Veileder til god praksis i compliance

3. utgave 2026



The Institute of
Internal Auditors
Norge

Innhold

Innhold 1

1. Om veilederen 2

Referansestandard 'god praksis' 2

2. Introduksjon til compliance 3

Ansvar for etterlevelse i virksomheten 3

Trelinjemodellen 4

Organisatorisk plassering 6

Compliance – integrert del av virksomhetsstyring 7

Complianceprogram 8

Etikk og kultur 9

Mandat og ressurser 10

Bruk av data og teknologiverktøy 11

3. Sentrale elementer i et complianceprogram 12

Årsplan og revisjon av complianceprogrammet 13

Integrert del av virksomhetens risikostyring 14

Risikoappetitt 15

Identifisering, vurdering og behandling av compliancerisikoer 16

Styrende dokumenter 16

Håndtering av tredjeparter og leverandørkjeder 18

Opplæring og bevisstgjøring 20

Periodisk kontroll og kontinuerlig overvåkning 20

Nøkkelindikatorer 22

Rapportering 22

Eskaleringsmekanismer 23

Egenevaluering 23

4. Vedlegg 24

Vurdering av modenhet 24

Sjekkliste AI 24

Nyttige kilder og rammeverk 25

1. Om veilederen

Som følge av strengere regelverk på tvers av bransjer, både nasjonalt og i EU, stilles det økende krav til etterlevelse. Et mer komplekst risikobilde, herunder digitalisering og bruk av kunstig intelligens, globale verdikjeder og økte transparenskrav fordrer også en revitalisering av compliancearbeidet. Særlig gjelder dette automatisering og bruk av teknologiverktøy for å understøtte prosesser, datainnsamling og –analyse.

Denne veilederen har som formål å bidra til å styrke virksomheters evne til å håndtere compliancerisiko og skape tillit. Den beskriver god praksis for compliancearbeid på tvers av ulike sektorer, og tar for seg hvordan virksomheter kan og bør innrette og allokere ressurser til arbeidet, samt redegjør for sentrale temaer, aktiviteter og prosesser som i samsvar med god praksis bør ivaretas av en compliancefunksjon.

Veilederen er utviklet av IIA Norges Nettverk Etikk & Compliance og bygger på tidligere utgaver. Denne veilederen erstatter forrige utgave utgitt i 2021.

Referansestandard 'god praksis'

Begrepet *complianceprogram* er ofte omtalt i norsk næringsliv. Det har sin forankring i det amerikanske Department Of Justice; Evaluation of Corporate Compliance Programs (2024) (heretter 'DOJ ECCP'). Dette dokumentet setter standarden for hva DOJ forventer av et risikobasert, dynamisk og effektivt complianceprogram, og brukes som beslutningsstøtte i strafferettslige vurderinger. Det er relevant for norske selskaper med internasjonal eksponering, har virksomhet i USA, er børsnotert internasjonalt, bruker amerikansk valuta, banker eller teknologi, og/eller er del av globale konsern.

I norsk praksis er DOJ ECCP et viktig normgivende rammeverk som påvirker forventninger til god virksomhetsstyring, særlig i større og internasjonalt orienterte selskaper. Det har altså ingen formell rettslig status, men brukes som en internasjonal referansestandard for hva som anses som et modent og effektivt complianceprogram.

OECD har også en kort og konsis veiledning for god praksis for complianceprogram og tiltak i deres OECD Good Practice Guidance on Internal Controls, Ethics, and Compliance. Se også vedlegg for oversikt over nyttige kilder og rammeverk.

Krav til compliancefunksjonen i finansbransjen er regulert i sektorlovgivning og det foreligger presiseringer og forventninger til funksjonen fra tilsynsorgan slik som European Banking Authority (EBA), European Securities and Markets Authority (ESMA) og European Insurance and Occupational Pensions Authority (EIOPA).

2. Introduksjon til compliance

Ansvar for etterlevelse i virksomheten

Styret (eller øverste ledelse i virksomheter uten styre) er øverste ansvarlig for at virksomheten etterlever relevante lover og forskrifter.

Compliancefunksjonen skal ha et klart og uavhengig mandat, med tilgang til styret eller toppledelsen når det er nødvendig. Ansvaret for compliancefunksjonen (heretter 'Compliance') bør legges til øverste ledelsesnivå, og personen som utpekes må ha tilstrekkelig erfaring, faglig kompetanse og personlig autoritet til å ivareta rollen og oppgaver beskrevet i mandatet.

Compliance har som oppgave å sikre at virksomheten etterlever relevante lover, forskrifter og etiske standarder, samtidig som den fremmer en sterk kultur for integritet og etisk atferd. Den støtter, rådgir og overvåker virksomheten slik at ledelsen og styret kan ivareta sitt ansvar for etterlevelse på en forsvarlig måte.

Risikobildet til virksomheten vil være avhengig av bransje, regulatoriske krav, markedet virksomheten opererer i og leverandørkjeden. Det er viktig at styret og ledelsen får tilstrekkelig bekreftelse på at compliancerisiko håndteres på tvers av virksomheten og at ikke vesentlige områder «faller mellom to stoler».

Dette arbeidet pålegges derfor gjerne en compliancefunksjon; *organisasjonsenheten eller rollen som har ansvar for å planlegge, koordinere og overvåke compliance-programmet.*

Virksomheten bør etablere og vedlikeholde et complianceprogram som identifiserer, behandler, følger opp og rapporterer alle vesentlige etterlevelsesrisikoer, inkludert regulatoriske, etiske, tredjepartsrelaterte, teknologiske og kulturelle risikoer som en del av virksomhetens samlede risikotaksonomi.

God praksis

Det er viktig at **styrende dokumenter** og **etiske retningslinjer** er tydelige, godt kommunisert og forstått og **solid forankret** i ledelsen. Disse styrende dokumentene og retningslinjene må omfatte alle deler av virksomheten, inkludert ulike enheter, geografiske områder og hele leverandørkjeden.

'Tone at the top' - styret og ledelsen viser aktivt at de både er fanebærere og ansvarlige for etterlevelse i virksomheten og promoterer god adferd.

Trelinjemodellen

Virksomheter trenger effektive strukturer og prosesser for virksomhetsstyring, risikostyring, etterlevelse og kontroll for å kunne oppnå sitt oppdrag, sine strategier og tilhørende mål. Overordnet styring er styrets ansvar (eller tilsvarende rolle). Styret stiller ressurser til rådighet og delegerer myndighet til toppledelsen slik at nødvendige tiltak kan iverksettes, inkludert håndtering av risiko. For å oppfylle sitt tilsynsansvar søker styret bekreftelse på at virksomheten fungerer slik det er tilsiktet.

Trelinjemodellen (se neste side) bidrar til å bygge denne tilliten ved å tydeliggjøre hvor styret kan hente den bekreftelsen og rådgivningen det trenger, og hvordan bidragene fra de tre linjene er forskjellige, samtidig som de er koordinerte og tilpasset styringsbehovene.

Modellens prinsipper gjelder alle virksomheter, men hvordan virksomhetsstyring, risikostyring, etterlevelse og kontroll utformes og gjennomføres vil variere. Ofte påvirkes virksomheten av lovkrav og regulatoriske bestemmelser.

