

INTERNKONTROLL

- for å kunne sove godt om natta

Møte i kontrollutvalget
01.03.24



Bakgrunn for arbeidet i Inderøy

Endringer i
Kommuneloven § 25

Det generelle
trusselbildet knyttet til
informasjonssikkerhet
og personvern

Behov for å utarbeide
en overordnet plan for
internkontroll i Inderøy
kommune – og et
styringssystem

Status våren 23 etter
modenhetsanalyse

- Risikoer/sårbarheter
- Styrker

Behov for å jobbe mer
systematisk, mer
formalisert

Omdømme –
«Gjør vi det vi sier at vi
gjør?»

... sikre regeletterlevelse

... sikre oppfylling av lovverk



Forholdet internkontroll og ledelse.

Kvalitetssystemet

Fokus på ...



Internkontroll/Egenkontroll



Kvalitetsverktøy/EQS



Informasjonssikkerhetsutvalg

Avvikssystem; EQS



📁 Oppgaver: 0 📄 Nye dokumenter: 0 ✉ Systemmeldinger: 0

MELDESKJEMA

Avviksskjema

Forbedringsforslag

Mine meldinger

DOKUMENTER

Kvalitet

Personal og HMS

Økonomi

Reglement
Lov og regelverk

IKT



TJENESTEYTING

Helse og omsorg

Plan, Landbruk og
Kommunalteknikk

Oppvekst

Kommunedirektør
Stab

Inn-Trøndelag
Regnskap og Lønn

Innherred
Anskaffelser

Ønsker du kontakt med systemadministrator (EQS)?
Send epost til:
kvalitet@nderoy.kommune.no

En modell for internkontroll må være ...

- **Helhetlig**
- **Risikobasert**
- **Tilpasset**
- ***Systematisk***



Hvorfor
risikobasert
internkontroll?

Forebyggende internkontroll

Unngå uønskede hendelser

Risikoanalyse gir tiltak basert på vurdering i forkant

Avvikshåndtering –
erfaringsbaserte tiltak og læring

Bidrar til trygghet og oversikt

Målsettinger i arbeidet

- Å se internkontroll i sammenheng med valgte strategier/målsettinger og innarbeide internkontroll i årshjulet
- Å etterleve lover og regler – og i tillegg sikre etterlevelse av andre vedtak som ikke kun gjelder oppfølging av krav i lover og forskrifter
 - **Å levere gode tjenester** som er innenfor krav fastsatt i lover og forskrifter
- Å etablere en risikobasert internkontroll – og en mer formalisert internkontroll
 - Systematisk og bygd på risikovurderinger (ROS)
 - Samme mal og framgangsmåte på alle nivå og for alle tjenester
- Å heve kompetansen og bevisstheten hos ledere og ansatte
 - felles plattform og forståelse for internkontrollarbeidet

Men også ...

- Pålitelig regnskapsrapportering
- Målrettet og kostnadseffektiv drift

Lovverk (ikke uttømmende)

Relevant lovverket vedr. internkontroll i kommunen:

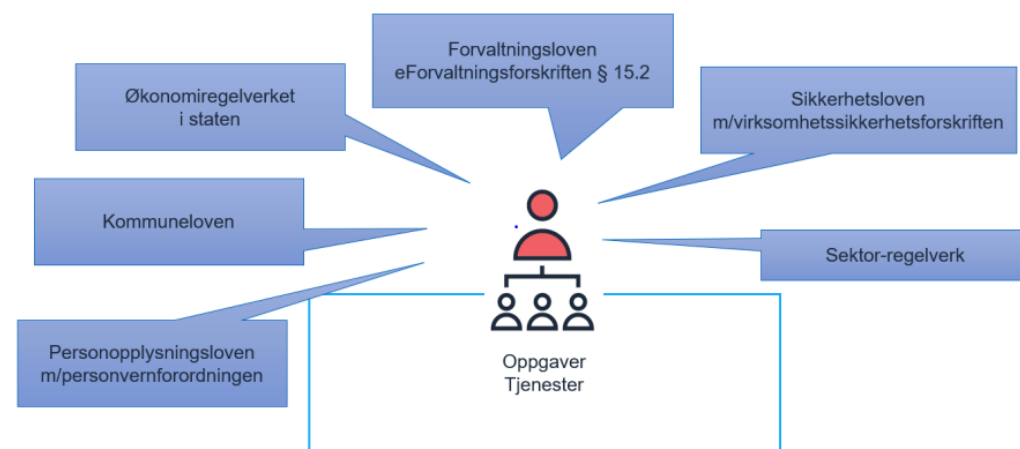
- Kommuneloven § 25
- Lov om kommunale helse- og omsorgstjenester m.m. (helse- og omsorgstjenesteloven)
- Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten
- Lov om statlig tilsyn med helse- og omsorgstjenesten m.m. (helsetilsynsloven)

I tillegg ...

- Personopplysningsloven
 - Personvernforordningen (kap 1/§ 1), GDPR
- eForvaltningsforskriften

Samt

- Forvaltningsloven
- Offentlighetsloven
- Sikkerhetsloven



Figur 6 – Mange regelverk stiller krav til ledelsens styring, og det er krevende å arbeide helhetlig for å ivareta alle hensyn.

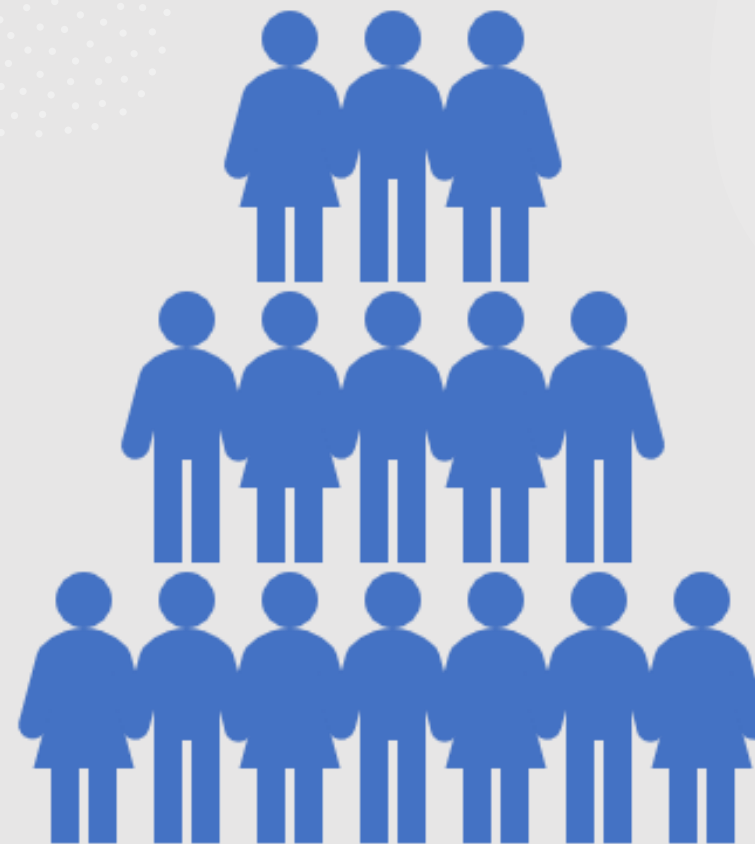
Ansvar og funksjoner

- Kommunedirektøren har det øverste ansvaret for internkontroll i kommunen jf. Kommuneloven § 25.
- Alle ledere i kommunen har gjennom delegering i linjen ansvar for internkontroll, og dermed også informasjonssikkerhet og personvern, på sitt område.
- Den enkelte ansatte har plikt til å sette seg inn i internkontrollsystemet - inklusive verktøy - og IKT-reglementet.

Funksjoner; bla.

- Rådgiver, internkontroll
- Informasjonssikkerhetsansvarlig
- Personvernombud
- Informasjonssikkerhetsutvalg/sikkerhetsutvalg
- Interkommunalt fagråd for informasjonssikkerhet og personvern på Innherred

I tillegg funksjoner knyttet til bla. Fiks digiorden (systemeier, systemansvarlig)



Modell for god internkontroll

Hensikt Hvorfor skal vi ha internkontroll?

- Helhetlig styring og riktig utvikling
- Kvalitet og effektivitet i tjenesteytingen
- Etterlevelse av lover og regler
- Godt omdømme og legitimitet

Virkeområde

Hvor skal vi ha internkontroll?

Sektorovergripende

Tjenestespesifikk

Støtteprosesser

Forutsetninger

Hvilke elementer består internkontrollen av?

Risikobasert

Formalisert

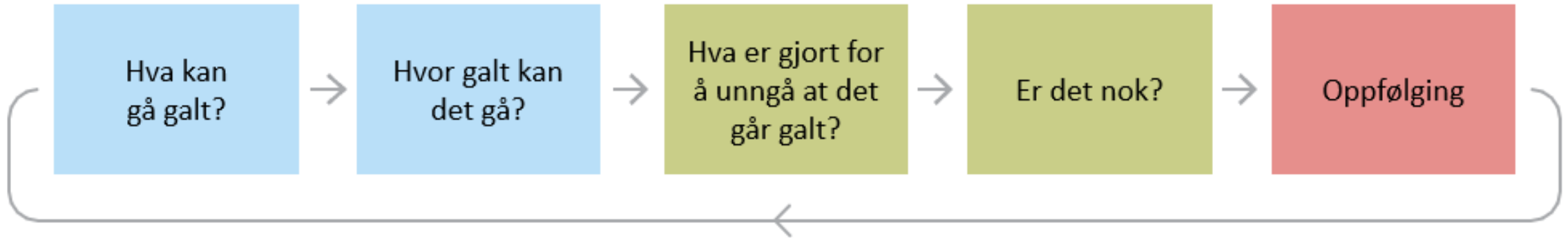
Kontrollaktiviteter

En samlet modell for internkontroll . Figur: KS

Modell for god internkontroll

En metode når man jobber risikobasert ...

ROS-analyse

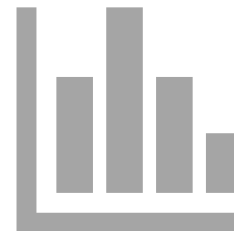


Rapportering til kommunestyret



Hyppighet

1.tertial
2.tertial
Årsrapport



Rapporterer om ...

Generelt om status
Avvik, statistikk
Aktiviteter og hendelser
Kompetanseheving, satsinger, læring
Tilsyn og revisjoner

Suksessfaktorer

God forankring i
toppledelsen

Avsatt ressurs

Tverrsektoriell
arbeidsgruppe

Faste
møtepunkter

Opplæring

Samlinger, kurs, workshops

Trinnvis oppstart

Være på
tilbudssiden

Informasjon/
kommunikasjon

Oppstart samarbeid med DigiTrøndelag

<https://www.digitrondelag.no/omdigitrondelag>

Utviklingstrapp internkontroll

Trinn 3: Utvikling og forbedring, fortsatt forankringsarbeid

Trinn 1: Informasjon, forankring, kompetanseheving, målbilde

- Kompetanseheving, Randi
- Introduksjon for ledergruppe (møter vår 2023)
 - Forankring og kompetanseheving
 - Prioritering: informasjonssikkerhet og personvern
 - Modenhetspyramiden
 - Målbilde
- Etablering av interkommunalt fagråd for inf. sikkerhet
- Etablering av kommunalt inf. sikkerhetsutvalg
- Digiorden – oppstart gjennomgang og utfylling
- Ferdigstilling av utkast , Inf. sikkerhetshåndbok

Trinn 2: Prosess med involvering av ledere og ansatte; roller og ansvar

- Informasjon i samarbeidsforum **24.08.23**
- Informasjon i utvidet ledergruppe **30.08.23**
- Møter med sektornivå/ledergruppa – kursing, forankring, workshop **Etter uke 36**
- Informasjon ut til fagområder som for eksempel Innherred Innkjøp og Regnskap og lønn
- Inf.sikkerhetsuke i oktober – (**1-2 KINS-kurs + databrukeravtaler**)
- Internkontrolluke i november
 - Utvidet ledermøte **man 20.11** – oppstart
 - KINS-kurs
 - Jobbing på enhets- og tjenestenivå med ROS, beredskap, risikovurdering, avvikshåndtering, dokumentasjon etc.
- Status Digiorden, **november**
- Statusrapport fra inf.sikkerhetsutvalget – **før 6.desember**
- Ledelses gjennomgang av internkontroll – **6.desember**

Innarbeidelse av struktur og system, dokumentasjon

- Politisk sak januar 2024
- Ferdigstilling av overordnet plan for internkontroll
- Utarbeidelse av årshjul
- Videre arbeid ute i tjenester og på enheter
 - Jobbing på enhets- og tjenestenivå med ROS, beredskapsplan, risikovurdering, avvikshåndtering, dokumentasjon etc.
- Sektor, enhet, tjenester rapporterer til KD (feb/mars)
- Rapportering til politikken – årsrapport mars
 - Y1 (x1, x2, x3 ...)
 - Y2 (x1, x2, x3 ...)
- Forankringsarbeid
- Sikring Digiorden
- Mer kommer ...

Oppstart 01.03.23

1.07.2023

Fra august 2023 →

2024 →



Et særlig fokus på

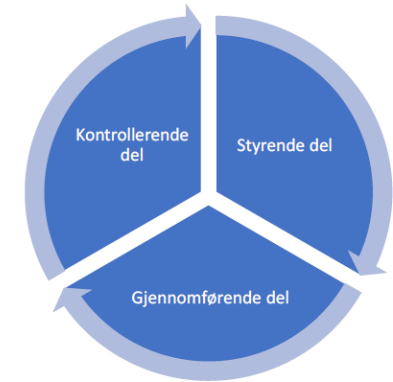
...

**Informasjonssikkerhet og
personvern**

Informasjonssikkerhet og personvern – lovverk

Viktige lovkrav:

- Kommunene må ha et styringssystem for informasjonssikkerhet
- Kommunene må definere sikkerhetsmål
- Kommunene må gjennomføre risikovurderinger
- Kommunene må gjennomføre sikringstiltak som står i henhold til risikoen
- Kommunene er ansvarlige for å sikre all behandling av personopplysninger



En policy beskriver *hvorfor* og *hva*, en prosedyre beskriver *hvordan*

- Policy for tilgangskontroll
- Policy for klassifisering av informasjon
- Policy for fysisk sikkerhet
- Policy for hjemmekontor
- Policy for sikkerhetskopiering (backup)
- Policy for nettverkssikkerhet

Sikkerhetsmål

- **Konfidensialitet** – det vil si at personopplysninger og annen beskyttelsesverdig informasjon som behandles i kommunen skal være beskyttet mot uautorisert tilgang.
- **Integritet** - det vil si at behandlingen skal sikre at informasjonen er korrekt, oppdater og formålstjenlig.
- **Tilgjengelighet** – det vil si at informasjonssystemet er tilgjengelig for autoriserte brukere ved behov.
- **Robusthet** – Det betyr at når uønskede fysiske eller tekniske hendelser inntreffer, bidrar beredskapstiltak til å begrense skaden og at kommunene raskt kommer tilbake til normal drift. Dette inkluderer å gjenopprette tilgjengelighet og tilgang til personopplysninger i rett tid.



Eksempler på forskjellige sikkerhetstiltak

Tekniske: kryptering, passord

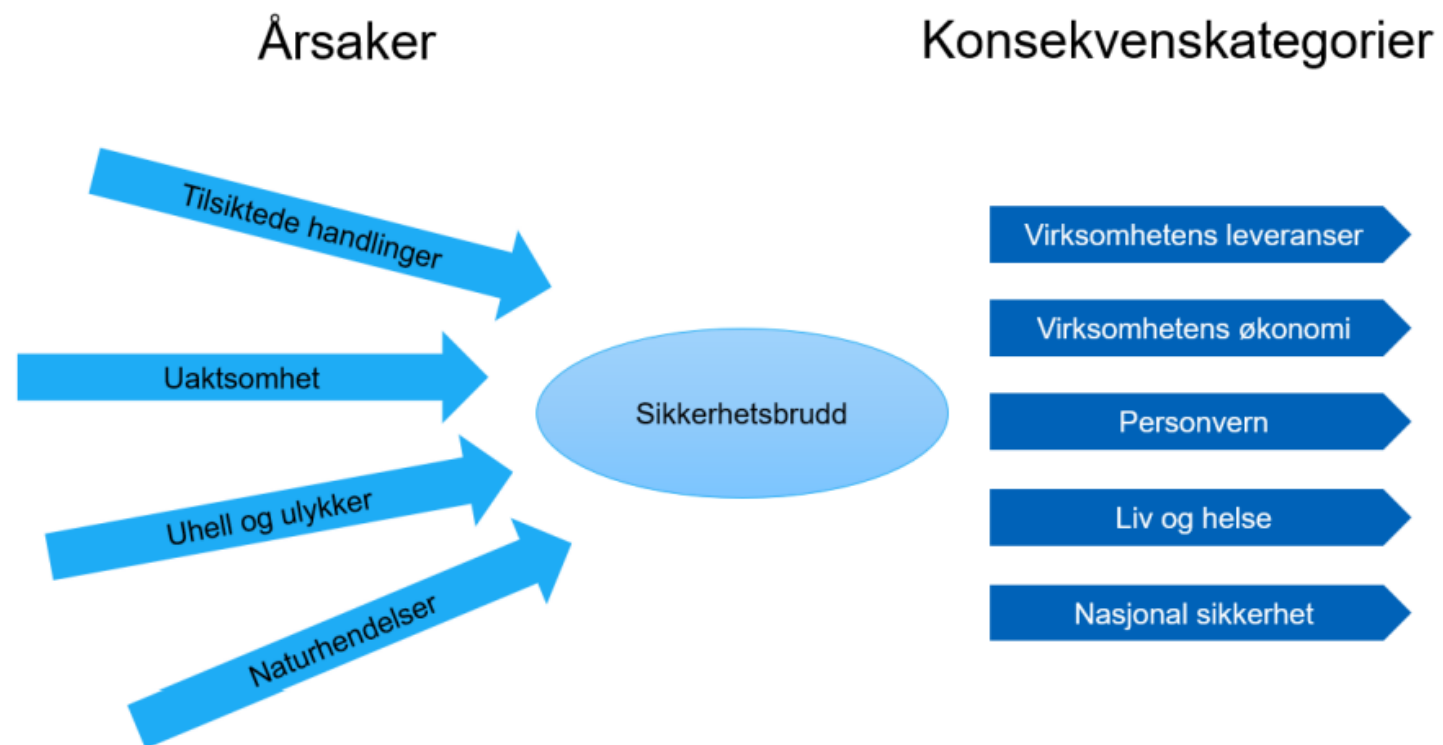
Organisatoriske: tilgangsstyring, ***etablert internkontroll***

Menneskelige: opplæring

Fysiske: adgangskontroll til eiendom, bygg og anlegg



Konsekvenser av informasjons- sikkerhetsbrudd



Figur 9 - Konsekvenser av informasjonssikkerhetsbrudd

Person- opplysninger

Ulik gradering av
personopplysninger ...



Sensitive opplysninger	Taushetsbelagte opplysninger	Alminnelig informasjon
Religion	Personnummer	Navn og adresse
Seksualitet	Bilder	Mobilnummer
Fagforeningsmedlemskap	Bilnummer	Mailadresse
Politisk og filosofisk overbevisning	Straffedommer, lovovertrедelser	m.m.
Rasemessig eller etnisk opprinnelse	Hemmelig adresse (6/7-koder)	
Genetiske og biometriske opplysninger		
Helseopplysninger		

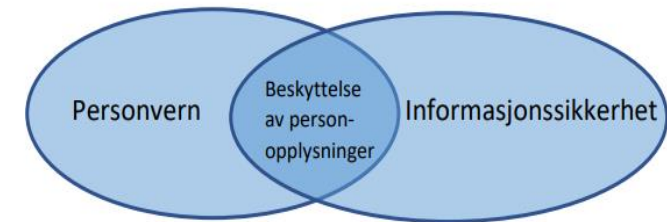
Informasjonssikkerhet og personvern

– har hatt særlig fokus på ...

- Utarbeidelse av en informasjonssikkerhet- og personvernhandbok (policy)
- Fiks digiorden – verktøy for registrering av applikasjoner/app-er
 - Opplæring med alle lederne i kommunen
 - Tett samarbeid med DIKO
- KiNS-kurs (KS Læring)
- Signering databrukeravtale

Arenaer for samhandling

- KDs ledermøter
- Utvidede ledersamlinger
- Ledelsens gjennomgang av den overordnede internkontroll
- Informasjonssikkerhetsutvalg, Inderøy
- Interkommunalt fagråd for informasjonssikkerhet og personvern på Innherred



Figur 3: Figuren forklarer sammenhengen mellom informasjonssikkerhet og personvern. Det er to ulike fagområder, men overlapper hva gjelder beskyttelse av personopplysninger.



Fiks digiorden

«Fiks digiorden er et styringsverktøy som hjelper kommunen å drive god informasjonsforvaltning. Styringsverktøyet kan brukes til å sikre et strategisk eierskap til kommunens informasjonsforvaltning og investeringer på digitaliseringsområdet.» (kilde: ks.no)

Fiks digiorden gir oversikt over kommunens:

- Applikasjoner
- Datasett (Et datasett er en samling med data - for eksempel i form av en tabell, liste eller en database. Beskriver hva man bruker applikasjonen til ...)
- Databehandleravtaler
- Behandlingsprotokoll av personopplysninger (GDPR)

Oppsummering

- Ferdigstilt Informasjonssikkerhet- og personvernhandbok (policy)
- Utarbeidet *Veileder for ledere*
- Utarbeidet *Overordnet modell for internkontroll i Inderøy kommune*
- Utarbeidet ROS-analyseskjema
- Utarbeidet årshjul
- Etablert informasjonssikkerhetsutvalg i Inderøy kommune
- Etablert interkommunalt fagråd for inf.sikkerhet og personvern
- Etablert et samarbeid opp mot DigiTrøndelag

Innarbeidet internkontroll i årshjulet

- Informasjonssikkerhetsuke (uke 42)
- Internkontrolluke (uke 47)
- Ledelsens overordnede gjennomgang av internkontroll (uke 49)
- Årsrapport

Intranett

<https://inntrondelag.sharepoint.com/sites/intranett-felles/SitePages/Informasjonssikkerhet-og-personvern.aspx>