Veileder for Compliancefunksjonen

2. utgave 2020

Hva er governance?

Et ansvarlig samspill mellom eiere, styret og ledelse sett i et langsiktig, bærekraftig perspektiv. Formålet er å sikre at virksomheten skaper verdier, når sine mål og følger lover og regler. Utgjør de strukturer, prosesser og verktøy som brukes for å styre aktiviteter, ressurser og risiko i en virksomhet.

Internrevisjon

Styrets verktøy for å fremme og beskytte virksomhetens verdier og påse god styring og kontroll. Opererer med risikobasert tilnærming til prioritering av revisjonsoppdrag. Gir objektive bekreftelser, råd og skaper økt innsikt for styret og ledelse.

Compliance

Compliance knyttes til etterlevelse av relevant lovverk, reguleringer både nasjonalt og internasjonalt, så vel som virksomhetens interne retningslinjer. Fokus på compliance risiko og bidrar til å styrke etterlevelse og øke bevissthet i virksomheten. Lovpålagt funksjon i bank og finans.

Risikostyring

Sentralt i god governance er helhetlig, proaktiv risikostyring. Denne prosessen bidrar til å sikre best mulig beslutningsgrunnlag på strategisk nivå i virksomheten. Dekker negative konsekvenser og muligheter.

Innhold

1. Innledning

Som følge av strengere regelverk i de fleste bransjer, sektorer og land stilles det store krav til etterlevelse. Raskere endringstakt, økte krav og forventninger til åpenhet og samfunnsansvar fra omgivelsene gir store muligheter, men fører også til økt risiko. Dette gjelder både i privat og offentlig sektor. Dels vil denne konteksten innebære at virksomheter selv må bygge nødvendig tillit og justere kurs og retning i samsvar med sine behov, mål og verdier, og dels vil aktørene i og rundt virksomheten som myndigheter, sektorer/bransjer, brukere, kunder, ansatte og leverandører pålegge og stille krav til at virksomheter tar sitt ansvar på alvor.

Styret og ledelsen må derfor sikre styring og kontroll av etterlevelse fra strategisk planlegging til operativ drift på tvers av hele virksomheten. Å kartlegge, vurdere og styre relevante risikoer knyttet til etterlevelse samt vurdere hva som er akseptabel og ikke akseptabel risiko, er en sentral prosess i all virksomhetsstyring. Herunder også compliancerisiko.

Kompleksiteten i compliancerisiko-universet vil eksempelvis være avhengig av bransje, regulatoriske krav, markedet virksomheten opererer i og leverandørkjeden i og rundt virksomheten. Compliancefunksjonen bidrar til virksomhetens verdiskapning ved helhetlig styring som reflekterer virksomhetens stragegi og compliancerisikobilde. Styringen krever en risikobasert tilnærming da enhver virksomhet er eksponert for mange og ulike typer av risiko.

I denne konteksten er det er viktig å danne seg et bilde av hvilke kontrollfunksjoner styret og ledelsen kan støtte seg til i utøvelsen og oppfølgingen av etterlevelse av relevante lover og regler, samt hvilke roller som har ansvar for hva. Vil funksjonene samlet sett gi styret og ledelsen en tilstrekkelig bekreftelse på at etterlevelsesrisiko håndteres i tråd med fastsatte mål? Eller er det opplevelsen av et mer fragmentert bilde som presenteres fra funksjonene til styret og ledelsen? Hvordan kan compliancefunksjonen bidra til at virksomheten når sine mål og strategier? Forankret i en risikobasert tilnærming må compliancearbeidet tilpasses virksomhetens konkrete risikobilde og fremtidige utvikling.

Veileder for compliancefunksjonen (heretter også referert til som "compliance") har som formål å beskrive «beste praksis» for compliance uavhengig av bransje, regelverk og størrelse på organisasjon og krever ikke anvendelse av et bestemt rammeverk. Veilederen beskriver hvordan virksomheter bør innrette og tilnærme seg for å etablere hensiktsmessig og tilstrekkelig styring på området for etterlevelse av lover og regler. Veilederen er utviklet av IIA Norges Nettverk Compliance og bygger videre på 1. utgave fra 2015.

Nettverk Compliance har bestått av:

Esther Borgen, KPMG
Ann Christin Flatland, TietoEVRY
Cecilie Wetlesen Borge, Advokatfirmaet Haavind
Edle Blomquist, Sporveien AS
Mazhar Bashir Ahmad, Helse Sør-Øst
Izabella Kibsgaard-Petersen, Veidekke
Torkel Fagerli, Norges Bank
Sverre Bjertnes, Statnett
Marit Trodal, IIA Norge

2. Compliancefunksjonens oppbygning

Dette kapittelet tar for seg sentrale elementer i oppbygningen av funksjonen, herunder områder som bør forankres og godkjennes i et mandat. Compliance sin rolle, organisering og rapportering i virksomheten bør fremgå klart og tydelig.

Oppbygningen av funksjonen legger en risikobasert tilnærming til grunn og gjøres på bakgrunn av virksomhetens art, kompleksitet og størrelse.

Virksomhetens behov, styringsmodell, kultur samt organisering og øvrige målsetninger er faktorer av betydning for oppbygning og arbeid. Ledelsen har en avgjørende rolle i forankring av både mandatet til compliance og virksomhetens complianceprogram. Man bør følgelig vurdere om mandat og funksjonsbeskrivelse skal godkjennes av øverste leder og/eller styret.

Mandatet kan inngå i en funksjonsbeskrivelse, stillingsinstruks eller i et eget mandat. Uavhengig av valg bør mandatet blant annet beskrive:

- Rolle og ansvar
- Organisering
- Complianceaktiviteter

Disse elementene er nærmere beskrevet i påfølgende kapitler.

2.I Roller og ansvar

Myndighet og ansvarsområder (*«fit and proper»*)

I private virksomheter vil styret være å regne som øverste ledelse, og således bli holdt ansvarlig for at virksomheten etterlever relevante lover og forskrifter. Tilsvarende vil den øverste ledelsen, f.eks. daglig leder, administrerende direktør eller virksomhetsleder være ansvarlig i øvrige virksomheter som ikke har et styre.

Det vil være en fordel om mandatet til compliance forankres og godkjennes på øverste nivå i virksomheten, særlig dersom det er behov for uavhengig kontroll av etterlevelse. Eierskap til prosesser og styrende dokumenter bør være en del av de avklaringene som gjøres for å sikre tydeliggjøring av compliance sin rolle og ansvar.

For å sikre nødvendig myndighet, anbefales det at ansvaret for compliance legges til øverste ledelsesnivå, og at personen som utpekes og rapporterer til dette nivået, har tilstrekkelig erfaring og faglig, personlig og profesjonell autoritet. Et begrep som sammenfatter dette er «fit and proper». I denne konteksten handler dette om om personlig egnethet så vel som faglig kompetanse. Videre bør særskilte forhold som krever en større involvering avklares, f.eks. granskninger av uregelmessige forhold.

Compliance må være tilpasset arten, kompleksiteten og størrelsen til virksomheten. Ledelsen bør nedfelle hvordan man sikrer tilstrekkelig fagkompetanse, uavhengighet, bransjekunnskap og ressurser til å kunne ivareta oppgaver beskrevet i mandatet.

Eksempler på ulike complianceroller kan typisk være:

- Leder for Compliance/Chief Compliance Officer
- Ethics & Compliance Officer
- Compliance Manager
- Compliance Koordinator
- Rådgiver Compliance/Forretningsetikk
- Personvernombud/Data Protection Officer

Belønning og incentiver

Virksomheten må ha etablert en belønningspolitikk og incentivmodell som bidrar til å sikre objektivitet, integritet og uavhengighet i arbeidet. Resultatavhengige komponenter som kan føre til interessekonflikter, må unngås.

Belønning må samtidig sikre at det er mulig å besette compliance med personer med nødvendig kompetanse, erfaring og faglig tyngde.

2.II Organisering

Plassering og rapporteringsansvar

Hvilken plassering som er mest hensiktsmessig, avhenger av fokusområder og hvilke andre miljøer og funksjoner compliance samhandler med og rapporterer til internt. Regulatoriske krav eller bransjestandarder kan også legge føringer for hvor compliance bør plasseres. Den organisatoriske plasseringen kan derfor variere, avhengig av virksomhetsspesifikke forhold og bransje-/sektorkrav.

Følgende hensyn kan være relevante å vurdere når ledelsen skal beslutte organisatorisk plassering:

1. Regulatoriske krav eller bransjestandarder.
2. Prioriterte fagområder/arbeidsoppgaver som compliance skal dekke.
3. Hvorvidt hovedvekten legges på kontrolloppgaver/testing av etterlevelse/undersøkelser eller bistand og/eller preventive, forebyggende tiltak.
4. Krav til funksjonens uavhengighet og integritet.
5. Hvorvidt tydeliggjøring av mandat og rapporteringslinjer kan kompensere for eventuelle ulemper ved valgte plassering.

Rapportering og eskalering

Compliance må rapportere til et nivå i virksomheten som gjør det mulig for funksjonen å ivareta sitt ansvar og samtidig sin uavhengighet til linjen/beslutningstakere. Uavhengig av hvordan den formelle plassering og organisering er lagt opp, er det hensiktsmessig at compliance har en løpende rapportering til virksomhetens øverste ledelse og/eller styrende organer, herunder at samhandling og grensesnitt mot andre funksjoner (stabsfunksjoner og linjen) er tydelig avklart.

Rapporteringsfrekvensen bør være minst en gang årlig. Ofte vil det være behov for en hyppigere rapporteringsfrekvens, men dette må tilpasses virksomhetens behov og risikobildet (ny virksomhet, nytt regelverk eller vesentlige endringer i eksisterende regelverk, nye systemer/prosjekter, nytt produkt e.l).

Det anbefales videre at compliance i tillegg rapporterer umiddelbart når resultatet av kontroller, alvorlighetsgrad av brudd på regler el. tilsier det, basert på tydelig etablerte eskaleringsregler.

I noen virksomheter er compliance organisert i en separat stabsenhet som rapporterer til øverste ledelsesnivå, på linje med andre stabsenheter. En fordel med dette er at det signaliseres at compliance har en klar objektiv og uavhengig rolle og ikke vil bli identifisert med andre linje-funksjoner i virksomheten. En av ulempene er at det kan bli vanskeligere i det daglige å samarbeide med og dra nytte av felles prosesser, metoder, verktøy og erfaringer i andre funksjoner.

Enkelte virksomheter har plassert compliance i stab for virksomhetsstyring e.l. og på denne måten samlet all risikostyringsrelaterte oppgaver og ansvar i ett miljø. Fordelen er at funksjonene kan dra nytte av felles prosesser, metoder, verktøy og erfaringer, samt bidra til å sikre et bedre samarbeid mellom funksjonene. For førstelinjen kan det være enklere med ett felles kontaktpunkt for spørsmål om risikostyring og etterlevelse. En potensiell ulempe er ulike krav til utøvelse av de ulike funksjonene, hvor hver av funksjonene har ansvar for å kontrollere deler av arbeidet i de andre stabsfunksjonene.

Virksomheter med en egen juridisk avdeling kan velge å plassere compliance i denne, ofte med rapportering til juridisk direktør. Dette kan være hensiktsmessig, gitt at den juridiske avdelingen har ansvar for fortolkning av regulatoriske krav så som lover, forskrifter og vedtak fattet av offentlige myndigheter og som ligger innenfor compliance sitt mandat.

Det kan imidlertid oppstå interessekonflikter dersom en juridisk avdeling bare bistår med den forretningsmessige driften, herunder inngåelse og forvaltning av kontrakter/avtaler. Her bør andre muligheter vurderes slik at compliance ikke kontrollerer eget arbeid eller blir identifisert med første linje. Enkelte virksomheter har i slike tilfeller gitt leder av compliance en mulighet til å rapportere direkte til det øverste ledelsesnivået (såkalt stiplet rapporteringslinje), slik at plasseringen likevel kan være forsvarlig også fra et uavhengighetsperspektiv.

Her vil det kunne være bransjeforskjeller som for eksempel:	
Industribedrifter	I industribedrifter vil funksjonen ofte være underlagt juridisk direktør, men ha compliancemedarbeidere med et begrenset ansvar for å arbeide med konkrete regelverk slik som anti-korrupsjon, konkurranserett osv. Funksjonen vil ofte prioritere rådgivende bistand og arbeide mindre med å teste etterlevelse.
Finansnæringen	Regulert gjennom bl.a. finanstilsynets veiledere og krav og forventninger fra tilsynet. Compliance vil eksempelvis ha større eierskap til å gjennomføre monitorering/test og uavhengig kontroll av etterlevelsen.

Det forekommer også at compliancerollen ivaretas av internrevisjonen. En slik løsning påvirker internrevisjonens uavhengighet til compliancearbeidet og representerer verken en internrevisjon som en uavhengig tredjelinjefunksjon eller en compliancefunksjon i andrelinjen.

Lokale compliancemedarbeidere i utvalgte enheter i virksomheten kan bidra til en effektiv og forsvarlig utøvelse av compliancearbeidet. De kan fungere som selvstendige complianceansvarlige og/eller som den sentrale stabsfunksjonens forlengede arm ut i organisasjonen, og ivareta oppgaver innen rådgivning, opplæring, monitorering/testing av etterlevelse og rapportering. Det er vanlig at slike roller utpekes i datterselskaper i et større konsernselskap.

I mange virksomheter kan compliancearbeidet i lokale enheter ivaretas av medarbeidere som har andre roller. For å sikre at oppgavene utføres tilfredsstillende må ansvar, oppgaver, rapporteringslinjer og samarbeid med stabsfunksjonen være tydelig avklart og definert.

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.

De tre forsvarslinjer

En utbredt modell for å beskrive styrings- og kontrollstrukturen i virksomheten på et overordnet nivå er «de tre forsvarslinjer». Denne modellen illustrerer ulike roller og ansvar knyttet til risikotaking, risikostyring og risikokontroll, og kan bidra til å øke bevisstheten rundt hvilke funksjoner en virksomhet bør ha på plass i en effektiv styringsmodell. Modellen har vært kritisert, blant annet fordi dens beskrivelse av tre predefinerte forsvarslinjer ikke er tilstrekkelig fleksibel og effektiv i forhold til virksomhetenes behov for en dynamisk styringsmodell. Den kan også oppfattes å ha mest oppmerksomhet på kontrollperspektivet samt å beskytte verdier fremfor kontinuerlig forbedring av kontrollene og verdiskapning. De tre forsvarslinjer er imidlertid en egnet modell å ta utgangspunkt i dersom virksomhetens styre og/eller ledelse har behov for å etablere en uavhengig kontroll av complianceaktivitetene i virksomheten. I praksis vil man se at ulike bransjer opererer med ulike former for organisering. God forankring og bevissthet på tvers av forsvarslinjene er sentrale suksessfaktorer for å skape god styring og kontroll.

Modellen skiller mellom tre grupper (eller linjer) som normalt inngår i en effektiv styringsmodell:

- Funksjoner som eier og håndterer/behandler risiko (første linje)
- Funksjoner som overvåker og følger opp risiko (andre linje)
- Funksjoner som gir uavhengig bekreftelse (tredje linje)

Første forsvarslinje eier og håndterer/behandler risiko knyttet til den daglige driften av virksomheten. Linjeledere og medarbeidere på ulike nivåer i en virksomhet fatter daglig beslutninger og må ta stilling til potensielle risikoer knyttet til disse. Ulike beslutninger omfatter ulike typer risiko, herunder også compliancerisiko samt compliancebrudd. I førstelinjen gjennomføres konkrete kontrolltiltak som skal sikre etterlevelse av eksterne og interne krav. Dette innebærer at en linjeleder har ansvar for å gjennomføre risikovurderinger, utarbeide nødvendige rutiner, følge opp egne medarbeidere, samt andre kontrolltiltak.

Andre forsvarslinje bistår og veileder linjeledere og medarbeidere i første forsvarslinje, og har ikke myndighet til å fatte forretningsmessige beslutninger. Det er dog hensiktsmessig at andre linjen er integrert i strategiske og operasjonelle beslutningsprosesser, slik at de kan veilede og bistå førstelinjen mest mulig effektivt. Rådgivning og kontrollaktiviteter i andre linje utføres som oftest av en stabs- og/eller kontrollfunksjon med ansvar for økonomi, compliance, risikostyring, kvalitet og sikkerhet, HMS med videre. Compliance har ansvar for å overvåke kontrollen i første linje gjennom for eksempel utarbeidelse av felles rammeverk for compliancerisiko og rapporteringsrutiner. Andre linje kan også iverksette egne risikovurderinger og granskninger av faktisk etterlevelse i første linje.

Tredje forsvarslinje gjennomfører objektiv og uavhengig bekreftelse og utøves av internrevisjonen. Internrevisjonen kan blant annet vurdere om virksomhetens prosesser for styring og kontroll er hensiktsmessige og om internkontrollen fungerer etter sin hensikt, herunder om første og andre forsvarslinje effektivt bidrar til at virksomheten når sine mål. Styret og toppledelsen kan også be om uavhengige vurderinger av en ekstern tredjepartsrevisor.

Styret og den øverste ledelsen har integrerte roller i modellen. Den øverste ledelsen er ansvarlig for utforming, implementering og forvaltning/utvikling av internkontroll innenfor rammene fastsatt av styret. Styret på sin side skal påse at ledelsen har etablert hensiktsmessig og tilstrekkelig internkontroll. Partene har derfor kollektivt ansvaret for å etablere og definere strategier og mål for å oppnå disse forutsetningene, og etablere styringsstrukturer for å håndtere compliancerisiko. Ledelsen må derfor utøve sitt arbeid på complianceområdet på en måte som understøtter effektiv virksomhetsstyring, risikostyring og internkontroll ettersom de har det endelige ansvaret for alle aktivitetene i første og andre forsvarslinje.

Uavhengighet og objektivitet

Det anbefales at personer som jobber i og er ansvarlig for virksomhetens compliancefunksjon i størst mulig grad skal organiseres uavhengig av den operative virksomheten (linjen). Dette innebærer eksempelvis at funksjonen ikke skal utføre eller være ansvarlig for den operasjonelle driften, eller at personer som arbeider i eller for en stabsfunksjon ikke skal arbeide i en enhet de er satt til å kontrollere. Uavhengigheten er ikke til hinder for at compliance kan ha en rådgivende funksjon overfor førstelinjen. Vektleggingen mellom rådgivende og kontrollerende oppgaver kan variere mellom virksomheter og over tid innen den enkelte virksomhet. Det er uansett viktig at compliance er bevisst hvilken rolle funksjonen ivaretar til enhver tid, og at den ikke kontrollerer seg selv.

Personer som har vært ansatt i den operasjonelle driften, bør i tillegg pålegges en karensperiode før vedkommende kan utføre kontrolloppgaver for den aktuelle delen av virksomheten vedkommende tidligere arbeidet i. Tilsvarende kan man tenke seg at en person som midlertidig utfører oppgaver hvor det kan stilles spørsmål ved objektivitet og uavhengighet, fritas for kontrolloppgaver innenfor gjeldende område i en karensperiode. Her kan de etiske retningslinjene for internrevisjon gi verdifull veiledning.

Tabellen under kan være et nyttig verktøy for å tydeliggjøre kjerneoppgaver compliance har ansvar for og oppgaver som kan vurderes og bør unngås dersom compliance har et kontrolloppgaver.

Kjerneoppgaver	Kan vurderes/ Krever kontrolltiltak	Unngås
Gi bekreftelse på ledelsens prosess for styring av compliance risiko	Fasilitere prosess for identifisering og evaluering av compliancerisiko	(Leder)ansvar for styring av compliancerisiko
Gi bekreftelse på at evaluering av compliancerisiko er riktig	Coache ledelsen i hvordan respondere på risiko	Implementere tiltak på vegne av ledelsen
Evaluere og rapportere sentrale compliancerisiko til ledelse	Koordinere complianceaktiviteter i virksomheten	Fatte beslutninger om type tiltak
Gjennomgå styring av sentrale compliancerisiko	Konsolidere rapportering til ledelse vedr. compliancerisiko	Bekreftelse til ledelsen
	Utvikle, opprettholde og videreutvikle compliance-styringsprogram	Påtvinge risikostyringsprosesser
	Ambassadør for compliance program og kulturbygging	Sette risikoappetitt
	Utvikle strategi for styregodkjennelse	

Ressurser og kompetansebehov

Ressurssituasjonen og kompetansebehovet, herunder behov for opplæringstiltak, bør vurderes jevnlig, og det anbefales at dette gjøres minst en gang i året i form av egenevaluering.

Av og til vil det også være behov for å trekke annen kompetanse inn i compliancearbeidet eller at andre områder/ funksjoner også utfører oppgaver relatert til etterlevelse. Dette arbeidet bør koordineres og vurderes samlet. Eksempelvis fikk mange compliancefunksjoner ved innføring av GDPR et behov for tverrfaglig kompetanse innen områder som risikostyring, informasjonssikkerhet og regelverksforståelse.

> ***Tips!***
> *Krav til kompetanse og ressurser kan også fremgå av regulatoriske krav så som kravene til personvernombudet i personopplysningsloven og compliancekontrollfunksjonen i retningslinjer gitt av Finanstilsynet for verdipapirforetak .*

3. Complianceaktiviteter

Dette kapittelet tar for seg de viktigste elementene i et complianceprogram. De samlede aktivitetene bør angis i et helhetlig complianceprogram eller plan, og må tilpasses den konkrete virksomhet. Compliance vil ikke nødvendigvis være den utøvende funksjonen som har ansvar for, eller gjennomfører alle aktivitetene som nevnes i kapittelet. For å sikre nødvendig dekning og minst mulig dobbeltarbeid, bør compliance dele informasjon og samordne aktiviteter med typisk tilgrensede områder som juridisk avdeling, risikostyringsenheter, HMS- og kvalitetsansvarlig, HR-ansvarlig, økonomiavdeling, internrevisjonen samt enkeltpersoner i førstelinje. Det viktigste vil være at hovedaktivitetene er ivaretatt samlet sett og at compliance bidrar i relevante prosesser som eventuelt utføres av andre funksjoner i virksomheten.

Complianceprogram og risikobasert tilnærming

For effektiv prioritering av oppgaver og ressursbruk skal compliance legge til grunn en risikobasert tilnærming i sitt arbeid. Kartlegging av risikoområder og risikovurderinger er en forutsetning for at et complianceprogram er tilpasset og støtter opp om virksomhetens mål og strategier. Gjennom risikovurderinger avdekkes hvilke aktiviteter og områder som trenger retningslinjer og rutiner i dag, og hvordan compliancearbeidet må tilpasses virksomhetens konkrete risikobilde og fremtidige utvikling.

Øverste ledelse har det overordnede ansvaret og bør beslutte hvor høy risiko som aksepteres på ulike områder i virksomheten. For enkelte områder og bransjer er det lovpålagt at virksomheten skal gjennomføre en slik kartlegging og risikovurdering. Risikovurderingen bør gjennomføres jevnlig, minst årlig, og ved store endringer i risikobildet.

Kartlegging og vurdering av compliancerisiko kan være en egen aktivitet. I de virksomheter hvor det er relevant bør den også inngå som en integrert del av virksomhetens kartlegging av operasjonell risiko. En vurdering av compliancerisiko tar utgangspunkt i eksterne lover og regler, herunder også interne føringer som gjelder for virksomheten. Faktiske brudd som kan få vesentlige konsekvenser, for eksempel i form av offentlige sanksjoner, økonomisk tap, erstatningskrav og tap av omdømme er ofte i scope. Det gjøres en nærmere vurdering av hvilke områder i virksomheten

(produktområder, fagområder, geografiske områder) som er mest eksponert for de identifiserte compliancerisikoene. Eksempler på compliancerisiko kan være brudd på lovgivning knyttet til korrupsjon, arbeidsmiljø, menneskerettigheter, personvern og hvitvasking. Det kan også være risiko for brudd på områder som ikke nødvendigvis er regulert av lov, men som vil utgjøre en betydelig tap av omdømme.

Brudd på virksomhetens etiske retningslinjer, samfunnsnormer eller kundekrav er eksempler på dette. I tillegg vil det være naturlig å vurdere risikodrivere som bransjekultur, bedriftskultur (holdninger, verdier, budskap fra ledelsen) og incentivsystemer, samt effektiviteten til interne kontrolltiltak. Videre bør resultatet av en slik vurdering inneholde tilhørende tiltak som kan være nødvendig for å hindre at ønsket risikonivå overskrides.

Basert på risikovurderingen bør det utarbeides en periodisk handlingsplan og/eller årshjul for compliancearbeidet. Dette defineres ofte som en complianceplan. En risikobasert plan er et nødvendig verktøy for effektiv styring av ressurser og compliancerisiko. Planen bør gi en oversikt over alle planlagte aktiviteter og oppgaver som skal gjennomføres i perioden knyttet til hensiktsmessig styring av compliancerisiko. I tillegg vil det være hendelsesdrevne aktiviteter og adminstrative oppgaver knyttet til blant annet råd og veiledning om innføring av nytt regelverk og forvaltning av styrende dokumenter. Planen bør forankres hos den øverste ledelsen og koordineres med andre styringsprosesser og relevante organisatoriske enheter og tilpasses det overordnende complianceprogrammet.

Styrende dokumenter

Virksomheten bør ha et styringssystem som er forankret i virksomhetens visjon, verdier og strategi. Styringssystemet skal beskrive og dokumentere styringsstrukturen (organisering, roller og ansvar), og rammeverket for virksomhetens overordnede styringsprosesser. Styringssystemet er ofte bygget opp ved hjelp av et overordnet dokumenthierarki bestående av styrende dokumenter hvor policyer og retningslinjer på øverste nivå understøttes av mer detaljerte instrukser, rutiner og prosedyrer med tilhørende stillingsinstrukser, rollebeskrivelser, prosesskart/flytskjema og sjekklister på underliggende nivå.

Utforming av styrende dokumenter bør ta utgangspunkt i nevnte risikovurderinger slik at de står i forhold til, samt adresserer, de risikoer virksomheten står overfor. Compliance skal også være en pådriver for å sikre at virksomheten etablerer og vedlikeholder styrende dokumenter på områder som er eksponert for høy compliancerisiko og er i samsvar med lover/regler.

Eksempler kan være dokumenter som etiske retningslinjer, prosedyrer for varsling og gransking, antikorrupsjonsprogram og instrukser for hvitvasking. Noen overordnede dokumenter, som eksempelvis etiske retningslinjer, vil det være naturlig å forankre hos den øverste ledelse og/eller styret. Compliance vil ofte ha ansvar for å sikre at styrende dokumenter som er tilknyttet område, til enhver tid er oppdatert i henhold til gjeldende regelverk**.**

Styringsdokumenter og internt rammeverk må være tilgjengelig for alle medarbeidere, og dokumentene må være gjenstand for jevnlige gjennomganger og oppdateringer. Det er videre ansett som god praksis at medarbeidere gis muligheten til å kunne komme med forbedringsforslag til virksomhetens interne styringsdokumenter og gis opplæring i disse.

Kommunikasjon, opplæring og rådgivning

For å sikre en høy bevissthet rundt compliance og compliancerisiko, samt legge til rette for kontinuerlig læring og forbedring i organisasjonen, bør man utarbeide en plan for kommunikasjon rundt temaer innenfor compliance, til personer både i og utenfor virksomheten. Eksempler på sistnevnte kan være leverandører, kunder, myndigheter og andre som virksomheten samhandler med. En kommunikasjonsplan kan inngå som en del av årshjulet til compliance, men det kan også utarbeides i forbindelse med kommunikasjon av større endringer. En slik plan bør si noe om hva som skal kommuniseres, til/fra hvem, hvordan og når.

Relevant og tilpasset opplæring er vesentlig for å bygge en ønsket compliancekultur. Compliance bør således utarbeide og vedlikeholde opplæringsmateriell og planer for opplæring i virksomheten. Formålet er å sette medarbeidere og andre interessenter inn i relevante eksterne og interne regelverk samt gjøre dem istand til selv å identifisere og håndtere compliancerisiko. Opplæring innenfor områder med høy iboende compliancerisiko bør være obligatorisk. Det kan også være nødvendig å tilpasse opplæringens omfang, innhold og hyppighet til forskjellige grupper av medarbeidere. Opplæringen kan være i form av presentasjon av regelverk, demonstrasjon av verktøy, case-diskusjoner og dilemmatrening, og kan gjennomføres som workshops, klasseromsundervisning, én-til-én opplæring eller e-læring.

For å bygge en compliancekultur er det viktig at ledelsen i virksomheten fremstår som rollemodeller. Ledelse her relaterer seg til alle ledelsesnivåer og ikke bare den øverste ledelsen. Ledelsen bør være synlige og aktive bidragsytere både ved å 'sette regler' og ved å følge dem («conduct at the top»).

Ved å ha compliance som tema i ledermøter og ved øvrig oppfølging, kan ledelsen sette en standard for virksomhetens arbeid med compliance. Videre må ledere engasjere seg i opplæring og kommunikasjon av etiske retningslinjer, policyer og prosedyrer, samt hvordan disse påvirker arbeidshverdagen til medarbeiderne. Ledelsen må få dedikert opplæring i aktiviteter der de har en særskilt rolle, og likeledes må gjelde medarbeidere.

Opplæring av medarbeidere skal dokumenteres, og innholdet i opplæringen må jevnlig evalueres. Det bør spesielt vurderes hvilken opplæring som skal være obligatorisk for nyansatte, ledere, innleide og leverandører. Det kan føres en logg over hvem som har gjennomført obligatorisk opplæring, eksempelvis gjennom å føre liste over deltakere eller ved bruk av digitale opplærings-plattformer. Linjeledere har ansvar for at egne medarbeidere deltar i relevant opplæring. Statusoppfølging bør være en del av årsplanen til compliance.

Forebygging og bevisstgjøring er sentralt. Rollen som rådgiver er derfor svært viktig for compliance. Compliance blir i økende grad brukt som 'sparringspartner' for ledelsen og andre funksjoner. Eksempler på når complianceopplæring er relevant, kan være ved potensielle interessekonflikter, prosesser knyttet til samarbeidspartnere, tredjeparter og andre forretningsforbindelser, evaluering av risiko ved nye produkt- og tjenesteområder, geografisk ekspansjon mv. Vurderingene bør dokumenteres og kommuniseres på en måte som sikrer læring samt en enhetlig praksis på tvers av virksomheten.

Håndtering av samarbeidspartnere, tredjeparter og andre forretningsforbindelser

Samhandling med samarbeidspartnere og tredjeparter, samt andre forretningsforbindelser, kan utgjøre en risiko for å bli innblandet i korrupsjon eller andre former for økonomisk kriminalitet. Risikoer kan være skatteunndragelse, hvitvasking eller sosial dumping, som igjen kan føre til anklager om medvirkning og/eller omdømmetap. I senere tid har man sett at flere myndighets-organer og andre organisasjoner stiller strengere krav til virksomhetens eget ansvar for egen verdikjede. Det gjelder også virksomhetens håndtering av tredjeparter. Compliance-programmet må omfatte hvordan man skal håndtere tredjeparter, inkludert krav og metode for utvelgelse, kontrahering og oppfølging. Eksempler på tredjeparter kan være kunder, samarbeidspartnere, agenter, innleide konsulenter/rådgivere og underleverandører.

Compliance-programmet vil typisk avklare hvilke aktiviteter som skal gjennomføres avhengig av gitt risikoeksponering og type motpart. For enkelte områder og bransjer er håndtering av tredjeparter lovpålagt. Et eksempel er hvitvaskingsloven og tilhørende krav til kundetiltak.

Compliance har ofte ansvaret for et risikobasert system for integritetsundersøkelse av samarbeidspartnere, også kalt «Integrity Due Diligence» (IDD). IDD er undersøkelser og vurderinger av motparter, inkludert dets eiere og nøkkelpersoner (som styremedlemmer og ledere). IDD gjennomføres for å skaffe en rimelig sikkerhet om deres integritet og forretningsetikk. En slik prosess bør være risikobasert og gjennomføres som en del av utvelgelsen av samarbeidspartnere og andre forretningsforbindelser. Et viktig ledd i vurderingen er hvorvidt det i det hele tatt skal inngås en avtale med motparten. Det kan også tas forbehold eller stilles særskilte krav i kontrakt, og/eller om det skal iverksettes risikoreduserende tiltak i oppfølgingen av motparten. Dersom en underleverandør ikke kan dokumentere opplæring innenfor compliance, kan man eksempelvis kreve at underleverandøren skal gjennomføre opplæring tilsvarende den som gis til medarbeidere i det kontraherende selskapet.

Forventninger og krav til samarbeidspartnere fremgår gjerne i egne retningslinjer. Retten til å revidere etterelevelse av disse kravene bør også fremkomme her. Dette gir virksomheten anledning til å verifisere samarbeidspartneres etterlevelse av de krav som følger av retningslinjene.

> ***Tips!***
> *OEDC har også egne retningslinjer for aktsomhetsvurderinger, se:*
> *https://www.responsiblebusiness.no/oecds-retningslinjer/*

Varsling og rapportering av uønskede hendelser/avvik

Alle virksomheter skal ha en forsvarlig varslingsordning i tråd med kravene i arbeidsmiljøloven. Compliance bør påse at det er etablert en tilfredsstillende varslingsordning i virksomheten. Det bør vurderes om virksomhetens varslingskanal skal legge til rette for anonym varsling, og om den skal være tilgjengelig for eksterne, eksempelvis via virksomhetens hjemmeside.

Det kan være naturlig at compliance har det faglige ansvaret for etablering og oppfølging av en varslingsordning. Compliance kan også være en egnet kanal for å motta varsler samt ha ansvar for å motta og påse at varslene undersøkes, følges opp og lukkes på en forsvarlig måte. Denne rollen kan også ivaretas av andre funksjoner i virksomheten, eksempelvis internrevisjon.

Det er viktig med tydelige grensesnitt mellom de ulike funksjonene som er del av varslings-ordningen og den videre prosessen. En virksomhet kan også velge å outsource ved å oppnevne en ekstern varslingsfunksjon.

En del av internkontrollsystemet i virksomheten er å legge til rette for rapportering av uønskede hendelser og avvik, samt relevante nestenhendelser/nestenulykker. Dette bør også inkludere compliancebrudd. Formålet er å avdekke om enkelthendelser/avvik skyldes tilfeldige feil eller har en mer systematisk og gjennomgående karakter, og om det skyldes bevisste eller ubevisste feilvurderinger. Ved å utarbeide en oversikt over enkeltstående avvik eller varsler som hver for seg har små konsekvenser, kan man bidra til å avdekke systematiske svakheter som samlet vil kunne ha vesentlige konsekvenser. Formålet med en slik oversikt er å bidra til at compliance kan identifisere risikoer og foreslå korrigerende og forebyggende tiltak, samt vurdere om retningslinjer, opplæring, rutiner og prosedyrer er tilstrekkelig effektive. Dokumentasjonen kan også bidra til å avdekke om det er enkelte avdelinger eller områder som skiller seg ut, og hvor det er nødvendig å iverksette spesifikke eller generelle tiltak for å avhjelpe manglende etterlevelse av regelverket.

> ***Tips!***
> *Arbeidstilsynet har også egne retningslinjer for varsling, se: https://www.arbeidstilsynet.no/tema/varsling*

Monitorering og kontroll

Virksomheten skal evaluere og teste internkontrollen for å se om den er hensiktsmessig og virker i praksis. Monitorerings- og kontrollaktiviteter skal være særlig oppmerksomme på eventuelle faktiske brudd, men også forbedringsmuligheter og effektivitetsgevinster knyttet til potensielle svakheter og nye risikoområder. Gjennomførte kontroller må dokumenteres. Dette skaper sporbarhet og etterprøvbarhet ved senere kontroll. Kontroll utføres av kontroll- og tilsynsorganer som internrevisjon, ekstern revisjon, tilsyns- og andre myndighetsorganer, og til og med overfor kunder/leverandører. Virksomheten kan også selv evaluere sitt arbeid.

Compliance skal monitorere og kontrollere effektiviteten og kvaliteten av internkontroll uført i førstelinje for å sikre etterlevelse av relevante lover, forskrifter og internt regelverk. Dette vil bidra til å avdekke om styrende dokumenter er mangelfulle eller operasjonaliseringen har uteblitt, om kontrollene er designet på en hensiktsmessig måte, om de er i samsvar med gjeldende regulatoriske krav og om de etterleves. Virksomhetens risikoeksponering avgjør omfanget av monitoreringen.

I tillegg til løpende oppfølging er aktuelle metoder for monitorering og kontroll frittstående evalueringer, dokumentasjonsgjennomgang, stikkprøver, spørreundersøkelser, intervjuer eller undersøkelsesaktiviteter og evalueringer. Aktivitetene kan gjennomføres separat, men det kan også her være hensiktsmessig å integrere dem i andre prosesser i virksomheten, eksempelvis inkludere relevante spørsmål som del av en medarbeiderundersøkelse.

For å sikre at compliance ivaretar sitt mandat bør det legges til rette for en evaluering eller periodisk gjennomgang. En slik gjennomgang bør gjennomføres av en uavhengig funksjon, eksempelvis i form av revisjon, gap-analyse mot beste praksis eller modenhetsvurderinger.

Rapportering og dokumentasjon

Dokumentasjon er en viktig del av compliancearbeidet. Dokumentasjon skal sikre sporbarhet og etterprøvbarhet for hva som er gjort, og implisitt ikke gjort, for å forebygge eller håndtere compliancerisiko. Manglende dokumentasjon vil kunne oppfattes som manglende etterlevelse. Det som ikke er dokumentert, vil ofte bli betraktet som ikke gjort, og det kan få konsekvenser i møte med rapporteringskrav fra myndigheter, granskninger eller rettslige prosesser. En viktig del av virksomhetens complianceprogram er å nedfelle hvordan man skal dokumentere de aktivitetene som gjennomføres, eksempelvis gjennom årsrapport, complianceplaner, liste over deltakere på opplæring e.l.

Virksomheten må etablere en hensiktsmessig rapportering fra compliance. Rapportene skal gi ledelsen og styret, samt eventuelle komitéer/utvalg, relevant og korrekt informasjon om forhold i virksomheten som er definert innenfor compliance sitt mandat, ansvarsområde og arbeidsoppgaver.

Rapportene inngår i grunnlaget for styrets og ledelsens totale vurdering av internkontrollen og vurdering av behovet for eventuelle tiltak på ulike områder. Rapportering skal dessuten tjene som dokumentasjon for å sikre sporbarhet og etterprøvbarhet internt og eksternt overfor tilsyns-myndigheter om beslutninger og prosesser som har funnet sted. Rapporteringen fra compliance kan integreres i annen virksomhetsrapportering så lenge funksjonens uavhengighet blir ivaretatt.

Compliance bør rapportere til den øverste ledelsen og styret minst en gang årlig, men det vil ofte være hensiktsmessig med hyppigere rapporteringsfrekvens. Det kan også legges til rette for eskaleringsmekanismer hvorpå funksjonen skal rapportere umiddelbart når alvorlighetsgrad, eksempelvis av resultatet av kontroller, brudd på regelverket, revisjoner, tilsynsmerknader e.l., tilsier det.

Typiske temaer for rapportering vil være:

- Vurdering av compliancerisiko overordnet
- Tiltak for å redusere compliancerisiko
- Varslede og pågående aktiviteter, herunder status på tiltak for oppfølging
- Status for etterlevelse på prioriterte områder – resultater fra monitorerings- og kontrollaktiviteter
- Uønskede hendelser
- Rapporter fra offentlige tilsynsorganer
- Eksterne hendelser med relevans
- Forankring av årshjul og strategiske initiativ for compliancefunksjonen
- Nytt regelverk og implikasjoner på drift, systemer og prosesser
- Årsrapport fra compliance

Rapportering fra compliance er også en måte å sikre kontinuerlig forbedring og læring på tvers av virksomheten. Det kan derfor være hensiktsmessig å legge til rette for periodisk rapportering til alle ledelsesnivåer, samt øvrige deler av virksomheten.

Teknologi som muliggjører

Det er en rekke teknologiske løsninger som støtter opp under arbeidet. Teknologi kan gi bedre dokumentasjon og gjøre det mulig å koble ulike typer styringsinformasjon. Man kan effektivisere ressursbruk eksempelvis ved å redusere bruken av manuelle testprosesser, samt implementere dashboardsløsninger som gir compliance et overblikk over virksomhetens risikoeksponering i sanntid. Man ser også flere eksempler på at compliance tar i bruk kunstig intelligens og maskinlæring for å ytterligere styrke sitt arbeid.

Eksempler på teknologiske løsninger kan være både virksomhetsomfattende, eksempelvis felles GRC-verktøy, hendelses- og avviksmonitorering, compliancerisikostyring eller systemer rettet mer mot konkrete aktiviteter som oppfølging av varslingsportal, opplæringsaktiviteter, spørre-undersøkelser og screening av tredjeparter mot relevante kilder (PEP/sanksjoner/negativ presse).

Ved å ta i bruk teknologiske løsninger vil compliance ikke kun minske antallet manuelle prosesser samt få økt sporbarhet, men man vil også få innhentet nyttig styringsdata fra hele virksomheten som vil være til stor hjelp for compliance i å oppdage endringer og nye trender innenfor virksomheten.