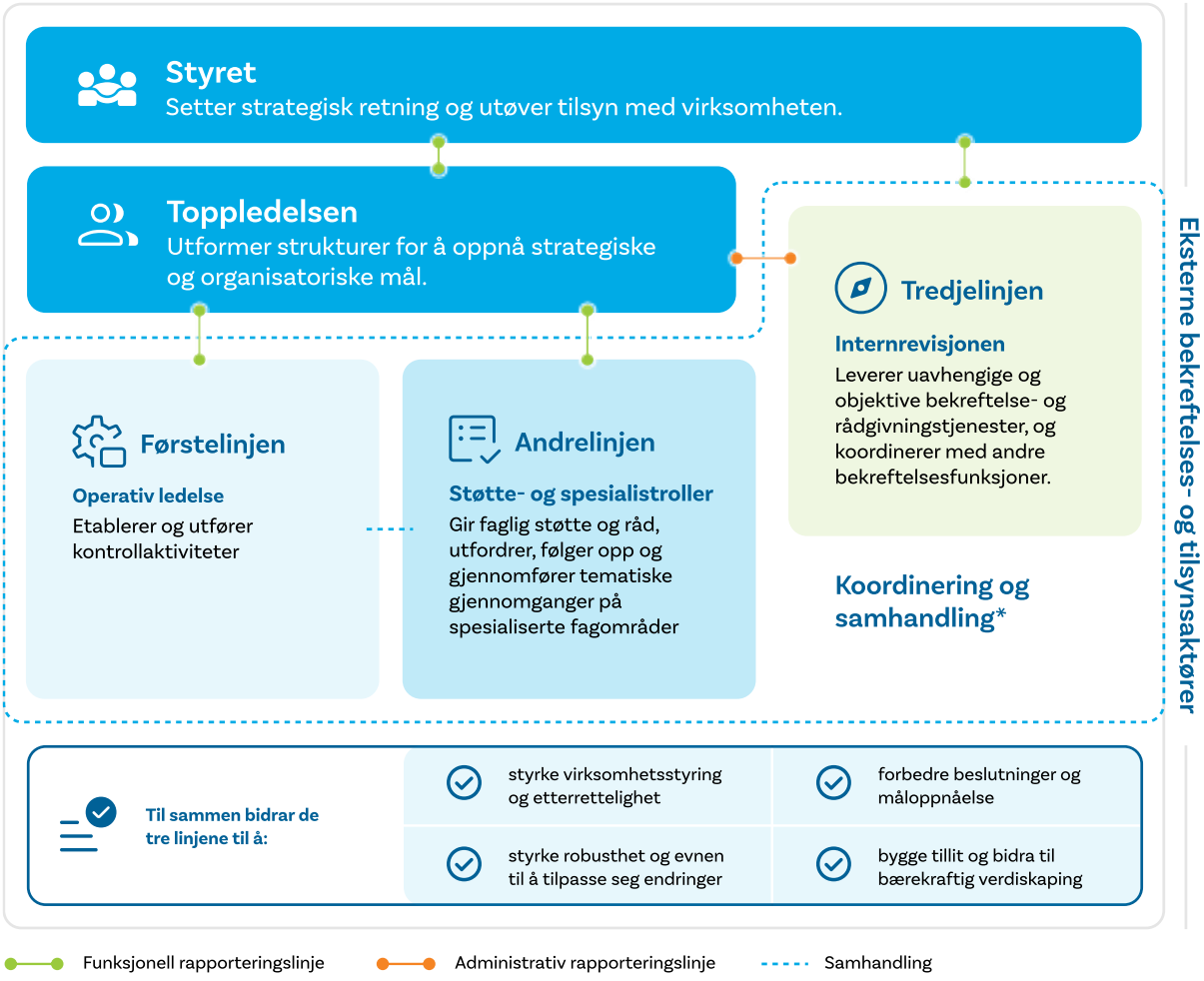
Styret (eller tilsvarende rolle) setter strategisk retning i tråd med interessentenes behov og utøver sitt tilsynsansvar, mens toppledelsen utformer strukturer og delegerer ansvar slik at risiko blir håndter og målene satt for virksomheten, nås.

Modellen bygger på et tydelig skille mellom roller, samtidig som den fremhever hvordan de gjensidig utfyller hverandre:

1. **Førstelinjen:** Ufører kjerneoppgaver og leverer tjenester og har ansvar for utforming og drift av prosesser og implementering av kontroller.
2. **Andrelinjen: Fag- og støttefunksjoner** som støtter førstelinjen gjennom faglig rådgivning, metodikk, overvåking 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 førstelinjen. Dette er typisk funksjoner som Compliance, IT-sikkerhet, Juridisk, HMS, Kvalitetsstyring etc.
3. **Tredjelinen: Internrevisjonen** gir uavhengig, risikobaserte og objektive bekreftelser på at styring, risikostyring, og internkontroll fungerer som den skal, samtidig som den kan gi rådgivning uten å overta ledelsesansvar.

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

Tydelige roller og ansvarsforhold	Uavhengighet og objektivitet for tredjelinjen	Verdi gjennom bekreftelse og rådgivning	Samarbeid og koordinering	Tilpasningsdyktig overfor endringer og nye risikoer

Et sentralt tema i modellen er betydningen av koordinering og hensiktsmessig bruk av hverandres arbeid. Ved å samordne bekreftelses- og rådgivningsaktiviteter på tvers av virksomheten, inkludert fra eksterne aktører der det er relevant, kan virksomheter redusere dobbeltarbeid, identifisere hull og gi styret et mer helhetlig og pålitelig bilde av risiko og resultater.

Uavhengighet understrekes som grunnlaget for troverdig bekreftelse, understøttet av hensiktsmessige organisatoriske strukturer og sikkerhetsmekanismer. Samtidig krever god virksomhetsstyring koordinering og åpenhet på tvers av roller, slik at uavhengighet ikke fører til isolasjon eller manglende innsikt i virksomheten.

Virksomheter er i praksis ulikt organisert, med roller og ansvar som går på tvers av de tre linjene og kan overlappe. Modellen kan gi nyttig veiledning om hvordan slike ordninger kan håndteres gjennom tydelig ansvar, åpenhet og sikkerhetsmekanismer som bevarer objektivitet og reduserer risiko for egenkontroll.

Organisatorisk plassering

God praksis tilsier at funksjonen skal være posisjonert og prioritert på linje med andre strategiske støttefunksjoner, slik at den kan utføre sitt mandat effektivt og uavhengig. Flere bransjer har også eksplisitte krav eller etablerte standarder som kan påvirke hvordan Compliance skal organiseres og utføre sitt arbeid, deriblant Finans og Helse- og omsorgssektoren. DOJ ECCP forventer at Compliance er tilstrekkelig høyt plassert, uavhengig og med direkte tilgang til øverste ledelse og styret. ISO-rammeverket forventer også at Compliance rapporterer direkte til øverste ledelse med tilstrekkelig myndighet. «Dual reporting», rapportering både til CEO og til styret/revisjonsutvalget, anbefales som god praksis.

Her følger noen eksempler fra ulike bransjer:

Bransje	Typisk plassering	Særtrekk
Finans	Ofte egen stabsfunksjon på konsernnivå, med rapportering direkte til CEO og Revisjons-utvalg/Styret	Lovpålagt funksjon. Finanstilsynets retningslinjer stiller detaljerte krav til organisering, uavhengighet og rapportering.
Industri	Ofte under konserndirektør (kan være delegert til juridisk direktør), med dedikerte compliance-medarbeidere for konkrete regelverk	Funksjonen prioriterer gjerne rådgivende bistand og arbeider mindre med kontroll av etter-levelse. Bør styrke kontrollsiden
Helse og omsorg	Ofte integrert med kvalitet/pasient-sikkerhet eller som egen funksjon i større virksomheter	Sektorspesifikke krav til etterlevelse av helseregulering, personvern for helseopplysninger og klinisk forskning

Offentlig sektor	Ofte integrert i virksomhetsstyring eller internkontroll	Forvaltningslov, offentlighetslov, anskaffelsesregelverk. DFØs forventninger til styring og kontroll
Teknologi/AI	Ofte kombinert med personvern og/eller informasjons-sikkerhet	Ny type compliancerisiko knyttet til AI, data governance og algoritimisk beslutningstaking

Det forekommer også at compliancerollen ivaretas av internrevisjonen. En slik løsning vil kunne svekke internrevisjonens uavhengighet og representerer verken en reell andrelinjefunksjon eller en uavhengig tredjelinjefunksjon, ref. Trelinjemodellen over.

Lokale compliancemedarbeidere i utvalgte enheter i virksomheten kan fungere som den sentrale stabsfunksjonens forlengede arm, og ivareta oppgaver innen rådgivning, opplæring, monitorering og rapportering. Det er ikke uvanlig at disse også har andre roller. For å sikre at oppgavene innen Compliance utføres tilfredsstillende, må ansvar, oppgaver, rapporteringslinjer og samarbeid med stabsfunksjonen være tydelig avklart og definert. Det er også viktig at kompetansebygging ivaretas.

