SYKEHUSINNKJØP

INTERNREVISJON I SYKEHUSINNKJØP HF

MANDAT for revisjonstema: Informasjonssikkerhet og personvern

Formål:
Revisjonens formål er å bekrefte at foretaket har etablert en egnet internkontroll for informasjons-sikkerhet og personvern.

Bakgrunn:
Sykehusinnkjøp HF utøver en spesialisert og profesjonell innkjøpstjeneste for spesialist-helsetjenesten. Tjenesteproduksjonen er i stor grad digitalisert, noe som innebærer et krav om god internkontroll for informasjonssikkerhet og personvern for å håndtere risiko. I styresak 115-2021, *Risikovurderinger og tiltaksarbeid II-2021*, er personvernområdet vurdert til høy risikoscore.

Omfang og avgrensning av revisjonen:
I denne revisjonen vil internrevisjonen undersøke hvordan Sykehusinnkjøp styrer og følger opp egen informasjonssikkerhet og personvern. Vi vil undersøke om styrende dokumenter er etablert, kontrollere om besluttede sikkerhetstiltak er implementert og teste om tiltakene har ønsket effekt.

Revisjonen vil ta utgangspunkt i Digitaliseringsdirektoratet sin veileder «*Internkontroll i praksis – Informasjonssikkerhet»* og Nasjonal Sikkerhetsmyndighet (NSM) sine *Grunnprinsipper for IKT-sikkerhet,* ettersom Sykehusinnkjøp HF har basert seg på disse ved etablering av sin internkontroll på området.

Revisjonen vil ikke omfatte bred sikkerhetstesting på alle områder, men på utvalgte områder hvor risikoen vurderes høyest.

Fokusområder:
Internrevisjonens omfang deles inn i seks ulike fokusområder, som samsvarer med styringsaktivitetene som kreves for å ha styring og kontroll med informasjonssikkerhet og personvern jf. Digitaliseringsdirektoratets veileder.

1. <u>Ledelsens styring og oppfølging</u>
   I hvilken grad har ledelsen systematisk styring og kontroll med informasjonssikkerhet og personvern?

2. <u>Vurdering av risiko</u>
   I hvilken grad identifiseres, analyseres og evalueres risiko som angår informasjonssikkerhet og personvern?

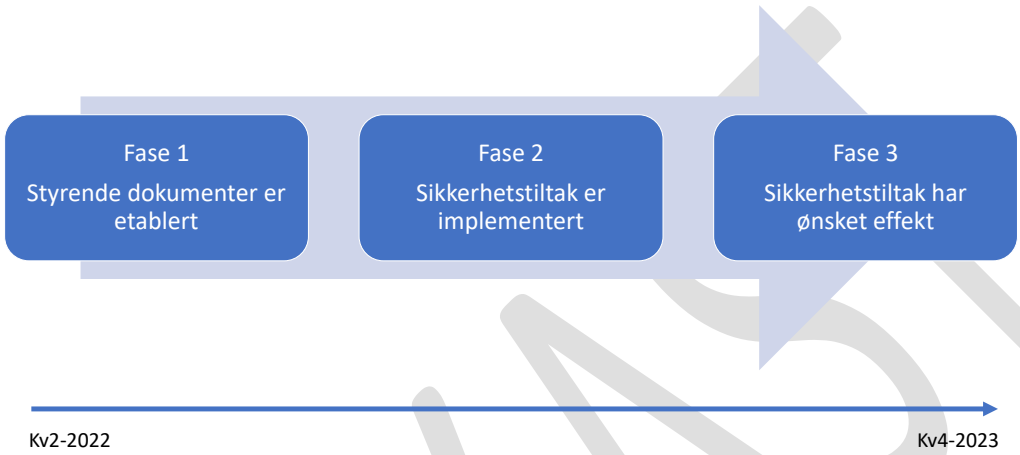
3. <u>Håndtering av risiko</u>
   I hvilken grad besluttes det egnede tiltak for å behandle risiko, og hvordan iverksettes og forvaltes det som blir besluttet?

4. <u>Overvåking og hendelseshåndtering</u>
   Hvilke tekniske og manuelle rutiner er implementert for å avdekke og følge opp vesentlige feil, avvik og uønskede hendelser?

5. Måling, evaluering og revisjon
   Hvilke målinger og evalueringer gjøres for å teste om tiltak fungerer og om pålegg blir etterlevd, både ved etablering og bruk av tiltak?

6. Kompetanse og kulturutvikling
   Hvordan sikres tilstrekkelig kompetanse og god sikkerhetskultur for styring av informasjonssikkerhet og personvern?

Metode / tilnærming:
Arbeidet med å etablere internkontroll for informasjonssikkerhet og personvern i Sykehusinnkjøp pågår fortsatt. Som en følge av det vil internrevisjonen gjennomføres i tre faser som illustrert under:



Revisjonen planlegges gjennomført primært ved bruk av dokumentgjennomgang, dataanalyse og intervjuer. På risikoutsatte områder vil vi også utføre sikkerhetstesting.

Revisjonsteam:
Janny Helene Aasen, Christin Ilstad og Hege Knoph Antonsen.

Vi vil benytte ekstern bistand ved planlegging og gjennomføring av dataanalyser og sikkerhetstester i fase 2 og 3.

Revisjonsperiode/fremdriftsplan:
Internrevisjonen tar sikte på oppstart av fase 1 i løpet av andre kvartal 2022. Plan for fase 2 og 3 fastsettes i samråd med ledelsen i Sykehusinnkjøp og i forbindelse med sluttføring av henholdsvis fase 1 og 2. Det utarbeides en delrapport for hver fase. Delrapport fra fase 1 planlegges levert i 2022. Delrapport fra fase 3 planlegges levert innen utgangen av 2023.