

# Om IIAs veileder for compliancefunksjonen

Nettverk Compliance

v/Edle Blomquist

Sporveien AS

[edle.blomquist@sporveien.com](mailto:edle.blomquist@sporveien.com)

Tel. 916 24 961

---

# Agenda



# Sporveien



## FAKTA:

### TRIKKEN:

6 linjer  
72 trikker  
2 baser

### T-BANEN:

5 linjer  
115 togsett  
2 baser

### UNIBUSS:

Rute- og turbuss  
Ekspress- og flyplassbuss

### INFRASTRUKTUR OG PROSJEKTER

Skinner, stasjoner, bygg,  
tuneller, eiendom, signal-  
og sikringssystemer

### SPORVEIEN:

3 734 ansatte  
4 755 mill. kr i omsetning  
267 mill. reisende

RUTER BESTILLER KOLLEKTIV-  
TRAFIKK FRA SPORVEIEN

## RESULTATER:

### TRIKKEN:

51 mill. reiser  
4,6 mill. vognkm.  
98 % kundetilfredshet

### T-BANEN:

118 mill. reiser  
9,1 mill. togkm.  
98 % kundetilfredshet

### UNIBUSS:

98 mill. reiser  
41,4 mill. busskm.  
97 % kundetilfredshet

### INFRASTRUKTUR OG PROSJEKTER

Oppgradering og  
modernisering.  
Bevaring av verdier.



Samfunnsoppdrag	Mer kollektivtrafikk for pengene
Visjon	Sammen gjør vi kollektivtrafikken til et naturlig førstevalg
Strategi	Innen utgangen av 2020 skal Sporveien være: «Beste nordiske løsning på effektiv og miljøvennlig persontransport»
Verdier	Pålitelig – Engasjert – Samhandlende

# Compliance i Sporveien



- > Del av Konsernjuridisk avdeling
- > Hovedoppgavene:
  - Råd og veiledning for å forebygge uønskede hendelser og korrupsjon
  - Etisk regelverk
  - Opplæring
  - Varslingssaker
  - Habilitetsvurderinger
  - Etske krav til leverandører og sosialt ansvar i leverandørkjeden
  - Konsernpolicy for risikostyring og internkontroll
  - Risk Management Forum
  - Årlig risikorapportering til konsernledelse og styre
  - Compliancerapportering og –årshjul
  - Styringsinstrukser
  - Oppfølging risikokartlegging og revisjoner
  - GDPR - personvern
  - Presentasjoner, foredrag

# Hvorfor veileder i compliance



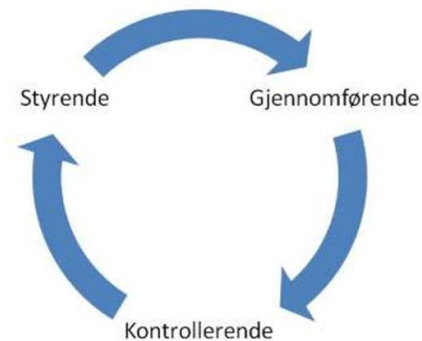
- Nettverk Compliance opprettet i 2014
- Møteplass der teoretiske og praktiske problemstillinger kan diskuteres
- Uavhengig av bransje og virksomhet
- Behov for compliancefunksjon vil variere
- Drivere er regulatoriske krav og eksponering for risiko for brudd på lover/forskrifter
- Veileder lansert 2015
  - Innføring i grunnleggende prinsipper, dvs. omhandler ikke evt. lovkrav til compliancefunksjon
  - Grensesnitt mot andre selskapsfunksjoner som kontrollere, internrevisjon, risiko, juridisk, kvalitet, HR, ...
  - Definisjoner og begreper, beste praksis, erfaring, maler mv.
  - Revideres/oppdateres vinteren 2018/19
  - Utarbeides av arbeidsgruppe som er del av Nettverk Compliance