Dersom ledelsen velger å sette ut hele eller deler av Compliance (outsourcing), må ledelsen sørge for at alle grunnleggende krav er ivaretatt. Det gjøres oppmerksom på at enkelte lover vil kunne innskrenke muligheten for outsourcing. Slik outsourcing er mest vanlig i startfasen av etablering av helhetlig risikostyring for en virksomhet, inntil organisasjonen tilegner seg felles språk, kultur og velfungerende rammeverk for risikostyring, inkludert styring av compliancerisiko.

Compliance – integrert del av virksomhetsstyring

En sentral del av god virksomhetsstyring er å identifisere, vurdere og håndtere risikoer knyttet til etterlevelse. Dette innebærer å definere hva som er akseptabel og uakseptabel risiko for virksomheten. Prosessen er tett knyttet til compliancearbeidet, da systematisk risikostyring danner grunnlaget for å sikre at virksomheten til enhver tid følger gjeldende lover, forskrifter og virksomhetens etiske retningslinjer. Dette bidrar også til å bygge og forsterke en kultur preget av integritet, tillit og ansvarlighet. For at dette skal fungere i praksis, må arbeidet struktureres i et samlet styringssystem, for eksempel med utgangspunkt i ISO-rammeverk. Kjernen i ISOs ledelsesstandarder kan illustreres som følger:

Styring → Gjennomføring → Kontroll → Evaluering → Forbedring

Denne strukturen gjør det mulig å omsette overordnede krav og verdier til konkrete forventninger, aktiviteter og ansvar. Styret og ledelsen fastsetter mål, policyer og akseptabel risiko, mens prosesseiere har ansvar for at krav omsettes til praktiske rutiner og arbeidsprosesser. Internkontrollen inngår som en naturlig del av prosessene gjennom kontrollaktiviteter som godkjenninger, avstemminger, oppfølging, tilgangsstyring og kvalitetskontroller. Kontrollaktivitetene skal redusere risiko og bidra til at virksomheten når sine mål, etterlever lover og regler og rapporterer korrekt. For mindre virksomheter bør styringssystemet tilpasses og bygges opp rundt noen få sentrale elementer, med utgangspunkt i risikoene og krav til virksomheten.

Compliance bidrar til å identifisere relevante krav, støtte implementering av disse i styringssystemet og følge opp etterlevelsen. Compliance bør også bidra til opplæring, risikovurderinger og vurdering av om kontrollene er tilstrekkelige for å håndtere etterlevelsesrisiko. Resultatene fra kontroller, avvikshåndtering og overvåkning rapporteres til ledelsen som grunnlag for forbedringer. Internrevisjon, der virksomheten har en slik funksjon, gir uavhengig bekreftelse på at styringssystemet, internkontrollen og compliancearbeidet fungerer etter hensikten. Til sammen skaper dette et helhetlig styringssystem der styring, gjennomføring, kontroll og kontinuerlig forbedring henger tett sammen.

Andre relevante rammeverk og veiledninger

COSO Internal control - Integrated framework (2013): Etterlevelse av lover og regler er definert som 1 av 3 overordnende mål for internkontroll.

COSO ERM (2017): Plasserer compliancerisiko eksplisitt innenfor virksomhetens samlede risikostyring og strategiske styring. Gir en tydelig forankring av compliancearbeidet.

Compliance Risk Management: Applying the COSO ERM framework (2020): Kobler COSO ERM-rammeverket til etablering og drift av et effektivt compliance- og etikkprogram. Gir en forankring av compliancearbeidet i styring og kontroll.

For virksomheter underlagt Finanstilsynet eller DFØ vil forventninger til styring og kontroll ofte være konkretisert i egne rundskriv og veiledere**. Finanstilsynets modul for intern virksomhetsstyring (30.09.2025)** gir god veiledning til hvordan ansvar og fullmakter bør være definert og fordelt.

Complianceprogram

Et complianceprogram er en kontinuerlig prosess som skal styrke virksomhetens arbeid med ansvarlig drift, etisk forretningsatferd og forebygging av regelbrudd. Det retter seg mot regelverk som har til hensikt å beskytte samfunnets interesser, og er et viktig virkemiddel for å ivareta integritet og opprettholde omverdenens tillit til virksomheten.

Programmet er et supplement til det løpende arbeidet med å sikre etterlevelse av operasjonell særlovgivning som ivaretas av egne fagenheter – for eksempel innen HMS, Økonomi og Personvern. Fordi disse fagområdene gjerne har egne fagmiljøer og kontrollmekanismer, favner programmet typisk om regelverk som krever en tverrgående og integritetsorientert tilnærming, og der ansvaret ikke naturlig er plassert i én enkelt fagavdeling.

Sentrale ansvarsområder for dagens Compliance knyttes ofte til antikorrupsjon, etikk, antihvitvasking, sanksjoner og eksportkontroll, personvern, databeskyttelse, ESG rapportering og transparenskrav, sektorspesifikk regulering, AI governance og ansvarlig bruk av teknologi. For offentlige virksomheter innebærer det også etterlevelse av forvaltningslov, offentlighetslov og anskaffelsesregelverk.

For å støtte en kultur der integritet prioriteres, er det også viktig at virksomheten har trygge varslingskanaler og tydelige mekanismer som gjør det mulig å melde bekymringer uten frykt for konsekvenser.

Etikk og kultur

En sterk kultur for etikk og integritet er en forutsetning for at complianceprogrammet skal fungere i praksis. Policyer, prosedyrer og kontroller får først reell effekt når ledere og medarbeidere oppfatter etterlevelse som en integrert del av hvordan virksomheten skaper verdier, ikke som en tilleggsaktivitet eller et «nødvendig onde». For at etterlevelse skal bli en naturlig del av organisasjonskulturen, må den innlemmes i ledelsens beslutningsprosesser, prioriteringer og daglige adferd, slik at dette setter standarden for resten av virksomheten. Ledere må 'walk the talk'. Motsatt kan bagatellisering av brudd og manglende konsekvens raskt undergrave hele programmet.

Compliance har en viktig rolle som pådriver for etisk kultur, men kan ikke alene «eie» kulturen. Linjeledere har hovedansvaret for hvordan verdier og retningslinjer faktisk praktiseres i det daglige. Compliance kan støtte gjennom råd, opplæring, analyser av kultur- og adferdsrisiko og ved å synliggjøre sammenhengen mellom kultur, hendelser og avvik.

Styret og ledelsen har en nøkkelrolle i å omsette etikk og integritet fra prinsipper til praksis. Styret har det overordnede ansvaret for at virksomheten har et effektivt program og for å følge opp rapportering om status, risiko og vesentlige brudd. Ledelsen må sikre tilstrekkelige ressurser, tydelige prioriteringer og en praksis som gjenspeiler verdiene virksomheten ønsker å stå for. Revisjonsutvalget overvåker programmets effektivitet og bidrar til at styret får nødvendig innsikt.

God praksis

Et risikobasert complianceprogram **integrert** i virksomhetens strategi, forankret i ledelsen og støttet av et sterkt **etisk rammeverk**.

Et dynamisk program tilpasset regulatoriske krav som omfatter hele virksomheten og dens verdikjede.

En styringsstruktur der Compliance har uavhengighet, tilstrekkelige ressurser og tydelige rapporteringslinjer.

En kultur som oppmuntrer til åpenhet og varsling.

En risikoprofil skreddersydd til virksomhetens faktiske eksponering.

