalyser. Basert på mottatt dokumentasjon fremstår utvalget som relativt spesifikt og avgrenset, og det er ikke dokumentert at rapportene inngår i en helhetlig styrt prosess for læring og oppfølging på tvers av direktoratets IKT-portefølje.

KPMGs gjennomgang av de mottatte post mortem-rapportene viser at rapportene varierer betydelig i detaljeringsgrad og kvalitet, både når det gjelder beskrivelse av hendelsesforløp, vurdering av årsaker, konkretisering av tiltak og dokumentasjon av oppfølging. Dette kan tyde på at det foreliggende dokumentet med tips til mal ikke praktiseres som en enhetlig standard på tvers av de mottatte rapportene.

Ansatte påpeker gjennomgående til KPMG at ansatte direktoratet har en kultur med høy åpenhet rundt feil i produksjon. I intervjuene KPMG har gjennomført fremkommer det samtidig at kulturen for formelle post mortem-analyser er begrenset. Det fremkommer gjennom intervjuene KPMG har

gjennomført at hendelser og feil håndteres ofte operativt og manuelt i de aktuelle miljøene, uten at det alltid gjennomføres en strukturert etteranalyse eller etableres læringspunkter som deles på tvers av organisasjonen.

Det fremkommer videre gjennom intervjuene og dokumentgjennomgangen at Post mortem rapportene ofte er teknisk orientert, bakenforliggende organisatoriske, prosessuelle og styringsmessige årsaker analyseres ikke alltid tilstrekkelig. Dette kan innebære at erfaringer fra hendelser i mindre grad systematiseres og benyttes som grunnlag for forbedring av prosesser, kontroller og tekniske løsninger på tvers av direktoratet.

3.11. Observasjoner knyttet til direktoratets internrevisjonsrapporter

KPMG har gjennomgått dokumentasjon knyttet til internrevisjoner av relevans for IKT-internkontroll. Basert på denne har vi notert oss følgende hovedtrender:

- Svak tiltaksoppfølging fra funn i internrevisjoner: Kun 27 % ble lukket innen avtalt frist i 2024-2025, selv om fristen er utsatt én eller flere ganger. Det tok i gjennomsnitt 449 dager fra tiltak ble avtalt til de ble gjennomført.
- IKT-kontroller (logging, tilgangsstyring og sporbarhet): Vesentlige svakheter som har vedvart over tid.
- Direktoratet har iverksatt flere reelle tiltak for å adressere hovedtrendene, spesielt etter 2024, inkludert etablering av et internkontrollprosjekt, styrking av fagmiljøer, nye rutiner for logging og tilgang, og strukturert oppfølging. Dokumentene fra internrevisjonen peker på at effekten foreløpig er begrenset og ujevn, og at flere tiltak fortsatt er i tidlig fase og ikke har løst de underliggende problemene. Tilstrekkelig tiltaksoppfølgning er fortsatt et vedvarende problem.

Særskilt relevante internrevisjoner for KPMGs oppdrag:

- *C2021-17 Kontroll med løpende ytelser*. Funn: Det mangler en helhetlig oversikt/plan som gjør det mulig å si om kontrollene samlet sett utgjør et hensiktsmessig kontrollregime. Ytelsesavdelingen har ikke implementert Direktørmøtets beslutning om at direktoratet skulle ha som mål å kontrollere løpende ytelser så tidlig at anmeldelser kunne forebygges.
- *C2021-15838 Budsjettdisponeringsmyndighet og IT-tilganger.* Funn: Dagens rutiner for tildeling og oppfølgning av fullmakter og IT-tilganger er ikke hensiktsmessige. I praksis er det ikke mulig å følge opp om gitte IT-tilganger samsvarer med tildelt budsjettdisponeringsmyndighet. Dette ble understreket med at konsekvensene av dette ble vurdert som små, gitt at lederne følger rutiner og retningslinjer.
- *C2022-10 Ny tilgangshåndtering*. Funn: Innføring forventet i løpet av 2025, men i 2022 manglet en helhetlig plan for å følge opp tilganger frem til løsningen ble innført.
- *C2023-08 Audit logging* (relatert til logging av hvem som har sett på brukernes saker). Funn: Området er lite tilfredsstillende og må forbedres. Proaktiv bruk av loggsystemet er ikke satt i bruk.
- *C2024-01 Risikostyring i NAV* viser at risikovurderinger nå gjennomføres på flere nivåer og er mer integrert i virksomhetsstyringen enn tidligere, men peker på at timingen og prosessen for rapportering gjør det vanskelig å innarbeide risikorapportering fra underliggende enheter, og at kvaliteten på aggregeringen kan svekkes. Oppfølging av

revisjonstiltak (C2019-03 og C2025-02) viser lav andel tiltak innen frist (27-41 %) og lange forsinkelser. Det ble konkludert med svak oppfølging av risikoreduserende tiltak.

- *C2024-16 Etterlevelseskrav for systemutvikling* viser at arkivering av etterlevelsesdokumentasjonen ikke er tilfredsstillende fordi rutiner ikke er kjent og derfor ikke følges.
- *C2024-17 Totrinnskontroll* viser stor variasjon i hvordan kontrollnivået er satt opp, og en designsvakhet på grunn-/hjelpestønad (risiko for at saker holdes utenfor kontroll).
- *C2025-10 3. partsrisiko i skyløsninger* viser at roller og ansvar er utydelige og at en rekke rutiner og etablert praksis mangler, inkludert for oppfølgning av databehandleravtalene, gjennomgang av eksterne rapporter og oppfølgning av endringer.
- *C2025-11 Generelle IT-kontroller i Linux-miljøet* viser betryggende kontroll, med små funn rundt rutiner for passord og logging.

Relevante observasjoner for rotårsaksanalysen:

- Mange av rotårsakene til kritiske hendelser var allerede identifisert av internrevisjonen, særlig på logging, tilgang, mislighetsrisiko og gjennomføring av tiltak.
- Gapet ligger ikke primært i «å se risikoen», men i:
    - prioritering og gjennomføring av tiltak,
    - etterlevelse i avdelingen,
    - styring/oppfølging av IKT-endringer og leverandører.
- Analyse av funn fra Internrevisjonen styrker tesen om et strukturelt lærings- og implementeringsproblem, mer enn et rent «blind spot»-problem i risikovurderingene.

4. Kritiske hendelser

Gjennomgangen viser at Riksrevisjonen gjentatte ganger har påpekt vesentlige svakheter i internkontrollen. Kritikken har blitt tydeligere og mer systemorientert over tid. Svakhetene er særlig knyttet til tilgangsstyring, logging og overvåking, gamle systemer og risikostyring. For rotårsaksanalysen har KPMG i tillegg sett nærmere på hendelser knyttet til at krav til tilgangskontroll og logging ikke var oppfylt samt at det i 2025 ble feilrapportert om rettingen av loggingsfeil. KPMG har også gjennomgått hendelsen i 2024 knyttet til manglende kontroll av utbetaling.

4.1. Innledning

KPMG har som del av oppdraget kartlagt nøkkelhendelser, dvs. vesentlige hendelser, revisjonsfunn, tilsynssaker og større endringer i styringssystemet for IKT og internkontroll. Hva som er definert som en kritisk hendelse for prosjektets formål skal derfor tolkes bredt, og inkluderer sentrale forhold som anses å ha relevans for prosjektets formål og mandat.

Formålet har vært å forstå *hvordan Arbeids- og velferdsdirektoratet har håndtert kritiske situasjoner*, og i *hvilken grad organisasjonen har evnet å lære og forbedre seg over tid*.

Gjennomgangen er basert på dokumentanalyse og intervjuer med nøkkelpersoner.

I dette kapittelet oppsummerer vi Riksrevisjonens funn og merknader knyttet til internkontroll innen IKT-utvikling, drift og forvaltning fra 2010-tallet og frem til i dag. Vi legger særlig vekt på funn i 2024 og 2025, herunder hendelsen knyttet til feilrapportering om loggingsfeil i 2025. Direktoratet hadde i dette tilfellet opplyst AID og Riksrevisjonen om at loggføringsfunksjonen var rettet/aktivert. I september 2025 informerte arbeids- og velferdsdirektøren om at loggføringen først ble aktivert i juni og september 2025, senere enn det som opprinnelig var kommunisert.

Gjennomgangen viser at Riksrevisjonen gjentatte ganger har påpekt vesentlige svakheter i internkontrollen.

Resultatet av rotårsaksanalysen er beskrevet i kapittel 5.

4.2. Om direktoratets dialog med Riksrevisjonen

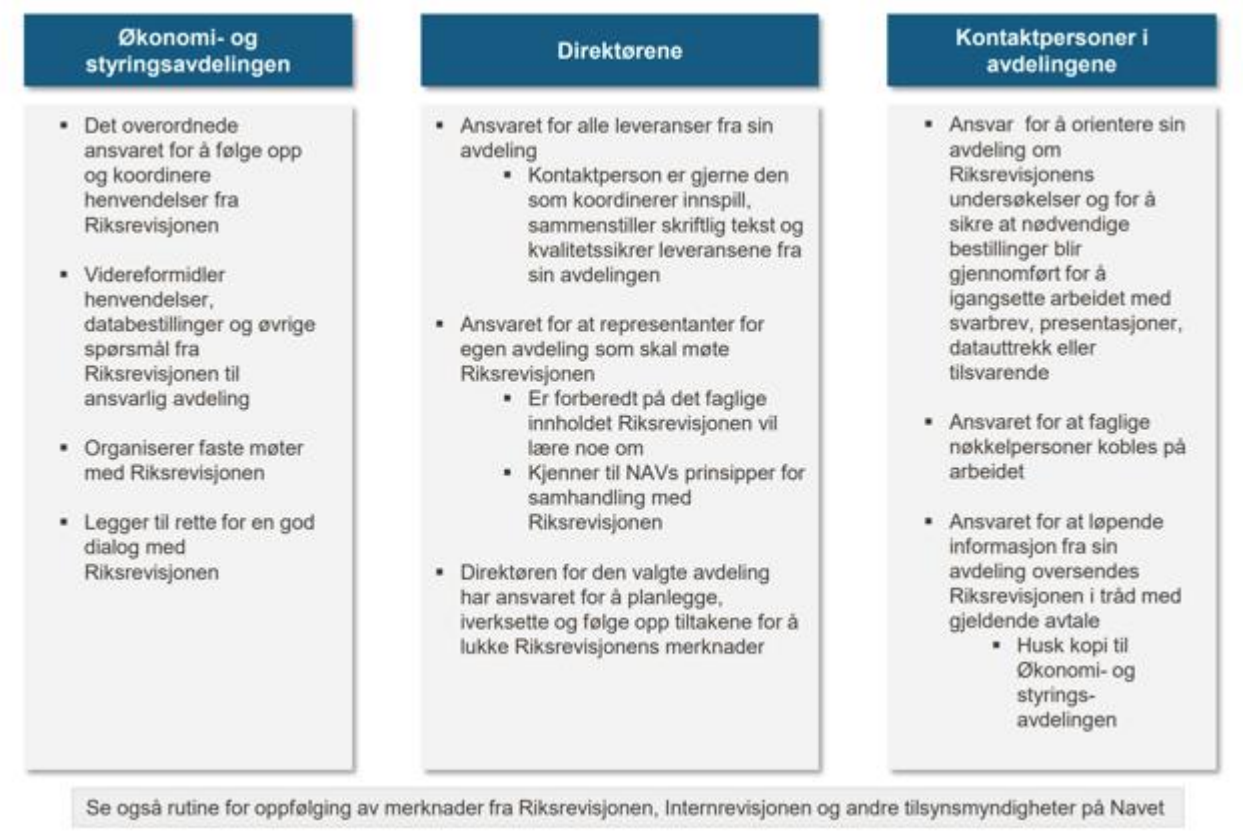
Riksrevisjonen har som rolle å kontrollere at staten bruker penger riktig og følger vedtakene fra Stortinget. Hvis Riksrevisjonen finner alvorlige problemer. Kan saken ble behandlet i Stortingets kontroll- og konstitusjonskomite. Dialogen mellom direktoratet og Riksrevisjonen foregår på mange ulike nivåer i organisasjonen:

- Ledelsen i direktoratet
- Økonomi- og virksomhetsstyring, juridiske avdelinger
- Internrevisjonen har jevnlige møter med Riksrevisjonen og går gjennom planlagte revisjoner

I dokumentet *Rutine for koordinering av NAVs arbeid med Riksrevisjonssaker* datert januar 2023 beskrives roller og ansvar knyttet til dialog med Riksrevisjonen. Økonomi- og styringsavdelingen

har det overordnede ansvaret for å følge opp og koordinere henvendelser fra Riksrevisjonen. Den enkelte leder i avdelingene har ansvar for å besvare henvendelser innenfor eget ansvarsområde.

Ved IT-revisjoner håndteres dialogen med Riksrevisjonen i all hovedsak av de enhetene som forvalter systemene for de aktuelle ytelsene. Dialogen mellom produktteamene og revisjonspersonell fra Riksrevisjonen i disse tilfellene opplyses å være tett.



Figur 17 Rutine for koordinering av NAVs arbeid med Riksrevisjonssaker datert januar 2023 - Intern ansvarsfordeling i direktoratet

4.3. Riksrevisjonens funn og merknader knyttet til IKT-internkontrollen

KPMG har gjennomgått Riksrevisjonens funn og merknader knyttet til IKT-internkontrollen i direktoratet fra tidlig 2010-tall og frem til i dag. Tabellen nedenfor oppsummerer Riksrevisjonens hovedfunn av relevans for IKT-internkontroll.

KPMG observerer at Riksrevisjonen over tid har pekt på flere gjentakende svakheter i IKT-internkontrollen i direktoratet. Kritikken har blitt tydeligere og mer systemorientert over tid. Svakhetene er særlig knyttet til tilgangsstyring, logging og overvåking, gamle systemer og risikostyring. Riksrevisjonen har vurdert funnene som alvorlige ettersom direktoratet forvalter svært store utbetalinger, store mengder sensitive personopplysninger og systemer med høy samfunnskritisk betydning.

I det følgende oppsummerer vi de viktigste gjentakende funnene:

Mangelfull tilgangsstyring

Riksrevisjonen har gjentatte ganger identifisert risiko for misbruk, feilutbetalinger, personvernbrudd og interne misligheter som følge av funn knyttet til:

- Brukere har hatt for omfattende rettigheter.
- Kontrollen med hvem som har hatt tilgang er for svak, periodisk kontroll av tilganger har ikke vært god nok.

Mangelfull logging, sporbarhet og overvåking

Riksrevisjonen har gjentatte ganger påpekt mangler som reduserer direktoratets evne til å oppdage misbruk, undersøke hendelser og dokumentere kontroll:

- Manglende logging av aktiviteter
- Manglende oppfølging av logger
- Manglende sporbarhet
- Utilstrekkelig overvåking av uvanlige hendelser

Gamle systemer

Riksrevisjonen har gjentatte ganger pekt på at IKT-moderniseringen tar for lang tid og at gamle systemer utgjør en betydelig sikkerhetsrisiko.

Risikostyring

Riksrevisjonen har gjentatte ganger de senere årene påpekt

- manglende systematiske risikovurderinger,
- svak dokumentasjon,
- utilstrekkelig oppfølging av avvik, og
- kontrolltiltak blir ikke gjennomført eller fulgt opp godt nok.

KPMG observerer at kritikken den senere tiden i større grad har blitt rettet mot selve styringsinformasjonen.

Problemer i styringsdialog og rapportering

- Revisjonsgrunnlaget viste seg svakere enn tidligere opplyst
- Direktoratet gav feil eller mangelfull informasjon til departementet og Riksrevisjonen
- Internrevisjonen og Riksrevisjonen hadde ulike vurderinger

Tabellen nedenfor gir en overordnet oppsummering av funnene. For tabellens formål er Arbeids- og velferdsdirektoratet omtalt som NAV. For rapportene før 2019 ga ikke Riksrevisjonen en overordnet vurdering. Her har derfor KPMG estimert vurderingen mot den gjeldende tredelingen av; Ikke tilfredsstillende, Kritikkverdig og Sterkt kritikkverdig.

År	Tema	Overordnet vurdering
2012	Gjennomgående svak internkontroll i Nav: Riksrevisjonen påpekte flere kritikkverdige forhold i Nav. Nav ble dermed gitt vesentlige merknader på femte året.	Sterkt kritikkverdig
2013	Riksrevisjonen rapporterte at moderniseringsprosjektet for Navs IKT-systemer mislyktes og ble stoppet.	Kritikkverdig
2014	Alvorlige mangler i økonomisystem og sikkerhet: Revisjonen avdekket store mangler i internkontroll og IKT-sikkerhet i Navs økonomisystem. Dette medførte risiko for feil og misligheter i regnskapsføringen. Riksrevisjonen anbefalte departementet å sikre at Navs internkontroll og IKT-sikkerhet etterlever kravene i økonomiregelverket. Kontrollkomiteen bemerket tilsvarende at god informasjonssikkerhet er grunnleggende, og forutsatte at statsråden følger opp for å utbedre svakhetene.	Kritikkverdig
2015	Riksrevisjonen slo fast at det er «sterkt kritikkverdig» at departementet ikke har fulgt opp Navs arbeid med å avdekke og behandle feilutbetalte ytelser. Riksrevisjonen påpekte også vesentlige mangler i Navs styringssystem for informasjonssikkerhet (IKT-sikkerhet), noe som ble fremhevet i Riksrevisjonens samlede rapport.	Sterkt kritikkverdig
2016	Riksrevisjonen fant «vesentlige svakheter» i Navs forvaltning av dagpenger. Revisjonen påpekte også at internkontrollen ikke fanger opp saksbehandlingsfeil før vedtak fattes.	Kritikkverdig
2017	Riksrevisjonen påpeker sikring mot dataangrep. Statsråden påpeker dette som sterkt kritikkverdig.	Sterkt kritikkverdig
2018	IKT-støtten for utbetalinger til tiltaksleverandører var mangelfull, uten full oversikt per avtale og dårlig sporbarhet mellom avtaler og fakturaer. Gjentatt svakhet i internkontroll førte til sterk kritikk, og Riksrevisjonen fulgte saken videre de neste årene.	Kritikkverdig
2019	I 2019 var det særskilt fokus på AFT og VTA - og 'konsernproblematikken' hos foretak som mottar tiltaksmidler. Stortingets kontrollkomité påpekte at svakheter i Navs internkontroll var kritikkverdige. Riksrevisjonen mente det var kritikkverdig at arbeids- og velferdsetaten ikke hadde systemer for å sikre nødvendig styringsinformasjon og tilstrekkelig internkontroll ved utbetaling til tiltaksleverandørene.	Kritikkverdig
2020	Ingen nye alvorlige avvik rapportert.	N/A
2021	Feilutbetalinger under pandemien: Riksrevisjonens særskilte gjennomgang av Navs koronarelaterte ytelser viste at omfanget av mulige feilutbetalinger var svært stort. Nav utbetalte enorme beløp i 2020–21, men hadde bare i begrenset grad gjennomført etterkontroller i etterkant. Riksrevisjonen anbefalte at Nav intensiverer etterkontrollene og sørger for innebygde kontroller i sine nye IKT-systemer for å forebygge feilutbetalinger.	Kritikkverdig
2022	Ingen nye alvorlige avvik rapportert.	N/A
2023	Betydelige beløp gikk tapt fordi feilutbetalinger ikke ble behandlet før de ble foreldet. Riksrevisjonen måtte understreke at slike praksiser strider med økonomiregelverket, og at beløpene representerer tap for fellesskapet. Statsrådens svar til Riksrevisjonen understreket at NAV gjorde aktive prioriteringer, og Stortinget ble orientert om disse.	Ikke tilfredsstillende
2024	Alvorlig svikt i IKT-sikkerhet og sporbarhet: Revisjonen for 2024 påviste betydelige svakheter i Navs internkontroll i databaser for sentrale ytelser (alderspensjon, uføretrygd, AFP, foreldrepenger). Konkrete krav til tilgangskontroll og logging var ikke oppfylt, i strid med økonomiregelverkets bestemmelser. Svakhetene ble ansett som så alvorlige at Riksrevisjonen ikke kunne innhente tilstrekkelig revisjonsbevis for Navs årsregnskap. For første gang fikk Nav derfor en revisjonsberetning med forbehold. Dette innebærer at Riksrevisjonen mente å ikke	Ikke tilfredsstillende

	kunne bekrefte riktigheten av store deler av Navs utbetalinger. (Ifølge kontrollkomiteen måtte det tas forbehold for ytelser på ca. kr. 475 mrd.) Riksrevisjonen anbefalte AID å påse at Nav skjerpet rutiner for sikkerhet og sporbarhet i etatens IT-portefølje, både for nyutviklede og eldre systemer.	

Figur 18 Overordnet oppsummering av funnene til Riksrevisjonen

For rotårsaksanalysens formål har KPMG sett nærmere på hendelsen i 2025 knyttet til feilrapportering om loggingsfeil / krav til tilgangskontroll og logging som ikke var oppfylt. KPMG har også gjennomgått hendelsen i 2024 knyttet til manglende kontroll av utbetaling, blant annet for ortopedi. Disse hendelsene/forholdene illustrerer slik KPMG ser det svakheter i ulike deler av IKT-internkontrollen, og egner seg dermed til å gi et helhetlig bilde av de primære rotårsakene.

4.3.1. Feilrapportering om loggingsfeil / krav til tilgangskontroll og logging ikke oppfylt

I oppsummeringsmøtet i forbindelse med 2024-revisjonen i desember 2024 påpekte Riksrevisjonen svakheter i logger i tre databaser for pensjon og uføretrygd. Disse digitale registreringene av aktiviteter og hendelser i IT-systemer sikrer sporbarhet ved å dokumentere brukerhandlinger og systemendringer, og utgjør et sentralt grunnlag for internkontroll, sikkerhetsoppfølging og revisjon. Tilstrekkelig logging er viktig for å kunne avdekke, undersøke og følge opp uønskede eller uautoriserte hendelser.

Økonomi- og styringsdirektør og IT-direktør orienterte deretter Arbeids- og velferdsdirektør og internrevisjonssjef om svakheten. Det var tett dialog mellom direktoratet og Riksrevisjonen gjennom resten av revisjonen for 2024. Det ble også gjennomført flere møter i januar 2025 i forkant av direktoratets besvarelse av nummerert brev 1 som direktoratet mottok 19. desember 2024. Ledere i Ytelsesavdelingen og Teknologiavdelingen enes om at det er et delt ansvar mellom dem og at de sammen følger opp svakhetene.

I løpet av januar 2025 avdekket direktoratet at det var flere systemer som potensielt var berørt av svakheten. Det var enighet mellom IT-direktør og Økonomi- og styringsdirektør om at det var nødvendig å etablere et Excel-ark med oversikt over hvilke systemer som var berørt og status på håndtering av svakhetene. Det var også enighet om å informere enhetene i direktoratet om alvoret i situasjonen slik at svakhetene kunne lukkes så raskt som mulig. Det var dialog rundt dette mellom direktoratet og Riksrevisjonen på flere nivåer av organisasjonen, og KPMG har fått forklart at det ble bekreftet at auditlogg var tatt i bruk for de tre databasene henholdsvis 10. desember 2024 og 21. januar 2025.

Den 24. januar 2025 sendte leder for Økonomi- og virksomhetsstyring ut en e-post til berørte avdelingsdirektører i Arbeidsavdelingen, Ytelsesavdelingen, Økonomi- og styringsavdelingen og Teknologiavdelingen. Der fremgikk det at arbeidet med svakhetene måtte intensiveres for å unngå at det påvirket revisjonen for 2025 vesentlig. I e-posten står det blant annet (sitat): «Vi ber om at dere, så raskt som mulig, kartlegger om de relevante databasene dere har ansvar over, har en aktiv auditlogg eller ikke. I det tilfelle en auditlogg mangler, bør det vurderes hvilke muligheter som finnes for å skru på logg. Dere bør da vurdere hvilke informasjonspunkt som er relevante å inkludere i loggen. Kravet i økonomibestemmelsene innebærer at personlig identifikasjon, dato og klokkeslett for handlingene er med i loggen. Det skal derfor brukes individuelle brukere når personer gjør endringer eller spørringer mot databasene», med beskjed om å kartlegge hvilke databaser som er underlagt økonomireglementet og henvisning til manglende etterlevelse av

punkt 4.3.6 i økonomireglementet. I e-posten ble det presisert at manglende auditlogger kunne påvirke revisjonen for 2025 og at det derfor var viktig at de mest kritiske databasene tok i bruk funksjonalitet for auditlogg fortløpende, og senest innen utgangen av februar 2025. Riksrevisjonen ønsket tilleggsinformasjon utover svaret på nummerert brev 1 og KPMG har fått referert at det ble sendt gradert svar via NBN (nasjonalt begrenset nett) 7. februar 2025.

I intervjuer KPMG har gjennomført uttaler ansatte som svarte på e-posten at det ikke var tydelig nok presisert hva slags logger det var snakk om. De ansatte som svarte ut spørsmålene hadde ulik forståelse av kravene til hvilke typer databasebrukere auditlogg skulle tas i bruk for. Dette gjaldt blant annet databasebrukere (Sys, System, Adminbruker) som benyttes for å administrere og vedlikeholde databasene, eksempelvis starte og stoppe databaser, gjøre oppgraderinger og administrere databasebrukere. Flere påpeker også at viktigheten av å sikre korrekt logging ikke var tydelig nok presisert i e-posten de mottok. De ansatte beskriver at det heller ikke kom tydelig frem hvem som hadde hvilket ansvar.

Økonomi- styringsavdelingen benyttet nevnte Excel-ark til å innhente svar i form av selv-rapportering fra ulike roller. Oversikten ble benyttet som grunnlag for videre rapportering til AID og Riksrevisjonen gjennom våren og høsten 2025. Oversikten var lagret på egen sak i JIRA og omfattet blant annet informasjon om type database, om auditlogg var på, dato og beskrivelse. Det ble imidlertid ikke innhentet fysisk bevis (dokumentasjon) fra systemene på at auditlogg var aktivert. I intervjuene KPMG har gjennomført med ansatte i Økonomi- og styringsavdelingen fremgår det at det ikke ble gjennomført en egen, uavhengig runde med kvalitetssikring av svarene som ble mottatt, og det ble heller ikke innhentet bevis for at korrekt logging faktisk var gjennomført i de ulike systemene. Tilbakemeldingssløyfen som ble etablert hadde fokus på om funksjonalitet for auditlogging var tatt i bruk, og de forskjellige områdene gav tilbakemelding på dette basert på deres egen forståelse. Manglende bruk av auditlogging av systembrukere ble ikke fanget opp.

Etter en periode med utbedringer rapporterte direktoratet i mars 2025 til AID og Riksrevisjonen at avviket var lukket. AID ble holdt løpende oppdatert frem mot endelig revisjonsberetning 18. juni 2025. Informasjon om at avvikene var lukket ble delt i møte med AID i slutten av juni samme år. AID fulgte opp saken gjennom sommeren og direktoratet sendte svar på brev om ytterligere informasjon 8. august 2025.

I forbindelse med forberedelsene til revisjonen for 2025 avdekket direktoratet tidlig i september 2025 at loggingen var utilstrekkelig flere steder. Det gjaldt eksempelvis at auditlogg var aktivert på NAIS, men at den var satt opp til å overskrives hver 30. dag. Det medførte blant annet at direktoratet ikke hadde mer enn 30 dagers auditlogg for sykepengeløsningen, og dermed at logg manglet for perioden 1. januar 2025 til rundt 15. august 2025. Direktoratet iverksatte etter dette arbeid med å få klarhet i status, og utbedret flere mangler. Riksrevisjonen og AID ble orientert om funnene. I tillegg startet direktoratet arbeidet med å fremskaffe kompenserende revisjonsbevis for å sannsynliggjøre at det ikke hadde blitt gjort endringer som har ført til feilaktige utbetalinger fra de aktuelle systemene. I november 2025 måtte arbeids- og velferdsdirektøren gå av på grunn av feilinformasjonen gitt til både AID og Riksrevisjonen.

4.3.2. Manglende kontroll av utbetaling for ortopedi

Forvaltningen av stønadsordningen for ortopediske hjelpemidler er organisert på tvers av flere avdelinger. Ansvar knyttet til regelverk, saksbehandling og utbetaling er fordelt mellom Velferdsavdelingen, Ytelsesavdelingen og Økonomi- og styringsavdelingen. Velferdsavdelingen har blant annet ansvar for regelverk, forskrift og rundskriv, anskaffelser og fagdialog med AID. Ytelsesavdelingen har ansvar for saksbehandlingssystem og linjeansvar for saksbehandling, mens Økonomi- og styringsavdelingen har ansvar for fakturahåndtering, utbetaling og anskaffelsesgjennomføring.

Saksbehandlingen inngår i en samlet prosess fra søknad til utbetaling. Når en person har behov for et ortopedisk hjelpemiddel, opprettes søknad av lege og sendes til et ortopedisk verksted. Verkstedet kompletterer søknaden før den behandles av Nav. Når vedtak er fattet, produseres og tilpasses hjelpemiddelet før faktura registreres i systemet ORTOK og inngår i grunnlaget for oppgjør. Riksrevisjonens rapport viser at Nav i 2024 mottok 158 726 søknader om ortopediske hjelpemidler, hvorav 153 933 ble helt eller delvis innvilget. I samme periode mottok Nav 288 420 fakturaer og utbetalte om lag 2,6 milliarder kroner i stønad. Av dette gjaldt i overkant av 2 milliarder kroner nye hjelpemidler, 345 millioner kroner reparasjoner og 138 millioner kroner justeringer.

Riksrevisjonen la i november 2025 frem en revisjon av stønad til dekning av utgifter til ortopediske hjelpemidler for 2024 og konkluderte med at kun ca. 0,6 % av fakturaene ble kontrollert før utbetaling og at direktoratet har gjort utbetalinger også før vedtak var fattet. Revisjonen omfattet kontroll av fakturabehandling før utbetaling og kontrolltiltak etter utbetaling, basert på analyser av data fra blant annet systemene ORTOK og Gosys, dokumentgjennomgang og intervjuer. Revisjonen identifiserte en rekke funn:

- Det fremgår at Nav har etablert rutiner for fakturakontroll før utbetaling. Ifølge rutinene skulle alle fakturaer over 100 000 kroner kontrolleres, mens fakturaer mellom 50 000 og 100 000 kroner kunne inngå i stikkprøvekontroller. Fakturaer under 50 000 kroner ble ikke kontrollert mot fakturagrunnlaget. Riksrevisjonens analyser viste at 97,5 prosent av alle fakturaene Nav mottok i 2024 var under 50 000 kroner, 1,9 % lå mellom 50 000 og 100 000 kroner, og 0,6 prosent var over 100 000 kroner.
- For fakturaer som kontrolleres, fremgår det at kontrollen i hovedsak er manuell og blant annet omfatter kontroll av timepris og tilvirkningstid. Samtidig fremgår det at det ikke gjennomføres kontroll av om det foreligger vedtak på utbetalingstidspunktet, om søknaden er innvilget, om fakturaen er i samsvar med vedtaket, eller om ferdigattest er mottatt.
- Når det gjelder dokumentasjon av kontroll, fremgår det at Nav arkiverer lister over godkjente oppgjør og noterer eventuelle funn, men at det ikke foreligger samlet dokumentasjon av hvilke fakturaer som er kontrollert eller hvordan kontrollene er gjennomført.
- Riksrevisjonen analyserte også sammenhengen mellom vedtak og utbetaling. I et utvalg på 36 276 tilfeller identifiserte revisjonen 42 tilfeller i 2024 der faktura var betalt før vedtak var fattet. I en manuell kontroll av 18 av disse tilfellene var 17 utbetalt før vedtak forelå. Videre identifiserte revisjonen 249 tilfeller der det var utbetalt stønad i saker hvor søknaden var avslått. I kontroll av et utvalg av disse viste gjennomgangen at enkelte tilfeller kunne forklares med forhold knyttet til dødsfall, mens øvrige tilfeller gjaldt utbetalinger hvor søknaden var avslått.

- Revisjonen omfattet også kontroll av ferdigattester. Det fremgår at Nav mottar ferdigattester fra leverandører, men at disse i begrenset grad inngår som del av kontrollen før utbetaling. I en gjennomgang av et utvalg fant Riksrevisjonen variasjoner i detaljeringsnivå og tilfeller hvor informasjonen i ferdigattestene i begrenset grad underbygget fakturagrunnlaget.
- Når det gjelder kontroll etter utbetaling, fremgår det at Nav har gjennomført enkelte analyser av fakturadata og oppfølging av leverandører, samt årlig materialavregning. Riksrevisjonen beskriver samtidig at det ikke er etablert et system for regelmessige analyser av utbetalinger for å identifisere avvik mot rammeavtalen.
- I analysene av fakturadata identifiserte Riksrevisjonen 900 tilfeller hvor fakturert fastpris ikke var i henhold til rammeavtalen, med en samlet differanse på under 360 000 kroner. Videre ble det identifisert 27 tilfeller med avvik i timepris og 66 avvik i tilvirkningstid hos enkelte verksteder.
- For reparasjoner og justeringer viste analysene at verkstedene i 2024 fakturerte over 483 millioner kroner, og at 98 prosent av disse fakturaene var under 50 000 kroner. Riksrevisjonen identifiserte 11 570 tilfeller hvor kostnaden for reparasjon eller justering oversteg prisen for nytt hjelpemiddel, med et samlet fakturabeløp på over 63 millioner kroner.
- Videre viste analysene 1 999 tilfeller hvor det var fakturert reparasjon for hjelpemidler samme år som de var utlevert, samt 864 tilfeller hvor reparasjon eller justering var fakturert før det forelå vedtak for det aktuelle hjelpemiddelet.
- Riksrevisjonen beskriver også en automatisert etterkontroll ved bruk av RPA-teknologi, hvor det i 2024 ble kontrollert over 277 000 fakturaer. I denne kontrollen ble det identifisert 1 155 avvik, hvorav 42 ble klassifisert som reelle avvik knyttet til manglende vedtak eller avslag.

Området har i etterkant vært gjenstand for oppfølging, blant annet gjennom etablering av et internkontrollprosjekt og arbeid med modernisering av systemer, regelverk og prosesser for hjelpemiddelområdet.

Nav ved direktoratet innga kommentarer til en rekke av Riksrevisjonens funn i sitt oversendelsesbrev til AID samt i utkastet til Riksrevisjonens rapport i 2025. KPMG har fått innsyn i disse dokumentene, og inntar enkelte sentrale nyanseringer i det følgende:

Riksrevisjonen: Fakturakontrollen dekker en svært begrenset andel av fakturaene, er ikke tilpasset risiko og vesentlighet, og er ikke dokumentert.

Navs kommentar: Internkontrollen skal ifølge økonomireglementet tilpasses risiko og vesentlighet. En svært høy andel av fakturaene består av små og likelydende beløp. Fakturakontrollen er ressurskrevende, delvis på grunn av papirbaserte løsninger. Vi vurderer at den iboende risikoen for at ortopediske verksteder bevisst avviker fra rammeavtalen er liten, fordi de risikerer at avtalen, og dermed hele eksistensgrunnlaget, forsvinner. Vi mener derfor det er riktig ressursbruk at fakturakontrollen bare dekker en svært begrenset andel av fakturaene. Fakturakontrollen er også tilpasset vesentlighet ved at fakturaer med høye beløp velges ut for kontroll. Riksrevisjonens undersøkelser har avdekket et veldig lite antall feil sett i forhold til det totale omfanget av fakturaer. Dette tilsier etter Navs vurdering at risikoen for vesentlige feil er liten, og understøtter vårt syn om at det er riktig å sjekke en begrenset andel av fakturaene. Nav mener det kan vurderes å styrke

de systematiske etterkontrollene og endre utvalget for stikkprøvekontroller, slik at man også på stikkprøvebasis kontrollerer noen av fakturaene under kr 50 000.

Riksrevisjonen: Nav har betalt for hjelpemidler før det er fattet vedtak, og der søknad er avslått.

Navs kommentar: Det er riktig at hjelpemidlene ikke skal betales før vedtak foreligger, og det skal ikke betales faktura hvis søknaden er avslått. Faktura er betalt til tross for avslag i 249 tilfeller av 158 726 vedtak. Stikkprøver av et lite utvalg saker viser at de fleste av disse sakene likevel skulle vært betalt, eksempelvis fordi bruker døde før vedtaket ble fattet. Da skal påløpte utgifter betales selv om det blir avslag. Vi anslår at de reelle feilene utgjør 0,07 prosent av tilfellene.

Riksrevisjonen: Nav kan ikke dokumentere at feil avdekket ved godkjenning av faktura er krevd tilbake.

Navs kommentar: Nav er enige i at det bør dokumenteres at feilutbetalinger blir tilbakebetalt. Nav mener det er forbundet med lav risiko å utbetale samleoppgjør som inneholder små feil og be om at dette blir kreditert på neste samleoppgjør, fordi leverandørene har langvarige rammeavtaler med Nav.

Riksrevisjonen: Nav kontrollerer ikke at hjelpemiddelet er mottatt før de betaler fakturaen.

Navs kommentar: Det mangler systemstøtte for å sjekke at det foreligger ferdigattest før faktura utbetales. Slik systemet fungerer med papirbaserte ferdigattester, vil det være en svært omfattende manuell jobb å kontrollere ferdigattestene manuelt før betaling av faktura. Nav mener at det gir god sikkerhet for at det kun betales for faktisk utleverte hjelpemidler, ved at de ortopediske verkstedene må sende inn ferdigattestene til Nav. Dette gir Nav mulighet til å sjekke i etterkant at hjelpemidlene faktisk er levert. Vi nevner også at det er svært lite sannsynlig at leverandørene bevisst vil fakturere hjelpemidler som ikke er levert, fordi de da risikerer hele rammeavtalen. Nav har heller aldri fått indikasjoner på at dette har skjedd.

Riksrevisjonen: Nav har ikke en internkontroll som sikrer at det er innvilget stønad for ortopediske hjelpemidler før fakturaen betales, slik forskriften og økonomireglementet krever.

Navs kommentar: Det er riktig at hjelpemidlene ikke skal betales før vedtak foreligger, og det skal ikke betales faktura hvis søknaden er avslått. Vi i Nav har imidlertid merket oss at dette har skjedd i et svært begrenset omfang. Faktura er betalt før vedtak i 42 tilfeller av 158 726 vedtak, dvs. i 0,03 % av tilfellene.

Riksrevisjonen: Nav har ikke etablert en internkontroll i henhold til bestemmelsene, som sikrer effektiv ressursbruk, eller som forebygger og avdekker feil og mangler i verkstedenes fakturagrunnlag. Med internkontrollen som Nav har per i dag er det en risiko for at det kan forekomme at verkstedet sender faktura på garantisaker, uten at Nav vurderer om denne er reell.

Navs kommentar: Ortopediske hjelpemidler blir ofte individuelt tilpasset hver bruker. Rammeavtalen tar hensyn til dette ved å tillate fakturering av medgåtte timer og materialer for mange typer hjelpemidler. Nav gjennomfører årlig kontroll av materialkostnadene, men det er utfordrende å kontrollere de fakturerte arbeidstimene tilfredsstillende. Systemet er derfor til en viss grad basert på tillit til at leverandørene fakturerer korrekt. Vi har undersøkt hva som kan være årsaken til at pris for reparasjon tilsynelatende kan være høyere enn prisen for nye sko. Personer

som får reparert/justert sine ortopediske sko har ofte diabetes og høy risiko for fotsår og amputasjon. Når disse får ortopediske spesialsko faktureres fastpris og fast stønadsbeløp. I tillegg er det veldig ofte behov for ombygging av spesialskoene. Ombyggingen føres på andre koder som det ikke er fastpris på. Personer som får reparert eller justert skoene vil så å si alltid være i denne kategorien. Man kan derfor ikke ta utgangspunkt i fastpris og fast stønadsbeløp, men må i tillegg ta hensyn til behov for ombygging og eventuelt også oppbygging av skoene for å finne den reelle alternative kostnaden til å reparere eller justere skoene. Disse pasientene er også ofte i en gråsone hvor det varierer om de kan bruke ombygde spesialsko eller må bruke spesialsydde sko. Noen ganger kan derfor det reelle alternativet til å reparere/ombygge spesialskoene være få nye individuelt sydde sko. Det er utbetalt mer enn fastpris tilsvarende 360 000 kroner, dvs. 0,01 % prosent av de totale utgiftene til ortopediske hjelpemidler.

Det pågår våren 2026 et systematisk arbeid med oppfølging av Riksrevisjonens rapport om stønad til dekning av utgifter til ortopediske hjelpemidler i 2024, som er organisert i tilknytning til det overordnede internkontrollprosjektet.

4.4. Observasjoner knyttet til læring fra kritiske hendelser

I intervjuer KPMG har gjennomført beskriver ansatte at det finnes arenaer for evaluering etter kritiske hendelser, deriblant funn fra revisjoner. Ansatte beskriver gjennomgående at erfaringer deles i enkelte deler av organisasjonen, men at det i ulik grad utarbeides rapporter for hendelser. Det pekes også på at læring og konklusjoner i mange tilfeller ikke omsettes videre i relevante prosesser og rutiner, og at denne manglende operasjonaliseringen er en faktor i det bildet som er tegnet av at avvik og funn ofte er gjentakende.

Det fremgår videre fra intervjuene med produktteamene at det ikke er etablert systematiske prosesser for implementering av læring på tvers av produktteamene. I intervjuene KPMG har gjennomført beskriver ansatte at de produktteamene som har vært mest eksponert for revisjoner fra bl.a. Riksrevisjonen er de teamene som nå er mest modne med hensyn til IKT-internkontroll. Ansatte beskriver at rollene til fagområdene og Teknologiavdelingen er utydelige med hensyn til å sikre læring.

5. Vurdering av internkontrollen

Internkontrollen fremstår med et uklart ambisjonsnivå og uten en tydelig helhetlig kobling mellom mål og strategi, styring og gjennomføring. Risikostyring er etablert som prosess, men det er variasjon i samspill mellom fagmiljøer og teknologimiljøer. Styringsprinsipper og kontrollkrav er delvis definert, men operasjonalisering og etterlevelse varierer. Roller og ansvar er overordnet beskrevet, men med vesentlige gap og gråsoner. Praktisering og forankring fremstår ulik på tvers av organisasjonen. Opplæring og kommunikasjon er gjennomført, men med ulik utbredelse og forståelse. Ulike former for avvik registreres og det er etablert oppfølgingsprosesser, men med variasjon i prioritering, oppfølging og lukking. Tilgjengelige data benyttes i ulik grad til styring og rapportering. Erfaringer fra hendelser og revisjoner brukes til læring og deles mellom områder i varierende grad.

5.1. Innledning

Fundamentet i forståelsen av direktoratets nåsituasjon er en analyse av underliggende årsaker (rotårsaksanalyse) til observerte forhold og hvilke implikasjoner disse har for virksomhetens evne til å sikre etterlevelse av regelverk og pålitelig rapportering. Rotårsaksanalysen gir kontekst til nåsituasjonen og er med på å beskrive hvorfor vi observerer det vi gjør.

Modenhetsvurderingen tar utgangspunkt i identifiserte forhold knyttet til virksomhetens internkontroll og vurderer disse opp mot forventninger fra Arbeids- og inkluderingsdepartementet og virksomhetens egne ambisjoner. Det gis en samlet fremstilling av status på sentrale områder som strategi og mål, risikostyring, styringsprinsipper, organisering, opplæring, etterlevelse, rapportering og læring, samt sammenhenger mellom disse. De identifiserte årsaksforholdene understøtter funnene i modenhetsvurderingen.

5.2. Forventninger fra Arbeids- og inkluderingsdepartementet og ambisjonsnivå

Forventningene til internkontrollen er blant annet regulert i *Instruks om virksomhets- og økonomistyring for Arbeids- og velferdsdirektoratet,* fastsatt av Arbeids- og inkluderingsdepartementet 1. januar 2026.

KPMG vurderer at kravene samlet sett **tilsvarer nivå 4, Implementert i modenhetsrammeverket,** som forutsetter faktisk operasjonalisering og konsistent praksis på tvers av virksomheten. Kravene innebærer at virksomhetsstyring, risikostyring, internkontroll, sikkerhet og personvern

- er helhetlig og integrert i virksomhetsstyringen,
- er risikobasert og styrt etter vesentlighet,
- er dokumentert, gjennomført og etterprøvbart,
- følges opp årlig med rapportering til departementet,
- har tydelige roller, ansvar og klar ledelsesforankring, og
- er implementert i hele organisasjonen, ikke kun definert.

KPMGs spørreundersøkelse viser videre at **både ledere og ansatte mener at modenhetsnivå 4, Implementert** bør være det samlede ambisjonsnivået for Arbeids- og velferdsdirektoratet i et 3–5 års perspektiv.

I det følgende redegjøres det for KPMGs vurdering av direktoratets internkontrollmodenhet innen IKT-utvikling, drift og forvaltning. Vi sammenligner dette med direktoratets egen vurdering, fremkommet gjennom besvarelser fra ulike deler av virksomheten i egen spørreundersøkelse.

5.3. Rotårsaksanalyse

5.3.1. Bakgrunn og problemformulering

Der modenhetsanalysen beskriver nåsituasjonen for direktoratets IKT-internkontroll er rotårsaksanalysens bidrag å gi en grundigere forståelse av nåsituasjonens grunnlag. Rotårsaksanalysens metodiske formål er å få tilstrekkelig klarhet i underliggende årsaker til at klasser av årsaker kan remedieres heller enn å fokusere på enkeltsymptomer og -hendelser, og dermed bygge et systemisk sikkerhetsnett som tar høyde for at menneskelige feil kan og vil forekomme.

Det er rotårsaksanalysens essens at det ikke er verken ønskelig eller nødvendig å fordele skyld for historiske feil eller mangler. Det er imidlertid sentralt for analytiske formål å belyse eksempelhendelser eller -forhold som er representative for det som ønskes undersøkt og som kan danne grunnlaget for den problemformulering analysen skal ta utgangspunkt i. De hendelsene KPMG har innlemmet i analysen ble presentert i rapportens kapittel 4. Disse ble valgt fordi de anses å dekke ulike aspekter ved direktoratets IKT-styring og internkontroll, og dermed kunne bidra til å besvare

- om direktoratets internkontroll er tilpasset risiko og vesentlighet, og
- om kontrollene fungerer effektivt i praksis, spesielt i lys av Riksrevisjonens kritikk av svakheter i kontrollmiljø, tilgangsstyring og rapportering.

KPMGs gjennomgang i kapittel 4 viser at Riksrevisjonen gjentatte ganger har påpekt vesentlige svakheter i internkontrollen, og at det som påpekes i stor grad går igjen over flere år. Basert på denne observasjonen valgte KPMG følgende problemstilling for rotårsaksanalysen:

Hvorfor har det fortsatt å skje flere kritiske feil hos Arbeids- og velferdsdirektoratet?

Problemformuleringen er dermed ment å legge særlig vekt på en flerårig tendens heller enn enkelthendelser, blant annet for å kunne si noe om læringsverdi og modenhet i internkontrollsystemet og hvordan erfaringer fra tidligere hendelser brukes til forbedring.

Direktoratet har deltatt i rotårsaksanalysen via arbeidssamlinger. Rapportens kapittel 2 beskriver at deltakerne fikk presentert problemformuleringen som referert over og deretter sparret frem forslag til både rotårsaker og tiltak over to samlinger. De kritiske hendelsene som beskrevet i kapittel 4 ligger til grunn for problemformuleringen gjengitt over, men det er problemformuleringen rotårsaksanalysen har hatt til formål å analysere. Deltakerne i arbeidssamlingene hadde naturlig nok varierende kjennskap til de utvalgte kritiske hendelsene, og ble bedt om å fokusere på

problemformuleringen. Analysen som presenteres i det følgende inkluderer direktoratets innspill fra disse arbeidssamlingene, men er et produkt av KPMGs tillegg og bearbeiding.

KPMG har i det følgende valgt å skille mellom rotårsaker og medvirkende årsaker. Dette skillet vil ikke alltid være absolutt, men der rotårsaker er de sentrale og grunnleggende forholdene som trigger uønskede hendelser eller forhold er de medvirkende årsakene gjerne mer kontekstuelle og fasiliterende. De medvirkende årsakene er ofte med på å hindre at uønskede hendelser eller forhold forhindres eller avdekkes. Det er derfor sentralt at også disse beskrives og forstås.

Rotårsaker og medvirkende årsaker beskrives i det følgende. Utfallet av rotårsaksanalysen vil oppsummeres i den samlede vurderingen i kapittel 5.5.

5.3.2. Rotårsaker

I tillegg til de fire definerte rotårsakene beskrevet i det følgende har KPMGs analyse identifisert to overordnede temaer som gjennomsyrer øvrige årsaksforhold.

Dersom man spør seg hvorfor noe er som det er i en organisasjon et tilstrekkelig antall ganger vil mye i siste instans peke tilbake på kultur. Rotårsaksanalysen som her er gjennomført er intet unntak, og mange av årsaksforholdene som ble identifisert og trukket frem av både direktoratet og KPMG indikerer en svak internkontroll- og kvalitetskultur som et gjennomgripende tema. Dette gir seg blant annet utslag i et manglende felles begrepsapparat, begrenset interkontrollkompetanse og -bevissthet og manglende faglig trygghet til å gjøre operasjonaliserbare prioriteringer. Samlet sett bidrar dette til en kultur der internkontroll og kvalitet ikke er tilstrekkelig integrert i den daglige virksomhetsstyringen. Dette svekker etterlevelse og åpenhet rundt risiko og feil, og forsterker øvrige rotårsaker.

Tilsvarende virker en manglende anerkjennelse av risiko hos toppledelsen å ligge til grunn for mange av årsaksforholdene. KPMGs intervjuer og øvrige kartlegging indikerer at det for flere av de avdekkede svakhetene og for tiltak i organisasjonen generelt virker å være en utilstrekkelig forståelse av hastverk og alvorlighet ved enkelte av forholdene. Dette henger nært sammen med rotårsakene som beskrives i det følgende, deriblant rotårsak 1.

Et knippe andre og mer særegne årsaksforhold belyses i gjennomgangen nedenfor. De fire rotårsakene som beskrives her har nær sammenheng med hverandre, og i noen grad er tematikken overlappende. Dette bidrar til å belyse årsaksforholdene fra ulike vinkler, og viser bredden i hvordan de utspiller seg i praksis.

Videre vil det som regel være tilfellet at rotårsaker kan ha en varierende grad av dybde. Vi trekker frem over at kultur ofte er siste stoppested dersom man graver lenge nok. Det er imidlertid slik at det kan ligge god styringsinformasjon og forståelse i de forhold som beskrives før man kommer så langt. Det følgende er derfor årsaksforhold med varierende grad av dybde, men der de samlet sett anses å gi det mest presise og anvendelige svaret på analysens problemformulering.

De identifiserte årsaksforholdene understøttes, gjenspeiles og detaljeres i stor grad i den påfølgende modenhetsvurderingen. De beskrives derfor kun kort i det følgende.

R1: Manglende risikobasert og tidsriktig tilnærming til styring og prioritering

Tilstrekkelig oversikt over og forståelse for risiko og vesentlighet er hygienefaktorer som må være til stede for hensiktsmessig og tilpasset håndtering av svakheter, hendelser og andre forhold. Mangel på omforent og systematisk forståelse fører til at styring og prioritering i stor grad blir reaktiv. Risiko brukes i begrenset grad som grunnlag for beslutninger, noe som bidrar til at kjente svakheter vedvarer over tid.

Det har blitt beskrevet for KPMG at mange har mindre bevissthet rundt balansegangen mellom å lukke varig og lukke fort. Samtidig er flere av forholdene som ligger til grunn for rotårsaksanalysens problemformulering forhold som over tid har vært kjent i organisasjonen, men der de har fått vedvare fordi håndteringen ikke prioriteres eller det overlates til den enkelte leder å mene noe om prioritering. KPMG vurderer at dette i stor grad gjenspeiler manglende evne i toppledergruppen til å fungere som et samlet, tverrfunksjonelt lederteam for styring og utvikling av internkontroll i direktoratet, med tilstrekkelig kapasitet til å prioritere, beslutte og følge opp internkontroll på tvers av fag- og teknologimiljøer.

R2: Mangelfull samhandling med teknologimiljøene

Samhandlingen mellom styrings-, regelverks- og teknologimiljøene fungerer ikke godt nok i direktoratets matriseorganisering. Krav, risiko og styringsambisjoner blir i for liten grad bearbeidet sammen med teknologimiljøene før de skal omsettes til praktiske løsninger og kontrollmekanismer.

Teknologi involveres ikke alltid tidlig nok eller på riktig nivå. Dialogen skjer ofte enten for operativt mot enkeltteam, eller for overordnet uten tilstrekkelig kobling til arkitektur, plattformer, tekniske avhengigheter og gjennomføringsevne.

I en organisasjon med autonome produktteam kreves et velfungerende mellomledd som kobler toppledelsens ambisjoner, kravstillernes forventninger og teknologimiljøenes praktiske virkelighet. Når dette mellomleddet ikke fungerer tilstrekkelig, svekkes endringsledelse, felles prioritering og evnen til å etablere standardiserte løsninger på tvers. Konsekvensen er at mulighetene for innebygget internkontroll i plattformer, arbeidsprosesser og produktutvikling ikke utnyttes fullt ut.

R3: Utilstrekkelig internkontrollrammeverk

Mangelen på et helhetlig og etterlevd internkontrollrammeverk gjør at internkontrollen blir personavhengig. Dette reduserer forutsigbarhet, konsistens og kvalitet i kontrollarbeidet. Manglende, mangelfulle, utydelige eller mindre tilgjengelige styrende dokumenter, inkludert beskrivelse av trelinjemodellen, roller og ansvar, bidrar til uklar styring og fragmentert etterlevelse. Når overordnede føringer ikke er tydelig definert og operasjonalisert, overlates mye til lokale tolkninger, noe som svekker helhetlig internkontroll. Dette gjelder både direkte (mangler i styringsdokumentasjon) og indirekte (uklarhet, ulik praksis).

R4: Utydelig ansvarsfordeling og svak påsefunksjon

Uklar grensedragning mellom første-, andre- og tredjelinje kombinert med matrisestrukturer og fortsatt autonome produktteam medfører uklar ansvarsfordeling. Dette gjør det vanskelig å sikre eierskap til risiko, kontroller og tiltak, og utfordrer dermed effektiv oppfølging og styring. Dette

innvirker videre på evnen til effektiv og tydelig kommunikasjon med eksterne, deriblant Riksrevisjonen.

5.3.3. Medvirkende årsaker

Rotårsakene som beskrevet over danner de primære underliggende strukturene som anses å ha bidratt til nåsituasjonen innen IKT-internkontroll i direktoratet. Andre aspekter ved direktoratets kontekst, virksomhet og organisasjon vil imidlertid også ha innvirkning. Disse er vurdert som medvirkende årsaker heller enn rotårsaker da de anses å springe ut av forholdene beskrevet over. De forsterker risikoen, men forklarer ikke alene svikten i styring. I det følgende peker KPMG på det vi mener er de mest sentrale og relevante medvirkende årsakene.

M1: Kapasitets- og prioriteringsutfordringer i en kompleks virksomhet

Høyt leveransepress, mange parallelle krav og begrenset kapasitet bidrar til at kontroll- og forbedringsarbeid nedprioriteres. Dette forsterker rotårsakene og gjør det utfordrende å lukke kjente svakheter på en varig måte. Dette har dermed direkte innvirkning på omfang og varighet av problemene, og er særlig nært knyttet til rotårsaken som beskriver manglende risikobasert tilnærming til styring og prioritering (rotårsak 5).

M2: Teknologiske begrensninger som undergraver kontroll og sporbarhet

Direktoratets IKT-arkitektur er i dag som beskrevet i kapittel tre sammensatt av standardiserte skytjenester, egenutviklede plattformsløsninger og eldre systemer som fortsatt driftes i virksomhetens egen infrastruktur. Eldre systemer er fortsatt knyttet til teknologiplattformer som stormaskin og Oracle Forms og driftes i direktoratets egen infrastruktur. Nye løsninger utvikles i hovedsak for sky og bygger i stor grad på den egenutviklede plattformen NAIS, som inngår som en sentral komponent i moderniseringen av IKT-porteføljen. Komplekse og aldrende systemløsninger kombinert med manglende logger og automatiserte kontroller gjør det vanskelig å utøve effektiv internkontroll, og sammensatte systemer og legacy-teknologi gir begrenset helhetsoversikt. Teknologien støtter i begrenset grad kontrollautomatisering, styring, oppfølging og dokumentasjon av etterlevelse.

M3: Svak operasjonalisering av regelverk og eksterne krav

IKT-bruken må oppfylle relevante krav i økonomiregelverket, forvaltningsloven, personvernregelverket og øvrig gjeldende regelverk. Direktoratets tolkning av regelverkskrav oppleves uklare, lite tilpasset mottaker og svakt oversatt til praktisk gjennomføring. Manglende kobling mellom krav, prosesser og kontroller gjør at etterlevelse vurderes ulikt og uføres ulikt i ulike fagmiljøer. Utstrakt bruk av bør-krav heller enn skal-krav gir stort rom for tolkning og personavhengige løsninger og vurderinger. Dette gir en direkte etterlevelsesrisiko.

M4: Manglende systematikk i avvikshåndtering og læringsprosesser

Uklarhet rundt hva som utgjør avvik, hvor de skal meldes og hvordan de følges opp fører til at feil i begrenset grad gir gjennomgående organisatorisk læring. Fokus på enkelttiltak fremfor rotårsaker bidrar til at de samme problemene gjentar seg. Læringsprosesser er etablert, men utfallet av prosessen blir i liten grad operasjonalisert og implementert i praksis på tvers av organisasjonen.

5.4. Modenhetsanalyse

KPMGs vurderinger av de ulike parameterne i modenhetsrammeverket beskrives i det følgende. Utfallet av modenhetsanalysen vil oppsummeres i den samlede vurderingen i kapittel 5.5, herunder en samlet oversikt i figur 18.

5.4.1. Strategi, mål og ambisjoner – uklart ambisjonsnivå, mangler helhetlig tilnærming og kobling til gjennomføring

Strategi, mål og ambisjoner		
1	Ikke etablert	Svak sammenheng strategi–planer; mål ikke operasjonalisert
2	Delvis etablert	Noe sammenheng; enkelte mål operasjonalisert og kjent
3	Etablert, men forbedringsbehov	God sammenheng; viktige mål operasjonalisert og kjent
4	Godt etablert	Sterk sammenheng; alle mål operasjonalisert; systematisk oppfølging
5	Fullt implementert og fungerer svært godt	Som 4 + oppfølging understøttet av teknologi

KPMG vurderer at internkontroll er tydelig prioritert i styringsdokumenter (herunder mål- og disponeringsbrev), men fremstår i begrenset grad operasjonalisert gjennom et samlet og omforent ambisjonsnivå og risikotoleranse på tvers av direktoratet. Dette gjelder særlig hvordan ambisjonsnivå omsettes til konkrete prioriteringer, styringsparametere og beslutningsgrunnlag i linjen, som fremhevet i rotårsak 1. Ledelsesoppfølging skjer i hovedsak periodisk og i begrensede fora, og historisk har bevisstheten rundt vesentlighet og tidsriktighet vært lav, selv om flere peker på forbedring det siste året. Internkontroll og kvalitet fremstår som tydelige temaer i styringsdialogen mellom departement og direktorat, med økt oppmerksomhet etter blant annet oppfølging av Riksrevisjonens funn.

Observasjoner:

- Direktoratet har i 2025 eksplisitt løftet internkontroll som én av toppledelsens hovedprioriteringer. En rekke forbedringstiltak pågår.

- KPMG etterlyser en konkretisering av ambisjonsnivå og en mer helhetlig tilnærming til internkontroll. For en virksomhet hvor utførelsen av samfunnsoppdraget i stor grad avhenger av en velfungerende IKT-ramme vil det ikke være hensiktsmessig å se internkontrollen knyttet til IKT som adskilt fra direktoratets helhetlige internkontrollsystem. Dette er et prinsipp KPMG også vektlegger i rapportens tiltaksanbefalinger og implementeringsplan. Rotårsaksanalysen peker også på utilstrekkelig internkontrollrammeverk som en av de primære driverne bak hendelser og uønskede forhold (rotårsak 3).

- KPMGs syn er at koblingen mellom strategi og operativ gjennomføring i dag er svak og ujevn med betydelig variasjon i praksis mellom enheter, noe som indikerer at operasjonaliseringen av strategiske ambisjoner i stor grad er person- og enhetsavhengig fremfor systematisk forankret i styringsmodellen. Spørreundersøkelsen understøtter dette

ved at flere respondenter opplever uklare forventninger til hva internkontroll faktisk innebærer i praksis.

- KPMG vurderer at involveringen av teknologimiljøene i arbeidet med å styrke internkontrollen per i dag er mangelfull, som også fremheves i rotårsak 2. I utarbeidelse av internkontroll innen IKT-utvikling, testing og forvaltning er KPMGs syn at det er en forutsetning for å lykkes at teknologiavdelingen og produktteamene er tungt involvert. I utvikling av førstelinjekontrollene bør Teknologiavdelingen være i førersetet for å legge grunnmuren i IKT-rammeverket på tvers av avdelingene, med sterk støtte fra kravstillerne.

Samlet samsvarer observasjonene over med kjennetegn på modenhetsnivå 2, Delvis etablert, der internkontroll er delvis forankret i strategi og planer, men i begrenset grad integrert i løpende styring, prioritering og oppfølging. Spørreundersøkelsen understøtter som omtalt over dette bildet ved at flere respondenter opplever uklare forventninger til hva internkontroll faktisk innebærer i praksis, særlig i teknologimiljøene der autonomi og leveransepress dominerer målbildet. Dette innebærer at strategiske ambisjoner i begrenset grad fungerer som et felles styringsanker for prioritering og etterlevelse i den operative hverdagen. Samlet vurderer direktoratet sin egen modenhet på dette området til å være 2,3.

5.4.2. Risikostyring – etablert som prosess, men svak kobling mellom kravstillere og teknologimiljø, mangel på tett tverrfaglig dialog

Risikostyring		
1	Ikke etablert	Ikke beskrevet; få/udokumenterte vurderinger
2	Delvis etablert	Delvis beskrevet; vurderinger gjøres, men dokumenters lite
3	Etablert, men forbedringsbehov	Beskrevet; vurderinger dokumenteres; tiltak er sporadiske; ledere involvert
4	Godt etablert	System for vurderinger og tiltak; effekt evalueres; sterk lederinvolvering
5	Fullt implementert og fungerer svært godt	Som 4 + bred teknologistøtte og kontinuerlig forbedring

Risikostyring er etablert som en prosess, inkludert krav til gjennomføring av risikovurderinger (ROS) og personvernvurderinger (PVK). Samtidig indikerer våre funn at koblingen mellom disse vurderingene og løpende styring og prioritering varierer på tvers av enheter og team. Dette kan bidra til at risiko håndteres ulikt i praksis, til tross for felles metodiske rammer. Risikovurderinger gjennomføres i stor grad lokalt, ofte ved bruk av ulike verktøy og regneark, med begrenset aggregering til et helhetlig risikobilde. Videre er oppfølgingen av risikoreduserende tiltak lite systematisk, med mange tiltak som blir stående åpne over lang tid uten dokumentert effektvurdering. Riksrevisjonens gjentakende funn over flere år – særlig innen IKT-relaterte kontrollområder – illustrerer manglende evne til å løfte læring fra enkeltapplikasjoner til helhetlige, strukturelle forbedringer. Samlet sett er dette et bilde som understøttes av rotårsaksanalysen, deriblant rotårsak 1 og medvirkende årsak 4.

Observasjoner:

- Risikostyring, herunder etterlevelse av lovkrav, er etablert som prosess. Det gjennomføres risikovurderinger på flere nivåer og risiko inngår i rapportering til toppledelsen. Samtidig vurderer KPMG at risikostyringen knyttet til IKT og etterlevelse av lovkrav per i dag i praksis har begrenset styringseffekt. Dette beskrives også i medvirkende årsak 3.

- Variasjon i metodikk og praksis for risikovurdering på tvers av enheter svekker sammenlignbarhet og styringsverdi, og bidrar til at risikostyringen fremstår mer dokumenterende enn aktivt styrende. Dette understøttes av Riksrevisjonens gjentakende funn, funn fra spørreundersøkelsen og intervjuer, som peker på lang lukketid på tiltak og begrenset systematikk i oppfølging, til tross for at kvaliteten på dokumentasjonen ofte oppleves som god.

- KPMGs syn er at det er for svak kobling mellom risikoeiere, kravstillere og teknologimiljøene, inkludert de tverrfaglige produktteamene. Den mangelfulle samhandlingen med teknologimiljøene trekkes også frem i rotårsaksanalysen (rotårsak 2). Det mangler etablerte prosesser for risikoprioritering. Risikovurderinger knyttet til etterlevelse av krav overlates i for stor grad til produktteamene. Direktoratet har etablert en strukturert modell med kraveiere (regelverk) og etterlevere (fag/produktteam), men denne rollefordelingen kan samtidig bidra til utfordringer i samhandlingen dersom den ikke operasjonaliseres gjennom tett tverrfaglig dialog.

- For risikostyring knyttet til etterlevelse av lovkrav og andre interne krav innen IKT-utvikling og drift har direktoratet etablert egne digitale løsninger. De digitale verktøyene «Behandlingskatalogen» og «Støtte til etterlevelse» brukes til å dokumentere etterlevelse av regelverk og interne krav, mens «TryggNok» brukes til å dokumentere risikovurderinger for digitale løsninger. KPMGs syn er at for en virksomhet av Navs størrelse er det et behov for et helhetlig GRC-verktøy (Governance, Risk and Compliance) som gir integrert og konsistent systemstøtte for risikostyring, etterlevelse, styring og kontroll, avvikshåndtering samt rapportering. Et slikt verktøy understøtter relevante policyer og anerkjente rammeverk, slik at etterlevelse av interne og eksterne krav kan gjennomføres på en mer strukturert og etterprøvbar måte, og samtidig legge til rette for mer helhetlig og beslutningsrelevant rapportering. Videre er etablering av effektive, sporbare og rollebaserte arbeidsflyter sentralt for å sikre korrekt, tidsriktig og tilstrekkelig dokumentasjon. På bakgrunn av virksomhetens størrelse, kompleksitet og styringsbehov fremstår dagens systemstøtte på dette området som utilstrekkelig.

Ledelsesinvolveringen i risikostyringen er tydelig på overordnet nivå, men KPMGs sin vurdering er at det i praksis er svak sammenheng mellom identifiserte risikoer, prioritering av tiltak og faktisk gjennomføring i linjen. Samlet sett gir dette risikostyringen begrenset effekt som styringsverktøy, herunder at identifiserte risikoer i varierende grad omsettes til tydelige prioriteringer, avgrensede

tiltak og systematisk oppfølging av faktisk risikoreduksjon. **KPMG vurderer direktoratets modenhet innen risikostyring til modenhetsnivå 2, Delvis etablert.**

Spørreundersøkelsen støtter dette bildet delvis. Her ser vi en spredning der noen respondenter peker på lang lukketid på tiltak og begrenset systematikk i oppfølging, selv om kvaliteten på dokumentasjonen ofte oppleves som god når tiltak først ferdigstilles. Andre peker på at risikovurderinger er beskrevet og dokumentert. Samlet vurderer direktoratet sin egen modenhet innen risikostyring til å være 2,5, noe som tilsvare mellom modenhetsnivå 2 og 3, Delvis etablert/ Etablert, men forbedringsbehov.

5.4.3. Styringsprinsipper og internkontroll – lite operasjonalisert, NAIS-plattformen godt utgangspunkt for forbedringsarbeid innen 1. linje IKT-internkontroller

Styringsprinsipper og internkontroll		
1	Ikke etablert	Mangler styrende dokumenter for styring/prosesser
2	Delvis etablert	Noe dokumentasjon; ujevn oppdatering og bruk
3	Etablert, men forbedringsbehov	Dekker de fleste prosesser; oppdatering satt i system; noe bruk
4	Godt etablert	Dekker alle sentrale prosesser; systematisk oppdatering og bruk
5	Fullt implementert og fungerer svært godt	Som 4 + lett digital tilgang og høy bruk

KPMG vurderer at direktoratet har et omfattende sett av styrende dokumenter og interne krav, særlig innen personvern og enkelte fagområder. Samtidig viser analysen at dokumentlandskapet er **fragmentert**, lite tilgjengelig og ikke konsekvent brukt i praksis. Mange styrende dokumenter er lite kjent blant relevante roller, og juridiske og økonomiske krav er **i begrenset grad operasjonalisert til konkrete, etterprøvbare kontrollkrav** – særlig innen IKT-utvikling, drift og forvaltning. De samme mekanismene trekkes frem i rotårsaksanalysen, deriblant rotårsak 3 og medvirkende årsak 3. Dette gjelder blant annet kontroller knyttet til logging, tilgangsstyring og endringshåndtering. Selv om det er etablert nye retningslinjer, veiledere og et felles dokumenthierarki, fremstår internkontrollrammeverket fortsatt som fragmentert og ikke fullt ut implementert eller operasjonalisert på tvers av direktoratet.

Det er igangsatt arbeid for å etablere et helhetlig system for kvalitet og internkontroll i Nav, inkludert utvikling av struktur og dokumenthierarki. Samtidig fremstår dette arbeidet som ikke fullt implementert eller operasjonalisert på tvers av direktoratet og medfører at internkontroll i praksis i større grad fremstår som desentralisert og delvis ulikt implementert. Direktoratet har uttrykt en ambisjon om å løfte internkontrollen til et mer strukturert modenhetsnivå, noe som indikerer at dagens praksis fortsatt er under utvikling.

Observasjoner:

- Styrende dokumenter gir en overordnet beskrivelse av interne krav, roller, ansvar og prinsipper og internkontroll er formelt integrert i lederansvaret. Samtidig vurderer KPMG at dokumentlandskapet er fragmentert, lite tilgjengelig og ikke konsekvent brukt i praksis. Mange styrende dokumenter er lite kjent blant relevante roller, og fremstår som for

overordnede til at de i tilstrekkelig grad kan operasjonaliseres i produktteamene. KPMG er kjent med at det det pågår nå en rekke forbedringsaktiviteter knyttet til denne observasjonen.

- Det mangler tilstrekkelig sammenheng mellom overordnede krav og faktisk praksis, særlig grunnet fravær av en tydelig mekanisme for etableringen av konkrete, etterprøvbare kontrollkrav. Dette bidrar til at internkontroll i praksis blir person-, team- og kontekstavhengig. Spørreundersøkelsen og intervjuer understøtter dette ved at respondentene i stor grad kjenner til kravene, men opplever etterlevelse og praktisering som ujevn og personavhengig.

- Direktoratet har utviklet en egen intern plattform for utvikling, drift og kjøring av applikasjoner; «NAIS». KPMGs syn er at NAIS er et kraftig verktøy for å institusjonalisere god IT-styring og internkontroll. NAIS tilbyr en rekke kontroller, men for at disse skal gi utbytte må produktteamene aktivt konfigurere eller benytte dem. Dersom ledelsen etablerer solide governance-prosesser rundt bruken av NAIS, kan plattformen fungere som en pilar i IKT-internkontrollsystemet. Et gjennomgående funn er manglende «oversetterfunksjon» fra juridiske og økonomiske krav til konkrete, tekniske og operative kontrollkrav for utvikling, drift og forvaltning. Dette gjelder særlig logging, tilgangsstyring og endringshåndtering, der kontroller finnes, men ikke er ensartet dokumentert eller etterprøvbart fulgt opp.

Internkontrollen fremstår derfor i stor grad som et rammeverk under oppbygging, snarere enn et fullt operasjonalisert system. Direktoratet har igangsatt et tverrgående internkontrollprosjekt med tydelig ledelsesforankring, som kan bidra til å styrke operasjonaliseringen av internkontroll fremover. KPMG vurderer modenheten innen styringsprinsipper og internkontroll som **modenhetsnivå mellom 2 og 3,** med tydelig forbedringsretning, men fortsatt betydelige gap i praktisk anvendelse.

Samlet samsvarer observasjonene over med kjennetegn på modenhetsnivå mellom 2 og 3 (Delvis etablert / Etablert, men forbedringsbehov). På den ene siden gir NAIS-plattformen et godt utgangspunkt for forbedringsarbeid innen førstelinje IKT-internkontroller, samt at styrende dokumenter gir en overordnet beskrivelse av interne krav, roller, ansvar og prinsipper og internkontroll er formelt integrert i lederansvaret. Samlet tilsvarer disse to elementene en modenhet på nivå 3. Samtidig er det KPMGs vurdering at dokumentlandskapet er fragmentert, lite tilgjengelig og ikke konsekvent brukt i praksis, samt at mange styrende dokumenter er lite kjent blant relevante roller. Dette tilsvarer en modenhet på nivå 2.

I spørreundersøkelsen vurderer direktoratet sin modenhet til nivå 3, som betyr at styringsprinsipper og internkontroll dekker de fleste prosesser er oppdatert og satt i system og noe i bruk.

5.4.4. Organisering – svak operasjonalisering av trelinjemodellen skaper uklarheter og ineffektivitet. Mangelfull utnyttelse av internkontrollkompetanse i teknologiavdelingen

Organisering, roller og ansvar		
1	Ikke etablert	Uklare roller; uenighet om prioriteringer; lite internkontrollfokus
2	Delvis etablert	Delvis klarhet; delvis arenaer for styring
3	Etablert, men forbedringsbehov	Stort sett klare roller; etablerte arenaer for styring
4	Godt etablert	Klare roller; trelinjemodell; systematisk forbedring via arenaer
5	Fullt implementert og fungerer svært godt	Som 4 + dynamisk justering av roller; linjene spiller hverandre gode

Direktoratet har de siste årene gjort vesentlige endringer i organiseringen, blant annet gjennom etablering av fagområder og klarere plassering av systemansvar. Formelle roller og ansvar for internkontroll fremgår av ansvarsdokumentet, og det er etablert ulike styrings- og beslutningsarenaer på tvers av fag, teknologi og styring. Det er også igangsatt et tverrgående internkontrollprosjekt med tydelig ledelsesforankring, som kan bidra til å styrke operasjonaliseringen av internkontroll fremover.

Observasjoner:

- Ansvar for internkontroll er plassert i linjen i tråd med ansvarsdokumentet av 1. mai 2025, og det er etablert styrings- og beslutningsarenaer på tvers av fag, teknologi og styring. Samtidig viser KPMGs analyse at rolle- og ansvarsforståelsen i praksis er uklar, særlig i grenseflatene mellom Teknologi, Økonomi- og styringsavdelingen og Juridisk, slik også rotårsak 4 fremhever. Dokumentasjonen indikerer samtidig at avklaringer mellom avdelinger i enkelte tilfeller må initieres av avdelingene selv, noe som kan bidra til uklarhet i praktisk operasjonalisering av ansvar. Manglende operasjonalisering av roller og ansvar bidrar til at sentrale internkontrolloppgaver i praksis faller mellom ulike enheter, og at oppfølging og prioritering blir fragmentert.

- Særlig fremstår andrelinjefunksjonen for internkontroll som lite operasjonalisert, med uklare forventninger til veiledning, påse-, verifikasjons- og eskaleringsansvar. Det pågår arbeid med å ferdigstille et styrende dokument som beskriver dette samt at etableres en egen kvalitetsseksjon med påse-ansvar for risiko, rammeverk og oppfølging av etterlevelse. Særlig fremstår kravstillers ansvar for å følge opp produktteamenes arbeid med oppfyllelse av krav som mangelfull. Dette innebærer at etterlevelsesverktøyet per i dag i stor grad er innrettet mot dokumentasjon av status, mens oppfølging og videre veiledning i stor grad synes å bero på den enkelte kraveier, det enkelte team og den generelle styringslinjen. Videre mangler et systematisk arbeid med forebygging og avdekking av ulike former for økonomiske misligheter (underslag, korrupsjon, etc).

- Enkelte krav er i etterlevelsesverktøyet formulert på svært overordnet nivå, og det overlates til 120 team å vurdere hvorvidt kravet treffer dem og i hvilken grad de oppfyller kravene. Dette er svært tidkrevende for produktteamene og fremstår som svært ineffektivt.

Kravstiller må operasjonalisere kravet og aktivt bidra med å evaluere i hvilken grad kravet treffer de ulike produktteamene.

- Dette bidrar til at etterlevelsesansvaret, spesielt innen IKT, fremstår som uklart og fragmentert, og at ingen har et helhetlig ansvar for eller oversikt over samlet risikobilde og prioritering på tvers av områder. Videre mangler det tydelige mekanismer for beslutningsmyndighet og fremdrift når risikoer og avvik går på tvers av organisatoriske enheter, noe som svekker gjennomslaget for prioriteringer.

Samlet samsvarer KPMGs funn omtalt over en modenhetsnivå 2, Delvis etablert. Analysen viser at rolle- og ansvarsforståelsen i praksis er delvis etablert og uklar, særlig i grenseflatene mellom fagområder, Teknologi, Økonomi- og styringsavdelingen og Juridisk. Spesielt fremstår andrelinjefunksjonen for internkontroll som lite operasjonalisert, og det er betydelig usikkerhet knyttet til hvem som har påse- og verifikasjonsansvar for etterlevelse og kontroller. Dette svekker forutsetningene for helhetlig styring, ettersom ingen funksjon har et tydelig og operativt ansvar for å følge opp, verifisere og utfordre praksis på tvers av organisasjonen. Som følge av dette faller viktige internkontrolloppgaver mellom ulike enheter, og prioriteringsmekanismer mister gjennomslag.

Spørreundersøkelsen understøtter dette funnet gjennom fritekstkommentarer om uklare grenseflater mellom fag, teknologi, juss og styring, og om manglende eierskap til helheten i internkontrollarbeidet. Samlet vurderer direktoratet sin egen modenhet på Organisering, roller og ansvar til 2,3.

5.4.5. Opplæring og kommunikasjon – styrket, men fragmentert. Stor usikkerhet på alle nivåer: «hva menes med internkontroll?»

Opplæring og kommunikasjon		
1	Ikke etablert	Få føringer; lite systematikk; ingen kompetansekrav
2	Delvis etablert	Delvis føringer; noe systematikk og teknologi; enkelte krav
3	Etablert, men forbedringsbehov	Tydelige føringer; god systematikk; de fleste krav ivaretatt; mye teknologi
4	Godt etablert	Sterk forankring; svært systematisk; repetisjon; utstrakt teknologi
5	Fullt implementert og fungerer svært godt	Som 4 + innhentede tilbakemeldinger brukes til kontinuerlig forbedring

Opplæring knyttet til internkontroll, regelverk og etterlevelse gjennomføres i direktoratet, men i varierende grad og med ulik systematikk. Direktoratet har nylig etablert et omfattende internkontrollprosjekt og er i ferd med å utvikle og implementere et helhetlig opplæringsløp for kvalitet og internkontroll. Opplæringen er strukturert med tydelige målgrupper, læringsmål og modulbasert oppbygning, og skal understøtte implementering av retningslinje og veileder for internkontroll. Samtidig fremstår opplæringen fortsatt som under utvikling, og effekten av tiltakene vil være avhengig av faktisk gjennomføring, prioritering og forankring i linjen.

Kompleksiteten i etterlevelseskravene, herunder behov for lokale vurderinger og filtrering av relevante krav i etterlevelsesverktøyet, kan bidra til opplevd usikkerhet rundt hva internkontroll innebærer i praksis.

Observasjoner:

- Det har det siste året vært økt oppmerksomhet rundt behovet for kompetanseheving innen internkontroll, økonomiregelverk og kvalitet. KPMGs analyse viser at opplæringen i begrenset grad er risikotilpasset og rollebasert, og at det mangler en helhetlig oversikt over kompetansekrav for sentrale roller.

- I intervjuene KPMG har gjennomført fremgår det tydelig at begrepet «internkontroll» ikke er et velkjent begrep for de fleste, og at det er et stor sprik i oppfatning av hva krav og forventninger til internkontroll innebærer i praksis. Beskrivelsene av internkontroll slik de fremgår av COSO, COBIT, ISO og IIA er gjennomgående lite kjent, også på ledernivå. Samtidig gjennomføres det en rekke aktiviteter i praksis, inkludert styrking av rutiner (ref. innebygget funksjonalitet i NAIS) o.l., uten at dette nødvendigvis forstås som internkontroll.

- Videre er det svake koblinger mellom hendelser, revisjonsfunn og målrettede opplæringstiltak, noe som bidrar til at kjente svakheter, særlig innen IT-kontroller, vedvarer over tid. Opplæring er i stor grad generell og ad hoc, noe som gir uklare forventninger til internkontroll, varierende etterlevelse og begrenset operasjonalisering av styringskrav i praksis.

KPMG vurderer derfor direktoratets modenhet innen opplæring og kommunikasjon til mellom nivå 2 og 3, men nærmere nivå 2 og med tydelig behov for økt systematikk og forankring. Våre analyser viser at opplæringen i begrenset grad er risikotilpasset og rollebasert, og at det mangler en helhetlig oversikt over kompetansekrav for sentrale roller. Videre er det svake koblinger mellom hendelser, revisjonsfunn og systematisk bruk av opplæring som forbedringstiltak. Opplæring er i stor grad generell og ad hoc, med svak rolle- og risikotilpasning. Dette gir uklare forventninger til internkontroll, varierende etterlevelse og begrenset operasjonalisering av styringskrav i praksis, noe som i stor grad kjennetegner nivå 2 på modenhetsskalaen. Samtidig kommer det frem at virksomheten det siste året har hatt økt oppmerksomhet rundt behovet for kompetanseheving innen internkontroll, økonomiregelverk og kvalitet, samt at enkelte fagområder, særlig innen ytelsesforvaltning, har etablert mer strukturerte opplæringsløp. Disse to observasjonene kjennetegner modenhetsnivå 3.

Spørreundersøkelsen viser at direktoratet vurderer sin egen modenhet til nivå 2,6, noe som betyr at de vurderer det til å være høyere grad av systematikk og at styringsarenaer brukes mer aktivt til oppfølging og forbedring enn det KPMGs analyser tyder.

5.4.6. Etterlevelse – lang lukketid på avvik, mangelfulle prosesser for prioritering av avvik og oppfølging på tvers av produktteam

Etterlevelse		
1	Ikke etablert	Få/ad hoc kontroller; manglende avvikssystem
2	Delvis etablert	Enkelte kontroller; avvikssystem lite kjent

3	Etablert, men forbedringsbehov	Risikobaserte kontroller; plan for noen områder; avvikssystem delvis kjent
4	Godt etablert	Planlagte, dokumenterte kontroller; teknologi noe brukt; avvikssystem brukt
5	Fullt implementert og fungerer svært godt	Som 4 + utstrakt teknologi og læringsprosess

Direktoratet gjennomfører kontrollaktiviteter og har etablerte prosesser for håndtering av avvik og revisjonsfunn. Avvikssystemer er på plass, og status på tiltak rapporteres til ledelsen. Det er etablert flere verktøy og prosesser for å støtte etterlevelse, inkludert krav til risikovurderinger (ROS), personvernvurderinger (PVK) og dokumentasjon av beslutninger og vurderinger og det pågår initiativer som også inkluderer styrket oppfølging av tiltak og etterlevelse gjennom internkontrollprosjektet. Samtidig indikerer våre funn at etterlevelse i praksis varierer, blant annet fordi verktøyene gir rom for lokale vurderinger og prioriteringer. Dette kan bidra til forskjeller i modenhet og etterlevelse på tvers av team og produktområder. Direktoratet peker selv på behov for forbedret etterlevelse og tydeligere krav, til tross for etablerte rammeverk og pågående tiltak. Samlet sett er dette observasjoner som underbygges av den gjennomførte rotårsaksanalysen, som blant annet vektlegger manglende systematikk i avvikshåndtering og læringsprosesser (medvirkende årsak 4) samt utydelig ansvarsfordeling og svak påsefunksjon (rotårsak 4).

Observasjoner:

- Direktoratet gjennomfører ulike former for kontrollaktiviteter på tvers av organisasjonen og har etablerte prosesser for håndtering av avvik og revisjonsfunn, inkludert et standardisert avvikssystem og rapportering av status på tiltak til ledelsen. Samtidig vurderer KPMG at etterlevelsesarbeidet har vesentlige svakheter knyttet til gjennomføring, dokumentasjon og oppfølging. Kontrollaktiviteter og krav følges i varierende grad opp i praksis, og etterlevelsesvurderingene fremstår i stor grad som egenvurderinger i produktteamene. KPMG har i begrenset grad sett dokumentasjon som tydelig beskriver hvilke krav som stilles til underliggende kontrollbevis. Det er også mangelfull sammenheng mellom kravstillere og produktteam når det gjelder oppfølging av etterlevelse.

- Direktoratet har etablert et sentralt verktøy for dokumentasjon av etterlevelse, som gir struktur og oversikt. Samtidig åpner praksis for at etterlevelsesdokumentasjon kan godkjennes selv om alle krav ikke er ferdig vurdert eller oppfylt, forutsatt at risikoeier aksepterer risiko. Dette kan bidra til variasjon i modenhet og etterlevelse på tvers av produktområder.

- Det mangler en helhetlig tilnærming til etterlevelse på tvers av eksterne og interne krav. Det er per i dag for svak kobling mellom produktteamene der IKT-utvikling, drift og forvaltning gjennomføres og kravstillerne. Rollen til Teknologiavdelingen er utydelig. Kravstillerne innenfor de ulike regulatoriske områdene arbeider i for stor grad i siloer, uten risikovurderinger og prioriteringer på tvers av krav. I tillegg kartlegges i liten grad synergier mellom internkontrollaktiviteter, bla. der én kontroll kan tilfredsstille flere lovkrav. Når krav ikke er tilstrekkelig operasjonalisert og ansvar ikke er tydelig forankret, overlates

etterlevelse i praksis til lokale vurderinger i produktteamene, noe som gir ujevn kvalitet og svak samlet styring.

Analysen peker på svakheter i planmessighet, dokumentasjon og lukking av tiltak. Mange kontrolltiltak blir stående åpne over lang tid, og det er mangelfull dokumentasjon på gjennomføring og faktisk risikoreduksjon. Tekniske kontroller innen IKT, særlig knyttet til logging og tilgangsstyring, har vist seg å være utilstrekkelige, noe også alvorlige hendelser de senere år illustrerer og som belyst av rotårsaksanalysen (medvirkende årsak 2).

Spørreundersøkelsen bekrefter variasjon i faktisk kontrollutførelse og peker på lang lukketid på avvik som et gjennomgående problem. Etterlevelse vurderes dermed ikke primært å være et spørsmål om vilje eller kompetanse, men om manglende struktur, prioritering og systematisk oppfølging over tid.

Samlet vurderer KPMG at etterlevelsesarbeidet vurderes til modenhetsnivå 2, Delvis etablert, med vesentlige utfordringer knyttet til gjennomføring og etterprøvbarhet. På dette området ser vi et relativt stort avvik til direktoratet, som vurderer sin egen modenhet til 2,7.

5.4.7. Rapportering – mangelfull analyse og rapportering av tilgjengelige data

Rapportering		
1	Ikke etablert	Noe rapportering; roller/ansvar ikke formalisert
2	Delvis etablert	Rapportering mål/økonomi; roller delvis formalisert
3	Etablert, men forbedringsbehov	Rapportering mål, økonomi og risiko; roller formalisert
4	Godt etablert	Integrert rapportering inkl. compliance; dashboards/KPIer
5	Fullt implementert og fungerer svært godt	Som 4 + kontinuerlig forbedring av prosessen

Direktoratet har etablert en tertialvis rapportering til toppledelsen som omfatter måloppnåelse, risiko, økonomi og etter hvert også internkontroll og etterlevelse. Det er særlig de siste to årene en tydelig utvikling mot økt omfang og struktur i rapporteringen på internkontroll og etterlevelse, blant annet gjennom etablering og videreutvikling av et eget kapittel for dette fra andre tertial 2024. Rapporteringen inkluderer blant annet status på tiltak fra revisjoner, oppfølging av ledelsens gjennomgang, kvalitetsarbeid og risikostyring, og er gradvis utvidet med mer detaljer, herunder personvern og avdelingenes egenvurderinger. Samtidig indikerer våre funn at tilgjengelige data og informasjon fra disse rapporteringsprosessene i begrenset grad utnyttes til helhetlig analyse og styringsinformasjon på tvers.

Observasjoner

- Direktoratet produserer rapportering om måloppnåelse og økonomi og har etablert faste arenaer for rapportering til ledelsen, hvor rapportering om risiko og internkontroll inngår. Samtidig vurderer KPMG at rapporteringen i begrenset grad gir et helhetlig bilde av risiko knyttet til etterlevelse og effekt av tiltak, og dermed er en bidragsyter til rotårsak 1 som vedrører manglende risikobasert og tidsriktig tilnærming til styring og prioritering.

- Rapporteringen har i hovedsak fokus på gjennomføringsstatus og aktivitetsnivå, fremfor faktisk kontrollnivå og oppnådd risikoreduksjon. Manglende sammenstilling av informasjon på tvers av enheter gjør det krevende for ledelsen å identifisere hvor internkontrollen er mest sårbar. Videre varierer bruk av dashboards, KPI-er og styringsinformasjon betydelig mellom enheter, og rapportering knyttet til etterlevelse i teknologimiljøene er i begrenset grad kjent og integrert i den overordnede styringen.

- Etterlevelsesverktøyet der alle 120 produktteam skal dokumentere status for sitt produkt er et godt utgangspunkt for rapportering på produktnivå. KPMGs undersøkelse viser imidlertid at ledelsen per i dag i liten grad har innsikt i data som er dokumentert her. Det er ikke etablert rutiner for systematisk analyse og rapportering basert på disse dataene.

Samlet sett vurderer KPMG direktoratets modenhet innen rapportering til modenhetsnivå mellom 1 og 2, Ikke etablert og Delvis etablert. Analysen viser at rapporteringen i begrenset grad gir et helhetlig bilde av risiko, etterlevelse og effekt av tiltak. Rapporteringen har hovedsakelig fokus på gjennomføringsstatus, fremfor faktisk kontrollnivå og risikoreduksjon. Bruk av dashboards, KPI-er og styringsinformasjon varierer betydelig mellom enheter. Når rapporteringen i hovedsak fokuserer på aktivitets og tiltaksstatus fremfor faktisk effekt på risiko og etterlevelse, reduseres rapporteringens verdi som beslutningsgrunnlag for ledelsen. Resultatene fra spørreundersøkelsen utført av Direktoratet er samlet 2,3 noe som tyder på en modenhet noe høyere enn KPMGs funn og observasjoner.

5.4.8. Læring og forbedring – svake helhetlige sløyfer. Produktteamene i stor grad «overlatt til seg selv» uten systematiske prosesser for læring på tvers

Læring og forbedring		
1	Ikke etablert	Rapportering brukes ikke; liten oppfølging av kontroller
2	Delvis etablert	Rapportering brukes noe; begrenset oppfølging og tilbakemelding
3	Etablert, men forbedringsbehov	Rapportering brukes; kontroller følges opp; tilbakemelding gis
4	Godt etablert	God sammenheng styring–oppfølging; evaluering og justering systematisert
5	Fullt implementert og fungerer svært godt	Helhetlig, lærende organisasjon; integrert kontinuerlig forbedring

Direktoratet har ambisjoner om å være en lærende organisasjon, og det finnes arenaer for evaluering etter hendelser, revisjoner og tilsyn. Erfaringer deles i enkelte deler av organisasjonen. Det er etablert mekanismer for oppfølging av avvik, hendelser og revisjonsfunn. Samtidig fremstår læring og forbedring som i begrenset grad systematisert og delt på tvers av organisasjonen. Manglende systematikk i avvikshåndtering og læringsprosesser fremheves også av rotårsaksanalysen (medvirkende årsak 4).

Observasjoner:

- Direktoratet har ambisjoner om å være en lærende organisasjon, og det finnes etablerte arenaer for evaluering etter hendelser, revisjoner og tilsyn. Erfaringer deles i enkelte deler

av organisasjonen, og det utarbeides blant annet rapporter for hendelser. Samtidig vurderer KPMG at læring og forbedring i begrenset grad er systematisert og institusjonalisert på tvers av organisasjonen.

- Produktteamene er etter KPMGs syn i for stor grad overlatt til seg selv. Det er ikke etablert systematiske prosesser for implementering av læring på tvers av teamene. I intervjuene KPMG har gjennomført fremgår det at de produktteamene som har vært mest eksponert for revisjoner fra bl.a. Riksrevisjonen er de teamene som nå er mest modne med hensyn til IKT-internkontroll. Rollen til Teknologiavdelingen er utydelig med hensyn til å sikre læring.

- KPMGs analyse viser at det er svak kobling mellom hendelser, revisjonsfunn og strukturelle forbedringer, noe som bidrar til at de samme problemstillingene går igjen over tid. Læring skjer, men omsettes i begrenset grad til varige endringer i styring, kontroller og praksis. Videre fremstår lærings- og forbedringssløyfene som svakt systematisert. Eksisterende verktøy for oppfølging av tiltak gir et potensielt godt grunnlag for læring, men utnyttelsen av dette på tvers fremstår som begrenset.

- Det er også et uutnyttet potensial for datadrevet oppfølging, da eksisterende data i for eksempel etterlevelsesverktøyet og risikostyringsverktøyet TryggNok i begrenset grad brukes til å gi sanntidsinnsikt i etterlevelse og risiko, og til å prioritere tiltak.

KPMGs analyse viser at læring i liten grad er systematisert på tvers av direktoratet. Hendelser og revisjonsfunn fører ikke konsekvent til varige endringer i styring, kontroller og praksis, og de samme problemstillingene går igjen over tid. Tiltaksoppfølging og evaluering av effekt fremstår som særlig svakt. Gjentakende funn innen sentrale IKT-kontrollområder indikerer at læring fra revisjoner og hendelser i begrenset grad omsettes til varige, strukturelle forbedringer på tvers av organisasjonen. Manglende strukturert oppfølging og deling av læring bidrar til at kjente svakheter vedvarer over tid, til tross for gjentatte revisjonsfunn og hendelser.

Lærings- og forbedringsarbeidet anses som utilstrekkelig innarbeidet i virksomhetens helhetlige styringssystem. Hendelser og revisjonsfunn benyttes kun i begrenset omfang til å iverksette varige forbedringstiltak på tvers av organisasjonen. At tilsvarende avvik innen tilgangsstyring, logging og endringshåndtering oppstår gjentatte ganger indikerer at den kontinuerlige forbedringsprosessen ikke gjennomføres helhetlig og kontinuerlig.

Læring og forbedring vurderes samlet sett å ha modenhetsnivå 2, Delvis etablert, med tydelige strukturelle barrierer for kontinuerlig forbedring. Her ser vi et gap til direktoratet egen vurdering i spørreundersøkelsen, som anslår egen modenhet til 2,75. Dette indikerer at de vurderer at funn og avvik knyttet til internkontroll og risikovurdering brukes mer aktivt i oppfølging og tilbakemelding enn det KPMGs funn tilsier.

5.5. Samlet vurdering

Samlet sett gir intervjuene, dokumentanalysen, arbeidssamlingene og spørreundersøkelsen et samstemt og konsistent bilde av direktoratets nåsituasjon innen internkontroll for IKT-utvikling, drift og forvaltning. Kombinasjonen av rotårsaksanalyse og modenhetsvurdering viser at

direktoratet har flere sterke forutsetninger for god internkontroll, herunder høy faglig kompetanse, dedikerte og erfarne medarbeidere, samt økt lederoppmerksomhet rundt kvalitet, etterlevelse og internkontroll de senere årene.

KPMGs gjennomgang viser at Arbeids- og velferdsdirektoratet det siste året har iverksatt flere viktige tiltak for å styrke internkontrollen. Etablering av nye retningslinjer, et tydeligere dokumenthierarki og oppstart av et eget internkontrollprosjekt i 2026 representerer steg i riktig retning. Tiltakene har imidlertid så langt ikke hatt tid til å gi tilstrekkelig effekt i praksis.

Samlet sett fremstår internkontrollen fortsatt som fragmentert, ujevnt operasjonalisert og preget av varierende etterlevelse på tvers av organisasjonen. Gjennomgangen viser at hovedutfordringen ikke primært er mangel på initiativer, men manglende evne til å etablere en helhetlig, risikobasert og konsekvent styrt internkontroll som fungerer i praksis. Internkontrollen er i for stor grad avhengig av lokal praksis i produktteam og fagmiljøer, noe som gir vedvarende svakheter innen sentrale områder som tilgangsstyring, logging, etterlevelse og oppfølging av avvik.

KPMG vurderer at manglende tydelig ambisjonsnivå, svak operasjonalisering av krav og uklare rolle- og ansvarsforhold er sentrale årsaker til utfordringsbildet. Internkontroll konkurrerer i praksis med andre hensyn i en presset hverdag, noe som gir ujevn prioritering, lang lukketid på avvik og begrenset gjennomføringsevne. Dette forsterkes av mangelfull samhandling mellom regulatoriske miljøer, styringsfunksjoner og teknologimiljøer, samt en svak operasjonalisering av trelinjemodellen – særlig i andrelinjen.

Gjennomgangen viser også at styringen av internkontrollområdet samlet sett ikke har vært tilstrekkelig tydelig i samspillet mellom Arbeids- og inkluderingsdepartementet og direktoratet. Utfordringen ligger i begrenset grad i kravbildet, men i oppfølging av gjennomføring og effekt. Etter KPMGs vurdering har verken etatsstyringen eller den interne styringen i tilstrekkelig grad bidratt til å etablere klare forventninger til modenhet, risikotoleranse og dokumentert effekt av tiltak.

På denne bakgrunn vurderer KPMG at direktoratets samlede modenhet innen internkontroll for IKT-utvikling, drift og forvaltning ligger i spennet mellom nivå 2 og 3, men med et helhetsbilde som samlet sett ligger **nærmere nivå 2, Delvis etablert**. Det er identifisert tydelige forbedringsbehov knyttet til:

- helhetlig styring og integrasjon av internkontroll i virksomhetsstyringen
- tydeligere roller og ansvar, særlig i andrelinjen og i grenseflatene mellom fag, teknologi og styring
- mer systematisk, risikobasert prioritering, oppfølging og lukking av tiltak
- styrkede, institusjonaliserte lærings- og forbedringssløyfer på tvers av produktområder

Direktoratet har klare strategiske ambisjoner knyttet til kvalitet, rettssikkerhet og internkontroll, og disse er overordnet godt forankret på toppledernivå. Strategiske prioriteringer er formulert gjennom flerårige føringer og årlige mål, og internkontroll er eksplisitt løftet frem som et sentralt ledelsesansvar. Analysen viser imidlertid at koblingen mellom disse ambisjonene og den operative styringen er ujevn på tvers av organisasjonen.

Flere deler av direktoratet har brutt strategiske mål ned i konkrete operative krav, kontroller og styringsparametere, mens dette i andre deler i større grad er person-, kultur- eller kontekstavhengig. Oppfølging av internkontroll skjer i hovedsak gjennom periodiske prosesser (bl.a. tertialvis), og i begrenset grad gjennom løpende, risikobasert styring og prioritering i den operative hverdagen.

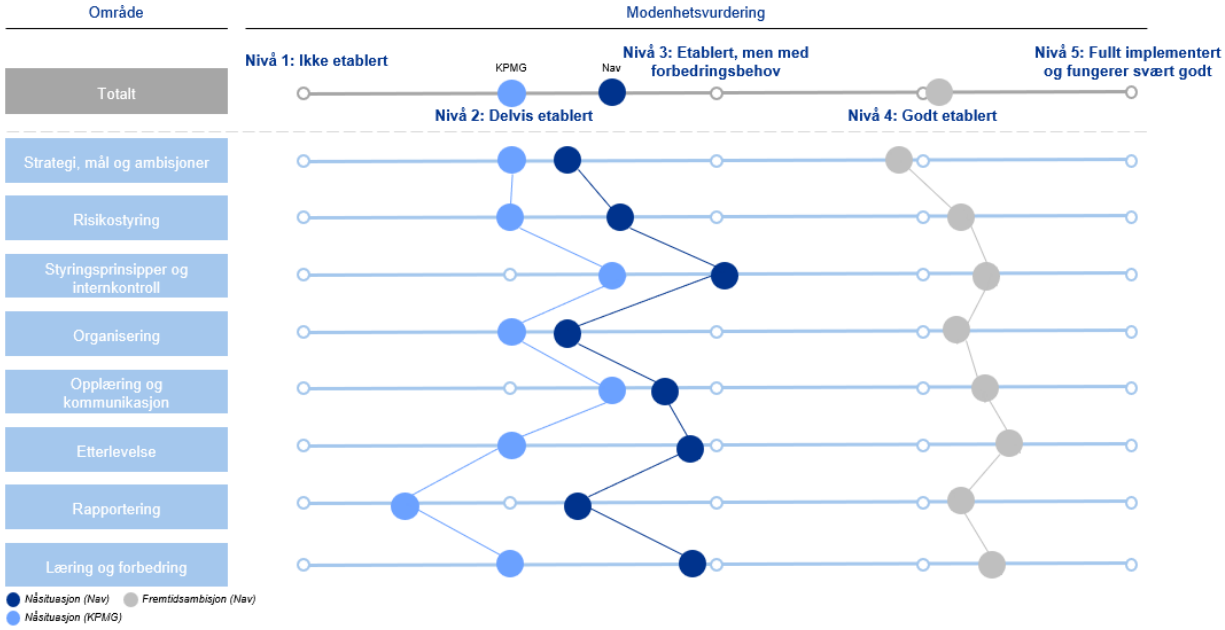
Basert på samlet vurdering av styrende dokumentasjon, intervjuer med ledelse og nøkkelpersoner, gjennomgang av intern- og eksternrevisjoner, observasjon av praksis og gjennomførte arbeidssamlinger, konkluderer KPMG med at direktoratet har etablert mange nødvendige elementer for god internkontroll, men at disse i for liten grad fungerer som et integrert og etterprøvbart system. Utfordringene knytter seg i hovedsak ikke til fravær av kontroller, men til manglende konsistent gjennomføring, dokumentasjon, verifikasjon og ledelsesmessig oppfølging av kontrollene i praksis. Dette samsvarer med og underbygges av utfallet av rotårsaksanalysen.

Rotårsaker		Medvirkende årsaker	
R1	Manglende risikobasert og tidsriktig tilnærming til styring og prioritering	**M1**	Kapasitets- og prioriteringsutfordringer i en kompleks virksomhet
R2	Mangelfull samhandling med teknologimiljøene	**M2**	Teknologiske begrensninger som undergraver kontroll og sporbarhet
R3	Utilstrekkelig internkontrollrammeverk	**M3**	Svak operasjonalisering av regelverk og eksterne krav
R4	Utydelig ansvarsfordeling og svak påsefunksjon	**M4**	Manglende systematikk i avvikshåndtering og læringsprosesser

Hovedobservasjoner

- **Strategi, mål og ambisjoner**: Ambisjoner er definert, men ikke tilstrekkelig konkretisert eller konsekvent operasjonalisert i styringsmodellen. Manglende felles forståelse av alvor, risikotoleranse og tidskritikalitet reflekterer etter KPMGs vurdering svak felles prioritering og forankring vedrørende internkontroll i toppledergruppen, og er en sentral årsak til at svakheter har vedvart over tid.
- **Risikostyring**: Det mangler en tydelig prioritering av risikoer opp mot direktoratets strategiske mål, en omforent risikotoleranse og klar kommunikasjon av denne til linjen. Samhandlingen mellom risikoeiere, kravstillere og teknologimiljøer er svak, og teknologi- og produktteam er i begrenset grad involvert i forbedringsarbeidet. Risikovurderinger knyttet til etterlevelse av krav overlates i for stor grad til produktteamene. Dette indikerer manglende helhetlig prioritering og tydelig styringssignaler fra topplednernivå.
- **Styringsprinsipper og internkontroll**: Overordnet godt beskrevet, men lite operasjonalisert til konkrete, etterprøvbare kontrollkrav. Direktoratets egenutviklede plattform for utvikling, drift og kjøring av applikasjoner (kalt NAIS) utgjør et godt, men delvis uforløst, utgangspunkt for IKT-internkontrollen.
- **Organisering**: Svak operasjonalisering av ansvar i organisasjonen. Uklarheter i trelinjemodellen (god praksis for internkontroll) mellom de operative enhetene og støtte- og kontrollfunksjoner, særlig i andrelinjen, skaper ineffektivitet. Organisasjonen mangler et helhetlig compliance-program, herunder systematisk arbeid med forebygging og avdekking av økonomiske misligheter.

- **Opplæring og kommunikasjon**: Opplæringen knyttet til internkontroll har vært fragmentert. Et strukturert opplæringsløp er under implementering. Det er i dag betydelig usikkerhet på alle nivåer i organisasjonen om hva internkontroll faktisk innebærer i praksis. Det er et behov for å styrke dialogen med Riksrevisjonen gjennom mer strukturert involvering av teknologisk spisskompetanse og ledelse.
- **Etterlevelse**: Kontroller og avvikssystemer finnes, men etterlevelsen svekkes av manglende kontrollrammeverk, svak operasjonalisering og uklare ansvarsforhold. Dette gir rom for lokal praksis og fragmentert sporbarhet/dokumentasjon, med konsekvenser som svak prioritering, lang lukketid på avvik og utfordringer med konsistent rapportering på tvers av produktteam.
- **Rapportering**: Det er behov for å styrke ledelsesrapporteringen slik at den gir et helhetlig og risikobasert bilde av faktisk kontrollnivå og oppnådd risikoreduksjon. Dette krever konsolidering av styringsinformasjon på tvers av enheter, standardisering av KPIer og dashboards, samt systematisk utnyttelse og integrasjon av etterlevelsesdata – særlig fra teknologimiljøene – i den overordnede styringen.
- **Læring og forbedring**: Læring skjer i hovedsak lokalt og reaktivt. Systematiske forbedringssløyfer på tvers av organisasjonen er svakt utviklet, og gjentakende funn fra internrevisjonen og Riksrevisjonen viser manglende kultur og ansvar for lukking av avvik.



Figur 19 Oppsummering av modenhetsvurderingen

Spørreundersøkelsen blant ansatte i Arbeids- og velferdsdirektoratet understøtter dette helhetsbildet. Respondentene vurderer samlet **modenhet til nivå 2,5**, men med betydelig variasjon mellom områder, roller og avdelinger, noe som samsvarer med funnene fra intervju- og dokumentanalysen. Dette samsvarer godt med funnene fra intervjuer og dokumentanalyse, og bekrefter bildet av en organisasjon med sterke enkeltmiljøer, men med manglende helhet og konsistens i internkontrollpraksis.

Tabellen nedenfor gir en samlet oversikt over direktoratets internkontroll knyttet til IKT. Vurderingene er basert på KPMGs analyse av intervjuer, styrende dokumentasjon og observert praksis, og er supplert og nyansert med resultater fra spørreundersøkelsen som har blitt gjennomført blant ansatte. Tabellen tydeliggjør hvordan funn fra KPMGs analyse og ansattperspektivet samlet underbygger modenhetsbildet, og gir sporbarhet mellom overordnede funn, kilder og vurdert modenhetsnivå. Den danner dermed et felles utgangspunkt for de prioriterte anbefalingene i rapportens videre kapitler.

Vurderings-dimensjoner	Kobling til årsaker	Vurdert modenhets-nivå	Nøkkelfunn	KPMG – intervjuer, dokumenter og praksis	Spørre-undersøkelsen – ansattperspektiv
Strategi, mål og ambisjoner	R1, R3, M3	Nivå 2	Svak og ujevn kobling mellom strategi og gjennomføring.	Ambisjoner definert, men ikke konsekvent brutt ned i operative mål og KPI-er. Ujevn ledelsesoppfølging.	Oppleves uklart hva internkontroll betyr i praksis; stor variasjon mellom miljøer.
Risikostyring	R1, R3, M4	Nivå 2	Etablert prosess, men begrenset styringseffekt.	Ulik metodikk, svak aggregering, mange tiltak med lang lukketid og gjentakende revisjonsfunn.	Tiltak tar lang tid å lukke; risiko styrer i liten grad prioriteringer i hverdagen.
Styrings-prinsipper og internkontroll	R1, R3, R4	Nivå 2/3	Godt beskrevet, men svakt operasjonalisert.	Fragmentert dokumentlandskap og manglende oversettelse til operative kontrollkrav.	Krav er kjent, men etterlevelse oppleves ujevn og personavhengig.
Organisering, roller og ansvar	R2, R4, M1	Nivå 2	Trelinjemodellen ikke operasjonalisert.	Uklare grenseflater og svak operativ andrelinje.	Uklart ansvar mellom teknologi, juss og styring; fragmentert eierskap.
Opplæring og kommunikasjon	R3, R4	Nivå 2/3	Delvis systematisert og lite risikotilpasset.	Mangler rollebasert opplæring og kobling til faktiske funn og hendelser.	Etterlyser mer praktisk og rollebasert opplæring.
Etterlevelse	R1, R3, R4, M3, M4	Nivå 2	Ujevn kontrollutførelse og lang lukketid på avvik.	Kontroller finnes, men kvalitet og dokumentasjon varierer.	Bekrefter ujevn praksis og svak oppfølging av avvik.
Rapportering	R1, R3, M2, M3	Nivå 1/2	Begrenset helhetlig styrings-informasjon.	Fokus på tiltaksstatus fremfor faktisk risikoreduksjon.	Varierende relevans og sammenheng mellom rapportering og prioritering.
Læring og forbedring	M4	Nivå 2	Overveiende reaktiv forbedring.	Gjentakende funn og manglende implementering av utfallet av læringen.	Opplever at læring ofte forblir lokal og ikke felles.

Figur 20 Sammendrag av KPMGs vurdering av modenhetsnivå

6. Anbefalte tiltak

6.1. Fra funn til styrt forbedring

KPMGs samlede vurdering er at varige forbedringer i direktoratets internkontroll forutsetter et tydelig og omforent ambisjonsnivå, med en felles forståelse av behovet for handling som er forankret i toppledelsen og forstått likt på tvers av organisasjonen. Uten felles forståelse av alvor, risikotoleranse og tidskritikalitet vil prioritering, gjennomføring og oppfølging vanskeliggjøres, særlig i grenseflatene mellom regelverk, styring, teknologiutvikling, drift og forvaltning.

Dette kapittelet samler KPMGs anbefalte tiltak i en helhetlig forbedringsplan. Tiltakene bygger på observasjonene i kapittel 3 og 4, rotårsaksanalysen i kapittel 5.3 og modenhetsvurderingen i kapittel 5.4. De er innrettet mot å redusere gapet mellom faktisk praksis på den ene siden og krav, forventninger og fremtidsambisjoner på den andre.

Et gjennomgående premiss er at internkontroll for IKT ikke kan vurderes eller forbedres isolert, men må inngå som en integrert del av direktoratets samlede internkontroll og virksomhetsstyring. Dette perspektivet ligger til grunn for alle anbefalte tiltak.

Direktoratet har etablert, eller er i ferd med å etablere, flere relevante virkemidler for å styrke internkontrollen. KPMGs vurdering er derfor at forbedringsbehovet ikke primært handler om å etablere flere styringsdokumenter, kontrollmatriser eller verktøy, men om å sikre at eksisterende og planlagte virkemidler operasjonaliseres, etterleves og følges opp på en konsistent måte. Krav må oversettes til konkrete og etterprøvbare kontrollaktiviteter, ansvar for kontrollutforming og kontrollutførelse må tydeliggjøres, kontrollbevis må kunne fremlegges, og avvik må følges opp, verifiseres og eskaleres på en enhetlig måte.

For AID innebærer dette at styringsdialogen i større grad bør dreies fra status på igangsatte tiltak til gjennomføringsevne, etterlevelse over tid, dokumentert effekt og risikoreduksjon. Der alvorlige eller gjentakende svakheter vedvarer, bør oppfølgingen bygge på tydelig ansvarliggjøring, eskalering og synliggjøring av konsekvenser.

For direktoratet innebærer tiltakene at internkontroll i større grad må flyttes fra overordnet kravstilling og dokumentasjon av status til konkrete arbeidsoppgaver i linjen, produktteamene og andrelinjen. Ikke-oppfylte krav, åpne avvik og revisjonsfunn bør som minimum ha risikovurdering, ansvarlig eier, frist, tiltak, eskaleringsnivå og eventuell beslutning om risikoaksept. Videre at direktoratet i større grad må bygge kompetanse rundt endringsledelse i toppledergruppen.

Departementets behov i oppfølgingen av og styringsdialogen med direktoratet vil skille seg fra direktoratets behov i implementeringen og operasjonaliseringen av nødvendige tiltak. I det følgende presenteres derfor 10 tiltak fordelt på fire tiltaksområder. Disse er myntet på departementets mer overordnede informasjonsbehov og skal beskrive tiltakenes innhold og formål samt tiltakenes estimerte effekt, kost og kompleksitet. For hvert tiltaksområde redegjøres det også kort og overordnet for hvordan de foreslåtte tiltakene bygger på og supplerer direktoratets pågående initiativer og forbedringsaktiviteter, og særlig der det er KPMGs syn at disse ikke vil være tilstrekkelige for å dekke gapene i modenhet mellom nåsituasjon og fremtidsambisjon. Det har imidlertid ikke vært en del av KPMGs mandat å besørge noen detaljert avstemming mellom disse, og direktoratet bør derfor gjøre det til en del av sitt implementeringsarbeid å se det som her foreslås i sammenheng med øvrig pågående arbeid.

I rapportens vedlegg C er disse tiltakene brutt ytterligere ned i 28 mer granulære tiltak, som blant annet hensyntar tiltakenes tidshorisont (kort, mellomlang og lang sikt). For å synliggjøre sammenhengen mellom årsaksbildet, modenhetsgapene og anbefalte tiltak er hvert tiltak også koblet til relevante rotårsaker, medvirkende årsaker og modenhetsområder.

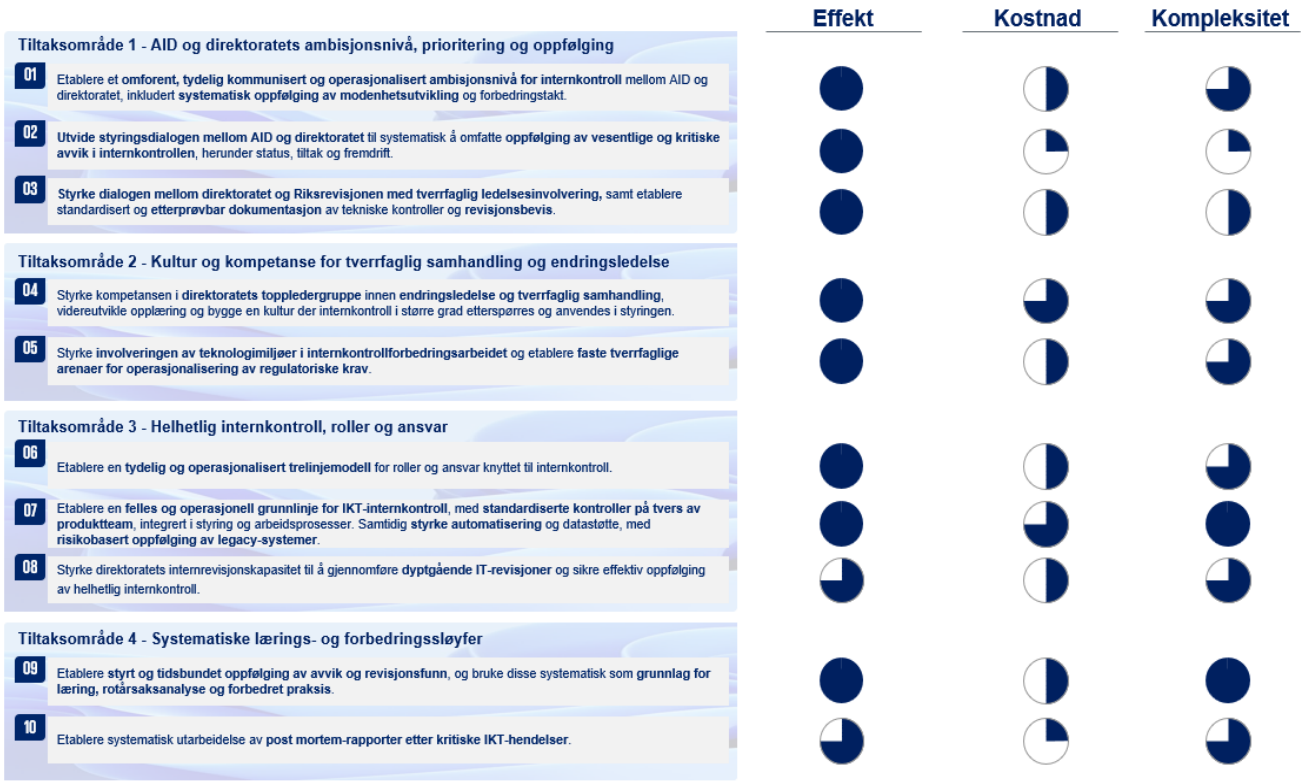
6.2. Tiltaksområder med anbefalte tiltak

Tiltakene er strukturert i fire tiltaksområder som samlet skal styrke direktoratets evne til å etablere en helhetlig, risikobasert og konsistent praksis for internkontroll. Tiltaksområdene følger forbedringslogikken fra funn og rotårsaker til operasjonelle tiltak:

1. **AID og direktoratets ambisjonsnivå, prioritering og oppfølging**
2. **Kultur og kompetanse for tverrfaglig samhandling og endringsledelse**
3. **Helhetlig internkontroll, roller og ansvar**
4. **Systematiske lærings- og forbedringssløyfer**

Hvert tiltaksområde inneholder en estimert rangering av tiltakenes effekt, kost og kompleksitet:

- Effekt: I hvilken grad et tiltak bidrar til å styrke internkontrollen og redusere risiko
- Kost: Ressursene som kreves for å etablere, drifte og vedlikeholde tiltaket
- Kompleksitet: Hvor krevende tiltaket er å planlegge, gjennomføre og følge opp



Figur 21 Oversikt over tiltak og tiltaksområder

Tiltakene er rangert på en skala fra 1 (lav) til 4 (betydelig). Den fulle vurderingsskalaen finnes i rapportens vedlegg A.

Tiltaksområde 1 omfatter særlig tiltak som retter seg mot AIDs styrings- og oppfølgingsrolle, samtidig som det tydeliggjør direktoratets ansvar for å operasjonalisere ambisjonsnivået i styring, prioritering og gjennomføring. Utover dette retter de fleste tiltakene seg mot direktoratet. Den mer granulære inndelingen av tiltak er å finne i rapportens vedlegg C.

6.2.1. Tiltaksområde 1: AID og direktoratets ambisjonsnivå, prioritering og oppfølging

1. Etablere et **omforent, tydelig kommunisert og operasjonalisert ambisjonsnivå for internkontroll** mellom AID og direktoratet, inkludert s**ystematisk oppfølging av modenhetsutvikling** og forbedringstakt.

2. **Utvide styringsdialogen mellom AID og direktoratet** til systematisk å omfatte **oppfølging av vesentlige og kritiske avvik i internkontrollen**, herunder status, tiltak og fremdrift.

3. **Styrke dialogen mellom direktoratet og Riksrevisjonen med tverrfaglig ledelsesinvolvering,** samt etablere standardisert og **etterprøvbar dokumentasjon** av tekniske kontroller og **revisjonsbevis.**

KPMG anbefaler at AID, i tett dialog med direktoratet, videreutvikler og operasjonaliserer et tydelig og omforent ambisjonsnivå for internkontroll, basert på akseptabel risikotoleranse. Ambisjonsnivået bør kommuniseres eksplisitt og fungere som felles referanse for prioritering, gjennomføring og ledelsesoppfølging på tvers av styringsnivåer, fagområder, teknologimiljøer og porteføljestyring. Dette forutsetter at toppledergruppen samlet utøver tydelig lederskap i prioritering og oppfølging, og har tilstrekkelig kompetanse og kapasitet innen endringsledelse til å sikre faktisk gjennomføring og varig effekt.

KPMGs vurdering er at manglende felles forståelse av alvor, risikotoleranse og tidskritikalitet er en grunnleggende årsak til at svakheter i internkontrollen har vedvart over tid. Selv om oppmerksomheten rundt internkontroll har økt, blant annet som følge av alvorlige hendelser, revisjonsfunn og tydeligere forventninger fra AID, har forventningene historisk i begrenset grad vært operasjonalisert i en tydelig måltilstand. Konsekvensen er at internkontroll i praksis kan konkurrere med andre hensyn i en presset hverdag, noe som bidrar til ujevn prioritering, lang lukketid på tiltak og fragmentert gjennomføring. Ambisjonsnivået bør derfor konkretisere hva direktoratet skal oppnå, hvilket modenhetsnivå som forventes over tid, hvilke risikoområder som er særlig kritiske, og hvordan risiko skal vurderes, prioriteres, aksepteres og eskaleres. Dette er nødvendig for at internkontroll skal bli en integrert del av ordinær styring, porteføljeprioritering og styringsdialogen mellom AID og direktoratet.

Gjennomgangen viser at Riksrevisjonen gjentatte ganger har påpekt vesentlige svakheter i internkontrollen, og at kritikken over tid har blitt tydeligere og mer systemorientert. Dialogen med Riksrevisjonen bør derfor styrkes gjennom mer strukturert involvering av teknologisk spisskompetanse og ledelse. Dette er særlig viktig for å tydeliggjøre hvordan plattformløsninger som NAIS understøtter tilgangsstyring, logging, endringshåndtering og revisjonsbevis, herunder gjennom innebygde og i stor grad preventive tekniske kontroller. En mer presis forklaring av disse kontrollene kan gi bedre grunnlag for vurdering av faktisk risiko, kontrollnivå og videre forbedringsarbeid.

KPMGs vurdering er at iverksatte tiltak i begrenset grad dekker våre anbefalinger. Internkontroll er løftet som et topprioritert område i 2025, og det er etablert et internkontrollprosjekt i 2026 under ØSA-direktør og med styringsgruppe på direktørnivå.

Til tross for dette vurderer KPMG at det fortsatt foreligger et vesentlig sprik i toppledelsen både i forståelsen av hva god internkontroll innebærer og i ambisjonsnivå. Ambisjonsnivået fremstår som utydelig og lite operasjonalisert, og det er ikke etablert konkrete tiltak for å adressere dette (tiltak 1).

Videre er det ikke etablert tiltak for å inkludere vesentlige avvik i internkontroll i styringsdialogen mellom AID og direktoratet (tiltak 2).

Direktoratet har et styrende dokument fra 2023 som regulerer dialogen med Riksrevisjonen, men KPMG har ikke identifisert tiltak som styrker en mer strukturert involvering av teknologisk spisskompetanse og ledelse i dette arbeidet (tiltak 3).

6.2.2. Tiltaksområde 2: Kultur og kompetanse for tverrfaglig samhandling og endringsledelse

4. Styrke kompetansen i **direktoratets toppledergruppe** innen **endringsledelse og tverrfaglig samhandling,** videreutvikle opplæring og bygge en kultur der internkontroll i større grad etterspørres og anvendes i styringen.

5. Styrke **involveringen av teknologimiljøer i internkontrollforbedringsarbeidet** og etablere **faste tverrfaglige arenaer for operasjonalisering av regulatoriske krav**.

KPMG vurderer at utfordringene i samhandling i stor grad har sitt utspring i manglende tydelighet i prioritering, beslutning og oppfølging på toppledernivå. KPMG anbefaler at direktoratet styrker kulturen og kompetansen for tverrfaglig samhandling mellom regulatoriske miljøer, teknologimiljøer og styringsfunksjoner, og reduserer person- og initiativavhengig praksis. Direktoratets samfunnsoppdrag realiseres i skjæringspunktet mellom komplekst regelverk og et teknologisk komplekst IKT-landskap. Dette forutsetter modenhet i matriseorganisering, evne og kompetanse til å oversette juridiske, økonomiske og styringsmessige krav til praktisk og teknisk etterlevelse. KPMGs vurdering er at samhandlingen mellom regulatoriske miljøer, teknologimiljøer og styringsfunksjoner i dag i for stor grad er avhengig av enkeltpersoner, uformelle relasjoner og lokale initiativer. Mangelen på faste arenaer, tydelige mandater og felles arbeidsformer bidrar til ulik praksis, ineffektiv ressursbruk og økt risiko for feilprioriteringer. Dette forsterkes av at regulatoriske krav ikke alltid samordnes og oversettes tilstrekkelig før de adresseres mot produktteamene.

KPMGs vurdering er at teknologimiljøer og produktteam i dag i for liten grad involveres i forbedringsarbeidet som pågår. For å redusere denne risikoen bør direktoratet tydeliggjøre forventninger til samhandling og rolleutøvelse i matriseorganiseringen. Samhandlingen bør understøttes av faste, forpliktende arenaer og tydelige beslutnings- og eskaleringslinjer, slik at krav kan forstås, prioriteres og operasjonaliseres mer konsistent på tvers av fag, styring og teknologi.

KPMGs vurdering er at iverksatte tiltak i begrenset grad dekker våre anbefalinger. Det pågår arbeid med å etablere kompetansekrav og opplæringsprogram innen internkontroll for sentrale roller. For å nå ambisjonsnivå 4 fra dagens nivå 2 kreves imidlertid betydelig kompetanse innen

endringsledelse og tverrfaglig samhandling (tiltak 4). Etter KPMGs vurdering er det per i dag ikke etablert tilstrekkelige tiltak for å sikre slik kompetanse i toppledergruppen eller øvrige nøkkelroller.

Videre vurderer KPMG at det foreligger et vesentlig sprik i toppledergruppen når det gjelder synet på graden av involvering av teknologimiljøer i internkontrollarbeidet, samt behovet for tverrfaglige arenaer. Det er etter KPMGs vurdering ikke etablert tilstrekkelige tiltak for å adressere dette (tiltak 5).

6.2.3. Tiltaksområde 3: Helhetlig internkontroll, roller og ansvar

6. Etablere en **tydelig og operasjonalisert trelinjemodell** for roller og ansvar knyttet til internkontroll.

7. Etablere en **felles og operasjonell grunnlinje for IKT-internkontroll,** med **standardiserte kontroller på tvers av produktteam**, integrert i styring og arbeidsprosesser. Samtidig **styrke automatisering** og datastøtte, med **risikobasert oppfølging av legacy-systemer.**

8. Styrke direktoratets internrevisjonskapasitet til å gjennomføre **dyptgående IT-revisjoner** og sikre effektiv oppfølging av helhetlig internkontroll.

KPMG anbefaler at direktoratet videreutvikler og sikrer effektiv implementering av et helhetlig og operasjonelt internkontrollrammeverk, tydelig forankret som et lederansvar og integrert i ordinære styrings- og beslutningsprosesser. Internkontroll bør anvendes aktivt som et styringsverktøy for prioritering, ressursbruk og risikohåndtering – og ikke primært som dokumentasjon eller rapportering. For en virksomhet der IKT er en bærende del av oppgaveløsningen, er det etter KPMGs vurdering lite hensiktsmessig å skille mellom internkontroll knyttet til IKT og øvrig internkontroll.

KPMG anbefaler videre at direktoratet operasjonaliserer og konkretiserer trelinjemodellen i praksis, med tydelig avklaring av roller, ansvar og samspill mellom risikoeiere, kravstillere, produktteam og Teknologiavdelingen. Uklar ansvarsdeling og svake grenseflater er etter KPMGs vurdering blant de mest sentrale årsakene til manglende gjennomføring og vedvarende svakheter i internkontrollen, særlig innen IKT-utvikling, drift og forvaltning. Selv om trelinjemodellen formelt er kjent, er den i begrenset grad oversatt til praktiske forventninger i linjen. Manglende felles forståelse av hvem som har ansvar for å identifisere risiko, stille krav, utforme og implementere kontroller, dokumentere kontrollbevis og følge opp etterlevelse bidrar til uklart ansvar, varierende praksis og ineffektiv ressursbruk. Særlig fremstår andrelinjens operative rolle som utydelig, herunder ansvar for veiledning, påse-oppgaver, verifikasjon, eskalering og oppfølging. KPMG vurderer derfor at trelinjemodellen må operasjonaliseres i samspillet mellom fag, styring og teknologi, og ikke begrenses til formelle beskrivelser eller kontrollfunksjoner.

Mandatet for kvalitetsseksjonen bør tydeliggjøres hva gjelder ansvar for og egen rolle i helhetlig risikostyring. Det bør legge til rette for tydelig prioritering av risikoer opp mot direktoratets strategiske mål, tydelig og omforent risikotoleranse og kommunikasjon av dette til linjen. Seksjonen bør også tillegges ansvaret for å fange opp eksterne risikoer og trender som kan påvirke virksomheten fremover.

Ansvaret for et helhetlig compliance-program, herunder systematisk arbeid med forebygging og avdekking av økonomiske misligheter, bør plasseres tydelig og med en stiplet linje til arbeids- og

velferdsdirektør. Slik direktoratet er organisert i dag er KPMGs anbefaling at det vil være naturlig å legge denne rollen til Juridisk avdeling.

Direktoratet bør samtidig gå fra en praksis preget av fragmentert dokumentasjon av etterlevelse til mer konsistent og risikobasert prioritering og oppfølging. Etterlevelsesarbeidet er i dag i for stor grad orientert mot registrering av status, og i for liten grad brukt aktivt til styring, prioritering og lukking av avvik basert på risiko og vesentlighet. Dette svekker ledelsens beslutningsgrunnlag og evnen til å målrette ressursinnsats der risikoen er størst. Styringssløyfene mellom produktteam, kravstiller og risikoeier bør derfor tydeliggjøres, med klare krav til eskalering, prioritering og ledelsesoppfølging.

Selv om det pågår relevante initiativer knyttet til videreutvikling av etterlevelsesverktøyet bør etterlevelsesinformasjon i større grad sammenstilles og brukes som ledelsesrettet styringsinformasjon, uten at verktøyet gjøres til et rent kontroll- eller avvikssystem. Dette innebærer blant annet at informasjon om manglende dokumentasjon, åpne restanser, risikoaksepter og vesentlighet bør brukes mer aktivt i prioritering, oppfølging og beslutninger.

NAIS bør inngå som et viktig virkemiddel i dette arbeidet. KPMG anbefaler at direktoratet etablerer tydelige og forpliktende styringsprosesser for bruk av NAIS, og utnytter plattformen som en bærende del av førstelinjens internkontroll. KPMG vurderer at NAIS representerer et svært godt teknisk utgangspunkt for robust og innebygd IKT-internkontroll, blant annet innen tilgangsstyring, logging, sporbarhet og endringshåndtering. Kontrollgevinsten realiseres imidlertid først når bruken av plattformen er standardisert, styrt og etterlevd på tvers av produktteam, og når dette inngår i direktoratets samlede internkontrollrammeverk. Tekniske tiltak er likevel ikke tilstrekkelige alene; effekten av NAIS forutsetter tydelig organisatorisk forankring, samspill med kravstillere og risikoeiere, og integrasjon i styrings- og rapporteringsprosesser.

KPMGs vurdering er at iverksatte tiltak i begrenset grad dekker våre anbefalinger. Det registreres enkelte positive utviklingstrekk, herunder godkjenning av tre styrende dokumenter i mai 2026, inkludert veileder for operasjonalisering av trelinjemodellen, samt styrking av kvalitetsseksjonen i ØSA.

Samtidig vurderer KPMG at sentrale rolle- og ansvarsforhold fortsatt er uavklarte ett år etter omorganiseringen i mai 2025. Dette gjelder særlig mellom første- og andrelinjen og innenfor førstelinjens matrisestruktur, herunder mellom Teknologiavdelingen og Ytelsesavdelingen, andrelinjens påseansvar og krav til rapportering fra produktteam. Det er ikke etablert tiltak for et helhetlig compliance-program for forebygging og avdekking av misligheter i tråd med anerkjent praksis (tiltak 6).

Videre pågår arbeid med felles grunnlinje for IKT-internkontroll og økt automatisering, men koblingen til standardisert og etterlevd bruk av NAIS er ikke tilstrekkelig operasjonalisert (tiltak 7).

KPMG har heller ikke identifisert tiltak for å styrke internrevisjonskapasitet, herunder evne til dyptgående IT-revisjoner og oppfølging av helhetlig internkontroll (tiltak 8).

6.2.4. Tiltaksområde 4: Systematiske lærings- og forbedringssløyfer

9. Etablere **styrt og tidsbundet oppfølging av avvik og revisjonsfunn**, og bruke disse systematisk som grunnlag for **læring, rotårsaksanalyse og forbedret praksis.**

10. Etablere systematisk utarbeidelse av **post mortem-rapporter etter kritiske IKT-hendelser.**

KPMG anbefaler at direktoratet etablerer forpliktende og systematiske lærings- og forbedringssløyfer basert på hendelser, revisjonsfunn, avvik og post mortem-rapporter. Formålet er å sikre at kjente svakheter ikke bare håndteres lokalt eller enkeltvis, men brukes som grunnlag for helhetlig forbedring av krav, kontroller, arbeidsprosesser, opplæring og styring på tvers av direktoratet.

KPMG vurderer at manglende systematisk læring er en vesentlig årsak til gjentakende funn og lang lukketid på tiltak. I dag håndteres hendelser og avvik i stor grad lokalt i enkeltmiljøer, og brukes i begrenset grad som grunnlag for strukturell forbedring på tvers av produktområder og fagmiljøer. Dette innebærer at læring i for stor grad blir person- og teamavhengig, og at likeartede svakheter kan oppstå flere steder uten at direktoratet samlet sett bygger tilstrekkelig modenhet.

Produktteamene arbeider i stor grad selvstendig, noe som gir fleksibilitet og lokal handlekraft. Samtidig innebærer denne arbeidsformen en risiko for at erfaringer, rotårsaker og korrigerende tiltak ikke deles systematisk på tvers. Direktoratet bør i større grad sikre at avvik og funn ikke bare registreres og lukkes, men også analyseres for rotårsak, følges opp med tydelig ansvar og frist, og vurderes i etterkant for å kontrollere om tiltakene faktisk har hatt ønsket effekt. KPMG observerer at det pågår initiativer som styrker håndtering av hendelser og avvik, men at disse i begrenset grad er samlet i en helhetlig og styrt forbedringssløyfe med tydelig ledelsesforankring.

KPMGs vurdering er at de tiltakene som per i dag er iverksatt av direktoratet i begrenset grad dekker våre anbefalte tiltak. Det er fortsatt ikke etablert tilstrekkelige mekanismer for styrt og tidsbunden oppfølging av avvik og revisjonsfunn, eller for å utnytte disse systematisk til læring, rotårsaksanalyse og forbedret praksis. En sentral rotårsak er, som beskrevet under tiltaksområde 3, at det fortsatt foreligger vesentlige uavklarte forhold knyttet til roller og ansvar, herunder mellom Teknologiavdelingen og Ytelsesavdelingen. Dette svekker forutsetningene for helhetlig og koordinert oppfølging. Det er videre ikke etablert formelle prosesser som sikrer at læring fra hendelser og avvik i ett produktteam systematisk overføres til øvrige produktteam, eller at forbedret praksis forankres i oppdaterte styrende dokumenter, kompetansekrav og underliggende støttesystemer, herunder NAIS-funksjonalitet (tiltak 9).

KPMG har heller ikke identifisert etablerte tiltak som sikrer systematisk utarbeidelse av post mortem-rapporter etter kritiske hendelser, i tråd med anerkjent praksis for utvikling, drift og forvaltning av IKT (tiltak 10).

6.3. Videre tiltaksarbeid

De anbefalte tiltakene er ment å forsterke og strukturere pågående forbedringsarbeid, ikke etablere et parallelt forbedringsløp. For å gi varig effekt bør forbedringsarbeidet rigges som et koordinert og flerårig endringsløp, med tydelig forankring i linjen og tett involvering av kravstillere, risikoeiere, teknologimiljøer og produktteam.

KPMG vurderer at tiltakene må ses i sammenheng og gjennomføres koordinert. Isolerte forbedringstiltak vil ha begrenset effekt dersom de ikke understøttes av tydelig styring, klare roller, systematisk oppfølging og praktisk operasjonalisering i linjen og produktteamene. Samlet sett skal forbedringsplanen balansere behovet for rask risikoreduksjon med bygging av varig modenhet.

Direktoratet forvalter en omfattende og kompleks IKT-portefølje, med høy regulatorisk kompleksitet og stor avhengighet av teknologi for å løse samfunnsoppdraget. Dette tilsier at internkontrollen må være helhetlig, operasjonell og risikobasert. Det tekniske utgangspunktet,

herunder NAIS-plattformen, vurderes som godt og representerer et betydelig potensial for standardisert og innebygd kontroll. Gjennomgangen viser imidlertid at dette potensialet i begrenset grad er realisert i praksis, som følge av manglende felles styring, operasjonalisering og konsistent etterlevelse på tvers av produktteam.

KPMG vurderer at pågående initiativer, herunder internkontrollprosjektet, er nødvendige, men at de fremstår som for avgrensede sett opp mot utfordringsbildets omfang og varighet. Dersom arbeidet i hovedsak videreføres som enkeltstående forbedringstiltak, er det risiko for at effekten blir begrenset. Etter KPMGs vurdering må arbeidet forankres som et flerårig, helhetlig styrings- og endringsløp, med tydelige krav til prioritering, gjennomføring, oppfølging og rapportering.

Det er særlig fem forhold som vurderes som kritiske for videre fremdrift:

- Etablere et tydelig og forpliktende ambisjonsnivå for internkontroll, basert på risikotoleranse og forventet modenhet
- Sikre tilstrekkelig kompetanse innen endringsledelse knyttet til internkontroll i toppledergruppen og hos øvrige nøkkelroller
- Styrke samhandling og operasjonalisere klare roller og ansvar, særlig i grenseflatene mellom fag, styring og teknologi
- Etablere risikobasert oppfølging av etterlevelse, med tydeligere krav til prioritering, eskalering og lukking av avvik
- Sikre systematiske lærings- og forbedringssløyfer på tvers av organisasjonen

Uten dette vil internkontrollen fortsatt være preget av fragmentering, svak læringsevne og begrenset gjennomføringskraft.

KPMG vurderer at både direktoratet og AID nå står ved et veiskille. Dersom det ikke etableres tydeligere styring og mer konsekvent oppfølging av gjennomføring og effekt, er det risiko for at pågående tiltak ikke gir tilstrekkelig varig forbedring. Dette kan svekke etterlevelse av krav, kvaliteten i styringsinformasjonen og evnen til å håndtere risiko på en betryggende måte.

Det anbefales at AID og direktoratet i samråd benytter det som her er skissert som et grunnlag og utgangspunkt for videre styring og oppfølging av internkontrollområdet. Her vil det være av særlig betydning at en samlet tiltaksplan hensyntar direktoratets pågående initiativer og at eventuelle justeringer i vurderingen av effekt, kostnad og kompleksitet inntas der behov. En fragmentert oppfølging av enkeltanbefalinger vil innebære risiko for redusert effekt og manglende sammenheng. Den videre oppfølgingen bør innrettes mot et helhetlig styringsløp, der AID og direktoratet avklarer ambisjonsnivå, prioriterer tiltak samlet og etablerer tydelige krav til ansvar, milepæler og rapportering. Dette er etter KPMGs vurdering en forutsetning for å oppnå varig forbedring og redusert risiko.