# Om arbeid med compliance

- Redusere risiko for manglende etterlevelse av eksternt og internt regelverk
- Styre compliancerisiko
  - En operasjonell risiko
  - Risiko for at virksomhetens drift forårsaker brudd med regulatoriske krav (herunder lover og forskrifter)
- Selv om det er lov, er det ikke sikkert at det er lurt!
- Forebyggende, rådgivende og kontrollerende rolle
- Kultur og opplæring
- Hovedsakelig innadrettet virksomhet
- Samarbeid med andre fagpersoner, avdelinger og selskapsfunksjoner
  - Bl.a. internrevisjon

# Om compliancefunksjonen

- En «compliancefunksjon» er ikke nødvendigvis en person eller en stilling
- System for etterlevelse av «alle» eksterne og interne krav
- En spesialisert tilnærming for å:
  - *Identifisere og vurdere risiko*
  - *Utforme og implementere internkontroll*
  - *Monitorere og rapportere effekt av kontrolltiltak*
  - *Gi råd om adferd, praksis og gjennomføring av egenevalueringer*
  - *Følge med på utvikling i regelverk*
  - *Sørge for opplæring*
- Operative oppgaver ligger i førstelinjen
- Etterlevelse er et linjeansvar og med ledelsen som øverste ansvarsnivå
- Compliancefunksjonen skal hjelpe linjen med å utarbeide og implementere et effektivt internkontroll system



# Compliancefunksjonen

**Compliance**  
«etterlevelse av  
lover og regler»



Hvilke lover  
og regler?

Hvem er  
ansvarlig for  
etterlevelse?

Plassering i  
organisasjonen?

Operasjonell  
risiko?





# Viktige ved etablering av compliancefunksjon

- Funksjonsbeskrivelse og ledelsesforankring
- Organisatorisk plassering, organisering og samhandling med ledelsen
- Rapporteringslinjer, uavhengighet og objektivitet
- Autoritet, informasjon, ressurser, kompetanse, avlønning

# Funksjonsbeskrivelse og ledelsesforankring

- Organisering, ansvar, arbeidsoppgaver og fullmakter bør fremgå av mandat eller instruks fra virksomhetens ledelse
- Bør bl.a. omhandle:
  - Organisatorisk plassering, samhandling og grensesnitt mot andre kontrollfunksjoner og mot linjen
  - Mandat og budsjett som balanserer med ansvarsområder, oppgaver og fullmakter
  - Tilgang til informasjon
  - Rapporteringsansvar

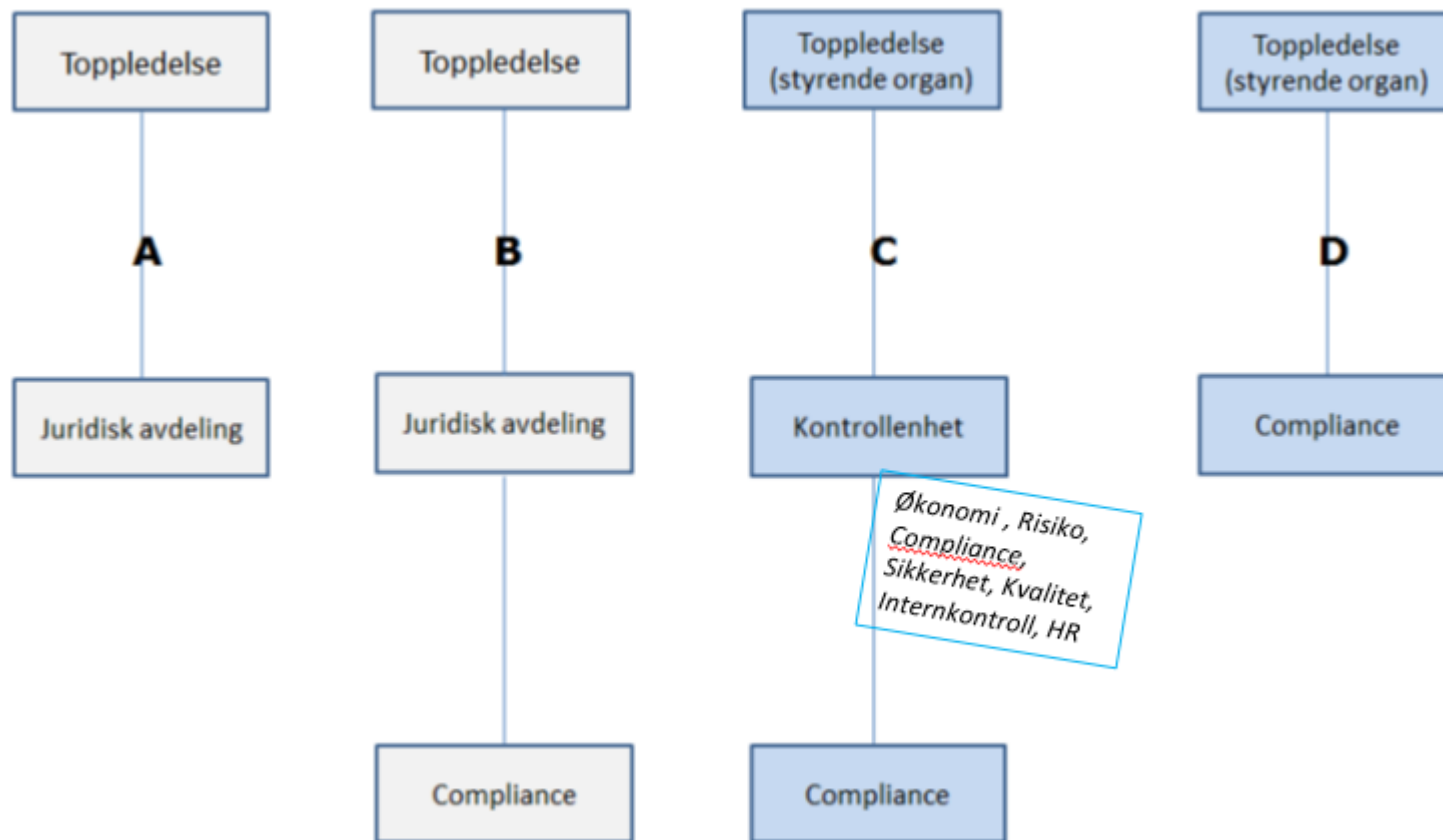
# Organisatorisk plassering og organisering

EIERE			
STYRE/REVISJONSUTVALG			
LEDELSEN			
1. FORSVARSLINJE	2. FORSVARSLINJE	3. FORSVARSLINJE	
Operasjonell ledelse, internkontroll i linjen	<b>Kontrollaktiviteter og funksjoner i stab:</b> <ul style="list-style-type: none"> <li>– Controller</li> <li>– Kvalitet og sikkerhet</li> <li>– Risikostyring</li> <li>– Compliance</li> <li>– HMS, miljø</li> <li>– Osv.</li> </ul>	Internrevisjon	Ekstern revisjon
Operative kontrolltiltak som linjen selv utfører.	Forskjellige typer av løpende risikostyring-, overvåkings- og kontrolltiltak som utføres av stab og kontrollfunksjoner.	Internrevisjonens objektive bekreftelser på prosessene for governance, risikostyring og kontroll, herunder hvordan første- og andrelinjeforsvaret fungerer.	Ekstern regnskapsrevisjon for uavhengig bekreftelse av regnskapsrapportering.

# Organisatorisk plassering og organisering

- Kontrollaspektet
  - Ikke obligatoriske krav til hvor compliancefunksjonen må være plassert
  - MEN - funksjonen må kunne opptre uavhengig av foretakets ledelse og/eller området man er satt til å kontrollere
- Alternative modeller
  - *Egen stabsenhet*
  - *Sammen med stab for risikostyring*
  - *Sammen med stab for kvalitetsstyring*
  - *Andre risiko og kontrollfunksjoner (for eksempel i økonomiavdelingen)*
  - *I juridisk avdeling*
  - *I HR*
  - *I internrevisjonen*
  - *Lokale compliance medarbeidere (selvstendige eller som forlenget arm av stabsfunksjon)*
  - *Outsourcing*

# Organisatorisk plassering og organisering



# Rapporteringslinjer og uavhengighet

- Mulighet til å rapportere til toppledelsen
- Compliance funksjonen bør rapportere til styret minst årlig
- Tilrettelegges for rapportering til styret ved behov

# Rapporteringslinjer og uavhengighet

## Core role of Compliance Control function with regards to compliance risks

- Give assurance on the compliance risk management process
- Give assurance that compliance risks are correctly evaluated
- Evaluating compliance risk management processes
- Evaluating and reporting on key compliance risks
- Reviewing the management of key risks

## Legitimate Compliance Control role (with safeguards)

- Facilitate identification and evaluation of compliance risks (self-assessments)
- Coaching management in responding to risks
- Coordinate compliance management activities
- Consolidated reporting on compliance risks
- Maintaining and developing compliance management framework
- Championing establishment of Compliance Program/Culture
- Development of Compliance Management Strategy for BoD approval

## Roles Compliance Control function should not undertake

- Accountability for Compliance Risk Management
- Implementing risk response on managers behalf
- Taking decisions on risk responses
- Management assurance on risks
- Imposing risk management processes
- Setting the risk appetite

# Autoritet, informasjon og kompetanse

- Leder med overordnet ansvar for compliancefunksjonen
- Plassering på senior management nivå
- Tilstrekkelig erfaring og kompetanse, ressurser og rammevilkår
- Tilgang til nødvendig informasjon om drift og beslutninger
- Avlønningsmodell som sikrer uavhengighet, kompetanse og tyngde
- Unngå resultatavhengige komponenter som kan føre til interessekonflikt og påvirke objektiviteten



# Viktigste elementer i et complianceprogram

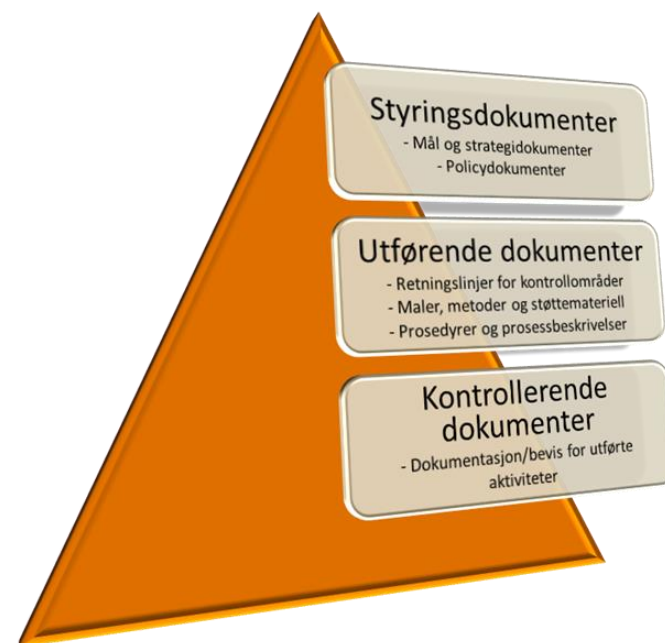
- Risikotilnærming
- Rammeverk
- Compliancekultur, tonen fra toppen, kommunikasjon, opplæring
- Integritetsundersøkelser (IDD)
- Avviksregistrering
- Varsling
- Monitorering
- Rapportering

# Vurdering av compliancerisiko

- Når kan compliancebrudd og manglende etterlevelse få vesentlige konsekvenser, f.eks. i form av offentlige sanksjoner, økonomisk tap, erstatningskrav og tap av omdømme
- Risikobasert tilnærming og forholdsmessighet
- Tilpasset virksomheten
- Jevnlig, årlig
- Risikoområder defineres med utgangspunkt i helhetlig risikokartlegging og dybdevurderinger
- Utvikling og endringer i interne og eksterne risikodrivere, samt regulatoriske krav og håndhevingen av disse
- Periodisk complianceplan/handlingsplan basert på risikovurderingen for effektiv styring av compliancerisiko
- Compliance skal ikke utøve risikostyringen, men bidra til å sikre etterlevelse

# Rammeverk for styrende dokumenter

- Compliance har en pådriverrolle ifm styringssystemet
  - Styringsstruktur med beskrivelse av organisering, roller, ansvar
  - Virksomhetsstyring
- Modell for risikostyring og internkontroll
- Samarbeid med juridisk, risiko, HR, økonomiavdeling, internrevisjonen samt enkeltpersoner i førstelinje for å unngå hull og/eller overlapp



# Opplæring – suksesskriterier

- Tema i ledermøter, ref. tonen fra toppen
- Tilpasset virksomheten og ansattes hverdag
- Integrert i annen opplæring og kjerneprosesser
- Variasjon – alene og i grupper, type verktøy
- Kommunikasjon av formålet med opplæringen
- Regelmessighet – blir aldri «ferdig»
- Vurdere incentiver

# Integritetsvurderinger - IDD

- Vurdere og styre risiko forbundet med forretningspartnere
  - Risiko avhenger av rolle i avtaleforholdet
  - Må kartlegge informasjon om selskap, eiere, styret og ledelse
  - Andre enheter kan utføre IDD, mens Compliance er ansvarlig for prosedyre, verktøy, opplæring og veiledning
-

# Avviksregistrering og -håndtering

- Nyttig styringsinformasjon
- Avdekkede hendelser blir lukket effektivt
- Forhindre at nye lignende hendelser inntreffer
- Alle skal melde avvik/hendelser, men Compliance har ofte ansvar for å følge opp rutinemessig håndtering og for å sammenstille, analysere, rapportere

# Varsling

## VARSLINGSPLAKATEN

Basert på § 24 i etisk regelverk for Sporveiskonsernet.

### HVA ER VARSLING?

Varsling er å gå videre med kritikkverdige forhold til noen som kan gjøre noe med det. Kritikkverdige forhold er brudd på lov/regler, brudd på interne regler eller brudd på etiske regler.

### VARSLING ER POSITIVT

Varsling er bra både for bedriften og for samfunnet, fordi kritikkverdige forhold kan rettes opp. Folk som er villige til å varsle, er en viktig ressurs for Sporveien. Vi oppfordrer derfor på det sterkeste alle som kjenner til kritikkverdige forhold i konsernet om å varsle om dette.

### RETT OG PLIKT TIL Å VARSLER

Alle ansatte, innleide, innehavere av verv og personer som gjør oppdrag for Sporveiskonsernet har rett til å varsle om kritikkverdige forhold. Også andre har rett til å varsle om kritikkverdige forhold.

Ansatte og innleide har plikt til å varsle om straffbare/kriminelle forhold knyttet til Sporveiskonsernets virksomhet og om forhold der liv og helse står i fare (sikkerhet).

### FREMANGSMÅTE FOR VARSLING

**Krav til forsvarlig varsling**  
Varsling skal skje på en forsvarlig måte. Ansatte og innleide har uansett rett til å varsle i samsvar med varslingsplikt eller Sporveiskonsernets rutiner for varsling. Det samme gjelder varsling til tilsynsmyndigheter eller andre offentlige myndigheter.

### INTERN VARSLING

Varsling skjer enten muntlig eller skriftlig til nærmeste overordnede. Hvis det oppleves som vanskelig å varsle nærmeste overordnede, kan du henvende deg til Compliance-funksjonen på e-post til [varsling@sporveien.com](mailto:varsling@sporveien.com) eller telefon **916 24 961**.

Personalsaker kan også varsles til tillitsvalgte og miljøsaker/arbeidsmiljø saker kan varsles til vernetjenesten.

### EKSTERN VARSLING

Sporveien har etablert en ekstern varslingskanal hos BDO Integrity Service.

Følg denne linken: <https://u.bdo.no/Sporveien> for å registrere varsel eller ring telefonnummer **970 86 000**. Gjennom denne linken kan du varsle anonymt.

Du kan også velge å la identiteten din være kjent for BDO Integrity Service, men anonym overfor Sporveiskonsernet.

Ved anonym varsling er det vanskelig for Sporveiskonsernet å følge opp varselet på en ordentlig måte. Varslere oppfordres derfor til å varsle med navn. Varsling kan skje konfidensielt.

### VARSELETS INNHOLD

Når du varsler er det viktig at du er så konkret som mulig. Beskriv hva som er skjedd, hvem var involvert, når, hvor, hvem du anser for å ha ansvaret etc. Dette er spesielt viktig når du varsler anonymt da det i slike tilfeller ikke vil være mulig å be om ytterligere opplysninger.

### BEHANDLING AV VARSEL

All varsling skal tas alvorlig og bli forsvarlig undersøkt. Sporveien har opprettet et varslingsråd til å behandle saker. Varslingsrådet består av juridisk direktør, Compliance-enheten, konserndirektør HR som er en egen funksjon i HR og hovedverneombudet.

Varslingsrådet avgjør selv hvordan den enkelte sak skal behandles. Varsler vil få informasjon om at saken er kommet inn i varslingsrådet og fremdrift i saken. I tilfelle varslingsrådet anbefaler ekstern granskning utarbeides et mandat. Etter at undersøkelsene er ferdige vil det skrives en sluttrapport om saken og anbefalte tiltak vil følges opp av varslingsrådet.

### FORBUD MOT GJENGJELDELSE

Sporveiskonsernet vil ikke akseptere noen represalier mot ansatte eller innleide som i god tro har varslet om kritikkverdige forhold. For innleide gjelder forbudet mot gjengjeldelse også egen arbeidsgiver.

Dersom du mener at varsling har medført gjengjeldelse kan du rapportere dette til din nærmeste overordnede eller til Compliance-enheten som plikter å undersøke saken. Du kan også kreve oppreisning og erstatning uten hensyn til arbeidsgiver skyld.



# Monitorering og evaluering

- Testing av førstelinjens internkontroll for etterlevelse av relevant regelverk
  - Avdekke potensielle svakheter og risikoområder
  - Vurdere effektiviteten av kontrolltiltak i f.eks. transaksjon-, innkjøps-, og salgsprosesser
  - Er policyer og prosedyrer hensiktsmessige, er de i samsvar med gjeldende regulatoriske krav, blir de etterlevd?
  - Revisjoner, stikkprøvekontroller, spørreundersøkelser, intervjuer, medarbeiderundersøkelser
- Etterprøvbarehet
  - Compliancelogg
  - Dokumentasjon til kontroll- og tilsynsorganer som f.eks. internrevisjon
  - Not documented, not done!





# Rapportering til styret og ledelsen

- Minst en gang årlig (umiddelbart hvis alvorlige brudd)
- Inngår i grunnlaget for styrets og ledelsens vurdering av internkontrollen og behovet for eventuelle tiltak
- Sikre etterprøvbarhet internt og eksternt overfor tilsynsmyndigheter
- Typiske temaer for rapportering:
  - *Regelverksendringer av betydning*
  - *Vurdering av overtredelsesrisiko/compliancerisiko*
  - *Tiltak for å redusere overtredelsesrisiko*
  - *Varslede og pågående granskninger*
  - *Status for etterlevelse på prioriterte områder – resultater fra monitorerings- og evalueringsaktiviteter*
  - *Overtredelser/uønskede hendelser*
  - *Rapporter fra offentlige tilsynsorganer*
  - *Tiltak for oppfølging av internrevisjonsrapporter eller granskninger*

# Takk for oppmerksomheten!