Mandat og ressurser

Compliance må ha et tydelig mandat som forankres og godkjennes på øverste nivå (styret eller tilsvarende) i virksomheten. Mandatet bør være tilpasset arten, kompleksiteten og størrelsen til virksomheten samtidig som det ivaretar uavhengigheten til funksjonen. Uavhengighet betyr at Compliance er uavhengig av den operative virksomheten og har direkte rapporteringslinjer til toppledelsen eller styret, slik at kritiske saker kan eskaleres uten hindringer. Mandatet bør beskrive:

- Roller og ansvar, organisering og rapporteringslinjer
- Complianceaktiviteter og metodikk
- Tilgang til data, systemer og personer
- Budsjett og ressurser til compliance
- Eskaleringsmekanismer
- At øverste nivå skal godkjenne eventuell oppsigelse av Compliance-ansvarlig

Virksomheten må ha etablert en avlønningspolitikk som bidrar til å sikre objektivitet, integritet og uavhengighet. Resultatavhengige komponenter som kan føre til interessekonflikter må unngås. Samtidig må avlønning sikre at det er mulig å rekruttere personer med nødvendig kompetanse, erfaring og faglig tyngde.

Compliance må ha god ressurstilgang – ikke bare antall ansatte, men også kompetanse, budsjett og tilgang til teknologi og data. Sentrale spørsmål for å vurdere hvorvidt ressurstilgangen er tilstrekkelig:

- Har Compliance tilstrekkelige ressurser (personell, budsjett, kompetanse og teknologi)?
- Har Compliance rettidig tilgang til relevante data for risikovurdering og overvåkning?

- Hvordan investerer virksomheten i videre opplæring og utvikling av Compliance og andre kontrollfunksjoner og -ressurser?
- Bruker virksomheten dataanalyseverktøy for å måle effektivitet?
- Er investeringene i Compliance proporsjonale med virksomhetens risikoprofil?
- Har Compliance mulighet til å eskalere kritiske saker uten hindringer?

Disse spørsmålene bør vurderes minst en gang i året, for eksempel i form av en egenevaluering og i forbindelse med budsjettplanlegging.

Når det gjelder kompetanse kan det være behov innen ulike områder som;

- regelverksforståelse og juridisk kompetanse, bransjespesifikk kunnskap,
- risikostyring, forståelse av teknologiske verktøy og AI-systemer,
- endringsledelse og kulturbygging, kommunikasjon og opplæring
- cybersikkerhet og digital motstandsdyktighet.

Krav til kompetanse og ressurser kan også fremgå av regulatoriske krav, så som kravene til Personvernombudet i *Personopplysningsloven* og Compliancefunksjonen i *Rundskriv gitt av Finanstilsynet for Verdipapirforetak.*

Bruk av data og teknologiverktøy

En stadig større del av virksomheters kjerneprosesser, beslutningsstøtte og kontroll-mekanismer er i dag datadrevet. Dette har betydelig påvirkning på Compliance og innebærer blant annet at man ikke lenger kan basere sitt arbeid utelukkende på periodiske kontroller og manuelle vurderinger, men utnytter tilgjengelige data og benytter relevante teknologiske verktøy som automatiserer og muliggjør løpende risikovurdering og overvåking. Disse forventningene gjenspeiles tydelig i DOJ ECCP. Her fremheves det eksplisitt at effektive programmer forutsetter at Compliance har «timely access to relevant data» og utnytter dataanalyse og teknologi for å kontinuerlig identifisere, overvåke og håndtere risikoer i virksomheten og hos tredjeparter.

Bruk av kunstig intelligens ('AI') i virksomheters kjerneprosesser øker raskt, både innen privat og offentlig sektor. AI kan bidra til mer effektiv saksbehandling, analyse og beslutningsstøtte, men samtidig utfordrer teknologien etablerte prinsipper for transparens, likebehandling og ansvar.

DOJ ECCP presiserer at virksomheter forventes å identifisere og håndtere risiko knyttet til ny teknologi, inkludert AI, både der teknologien brukes i virksomheten og der den benyttes i compliancearbeidet selv. Veiledningen fremhever at svak styring av teknologisk risiko kan indikere manglende modenhet i virksomhetens risikovurderings- og kontrollprosesser.

I europeisk kontekst etablerer EU AI Act et omfattende, risikobasert regulatorisk rammeverk for utvikling og bruk av AI. Dette området er i rask utvikling, med omfattende

lovkrav som berører virksomheter – enten direkte eller indirekte. For det som betegnes som 'høyrisiko-AI-systemer' stilles det blant annet krav til risikostyring, data governance, dokumentasjon, menneskelig kontroll og løpende overvåking. I tillegg til risiko knyttet til AI-systemer, er det nødvendig å vurdere hvordan AI påvirker, forsterker eller reduserer risikoer som virksomheten allerede håndterer. Dette innebærer at AI-risiko må inngå som en integrert del av virksomhetens compliance- og internkontrollrammeverk, på linje med andre vesentlige risikoer.

AI governance forutsetter derfor et godt samspill mellom flere funksjoner, herunder ledelse, forretning, IT, informasjonssikkerhet, personvern, compliance, risikostyring og internrevisjon. Compliance sin rolle er normalt ikke å eie AI-løsningene, men å bidra til klare rammer for etterlevelse, styring og kontroll. Compliance bør bidra til at AI-policyer, risikovurderinger og kontrolltiltak er dokumenterte, konsistente og etterprøvbare, og at vesentlige endringer i modeller eller bruksområder vurderes før de tas i bruk. Der AI-løsninger leveres av tredjeparter, bør Compliance bidra til at virksomheten vurderer leverandørens etterlevelse av relevante krav og regelverk.

God praksis

Tilgang til relevante, pålitelige og tidsriktige **datakilder** på tvers av virksomheten er **fundamentalt** i dagens Compliance.

Compliance må ha en tydelig forståelse av hvilke data som er nødvendige for å overvåke virksomhetens vesentlige risikoer, samt hvordan disse dataene genereres, lagres og brukes.

Mangelfull datatilgang anses av DOJ ECCP som et tegn på at programmet ikke er tilstrekkelig forankret eller operativt effektivt. Å sikre god datakvalitet bør derfor forstås som en integrert del av internkontroll og styringsstruktur.

3. Sentrale elementer i et complianceprogram

Dette kapittelet går mer detaljert inn i sentrale elementer som sammen utgjør et program, og redegjør for en rekke regulatoriske krav som i praksis ofte involverer Compliance. Programstruktur og minimumskrav innebærer at virksomheten skal ha en dokumentert prosess for å:

- **identifisere** og vurdere etterlevelsesrisiko basert på virksomhetens aktiviteter, geografi, kunder/partnere, regulatoriske krav og marked
- **vurdere fremvoksende** etterlevelsesrisikoer, herunder regulatoriske endringer, teknologiutvikling, geopolitiske forhold og endringer i virksomhetens strategi eller forretningsmodell

- **oppdatere** risikovurderingen periodisk og ved vesentlige endringer, f.eks. nye produkter, nye markeder, omorganisering, funn/hendelser
- ha en **metodikk** for compliance-risikovurdering
- sikre at risikovurderingen brukes **aktivt** til å prioritere policyer, kontroller, opplæring og overvåkning.

Alle virksomheter skal ha en forsvarlig varslingsordning i tråd med *Arbeidsmiljøloven*. Internasjonale virksomheter må også forholde seg til EUs varslingsdirektiv. Compliance bør påse at det er etablert en tilfredsstillende ordning. Roller og ansvar knyttet til både varsling og gransking kan variere for Compliance. For mer utdypende informasjon viser vi her til *veileder for god varslingshåndtering*, tilgjengelig via www.iia.no.

Årsplan og revisjon av complianceprogrammet

Strukturerte, dokumenterte og kommuniserte prosesser er viktig for å styrke effektiv compliance og bidra til kontinuerlig forbedring. Å ha en årsplan eller årshjul er god praksis. Årsplanen skal være risikobasert og dokumentere sammenhengen mellom:

- virksomhetens risikoprofil og identifiserte compliancerisikoer
- prioriterte aktiviteter, ressursbruk
- rapporteringsbehov og planlagte kontroller.

Programmet revideres minimum årlig og ellers ved behov, eksempelvis ved vesentlige endringer i virksomhetens risikoprofil, regulatoriske krav, vesentlige hendelser eller funn fra testing, internrevisjon eller tilsyn. Endringer skal godkjennes i henhold til virksomhetens delegerings- og styringsstruktur.

God praksis

En **årsplan** bør som minimum inkludere:

- Oppdatert compliance-risikovurdering
- Plan for policygjennomgang og oppdatering, kommunikasjon og forankring
- Opplæringsplan og rådgivning (roller/risiko)
- Overvåkning- og kontrollplan
- Plan for tredjepartsaktiviteter
- Rapporteringsterminer til ledelse/styre

Plan for måling og forbedring ved for eks. forbedring av data, kontrollplan, teknologi og verktøy, kompetanseløft.

Integrert del av virksomhetens risikostyring

Complianceprogrammet skal være en integrert del av virksomhetens samlede rammeverk for risikostyring. Compliancerisiko skal identifiseres, vurderes, overvåkes og rapporteres gjennom de samme styringsmekanismene som øvrige strategiske, operasjonelle, finansielle og regulatoriske risikoer. Compliance skal gjennom et effektivt program bidra til en helhetlig risikoforståelse og sikre at relevante etterlevelsesforhold inngår i virksomhetens samlede risikobilde.

Compliance må samhandle med andre kontrollfunksjoner for å danne seg et helhetlig bilde av «hvem som gjør hva». Dette inkluderer harmonisering av rammeverk, risikoskalaer og rapportering. I tillegg er det viktig at datainnsamling og verktøybruk styrkes. God samhandling og klare grensesnitt mot andre risiko- og kontrollfunksjoner i virksomheten bidrar til bedre oppfølging og rapportering til ledelse og styre.

Dette kan være følgende funksjoner:

- **Risikofunksjonen:** Compliancerisiko inngår i helhetlig risikostyringsrammeverk. Viktig å ha felles forståelse av virksomhetens risikounivers, harmoniserte risikoskalaer og -definisjoner, og koordinert rapportering. Risikovurderinger bør deles og gjensidig informere hverandres arbeid.
- **ESG/Bærekraft**: Koordinering med bærekrafts-, HR- og innkjøpsavdelinger for helhetlig tilnærming, integrasjon av ESG-risiko, overvåkning av tredjeparters etterlevelse som del av integrity due diligence, bidra til etterrettelighet og god rapportering.
- **Internrevisjon:** Internrevisjon gir uavhengig bekreftelse på effektiviteten av Compliance-programmet. Compliance og internrevisjon bør koordinere sine planer for å sikre dekning og unngå dobbeltarbeid. Se standard 9.5 i de Globale standarder for internrevisjon.
- **Personvernombud:** Særlig relevant der Compliance har ansvar for GDPR-etterlevelse. Klare grensesnitt mellom Compliance og Personvernombudets rolle må defineres.
- **Kvalitetsrevisjon/HMS:** Koordinering rundt sektorspesifikke kontroller og regulatoriske krav.
- **IT-sikkerhet/CISO:** Særlig viktig for cyberrisiko, DORA-etterlevelse og AI-governance.

I tillegg bør ledelsen/styret sikre at Compliance er involvert i strategiske endringsprosesser og har tilgang til relevante kontrolldata og verktøy. Målet er å optimalisere ressursbruken og den samlede nytteverdien for virksomheten. Et modent styringssystem kjennetegnes ved god integrasjon og samhandling mellom compliance, risikostyring, internkontroll og internrevisjon.

Risikoappetitt

Øverste ledelse fastsetter hvor høy risiko virksomheten totalt sett aksepterer (risikoappetitt). Deretter operasjonaliseres dette i praksis gjennom risikotoleranser som angir hvor store avvik eller enkeltrisikoer som kan tolereres før tiltak må settes inn.

Hvis vi knytter dette opp mot etterlevelse av regelverk, så kan en virksomhet ha *lav risikoappetitt*, fordi brudd på regelverk kan gi bøter, omdømmetap og regulatoriske konsekvenser.

Lav risikoappetitt betyr at virksomheten generelt ikke ønsker å ta compliancerisiko. Dette oversettes til stramme toleransegrenser i praksis.

Eksempel på toleransenivåer kan være 0 alvorlige lovbrudd, maksgrenser på antall mindre avvik per kvartal, 100 % gjennomføring av obligatorisk opplæring for alle ansatte.

Hvis toleransen overskrides (f.eks. mange avvik eller manglende opplæring), betyr det at virksomheten opererer utenfor sin risikoappetitt, og ledelsen må gripe inn og tiltak forsterkes.

God praksis

Å **vurdere risiko i praksis** handler om å kombinere systematisk metode med forretningsforståelse. Her følger en trinn-for-trinn-prosess:

1. **Identifiser risikoer:** Kartlegg prosesser, systemer og aktiviteter med mulig risiko. Bruk flere informasjonskilder: lover og forskrifter, bransjekrav og tidligere hendelser.
2. **Analyser sannsynlighet og konsekvens:** Vurder hvor sannsynlig det er at risikoen inntreffer, og hvilken konsekvens den vil ha. Visualiser i en 3x3- eller 5x5-risikomatrise.
3. **Vurder eksisterende kontroller:** Kartlegg eksisterende policyer, systemer, opplæring og teknologiske kontrollmekanismer. Vurder om dagens tiltak fungerer som planlagt.
4. **Fastsett residual risiko:** Vurder risikonivået som gjenstår etter at eksisterende tiltak er hensyntatt.
5. **Prioriter og planlegg tiltak:** Høy risiko: Strengere kontroller, mer opplæring, hyppigere revisjon. Moderat risiko: Justering av eksisterende kontroller. Lav risiko: Standardtiltak.
6. **Dokumenter og følg opp:** Identifiserte risikoer, vurdering før og etter kontroller, tiltak, ansvar og tidsfrister. Oppdater minst årlig og ved endringer.

Identifisering, vurdering og behandling av compliancerisikoer

Risikovurderinger skal være systematiske, tilstrekkelig dokumentert, forankret i virksomhetens mål og strategi, nært knyttet til internkontroll og gjenstand for løpende forbedring. Risikobaserte tiltak skal være proporsjonale med risikoen og prioriteres der konsekvensene av brudd er størst.

Compliance skal gjennomføre minst én årlig vurdering av fremvoksende etterlevelsesrisikoer, herunder regulatoriske endringer, teknologiutvikling, geopolitiske forhold og endringer i virksomhetens strategi eller forretningsmodell.

Compliance skal definere hvilke datakilder som skal overvåkes (nasjonale, EU og andre internasjonale lovkilder), etablere prosesser for jevnlig oppdatering i funksjonen og dokumentere hvordan regelverk og endringer er identifisert og vurdert. Virksomheten skal ha prosesser for rask tilpasning ved endringer i regelverk, for eksempel behov for endringer i styrende dokumenter og prosesser. For offentlige virksomheter kan endringshåndtering kreve høringsprosesser og politisk behandling.

Risikoområde	Tiltak	Eksempel
Tredjepartsrisiko (eks. leverandører, agenter, business partnere)	Utvidet integrity due diligence (IDD) for tredjeparter i høyrisikoområder	Screeningverktøy for å sjekke mot internasjonale sanksjonslister og Politically Exposed Persons (PEPs)
Antikorrupsjon	Strengere godkjenningsprosesser for gaver, ytelser, representasjon	Forhåndsgodkjenning fra Compliance for gaver over definert beløpsgrense
AML / hvitvasking	Økt overvåkingsfrekvens for transaksjoner i høyrisikobransjer	Automatiserte verktøy for å flagge uvanlige transaksjonsmønstre
Personvern/ GDPR	Ekstra kontroller for behandling av sensitive persondata	Kryptering og tilgangsstyring for HR-data og helseinformasjon
ESG / Åpenhetsloven	Aktsomhetsvurderinger for leverandørkjeder i høyrisikoland	Tredjepartssertifiseringer, f.eks SA8000, for leverandører
Intern kultur / varsling	Styrk opplæring i enheter med høy risiko for etiske brudd	Obligatoriske dilemma-workshops for salg og innkjøpsavdelinger
Teknologi / cyber	Penetrasjonstester og strengere tilgangskontroller	Multifaktor-autentisering for alle med tilgang til finanssystemer
AI-risiko	Risikovurdering av AI-systemer; klassifisering etter EU AI Act	Register over AI-systemer med vurdering av algoritmisk skjevhet (bias), sporbarhet og menneskelig overprøving (human-in-the-loop)
Virksomhetsregler, forretningsprosesser og god forretningsskikk	Kontroll av krav til virksomheten, forretningsprosesser og god forretningsskikk	Kontroll av krav til styring og kontroll, fullmakter, produktutvikling, investeringer, salg, samt ansattes autorisasjon og egnethet

Styrende dokumenter

Virksomheten bør ha et styringssystem forankret i virksomhetens visjon, verdier og strategi. Videre bør utformingen av styrende dokumenter og minimumskrav ta utgangspunkt i risikovurderinger slik at de adresserer de compliancerisikoer virksomheten står overfor. Compliance skal være en pådriver for at virksomheten etablerer og vedlikeholder styrende dokumenter. Et godt dokumenthierarki kan illustreres som en pyramide med få policyer i toppen. Hvert nivå utdyper nivået over og kan aldri stride mot det. En gyllen regel er at jo lenger ned i dokumenthierarkiet, jo mer detaljert og jo lavere godkjenningsnivå. Styret skal ikke godkjenne sjekklister, og en prosedyre skal ikke inneholde prinsipper som hører hjemme i en policy.

I en konsernmodell legges det til et konsernnivå over selskapsnivået da et datterselskap er et eget rettssubjekt med eget styre. En konsernpolicy blir derfor ikke automatisk bindende i hele konsernet, men må godkjennes av de respektive styrene i datterselskapene. Det bør foreligge en styringsmodell som forklarer hele dokumenthierarkiet i virksomheten og hvordan dette henger sammen. Uansett virksomhetens størrelse bør hvert dokument ha en navngitt eier, godkjenner i tråd med fullmaktsmatrisen, versjon og ikrafttredelsesdato, neste revisjonsdato, og referanse oppover (hvilken policy/standard det utleder krav fra). Alt dette bør samles i et dokumentregister som viser status og forfalte revisjoner.



Nivå	Svarer på	Typisk vedtatt av	Endres
0. Styringsrammeverk	Hvem bestemmer?	Generalforsamling / styre	Sjelden
1. Policy	Hva og hvorfor?	Styret	Årlig gjennomgang
2. Retningslinje / standard	Hvilke krav gjelder?	Daglig leder / ledergruppe	Ved behov, minst hvert 2. år
3. Prosedyre / rutine	Hvordan, hvem og når?	Prosess- eller fagansvarlig	Løpende
4. Instruks, sjekkliste, mal, skjema	Nøyaktig hva gjør jeg?	Linjeleder / fagmiljø	Løpende

Nivå 0 – Styringsrammeverk. Vedtekter, eventuell aksjonæravtale, styreinstruks, instruks for daglig leder og fullmaktsmatrise. Dette er ikke policyer, men dokumentene som

avgjør *hvem som har myndighet* til å vedta alt under. Fullmaktsmatrisen er ofte det viktigste – den kobler beslutninger til roller og beløpsgrenser. (For selskaper med ansattevalgte styremedlemmer er styreinstruks lovpålagt etter aksjeloven.)

Nivå 1 – Policyer. Korte (gjerne 2–5 sider), prinsipielle og få. De uttrykker styrets holdning og risikovilje: etiske retningslinjer, risikostyring, internkontroll, antikorrupsjon, informasjonssikkerhet, AI, personvern, varsling, bærekraft/menneskerettigheter. En policy sier *hva* virksomheten forplikter seg til og *hvorfor*, og plasserer ansvar.

Nivå 2 – Retningslinjer/standarder. Operasjonaliserer policyen til konkrete, etterprøvbare minimumskrav. Eksempel: antikorrupsjonspolicyen sier nulltoleranse; retningslinjen fastsetter beløpsgrenser for gaver, krav til integritetsvurdering av tredjeparter og hvem som godkjenner unntak. Dette er nivået hvor internrevisor og compliance typisk gjennomfører kontrollaktiviteter.

Nivå 3 – Prosedyrer/rutiner. Beskriver arbeidsprosessen trinn for trinn: roller, rekkefølge, kontrollpunkter og dokumentasjon. Eies av den som eier prosessen, ikke av compliance. Gjerne med prosesskart og innebygde kontroller.

Nivå 4 – Arbeidsinstrukser og støttedokumenter. Sjekklister, maler, skjemaer og systembrukerveiledninger. Mest volum, minst formalitet, raskest endring.

Eksempelet under viser hvordan dette kan se ut i praksis:

Nivå	Eksempel
Policy	"Virksomheten skal etterleve GDPR."
Standard	"Personopplysninger skal klassifiseres og beskyttes."
Prosedyre	"Slik gjennomføres DPIA."
Kontroller	"Alle DPIA-er kvalitetssikres før implementering."
Evaluere og forbedre	"Måling av antall gjennomførte DPIA-er"
Internrevisjon	"Uavhengig vurdering av om prosessen fungerer"

Håndtering av tredjeparter og leverandørkjeder

Samhandling med tredjeparter kan utgjøre en vesentlig risiko knyttet til informasjonssikkerhet, AI, mulige sanksjoner og politisk eksponerte personer (PEPs), korrupsjon, brudd på menneskerettigheter, klima/miljøskade eller andre risikoområder.

Programmet må derfor omfatte hvordan man skal håndtere tredjeparter gjennom hele **forretningsforholdets livssyklus**:

Fase	Aktiviteter
1. Identifisering og screening	Kartlegging av tredjeparter (vesentlige, strategiske etc.) risikokategorisering, sanksjonsscreening, PEP-kontroll, negativ mediedekning
2. Due diligence	Risikobasert Integrity Due Diligence (IDD), bakgrunnsundersøkelser, vurdering av motpartens complianceprogram
3. Kontrahering	Etiske retningslinjer for leverandører, integritetsklausuler, rett til revisjon, compliancekrav, sanksjonsklausuler, oppsigelsesrett ved brudd
4. Kontinuerlig overvåkning	Periodisk re-screening, hendelsesbasert oppfølging, automatiserte verktøy for kontinuerlig overvåkning
5. Avslutning/exit	Prosesser for opphør ved uakseptabel risiko, dokumentasjonskrav

EUs aktsomhetsdirektiv (CSDDD) krever at store virksomheter gjennomfører aktsomhets-vurderinger for menneskerettigheter og miljøpåvirkning i egne operasjoner og verdi-kjeder. Åpenhetsloven (i kraft fra 2022) stiller krav til aktsomhetsvurderinger relatert til grunnleggende menneskerettigheter og anstendige arbeidsforhold. Virksomheter bør vurdere forholdet mellom Åpenhetsloven og CSDDD når begge gjelder. Compliance bør vurdere omfanget av involvering i denne prosessen og eventuelt koordinere med andre som Innkjøp, ESG og juridisk avdeling for å sikre helhetlig tilnærming.

Compliance har i enkelte sektorer eller bransjer ofte ansvaret for integrity due diligence, et risikobasert system for integritetsundersøkelse av samarbeidspartnere ('IDD'). IDD er undersøkelser og vurderinger av motparter, inkludert dets eiere og nøkkelpersoner. IDD gjennomføres for å skaffe en rimelig sikkerhet om deres integritet og forretningsetikk. Prosessen bør være risikobasert og gjennomføres som del av utvelgelsen av tredjeparter. Et viktig ledd er vurderingen av hvorvidt det i det hele tatt skal inngås en avtale med motparten. Forventninger og krav til tredjeparter bør fremgå i egne retningslinjer. Retten til å revidere etterlevelse av disse kravene bør også fremkomme her.

Her er en rekke eksempler på 'røde flagg' og mulige tiltak for håndtering av tredjeparter:

Risiko-område	Røde flagg	Tiltak
Korrupsjon	Uvanlig høye kompensasjoner, manglende dokumentasjon, bruk av agenter uten klar rolle eller definert scope	Utvidet IDD kontraktsklausuler og eskalering
Sanksjoner og eksportkontroll	Eierstruktur i høyrisikoland, koblinger til sanksjonerte personer eller virksomheter	Kontinuerlig screening mot sanksjonslister før og under kontrakts-perioden
Menneskerettigheter og arbeidsforhold	Bruk av arbeidskraft fra land med høy risiko for menneske-rettighetsbrudd, innleie gjennom flere	Leverandørrevisjon, arbeidstakerintervju, revisjonsklausuler,

	ledd, manglende arbeidskontrakter og lønns-dokumentasjon	kontraktsklasuler som setter krav til aktsomhetsvurderinger
AI og teknologi	Bruk av AI-systemer uten dokumentert risikovurdering eller styring	Krav til AI governance, dokumentasjon og risikovurdering

Opplæring og bevisstgjøring

Relevant og tilpasset opplæring er vesentlig for å bygge en ønsket kultur. Compliance bør utarbeide en årlig opplæringsplan tilpasset målgrupper, innhold, frekvens og målemetode, sikre at opplæring er i relevant form og språk og gir praktisk bruk, måle effekt gjennom testing, evaluering, og oppfølging av manglende gjennomføring/ forståelse, kommunisere tydelig om forventninger og konsekvenser ved brudd.

Opplæring innenfor områder med høy iboende compliancerisiko bør være obligatorisk. Det kan være nødvendig å tilpasse opplæringens omfang, innhold og hyppighet til ulike grupper:

- Nyansatte: Grunnleggende opplæring som del av onboarding.
- Ledere: Dedikert opplæring i deres særskilte rolle og ansvar.
- Medarbeidere med tredjepartskontakt: Målrettet opplæring i f.eks. anti-korrupsjon, menneskerettigheter, røde flagg og eskalering.
- AI-utviklere og -brukere: AI-kompetanse ('literacy') i tråd med EU AI Act artikkel 4.
- Innleide og leverandører: Opplæring tilpasset rolle og risikoeksponering.

Opplæringen kan være i form av presentasjon av regelverk, demonstrasjon av verktøy, case-diskusjoner, dilemmatrening, workshops, klasseromsundervisning, én-til-én opplæring eller e-læring. Opplæringen bør videre dokumenteres, og innhold jevnlig evalueres. Det bør føres logg over hvem som har gjennomført obligatorisk opplæring, og oppfølging bør være del av årsplanen til Compliance.

Forebygging og bevisstgjøring er sentralt, og Compliance blir i økende grad brukt som sparringspartner for ledelsen. Vurderinger herfra bør dokumenteres og kommuniseres på en måte som sikrer læring samt en enhetlig praksis på tvers av virksomheten.

Periodisk kontroll og kontinuerlig overvåkning

Compliance skal etablere en risikobasert plan for overvåkning og kontroll som minimum omfatter tematiske gjennomganger av høyrisikoområder, kontrolltesting (både design av kontroller og operativ effekt), analyser av varsler, hendelser, avvik, og mønstre, oppfølging av tiltak og lukking av funn. Dette forutsetter at det, som tidligere omtalt, er etablert tydelige krav (styrende dokumenter) til etterlevelse på høyrisikoområdene både overfor interne medarbeidere og leverandører.

Ved vesentlige brudd eller gjentakende avvik skal virksomheten gjennomføre rotårsaks-analyse, identifisere systemsvakheter (kontroller, prosesser, ledelse, kultur), iverksette korrigerende og forebyggende tiltak, oppdatere risikovurdering, rutiner og opplæring basert på læring.

Effektiv compliance krever imidlertid både periodisk kontroll og kontinuerlig overvåkning. Mens periodisk kontroll gjennomføres på fastsatte tidspunkter, innebærer kontinuerlig overvåkning løpende vurdering av prosesser og transaksjoner:

- Automatiserte overvåkningsverktøy for transaksjonsovervåkning, sanksjonsscreening og avviksdeteksjon.
- Dashbord som gir realtidsoversikt over compliance-status, risikonivåer og nøkkelindikatorer.
- Prediktiv analyse for å identifisere mønstre og trender som kan indikere fremtidige risikoer.
- Policy-drift-overvåkning: Identifisere avvik fra gjeldende retningslinjer i sanntid.

Funn fra den kontinuerlige overvåkningen bør finnes igjen i risikovurderingen.

- Risikobasert utvalg: Fokuser testing av kontroller i områder med høyest iboende risiko og der svikt har størst konsekvens. Fungerer disse?
- Metodikk: Stikkprøver, dataanalyse, intervjuer, gjennomgang av dokumentasjon og prosessgjennomganger.
- Dokumentasjon: Testresultater, avvik, årsaksanalyse og anbefalte tiltak må dokumenteres.
- Koordinering: Avstem med internrevisjon for å unngå dobbeltarbeid og sikre helhetlig dekning.
- Oppfølging: Avvik må følges opp med korrigerende tiltak, ansvarlige og tidsfrister.

Her er noen eksempler på periodiske kontroller og kontinuerlig overvåkning:

Risikoområde	Periodisk kontroll	Kontinuerlig overvåkning
Antikorrupsjon	Stikkprøvekontroll av sponsorater, donasjoner, gaver og bevertning	Transaksjonsovervåkning ift. fastsatte terskelverdier eller uvanlige betalings-mønstre
Sanksjoner og eksportkontroll	Gjennomgang av eksporttransaksjoner og kunder i høyrisikoland	Automatisk screening av kunder, leverandører og transaksjoner mot oppdaterte sanksjonslister
Menneskerettigheter og arbeidsforhold	Leverandørrevisjoner, arbeidstakerintervjuer og dokumentgjennomgang	Overvåkning av varsler, revisjonsfunn og medieomtale

Varsling	Analyser av lukkede saker, behandlingstid og kontrolltiltak	Trendanalyse av varsler, bekymringsmeldinger og medarbeiderundersøkelser
Etikk og interessekonflikter	Stikkprøver av habilitet, oppslag mot aksjonærregistre, sjekk av styreverv opp mot eget leverandørregister	Overvåking av habilitetsregister
Personvern	Testing av tilgangsstyring og gjennomgang av behandlingsprotokoller	Varsler om uautoriserte tilganger, datalekkasjer eller avvik fra etablerte tilgangsprofiler
AI governance	Årlig vurdering av AI-systemers risikoklassifisering og kontrollmiljø	Overvåkning av modellendringer, avvik, bias-indikatorer og høy-risiko brukstilfeller

Nøkkelindikatorer

Nøkkelindikatorer kan bestå av både kvalitative og kvantitative målinger og vurderinger. Her er en rekke eksempler på mulige indikatorer:

Kategori	Eksempler på indikatorer
Risikovurdering	Andel risikoer med definerte tiltak; antall endringer identifisert; dekning av risikovurdering
Opplæring	Fullføringsgrad obligatorisk opplæring; tid til fullføring; testresultater
Tredjeparter	Andel høyrisikotredjeparter med gjennomført IDD; antall avvik; tid til re-screening
Varsling	Antall varsler mottatt; behandlingstid; andel med korrigerende tiltak; type varsler
Kontroller	Gjennomført vs. planlagt; andel avvik; tid til utbedring
Kultur/adferd	Kulturundersøkelser; bruk av varslingskanaler; policy-bevissthet; dilemmatrening
AI governance	Andel AI-systemer klassifisert; gjennomførte risikovurderinger; bias-tester utført

Rapportering

Compliance skal rapportere kvartalsvis (eller avtalt frekvens) til ledelse og styre/utvalg om status på compliancerisiko og risikotrend, eksempelvis vesentlige avvik/hendelser og håndtering, resultat av overvåkning og kontroller, status på tiltaksplan og rest-risiko, opplæringsstatus og effektmålinger, tredjepartsstatus (høyrisiko, funn, tiltak).

Virksomheten skal også ha klare, rettferdige og konsekvente reaksjoner ved brudd, sikre at disiplinærpraksis anvendes konsistent på tvers av nivåer, vurdere kobling mellom etterlevelse og belønning/ledermål, kunne dokumentere at konsekvenshåndtering

fungerer i praksis (inkl. relevante måleparametre). Det kan variere hvor involvert Compliance er i et brudd, om virksomheten for eksempel har en varslingsrutine som innbefatter Compliance eller ei. Hvis ikke så blir Compliance gjerne involvert på et senere tidspunkt for å finne og gjennomføre mitigerende tiltak for å unngå at lignende brudd skjer igjen, samt mulig rapportering om antall brudd eller hendelser.

Det er også viktig å ha mekanismer for ad hoc-rapportering ved alvorlige brudd eller hendelser.

Eskaleringsmekanismer

Virksomheten bør ha klare og dokumenterte eskaleringsregler som definerer:

- Alvorlighetsgrader: Kategorisering av brudd etter alvorlighet (lav, middels, høy, kritisk).
- Eskaleringsveier: Hvem som skal informeres på hvert nivå, og innen hvilken tidsfrist.
- Undersøkelsesansvar: Hvem som har ansvar for å undersøke brudd på hvert alvorlighetsnivå.
- Beslutningsfullmakter: Hvem som kan beslutte korrigerende tiltak og sanksjoner.
- Ekstern varsling: Når og hvordan myndigheter, tilsynsorganer eller andre eksterne parter skal informeres.

Egenevaluering

Compliance bør gjennomføre en årlig egenevaluering og rapportere resultatene til revisjonsutvalg/styret. ISO har utviklet en egen standard som kan legges til grunn. Viser til kilder for mer info. DOJ ECCP gir som allerede nevnt også nyttig veiledning. Tre hovedspørsmål gir et naturlig rammeverk for egenevalueringen:

1. **Er programmet godt designet?** Risikovurdering, policyer, opplæring, kontroller, tredjepartshåndtering.
2. **Er programmet tilstrekkelig implementert?** Ressurser, uavhengighet, datatilgang, kompetanse og ledelsesinvolvering.
3. **Fungerer programmet i praksis?** Evne til å avdekke og respondere på brudd, læring fra hendelser, forbedring over tid.

4. Vedlegg

Vurdering av modenhet

1. Tilfeldig	«Paper compliance». Dokumenter er utarbeidet, ofte for å svare på krav fra kunder, investorer, banker eller myndigheter, men følges ikke opp. Ingen compliancefunksjon, eller funksjonen er nylig etablert. Compliance håndteres først når noe går galt.	Policyer skrevet eller kjøpt inn, men ikke kommunisert. Lite eller ingen opplæring eller kontroller. Hendelser håndteres enkeltvis uten læring.	Enkelte policyer finnes, ofte basert på maler eller kopiert fra andre. Ukjent for de fleste ansatte, ingen eier, ikke tilpasset egen virksomhet og ikke oppdatert.
2. Under oppbygging	Noe arbeid med compliance, men innsatsen er ustrukturert og personavhengig. Et ansvar er plassert, ofte som tillegg til en annen rolle (for eksempel juridisk eller økonomi). Aktivitetene er ikke risikobaserte.	Generell opplæring, gjerne årlig e-læring. Ad hoc-kontroller. Varslingskanal etablert. Sporadisk rapportering til ledelsen, gjerne på forespørsel.	Flere dokumenter finnes, men uten tydelig struktur eller hierarki. Etterleves bare delvis, og i praksis følges ofte uskrevne rutiner. Uklart eierskap, overlapp og utdaterte versjoner.
3. Etablert	Risikobasert program med definerte prosesser, roller og ansvar. Compliancefunksjonen har tydelig mandat og rapporterer jevnlig til ledelse og styre.	Dokumentert risikovurdering, risikobasert opplæring, planlagte kontroller, integritetsvurdering av tredjeparter, oppfølging av varsler, regelmessig rapportering	Etablert dokumenthierarki (policy – standard – prosedyre) med eiere, godkjenning i tråd med fullmakter, versjonskontroll og dokumentregister. Dokumentene er kjent og i hovedsak etterlevd.
4. Integrert og lærende	Compliance er bygd inn i forretningsprosesser og kultur. Datadrevet oppfølging, og programmet evalueres og forbedres systematisk.	Nøkkelindikatorer og dashbord, automatiserte kontroller, rotårsaksanalyse, kulturmåling, uavhengig evaluering, benchmarking	Krav er innarbeidet i prosesser og systemer, med sporbarhet fra lovkrav til kontroll. Dokumentverket er kompakt, brukervennlig og forenkles jevnlig basert på erfaringer.

Sjekkliste AI

Bruk av AI i virksomheten (herunder også i Compliance) eller hos tredjeparter må håndteres forsvarlig, og krever kontinuerlig fokus. Denne sjekklisten er ment som et praktisk støtteverktøy.

1. **Oversikt og klassifisering**
   Er virksomhetens utvikling og bruk av AI kartlagt og ivaretas håndtering av AI-systemets livssyklus, samt at systemene er klassifisert i tråd med risikokategoriene i EU AI Act?

2. **Roller og ansvar**
   Er ansvar for utvikling og bruk, styring og kontroll av AI tydelig definert, og er Compliance involvert i, eller har tilgang til vurdering av nye eller endrede AI-løsninger?

3. **Risikostyring og kontroll**
   Er risikoer knyttet til utvikling og bruk av AI vurdert, dokumentert og håndtert, herunder risiko for virksomheten samt risiko for påvirkning på kunder eller andre

berørte personer, eksempelvis påvirkning på grunnleggende rettigheter, diskriminering, manglende transparens og effekten av automatiserte beslutninger? Er risiko knyttet til andre særlige interessenter, miljø eller samfunn relevant?

4. **Dokumentasjon og sporbarhet**
   Foreligger det tilstrekkelig dokumentasjon som muliggjør etterprøving av AI-baserte prosesser og beslutninger?

5. **Data og personvern**
   Er datagrunnlaget korrekt/oppdatert, relevant, representativt og i samsvar med krav til personvern og dataminimering?

6. **Leverandører og tredjepart**
   Er AI-leverandører vurdert opp mot regulatoriske krav, og er nødvendige compliancekrav kontraktsfestet?

7. **Overvåking og forbedring**
   Overvåkes AI-systemer løpende gjennom livssyklusen til AI-systemet, og brukes erfaringer og hendelser til forbedring av kontroller og rammeverk?

8. **Opplæring og kompetanse**
   Er opplæring og krav til kompetanse for ledere og medarbeidere tilpasset og tilstrekkelig for å ivareta risiko knyttet til utvikling og bruk av AI?

Nyttige kilder og rammeverk

- Statement of Position from the IIAThree Lines Model – Assurance and Advice in Support of Effective Governance (2026)
- DOJ Evaluation of Corporate Compliance Programs (september 2024)
- DOJ Corporate Enforcement Policy (mars 2026)
- OECD Good Practice Guidance on Internal Controls, Ethics, and Compliance
- ISO-standarder innen corporate integrity and compliance
- EU AI Act (forordning 2024/1689)
- EU CSDDD (direktiv 2024/1760) med Omnibus I (direktiv 2026/470)
- EU CSRD (direktiv 2022/2464) med Omnibus I-endringer
- GDPR (forordning 2016/679)
- DORA (forordning 2022/2554)
- NIS2 (direktiv 2022/2555)
- Åpenhetsloven (åpenhet og arbeid med grunnleggende menneskerettigheter
- Finanstilsynets modul for intern virksomhetsstyring (30.09.2025)
- Finanstilsynets veileder til hvitvaskingsloven
- OECD retningslinjer for aktsomhetsvurderinger
- ESMA provides guidance on the compliance function under MIFID II (2020)
- Guidelines on the role of AML/CTF Compliance officers (2022)

Hold deg oppdatert. Utvid ditt faglige nettverk. 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.

IIA Norge 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.

Vil du lære mer om compliance, har vi e-kurs og fysiske praktiske kurs rettet mot de som arbeider med compliance. Vi har også nettverk for praktisk deling av erfaring, se www.iia.no.

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.iia.no eller skann QR-koden nedenfor for mer informasjon: