

Veileder for god internkontroll

1. utgave 2026



The Institute of
Internal Auditors
Norge

Innhold

Innhold	1
1. Om veilederen	2
2. Hva er «internkontroll»?	2
3. Kontrollmiljøet – internkontrollens fundament	3
Det uformelle kontrollmiljøet - kultur for ansvar, integritet og læring	3
Roller og ansvar for internkontroll	4
Samspill og koordinering	7
4. Hvordan utvikle internkontrollen	8
Planlegging	8
Risikovurdering	9
Utforme kontrollaktivitet	9
Gjennomføring	10
Oppfølging	10
Rapportering og styringsdialog	11
Kontinuerlig forvaltning av internkontroll	11
5. Kunstig Intelligens (KI) og fremtidens internkontroll	12
Kunstig intelligens som internkontrollutfordring	12
KI sett gjennom COSOs internkontrollkomponenter	13
Implementering av internkontroll for KI	13
Vedlegg A. Evalueringsspørsmål for å vurdere internkontrollen	16
Vedlegg B. COSOs 17 internkontrollprinsipper anvendt på KI	21
Nyttige kilder og referanser	24

1. Om veilederen

Denne veilederen beskriver hvordan internkontroll kan forstås og utøves som en integrert del av virksomhetsstyringen.

Formålet er å gi et helhetlig og anvendbart grunnlag for å utvikle internkontroll som et aktivt styringsverktøy. Internkontroll skal bidra til måloppnåelse gjennom effektiv ressursbruk, pålitelig rapportering og etterlevelse av lover og regler. Samtidig skal den understøtte virksomhetens evne til å håndtere usikkerhet og gjennomføre strategiske initiativer.

Veilederen retter seg mot både styre, ledere og øvrige medarbeidere i linje og kontrollfunksjoner. Den er prinsippbasert og sektoruavhengig, og kan anvendes både i offentlig og privat virksomhet.

2. Hva er «internkontroll»?

I COSO – Internal Control – integrated framework¹ er internkontroll definert som «en prosess, utført av en virksomhets styre, ledelse og øvrige ansatte, utformet for å gi rimelig sikkerhet for oppnåelse av målsettinger relatert til drift, rapportering og etterlevelse».

COSO-definisjonen reflekterer noen grunnleggende konsepter, nemlig at internkontroll iverksettes på forskjellige nivåer og omfatter – i tillegg til håndbøker, systemer og skjemaer – også mennesker og de handlingene de utfører på alle nivåer i organisasjonen for å ivareta internkontrollen.

Definisjonen legger videre til grunn at internkontroll:

- *er rettet mot oppnåelse av målsettinger i én eller flere kategorier – drift, rapportering og etterlevelse*
- *er en prosess som består av løpende oppgaver og aktiviteter – et middel for å nå et mål, ikke et mål i seg selv*
- *igangsettes og gjennomføres av mennesker og omfatter ikke bare håndbøker, systemer og skjemaer, men også mennesker og de handlingene de utfører på alle nivå i organisasjonen for å ivareta internkontrollen*
- *kan gi rimelig sikkerhet – men ikke absolutt sikkerhet, til virksomhetens toppledelse og styre*
- *kan tilpasses virksomhetens struktur – kan anvendes på hele virksomheten eller på et datterselskap, en divisjon, en driftsenhet eller en forretningsprosess*

COSO-rammeverket strukturerer internkontroll i fem komponenter: kontrollmiljø, risikovurdering, kontrollaktiviteter, informasjon og kommunikasjon samt oppfølging.

¹ IIA Norges oversettelse i 2014

Videre er de fem komponentene bestående av 17 prinsipper². Effektiv internkontroll forutsetter at alle elementene virker sammen.

Internkontroll må forstås i sammenheng med virksomhetsstyring og risikostyring hvor internkontroll fungerer som bindeleddet mellom styringsintensjon og faktisk gjennomføring. Selv om det etableres et effektivt internkontrollsystem er det ikke sikkert at virksomhetens målsettinger nås; svikt kan fortsatt forekomme hvis målsettingene er mangelfulle eller lite egnede, ledelsen overstyrer etablert internkontroll eller at det oppstår eksterne hendelser utenfor virksomhetens kontroll.

3. Kontrollmiljøet – internkontrollens fundament

Kontrollmiljøet utgjør fundamentet for internkontrollen og påvirker hvordan ansvar utøves i praksis, og kan deles inn i formelle og uformelle strukturer i en virksomhet. Det formelle kontrollmiljøet setter de formelle rammene for virksomheten og omfatter formaliserte og dokumenterte krav som alle ansatte forventes å etterleve.

Eksempler på det formelle er organisering og fullmaktstrukturer, kompetansekrav, policyer og prosedyrer som virksomhetens ansatte må forholde seg til. Det uformelle kontrollmiljøet dreier seg om holdninger, integritet, etiske verdier og normer som preger virksomheten, og omtales ofte som virksomhetskulturen.

Det uformelle kontrollmiljøet - kultur for ansvar, integritet og læring

Kultur er selve bærebjelken i kontrollmiljøet. En organisasjon med godt utviklede styrende dokumenter, men svak kultur, vil over tid utvikle styringssvikt. Kultur for ansvar og integritet skapes gjennom ledelsens faktiske adferd, ikke gjennom formelle styrende dokumenter og føringer alene.

Internkontroll fungerer ikke primært fordi rutiner er dokumentert, men blant annet fordi medarbeidere forstår hva som forventes, ledelsen følger opp og avvik brukes som grunnlag for forbedring. Kontrollaktiviteter bør utformes i samarbeid med de som utfører aktiviteten i praksis. Svakheter i internkontrollen kan derfor ofte spores tilbake til mangler i kontrollmiljøet, selv der formelle strukturer er på plass.

Et sentralt kjennetegn ved et modent kontrollmiljø er balansen mellom tillit og kontroll. Tillitsbasert styring innebærer ikke fravær av kontroll, men en bevisst balanse der kontrollaktivitetene oppleves som relevante og understøtter oppgaveløsningen. En for detaljert styring kan svekke motivasjon og ansvarsfølelse, mens for svak styring kan gi manglende retning.

² Se prinsippene i Vedlegg A Modenhetsmodell

Når ledelsen systematisk etterspør status på internkontrollen, følger opp avvik og tydelig kobler etterlevelse til verdiskaping, forsterkes internkontrollens legitimitet i organisasjonen. Over tid bidrar dette til å etablere en kultur der kontroll ikke oppfattes som et tillegg, men som en naturlig del av virksomhetens leveranser.

Et annet sentralt element er en læringsorientert tilnærming. **En lav terskel for å melde fra om svakheter er ofte et tegn på et sterkt kontrollmiljø – ikke det motsatte.**

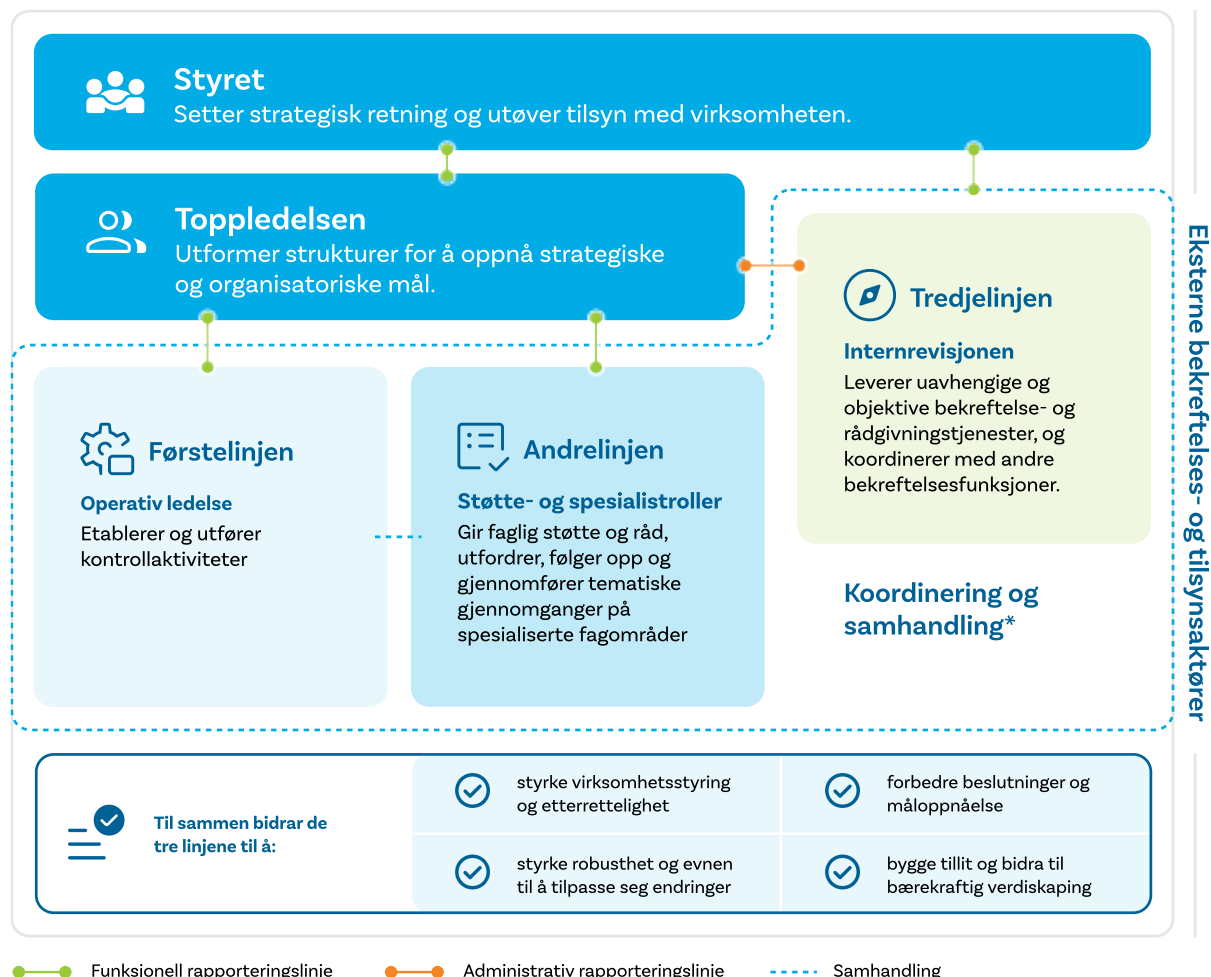
Bruk av ny teknologi, herunder kunstig intelligens, forsterker betydningen av kultur og ansvar. Når beslutninger påvirkes av algoritmer eller automatiserte analyser, må det være tydelig at ansvar alltid ligger hos mennesker og at etiske rammer og etterprøvbarehet gjelder også når beslutningsstøtte er automatisert. Uklare forventninger til ansvar i møte med teknologi er et tydelig signal om svakheter i kontrollmiljøet.

Roller og ansvar for internkontroll

Et grunnleggende prinsipp i COSO er at internkontroll ikke kan outsources til støttefunksjoner eller kontrollmiljøer; den utøves i linjen, der virksomhetens aktiviteter faktisk gjennomføres.

Trelinjemodellen

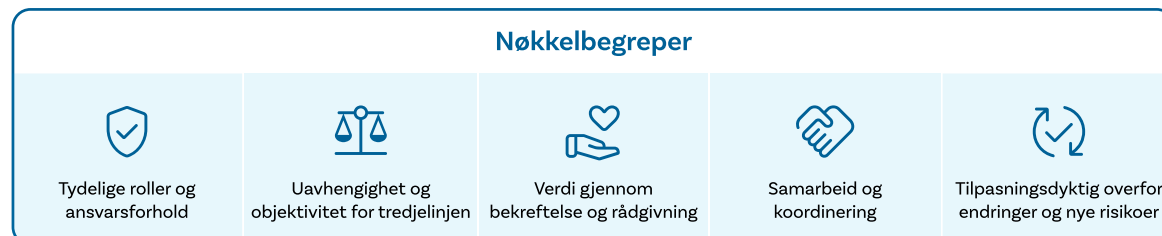
Bekreftelses- og rådgivningstjenester gjennomføres i hele virksomheten for å vurdere og forbedre dens evne til å nå sine mål gjennom effektive prosesser for virksomhetsstyring, risikostyring, etterlevelse og kontroll.



*Koordinering og samhandling

- Integrere bekreftelse og rådgivning på tvers for en helhetlig forståelse av virksomhetsstyring, risiko og kontroll.
- Kombinere innsikt og fremtidsrettede vurderinger for å støtte oppfølging og beslutningstaking.
- Gjennom sin helhetlige forståelse av virksomheten og rapporteringslinje til styret kan internrevisjonen bidra som koordinator

Nøkkelbegreper



Figur 1 Statement of Position: Three Lines Mode. Assurance and Advice in Support of Effective Governance. The IIA

Modellen er bygd opp rundt følgende prinsipper:

1. **Virksomhetsstyring.** God virksomhetsstyring krever tydelige strukturer, roller og prosesser. Styret har ansvar overfor interessenter gjennom integritet, lederskap og åpenhet. Ledelsen skal nå virksomhetens mål gjennom risikobaserte beslutninger, mens internrevisjonen gir uavhengig bekreftelse og råd som bidrar til forbedring
2. **Styrets (eller tilsvarende) rolle.** Styret skal sikre at virksomheten har en effektiv styringsmodell og at mål og aktiviteter er i tråd med interessentenes behov. Styret delegerer ansvar og ressurser til ledelsen, samtidig som det følger opp at lover, regler og etiske krav etterleves. Styret skal også etablere og overvåke en uavhengig internrevisjonsfunksjon
Ledelsen samt første- og andrelinjen. Ledelsen har hovedansvaret for å nå virksomhetens mål og håndtere risiko. Førstelinen utfører kjerneoppgaver og leverer tjenester, mens andrelinjen støtter førstelinen gjennom faglig rådgivning, metodestøtte og oppfølging innen områder som risikostyring, internkontroll, etterlevelse, sikkerhet og andre spesialiserte fagområder. Selv om andrelinjen bidrar med støtte og oppfølging, ligger ansvaret for risiko fortsatt hos ledelsen og førstelinen.
3. **Tredjelinjen.** Internrevisjonen utgjør tredjelinjen og gir uavhengig og objektiv bekreftelse på at styring, risikostyring og internkontroll fungerer som de skal. Revisjonen bruker systematiske metoder og faglig kompetanse for å vurdere virksomheten. Resultatene rapporteres til ledelsen og styret for å støtte kontinuerlig forbedring.
4. **Uavhengighet i tredjelinjen.** Internrevisjonens uavhengighet er avgjørende for dens troverdighet og objektivitet. Funksjonen skal være ansvarlig overfor styret, ikke ledelsen, og ha fri tilgang til nødvendig informasjon, ressurser og ansatte. Arbeidet skal gjennomføres uten påvirkning eller innblanding fra andre.
Skape og beskytte verdi. Verdi skapes og beskyttes når styret, ledelsen og internrevisjonen arbeider mot felles mål. God kommunikasjon, samarbeid og koordinering sikrer at aktiviteter henger sammen og støtter interessentenes interesser. Dette gir bedre beslutningsgrunnlag og mer effektiv risikostyring.

Mange styringssvakheter kan knyttes til uklar rolleforståelse eller mangelfull samhandling mellom første-, andre- og tredjelinjen. Erfaring viser imidlertid at svak utøvelse av andrelinjens ansvar ofte kan føre til redusert oversikt over risiko, internkontroll og etterlevelse.

De tre linjene har ulike styrker, begrensninger og grader av uavhengighet. Førstelinen eier og håndterer risikoer i den daglige driften og har derfor best innsikt i virksomhetens aktiviteter, men begrenset objektivitet i vurderingen av egne kontroller. Andrelinjen bidrar med fagkompetanse, rådgivning og oppfølging på tvers av virksomheten, men er fortsatt en del av ledelsens styringsstruktur. Styret må da sikre at det finnes en tilstrekkelig uavhengig kontrollmekanisme som kan utfordre og bekrefte ledelsens vurderinger; tredjelinjen.

For at kontrollmiljøet skal fungere i praksis, må kontrollfunksjonene ha reell evne til å utøve sitt ansvar. Dette forutsetter tydelig mandat, forankret på øverste nivå, tilstrekkelige ressurser, både i form av kapasitet og kompetanse og rettidig tilgang til relevante data, på tvers av virksomheten.

Samspill og koordinering

I mange virksomheter utfører både førstelinje, andrelinje, internrevisjon og eksterne aktører aktiviteter som gir ledelsen og styret informasjon om risiko, etterlevelse og måloppnåelse. For å unngå overlapp, blindsoner og unødvendig ressursbruk bør virksomheten legge til rette for koordinering mellom disse aktivitetene. En samordnet tilnærming til bekreftelser gir ledelsen og styret et mer helhetlig bilde av virksomhetens risikoer, kontroller og forbedringsbehov. Formålet med en integrert og koordinert rapportering mellom linjene er å:

- redusere overlappende aktiviteter
- identifisere blindsoner
- gi styret et mer helhetlig risikobilde
- øke effektiviteten i virksomhetens samlede kontroll- og oppfølgingsaktiviteter
- styrke kvaliteten på beslutningsgrunnlaget for ledelsen og styret.

Internrevisjonen kan bidra til koordinering og sammenstilling av informasjon fra ulike bekreftelsesaktiviteter, men uten å overta ansvaret til første- eller andrelinjen.

4. Hvordan utvikle internkontrollen

Internkontroll er en kontinuerlig prosess som omsetter mål og risikoforståelse til konkret handling. Prosessen omfatter identifisering av risiko, utforming av tiltak, gjennomføring i praksis og systematisk oppfølging over tid.



Arbeidet bør starte med en prioritering av hvilke områder som er mest kritiske for måloppnåelse. Innsatsen må rettes mot områder der svikt vil få størst konsekvens.

Risikovurdering er kjernen i prosessen. For å sikre treffsikre tiltak må vurderingene ikke bare identifisere hva som kan gå galt, men også hvorfor risiko oppstår. Tiltak som retter seg mot rotårsaker vil gi langt bedre effekt enn tiltak som kun adresserer symptomer.

Kontrollaktiviteter bør integreres i arbeidsprosessene og være forståelige for dem som utfører dem. Der det er mulig, bør kontrollaktiviteter automatiseres, men alltid med tydelig menneskelig ansvar.

Oppfølging og rapportering skal gi ledelsen et realistisk bilde av internkontrollens tilstand. Dette krever en balanse mellom detaljer og helhet, slik at informasjonen er beslutningsrelevant uten å bli for omfattende.

Planlegging

Før virksomheten kan styre risiko effektivt, må den ha oversikt over hva som er kritisk, og hvor svikt kan få størst konsekvens for måloppnåelse, etterlevelse eller tillit.

Internkontroll handler ikke om å kontrollere alt, men om å prioritere riktig. Oversiktsarbeidet bør derfor ta utgangspunkt i:

- virksomhetens mål og strategi
- kritiske prosesser og leveranser
- regulatoriske og samfunnsmessige forventninger

For å strukturere prioriteringen kan virksomheten ta utgangspunkt i fire sentrale dimensjoner: **viktighet, vanskelighetsgrad, volum og variasjon**. Viktighet knytter seg til hvor kritisk en oppgave er for måloppnåelsen, mens vanskelighetsgrad reflekterer kompleksitet og behov for skjønn. Volum peker på omfanget av aktiviteter eller transaksjoner, og variasjon beskriver grad av unntak og endringer i praksis. Områder som skårer høyt på én eller flere av disse dimensjonene, bør normalt prioriteres i internkontrollarbeidet.

Risikovurdering

Når prioriterte områder er identifisert, må risikoene analyseres systematisk. En god risikovurdering tar alltid utgangspunkt i mål, ikke i hendelser isolert sett.

Erfaring viser at mange kontrollaktivitet svikter fordi de adresserer symptomet, ikke årsaken. Derfor bør risikovurderingen alltid inkludere en vurdering av hvorfor risikoen oppstår, for eksempel manglende kompetanse, uklare roller eller ansvar eller utilstrekkelig systemstøtte. Uten forståelse av rotårsaken risikerer virksomheten å etablere kostbare kontrollaktiviteter med begrenset effekt.

Utforme kontrollaktivitet

Når risikoene er analysert, må virksomheten beslutte hvordan risikoene skal håndteres i praksis. Dette skjer gjennom etablering av kontrollaktiviteter. Kontrollaktiviteter er konkrete handlinger, rutiner eller mekanismer som skal redusere sannsynlighet for at feil oppstår og/eller konsekvensen dersom feil likevel inntreffer.

Typer kontrollaktiviteter

Kontrolltype	Formål	Eksempler
Forebyggende	Gjøre ting rett første gang	Tilgangsstyring, klare fullmakter, obligatoriske felt i systemer
Avdekkende	Avdekke feil som har oppstått	Avstemminger, stikkprøver, logganalyse

Korrigerende

Hindre gjentakelse

Tiltaksplaner, prosessforbedringer, opplæring

Der det er hensiktsmessig, bør automatiserte kontrollaktiviteter prioriteres fremfor manuelle.

Gjennomføring

Kontrollaktiviteter har ingen verdi før de faktisk gjennomføres som forutsatt. Den største risikoen i mange virksomheter ligger i gapet mellom hvordan kontrollene er beskrevet (design) og hvordan arbeidet faktisk utføres (praksis). For å redusere dette gapet bør virksomheten legge til rette for at kontrollene er integrert i arbeidsprosessen, ansvar er tydelig og kjent, og at dokumentasjonskrav er tilpasset risiko og ikke unødig byråkratiske.

Dokumentasjon skal være «**godt nok**», det vil si gi svar på:

- hvem som utførte kontrollaktiviteten
- hva som ble utført
- når det ble gjort
- hva resultatet var

Formålet er etterprøvbarehet – ikke dokumentasjon for sin egen skyld.

Oppfølging

Internkontroll har først verdi når virksomheten systematisk vurderer om den faktisk fungerer. COSO skiller mellom to dimensjoner:

- Utforming. Er kontrollen riktig utformet for å håndtere den identifiserte risikoen?
- Operasjonell effektivitet. Fungerer kontrollen i praksis og over tid?

Begge dimensjoner må vurderes for å gi et reelt bilde av internkontrollens tilstand.

Oppfølging skjer gjennom en kombinasjon av løpende linjeoppfølging, bruk av nøkkelindikatorer, analyse av avvik og hendelser, samt uavhengige vurderinger fra internrevisjon eller andre linjefunksjoner. Samspillet mellom disse mekanismene gir et helhetlig bilde av om internkontrollen fungerer etter hensikten.

Der risiko og kompleksitet tilsier det, bør virksomheten bevege seg fra periodiske kontrollaktiviteter til kontinuerlig, datadrevet overvåking.

Rapportering og styringsdialog

Internkontroll skal gi ledelsen et beslutningsrelevant og balansert bilde av risiko og kontroll. Rapportering bør derfor fokusere på status for gjennomføring av planlagte kontrollaktiviteter, vesentlige funn, tiltak og ansvar for forbedring. I tillegg kan begrensninger og kjente risikoområder være en del av rapporteringen. Rapportering er ikke et mål i seg selv, men et grunnlag for styringsdialog og ansvarliggjøring.

Kontinuerlig forvaltning av internkontroll

Internkontroll må forvaltes som et kontinuerlig styringsprogram, ikke som et tidsavgrenset prosjekt. En vanlig utfordring er at forbedringsarbeid startes som respons på tilsyn eller avvik, men ikke følges opp systematisk over tid.

En helhetlig tilnærming innebærer at internkontroll integreres i virksomhetens styringssyklus, med tydelig eierskap, fast struktur og regelmessig rapportering. Årshjul og faste oppfølgingspunkter bidrar til forutsigbarhet og sikrer at kritiske aktiviteter gjennomføres.

Oppfølging bør gi ledelsen et samlet bilde av internkontrollens tilstand, snarere enn fragmenterte rapporter fra ulike deler av organisasjonen. Dette gjør det mulig å prioritere tiltak der behovet er størst.

Videreutvikling av internkontroll forutsetter læring på tvers av enheter. Erfaringer fra ulike deler av virksomheten må deles og brukes aktivt i forbedringsarbeidet.

En strukturert årsplan for internkontroll sikrer forutsigbarhet og sørger for at alle kritiske aktiviteter blir gjennomført til rett tid. Årsplanen bør integreres i virksomhetens ordinære styringssyklus og tertialvise rapportering.

Internkontroll bør forvaltes som et kontinuerlig program, kjennetegnet av tydelig eierskap, fast struktur og årshjul og systematisk rapportering til ledelsen. Dette innebærer at ledelsen ikke bare etterspør status på kontrollaktiviteter, men vurderer om kontrollene faktisk gir ønsket styringseffekt. Dette innebærer at ambisjonsnivået justeres i takt med risikobildet og at ledelsen sikrer at ressursbruk står i forhold til vesentlighet.

5. Kunstig Intelligens (KI) og fremtidens internkontroll

Tradisjonell internkontroll har i stor grad vært basert på stabile prosesser, manuelle kontrollaktiviteter, periodisk oppfølging og etterfølgende dokumentasjon.

Digitalisering og automatisering utfordrer disse forutsetningene. I dag kjennetegnes mange virksomheter av store mengder tilgjengelige data, færre synlige beslutningspunkter og raskere endring i både teknologi og arbeidsformer. Dette medfører et skifte:

- fra periodiske kontrollaktiviteter til løpende overvåking
- fra manuell kontroll til analysebasert innsikt
- fra etterkontroll til tidlig varsling og forebygging

Internkontroll må derfor i større grad forstås som en kontinuerlig styringsmekanisme, der data og teknologi brukes til å støtte – ikke erstatte – menneskelig ansvar og beslutningstaking.

Kunstig intelligens som internkontrollutfordring

Bruk av kunstig intelligens, og særlig generativ KI, forsterker behovet for moden internkontroll. KI-baserte løsninger kan bidra til effektivisering, analyse og beslutningsstøtte, men innebærer også risiko for at feil kan eskalere raskt, redusere synlighet i beslutningsgrunnlag og svekke etterprøvbarehet dersom styringen er svak.

KI introduserer ikke nødvendigvis helt nye risikokategorier, men forsterker eksisterende risikoer. Samtidig stiller bruk av KI nye krav til internkontrollen knyttet til ansvar og rolleforståelse, kvalitet på styringsinformasjon og endring over tid uten tydelige varsler.

Et sentralt trekk ved KI-baserte systemer er at de ofte er probabilistiske, ikke deterministiske. Det innebærer at samme input kan gi ulik output og resultatene kan fremstå plausible uten å være riktige.

Internkontroll kan derfor ikke baseres på forventningen om ett «riktig svar», men må ta høyde for variasjon og usikkerhet. Dette forsterker behovet for menneskelig overstyring i vesentlige beslutninger, tydelige bruksbegrensninger og kontinuerlig overvåking av resultater.

Ny teknologi endrer ikke ansvarsdelingen i trelinjemodellen, men øker kravene til andrelinjens utøvelse av påse-ansvaret.

Andrelinjen må ha oversikt over faktisk bruk av teknologi og KI, definere krav til kontroll og følge utvikling i risikobilde over tid. Uten en aktiv og kompetent andrelinje risikerer KI å bli en ny styringsmessig blindsoner, snarere enn et verktøy for bedre kontroll.

KI sett gjennom COSOs internkontrollkomponenter

COSO Internal Control – Integrated Framework er fullt anvendelig også for KI-baserte prosesser. Det avgjørende er bevisst bruk av prinsippene.

Kontrollmiljø:

Ansvar for beslutninger kan ikke delegeres til algoritmer. Det bør utpekes en ansvarlig eier for hver KI-løsning, og retningslinjer for tillatt bruk av KI og gjennomføre opplæring i sikker og ansvarlig bruk bør utarbeides.

Risikovurdering:

KI-bruk må identifiseres eksplisitt, vurderes regelmessig og revurderes ved endringer i modeller, data eller bruksområde. Risikovurderinger bør inkludere risiko for feilinformasjon, personvernbrudd, modellendringer og leverandøravhengighet

Kontrollaktiviteter:

Kontrollaktivitetene må være tilpasset probabilistiske systemer, blant annet gjennom «human-in-the-loop», fastsette terskelverdier som krever manuell kontroll, dokumentere endringer i modeller og godkjenne vesentlige endringer før produksjonssetting.

Informasjon og kommunikasjon:

KI-basert styringsinformasjon må være forståelig for beslutningstakere. Hvis det er vanskelig å forklare hvordan informasjon er frembrakt svekker dette kvaliteten. Det bør utvikles krav om kildehenvisninger i KI-genererte analyser, og videre lagring av prompter, datakilder, modellversjoner og sentrale beslutningsgrunnlag slik at resultatene kan etterprøves

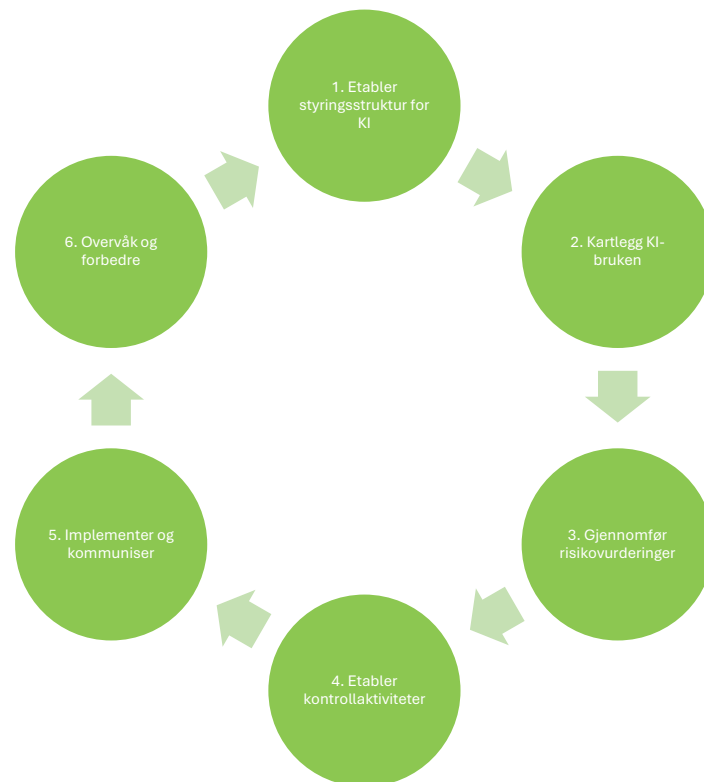
Oppfølging:

KI forutsetter løpende oppfølging. Dersom et KI-basert system ikke kan overvåkes eller revideres, bør det ikke brukes i kritiske prosesser. Det bør etableres terskler som utløser ny validering eller stans av modellen dersom kvaliteten faller under akseptabelt nivå.

Se også vedlegg B for hvordan de 17 internkontrollprinsippene kan relateres til bruk av KI.

Implementering av internkontroll for KI

Innføring av KI bør ikke håndteres som et rent teknologiprojekt. Virksomheten må etablere styrings- og kontrollmekanismer som sikrer at bruk av KI understøtter måloppnåelse, skjer innenfor akseptabel risiko og er i samsvar med virksomhetens etiske, juridiske og regulatoriske krav. En praktisk tilnærming er å ta utgangspunkt i COSOs internkontrollrammeverk og etablere KI-styringen som en kontinuerlig prosess.



1. Etabler styringsstruktur for KI. Virksomheten bør etablere tydelige roller, ansvar og beslutningsprosesser for bruk av KI. Dette inkluderer eierskap til løsninger, ansvar for risikovurderinger og mekanismer for eskalering av hendelser og avvik. For større virksomheter kan et tverrfaglig forum med representanter fra virksomhet, IT, juss, sikkerhet, risikostyring og internkontroll være hensiktsmessig.

2. Kartlegg KI-bruken. Virksomheten bør ha en samlet oversikt over hvilke KI-løsninger som brukes, hvilke prosesser de støtter, hvilke data som benyttes og hvilke beslutninger som påvirkes. Kartleggingen bør omfatte både formelt godkjente løsninger og eventuell «skygge-KI» etablert utenfor ordinære styringsprosesser.

3. Gjennomfør risikovurderinger. For hver KI-løsning bør virksomheten identifisere og vurdere risiko. Eksempler på risikoer som bør identifiseres og vurderes er: feil eller hallusinasjoner, bias og diskriminering, datakvalitet, personvern, tredjeparter og manglende transparens. Risikovurderingene må oppdateres ved vesentlige endringer i modeller, datagrunnlag eller bruksområde.

4. Etabler kontrollaktiviteter. Kontrollaktivitetene bør tilpasses risikoen ved den enkelte KI-løsningen. Eksempler på kontrollaktiviteter:

- krav om menneskelig kvalitetssikring før kritiske beslutninger («human-in-the-loop»)
- krav om kildehenvisninger i KI-genererte analyser
- tilgangsstyring og rollebaserte rettigheter
- godkjenningssprosess for endringer i modeller, prompter og parametere

- logging og sporbarhet for sentrale beslutninger
- uavhengig validering av kritiske modeller

Kontrollaktiviteter bør være dokumenterte, målbare og etterprøvbare.

5. Implementer og kommuniser. Kontrollaktiviteter og retningslinjer må integreres i virksomhetens ordinære arbeidsprosesser. Ansatte må forstå når KI kan brukes, hvilke begrensninger som gjelder og hva som krever manuell kontroll eller eskalering. Kompetansebygging blir derfor en viktig del av internkontrollen.

6. Overvåk og forbedre. KI-systemer er dynamiske og må derfor overvåkes kontinuerlig. Virksomheten bør etablere indikatorer for kvalitet, nøyaktighet, sikkerhet og etterlevelse. Vesentlige avvik må analyseres, korrigeres og rapporteres til relevant ledelsesnivå. Ved behov må modeller re-trenes, justeres eller tas ut av bruk.

Implementering av internkontroll for KI er ikke en engangsaktivitet. Etter hvert som teknologi, regelverk og bruksområder utvikler seg, må virksomheten løpende revidere risikovurderinger, kontrollaktiviteter og kompetansebehov. På samme måte som øvrig internkontroll bør styringen av KI inngå som en integrert del av virksomhetens ordinære styrings- og forbedringsprosesser.

Vedlegg A. Evalueringsspørsmål for å vurdere internkontrollen

Dette vedlegget er utviklet som et praktisk hjelpemiddel for å vurdere og diskutere virksomhetens internkontroll. Vurderingsspørsmålene bygger på de 17 prinsippene i COSO Internal Control – Integrated Framework og kan benyttes i egenvurderinger, workshops, ledergjennomganger, internrevisjoner eller andre evalueringer av internkontrollsystemet.

Formålet er ikke å etablere en eksakt måling av internkontrollens kvalitet, men å legge til rette for en strukturert vurdering av hvordan internkontrollen fungerer i praksis, og identifisere områder som kan videreutvikles. Spørsmålene er utformet for å stimulere til refleksjon, diskusjon og læring på tvers av ledelse, linjeorganisasjon og kontrollfunksjoner.

For hvert prinsipp er spørsmålene gruppert i tre dimensjoner:

- **Prosess og styring** – omfatter rammeverk, metodikk, roller, ansvar, styrende dokumenter og oppfølging.
- **Mennesker og kultur** – omfatter kompetanse, rolleforståelse, ansvarlighet, ledelsesforankring og organisasjonskultur.
- **Teknologi og data** – omfatter systemstøtte, automatisering, datakvalitet, rapportering og analyse.

Dimensjonene er valgt fordi effektiv internkontroll sjelden er et resultat av prosesser, mennesker eller teknologi alene. God internkontroll forutsetter at disse samvirker og understøtter hverandre.

Spørsmålene bør brukes som grunnlag for faglige diskusjoner og identifisering av forbedringstiltak. Det er ikke et mål at alle virksomheter skal oppnå samme nivå på alle områder. Hensiktsmessig internkontroll må tilpasses virksomhetens størrelse, kompleksitet, risikoeksponering og modenhet.

Kontrollmiljø (Prinsipp 1–5)

Prinsipp	Prosess	Mennesker	Teknologi og data
1. Integritet og etiske verdier	Er etiske retningslinjer definert og oppdatert?	Forstår ansatte virksomhetens verdier og forventninger til adferd?	Finnes systemer for varsling og oppfølging av etiske brudd?

<i>Organisasjonen er opptatt av integritet og etiske verdier, og viser dette i praksis</i>	Er varsling, habilitet og interessekonflikter regulert?	Etterlever ledelsen verdiene i praksis?	Finnes data om varsler, avvik og trender?
2. Styrets tilsyn <i>Styret er uavhengig av ledelsen og fører tilsyn med utvikling og gjennomføring av internkontrollen</i>	Er styrets oppfølging av internkontroll strukturert?	Har styret tilstrekkelig kompetanse innen risiko og internkontroll?	Får styret relevant og oppdatert styringsinformasjon?
	Behandles risiko og internkontroll regelmessig?	Utfordrer styret ledelsen på vesentlige områder?	Finnes rapporteringsløsninger som understøtter styrets arbeid?
3. Struktur, ansvar og myndighet <i>Ledelsen, under styrets tilsyn, etablerer strukturer, rapporterings-linjer og myndighet og ansvar som er egnet for å oppnå målsettingene</i>	Er roller og ansvar dokumentert?	Forstår ansatte egen rolle og myndighet?	Er systemroller og tilganger i samsvar med ansvar?
	Er rapporterings-linjer tydelige?	Oppstår det uklarhet om ansvar?	Understøtter systemene organisasjonsstrukturen?
4. Kompetanse <i>Organisasjonen er opptatt av å rekruttere, utvikle og beholde kompetente medarbeidere i samsvar med målsettingene</i>	Finnes prosesser for kompetanse-styring?	Har medarbeiderne nødvendig kompetanse?	Finnes oversikt over kompetanse og opplæring?
	Gjennomføres opplæring systematisk?	Er kompetanse-behov identifisert?	Understøttes læring gjennom digitale verktøy?
5. Ansvarliggjøring <i>Organisasjonen holder enkeltpersoner ansvarlig for de internkontroll-oppgavene de er tildelt i arbeidet med å oppnå målsettingene</i>	Er mål og forventninger tydelige?	Holdes ansatte ansvarlige for sine oppgaver?	Finnes KPI-er og rapportering som støtter oppfølging?
	Er konsekvenser ved manglende etterlevelse definert?	Oppmuntres ønsket adferd?	Kan prestasjoner og etterlevelse måles?

Risikovurdering (Prinsipp 6–9)

Prinsipp	Prosess	Mennesker	Teknologi og data
6. Fastsettelse av mål	Er mål definert og dokumentert?	Forstår ansatte målene?	Finnes styringsdata som måler måloppnåelse?

<i>Organisasjonen spesifiserer målsettinger som er tydelige nok til at man kan identifisere og vurdere risikoene knyttet til dem</i>	Knytter målene seg til risiko?	Deltar relevante personer i målprosessen?	Er målene tilgjengelige i styringssystemene?
7. Identifisere og analysere risiko <i>Organisasjonen identifiserer risikoer for ikke å nå målsettinger i hele virksomheten, analyserer dem og avgjør hvordan de bør håndteres</i>	Finnes en strukturert risikoprosess?	Har risikoeiere nødvendig kompetanse?	Benyttes data i risikovurderingene?
	Oppdateres risikoer regelmessig?	Deltar relevante fagmiljøer?	Er risiko registrert og sporbar i systemer?
8. Mislighetsrisiko <i>Organisasjonen tar hensyn til muligheten for misligheter når den vurderer risiko for ikke å nå målsettinger</i>	Vurderes mislighetsrisiko systematisk?	Har ansatte bevissthet om misligheter?	Benyttes analyseverktøy og overvåking?
	Finnes forebyggende tiltak?	Er det kultur for å si ifra?	Overvåkes uvanlige transaksjoner eller mønstre?
9. Endringer <i>Organisasjonen identifiserer og vurderer endringer som i betydelig grad kan få konsekvenser for internkontroll-systemet</i>	Er endringsprosesser etablert?	Har ledere kompetanse til å håndtere endringer?	Støtter systemene endringsstyring?
	Risikovurderes endringer?	Involveres berørte ansatte?	Dokumenteres endringer systematisk?

Kontrollaktiviteter (Prinsipp 10–12)

Prinsipp	Prosess	Mennesker	Teknologi og data
10. Kontrollaktiviteter <i>Organisasjonen velger og utvikler kontrollaktiviteter som bidrar til at risiko for ikke å nå målsettinger reduseres til akseptable nivåer</i>	Er kontroll-aktivitetene risikobaserte?	Forstår de som utfører kontrollaktivitetene formålet?	Er kontrollaktivitetene automatisert der det er hensiktsmessig?
	Er kontroll-aktivitetene dokumentert?	Utføres kontrollene som forutsatt?	Etableres kontrollbevis automatisk?
11. Teknologikontroller	Finnes etablerte IT-kontroller?	Har ansatte sikkerhetskompetanse?	Er tilgangsstyring, logging og

Organisasjonen velger og utvikler generelle kontrollaktiviteter vedrørende teknologi til støtte for arbeidet med å oppnå målsettinger			endringskontroll etablert?
	Er sikkerhetskrav definert?	Følger ansatte sikkerhetskravene?	Overvåkes sentrale IT-risikoe?
12. Retningslinjer og prosedyrer Organisasjonen iverksetter kontrollaktiviteter gjennom retningslinjer/policyer som sier hva som forventes, og rutiner/prosedyrer som setter retningslinjene ut i livet	Er retningslinjer dokumentert?	Kjenner ansatte til prosedyrene?	Er dokumentasjonen lett tilgjengelig?
	Oppdateres dokumentene jevnlig?	Etterleves prosedyrene?	Finnes versjonskontroll og dokumentstyring?

Informasjon og kommunikasjon (Prinsipp 13–15)

Prinsipp	Prosess	Mennesker	Teknologi og data
13. Informasjonskvalitet Organisasjonen innhenter eller genererer og bruker relevant informasjon av høy kvalitet til støtte for gjennomføringen av internkontrollen	Er krav til datakvalitet etablert?	Forstår ansatte betydningen av informasjonskvalitet?	Er data komplette, korrekte og oppdaterte?
	Er dataeierskap definert?	Følges kvalitetskrav opp?	Finnes automatiske kvalitetskontroller?
14. Intern kommunikasjon Organisasjonen kommuniserer informasjon internt, herunder målsettinger og ansvar for internkontroll, som trengs for å støtte en fungerende internkontroll	Er kommunikasjonsrutiner etablert?	Forstår ansatte informasjonen som kommuniseres?	Støtter verktøyene informasjonsdeling?
	Kommuniseres ansvar og forventninger tydelig?	Oppmuntres det til dialog og tilbakemeldinger?	Er kommunikasjonskanalene effektive?
15. Ekstern kommunikasjon	Er ekstern rapportering definert?	Har ansvarlige tilstrekkelig kompetanse?	Er data som rapporteres eksternt pålitelige?

<i>Organisasjonen kommuniserer med eksterne aktører om saker av betydning for internkontrollen</i>	Finnes rutiner for interessentdialog?	Håndteres henvendelser effektivt?	Understøttes rapporteringen av systemer?
--	---------------------------------------	-----------------------------------	--

Oppfølging (Prinsipp 16–17)

Prinsipp	Prosess	Mennesker	Teknologi og data
16. Evaluering <i>Organisasjonen velger, utvikler og utfører løpende og/eller frittstående evalueringer for å fastslå om internkontroll-komponentene er til stede og fungerer</i>	Gjennomføres løpende evalueringer?	Har de som evaluerer tilstrekkelig kompetanse?	Benyttes data til oppfølging?
	Er evalueringsmetodikken definert?	Deltar ledelsen aktivt?	Finnes dashboard og oppfølgingssverktøy?
17. Oppfølging av svakheter <i>Organisasjonen evaluerer og kommuniserer internkontrollmangler til rett tid til de med ansvar for å treffe korrigerende tiltak, inkludert toppledelsen og eventuelt styret</i>	Finnes prosess for avvikshåndtering?	Tar ledelsen ansvar for korrigerende tiltak?	Finnes systemstøtte for oppfølging av avvik?
	Følges tiltak opp til de er lukket?	Læres det av feil og svakheter?	Kan gjennomføring og effekt dokumenteres?

Vedlegg B. COSOs 17 internkontrollprinsipper anvendt på KI

Kontrollmiljø (Prinsipp 1–5)

Prinsipp	Knyttet til bruk av KI
1. Integritet og etiske verdier <i>Organisasjonen er opptatt av integritet og etiske verdier, og viser dette i praksis</i>	Virksomheten må etablere etiske prinsipper for bruk av KI. Dette omfatter krav til rettferdighet, transparens, personvern og ansvarlighet. KI må brukes på en måte som er i tråd med virksomhetens verdier og samfunnsoppdrag
2. Styrets tilsyn <i>Styret er uavhengig av ledelsen og fører tilsyn med utvikling og gjennomføring av internkontrollen</i>	Styret bør forstå hvordan KI brukes i virksomheten og hvilke risikoer teknologien medfører. Dette innebærer regelmessig rapportering om vesentlige KI-løsninger, risikoeksponering og kontrollaktiviteter
3. Struktur, ansvar og myndighet <i>Ledelsen, under styrets tilsyn, etablerer strukturer, rapporteringslinjer og myndighet og ansvar som er egnet for å oppnå målsettingene</i>	Det må være tydelig hvem som eier KI-løsninger, godkjenner bruk, følger opp risiko og håndterer avvik. Ansvar kan ikke delegeres til modellen eller leverandøren
4. Kompetanse <i>Organisasjonen er opptatt av å rekruttere, utvikle og beholde kompetente medarbeidere i samsvar med målsettingene</i>	Virksomheten må sikre tilstrekkelig kompetanse om KI hos både ledere, brukere og kontrollfunksjoner. Manglende forståelse av teknologiens begrensninger kan i seg selv utgjøre en vesentlig risiko
5. Ansvarliggjøring <i>Organisasjonen holder enkeltpersoner ansvarlig for de internkontrolloppgavene de er tildelt i arbeidet med å oppnå målsettingene</i>	Mennesker må kunne holdes ansvarlige for beslutninger som støttes av KI. Ansvarsforhold må være tydelige også når prosesser er delvis automatiserte

Risikovurdering (Prinsipp 6–9)

Prinsipp	Knyttet til bruk av KI
6. Fastsettelse av mål <i>Organisasjonen spesifiserer målsettinger som er tydelige nok til at man kan identifisere og vurdere risikoene knyttet til dem</i>	Formålet med KI-bruken må være klart definert. Uklare mål gjør det vanskelig å vurdere om teknologien bidrar til verdiskaping eller introduserer unødvendig risiko

7. Identifisere og analysere risiko <i>Organisasjonen identifiserer risikoer for ikke å nå målsettinger i hele virksomheten, analyserer dem og avgjør hvordan de bør håndteres</i>	Virksomheten må vurdere risikoer som skjevheter i data, feilaktige resultater, manglende forklarbarhet, sikkerhetsutfordringer og operasjonell avhengighet av KI
8. Mislighetsrisiko <i>Organisasjonen tar hensyn til muligheten for misligheter når den vurderer risiko for ikke å nå målsettinger</i>	KI kan både avdekke og muliggjøre misligheter. Risikoen for manipulasjon av treningsdata, falskt innhold og misbruk av generativ KI bør vurderes særskilt.
9. Endringer <i>Organisasjonen identifiserer og vurderer endringer som i betydelig grad kan få konsekvenser for internkontrollsystemet</i>	Modeller, algoritmer og datagrunnlag kan endres over tid. Vesentlige endringer bør derfor underlegges risikovurdering og formell godkjenning før implementering

Kontrollaktiviteter (Prinsipp 10–12)

Prinsipp	Knyttet til bruk av KI
10. Kontrollaktiviteter <i>Organisasjonen velger og utvikler kontrollaktiviteter som bidrar til at risiko for ikke å nå målsettinger reduseres til akseptable nivåer</i>	Kontrollaktiviteter må tilpasses KI-baserte prosesser. Eksempler er menneskelig kvalitetssikring, terskelverdier for automatiserte beslutninger og krav om manuell godkjenning ved høy risiko.
11. Teknologikontroller <i>Organisasjonen velger og utvikler generelle kontrollaktiviteter vedrørende teknologi til støtte for arbeidet med å oppnå målsettinger</i>	Tilgangsstyring, logging og kontroll med treningsdata blir sentrale teknologikontroller ved bruk av KI.
12. Retningslinjer og prosedyrer <i>Organisasjonen iverksetter kontrollaktiviteter gjennom retningslinjer/policyer som sier hva som forventes, og rutiner/prosedyrer som setter retningslinjene ut i livet</i>	Virksomheten bør etablere styrende dokumenter som regulerer utvikling, anskaffelse, bruk, overvåking og avvikshåndtering for KI-løsninger

Informasjon og kommunikasjon (Prinsipp 13–15)

Prinsipp	Knyttet til bruk av KI
13. Informasjonskvalitet	Resultater fra KI må være tilstrekkelig pålitelige, relevante og etterprøvbare til å kunne brukes i styring og

<i>Organisasjonen innhenter eller genererer og bruker relevant informasjon av høy kvalitet til støtte for gjennomføringen av internkontrollen</i>	beslutninger. Datakvalitet er en grunnleggende forutsetning.
14. Intern kommunikasjon <i>Organisasjonen kommuniserer informasjon internt, herunder målsettinger og ansvar for internkontroll, som trengs for å støtte en fungerende internkontroll</i>	Ansatte må forstå hvor og hvordan KI brukes, hvilke begrensninger som gjelder og hvilket ansvar den enkelte har. Dette reduserer risikoen for feil bruk og overdreven tillit til teknologien
15. Ekstern kommunikasjon <i>Organisasjonen kommuniserer med eksterne aktører om saker av betydning for internkontrollen</i>	Virksomheten bør være åpen om vesentlig bruk av KI når dette påvirker kunder, brukere, samarbeidspartnere eller myndigheter. Transparens bidrar til tillit og etterlevelse

Oppfølging (Prinsipp 16–17)

Prinsipp	Knyttet til bruk av KI
16. Evaluering <i>Organisasjonen velger, utvikler og utfører løpende og/eller frittstående evalueringer for å fastslå om internkontrollkomponentene er til stede og fungerer</i>	KI-løsninger bør evalueres jevnlig for å sikre at de fortsatt fungerer etter hensikten og leverer forventede resultater. Dette inkluderer testing av nøyaktighet, robusthet og kontrollmiljø.
17. Oppfølging av svakheter <i>Organisasjonen evaluerer og kommuniserer internkontrollmangler til rett tid til de med ansvar for å treffe korrigerende tiltak, inkludert toppledelsen og eventuelt styret</i>	Feil, sikkerhetshendelser og andre svakheter knyttet til KI må rapporteres, analyseres og følges opp på samme måte som andre internkontrollmangler. Læring og forbedring bør inngå som en del av forvaltningsprosessen

Nyttige kilder og referanser

- Statement of Position: Three Lines Model, The Institute of Internal Auditors, 2026
- Achieving Effective Internal Control Over Generative AI, COSO, 2026
- Internal control - integrated framework, COSO (Committee of Sponsoring Organizations of the Treadway Commission), 2013
- Veileder for internkontroll, Direktoratet for økonomistyring (DFØ), Nettsider 2026 og veileder 2013

IIA Norge - et fagmiljø for god styring, risiko og kontroll

Hold deg oppdatert. Utvid nettverket ditt. Styrk din kompetanse.

IIA Norge er foreningen for deg som er opptatt av virksomhetsstyring, risikostyring, compliance og internrevisjon. Vi er bransjeuavhengig og er en del av den globale organisasjonen, The Institute of Internal Auditors.

Vi gir deg tilgang til faglige nettverk, sertifiseringer, kurs, veiledere og verktøy som du trenger for å lykkes i en tid med økende krav til styring, risiko og kontroll. Vårt mål er at du gjennom erfaringsutveksling og kunnskapsdeling med andre medlemmer fra privat og offentlig sektor, får innsikt som kan omsettes til praksis for bedre virksomhetsstyring.

Vi har e-kurs, og fysiske praktiske kurs og faglitteratur for deg som vil lære mer om internkontroll.

Denne veilederen inngår i en samling veiledere og fagstoff utviklet av engasjerte medlemmer fra disse nettverkene. Våre nettverk er åpen for alle:

- Nettverk virksomhetsstyring
- Nettverk risikostyring
- Nettverk etikk & compliance
- Nettverk internrevisjon
- Nettverk finans
- Nettverk offentlig virksomhet
- Nettverk teknologi & sikkerhet

Takk til alle medlemmer og bidragsytere som gjennom sitt engasjement bidrar til å utvikle og dele kunnskap om god virksomhetsstyring.

Vil du melde deg inn eller vite mer om våre kurs, veiledere, verktøy og nettverk?

Se www.iaa.no eller skann QR-koden nedenfor for mer informasjon:

