Veiledningsmateriellet

Internkontroll i praksis - informasjonssikkerhet

For toppleder

Oppdatert: 7.6.2017

Direktoratet for forvaltning og IKT

Internkontroll i praksis - informasjonssikkerhet
For toppleder

Som toppleder er du ansvarlig for at din virksomhet har velfungerende styring og kontroll. Det gjelder også på informasjonssikkerhetsområdet. Her er en enkel oversikt med sjekkliste som forteller hva internkontroll er og hva du som toppleder må gjøre.

Internkontroll = intern styring og kontroll

Intern styring og kontroll – internkontroll – er aktiviteter som hjelper deg å nå virksomhetens mål. Ditt ansvar er å etablere og følge opp et *system av aktiviteter*, slik at du kan ha tillit til at ledere på alle nivå håndterer risiko innen sine ansvarsområder i samsvar med dine føringer. Slik får alle ledere tilstrekkelig sikkerhet for at dere når virksomhetens mål.

1. Hvordan få til internkontroll for informasjonssikkerhet?

1.1 Analyse av status og plan for etablering eller forbedring

Dersom du er usikker på kvalitet og etterlevelse i dagens internkontroll, bør du få gjennomført en analyse av status. Analysen bør vurdere status opp mot pålagt og anbefalt innhold i internkontrollarbeid.

Difi anbefaler offentlige virksomheter å vurdere status på deres internkontroll opp mot anbefalingene i vårt veiledningsmateriell "Internkontroll i praksis - informasjonssikkerhet". En slik vurdering tilsvarer «benchmarking». Difis veiledning har hjelpemidler til å gjennomføre dette.

Slik får virksomhetsledelsen vite hvor deres virksomhet er i forhold til det som er anbefalt. Det gir et godt grunnlag for å akseptere status eller å få laget en plan for å etablere eller forbedre internkontrollen.

1.2 Tydelige føringer for aktivitetene

Fundamentet i internkontrollen er overordnede styrende dokumenter besluttet av dere i virksomhetsledelsen. Dokumentene må være klare på hvilke aktiviteter som skal gjennomføres i internkontrollarbeidet og hvem i virksomheten som har ansvar for hva. Dokumentene må også gi tydelige føringer for innholdet i aktivitetene.

Utforming av de overordnede styrende dokumentene er en av etableringsaktivitetene man gjennomfører når man skal etablere eller forbedre internkontrollen.

For at internkontrollen skal fungere må alle ansatte

- utføre de systematiske aktivitetene de er pålagt i de styrende dokumentene
- etterleve og følge opp de prosedyrer, krav, tekniske tiltak og andre sikkerhetstiltak som blir etablert og justert gjennom de systematiske aktivitetene og etableringsaktivitetene

1.3 En ledelse som bryr seg

En avgjørende faktor for en velfungerende internkontroll er en ledelse som bryr seg. Det gjelder ledere på alle nivå. Lederne må selv forstå hva internkontroll og informasjonssikkerhet handler om, og dere må kommunisere viktigheten ofte og tydelig, og prioritere arbeidet i budsjett og ressursdiskusjoner.

Dere må også selv gjennomføre deres del av internkontrollaktivitetene og etterleve de sikkerhetstiltak som blir etablert. Hvorfor skal de ansatte bry seg om internkontroll og informasjonssikkerhet dersom ledelsen ikke bryr seg?

1.4 Fagansvarlig informasjonssikkerhet som rådgiver og pådriver

Det er viktig for en velfungerende internkontroll at dere har, eller tidlig får på plass, en fagansvarlig informasjonssikkerhet eller lignende rolle.

De viktigste oppgavene til denne rollen er å

- støtte virksomhetsledelsen i arbeidet med informasjonssikkerhet
- være en ressursperson, pådriver og tilrettelegger for etablering og gjennomføring av virksomhetens samlede internkontroll innen informasjonssikkerhet

Det er viktig at vedkommende har tilstrekkelige ressurser, kompetanse og personlige egenskaper til å kunne utføre disse oppgavene.

2. Internkontroll, risiko og informasjonssikkerhet

2.1 Internkontroll er risikostyring i hele virksomheten

De ulike aktivitetene i internkontrollen utføres systematisk av en rekke aktører rundt om i hele virksomheten. Aktørene skal identifisere, vurdere, håndtere og følge opp risikoer ved alt virksomheten driver med. Risikoer kan endre seg over tid, så aktivitetene må gjentas jevnlig.

De ansatte må ha klare roller og ansvar i internkontrollarbeidet. Lederne i linjen vil alltid ha et hovedansvar. Det er de som har ansvar for arbeidsoppgaver og mål, og dermed risikoene i virksomheten. Fellesfunksjoner gir støtte: de som leverer sikkerhetstiltak (IT-drift, bygningsansvarlig mv), de som veileder i vurderinger av risiko, og en fagansvarlig som følger opp helheten.

De syv områdene med systematiske aktiviteter i Difis forklaringsmodell for internkontroll. De ulike aktivitetene skal utføres av ulike aktører rundt om i virksomheten

2.2 Risiko handler om mulige konsekvenser – mulige avvik fra mål

Risiko er **kombinasjonen av mulige konsekvenser og tilhørende sannsynligheter** for hendelser som kan inntreffe, eller valg som blir gjort**.** Vi sier at denne kombinasjonen uttrykker størrelsen på en risiko.

Konsekvensene er i realiteten avvik fra mål – de resultatene vi ønsker å nå. Indirekte uttrykker derfor risikoer mulige målavvik og tilhørende sannsynligheter. For å få gode risikovurderinger grupperer man ofte målene i målområder, for eksempel tjenestenivå, økonomi, personvern og HMS. Disse benyttes i risikovurderingene som konsekvenskategorier. Størrelsen på risikoene kan da vurderes og uttrykkes innen ulike kategorier.

Risikoer må reduseres, aksepteres eller håndteres på annen måte. Det må skje som en del av internkontrollen i samsvar med virksomhetsledelsens føringer i de overordnede styrende dokumentene.

2.3 Informasjonssikkerhet er en del av den samlede internkontrollen

Informasjonssikkerhet handler om å ivareta nødvendig konfidensialitet, integritet og tilgjengelighet på informasjonen som behandles;

- konfidensialitet
  - at informasjon ikke blir kjent for uvedkommende
- integritet
  - at informasjon ikke blir endret utilsiktet eller av uvedkommende
- tilgjengelighet
  - at informasjon er tilgjengelig ved behov

Brudd på en av disse er brudd på informasjonssikkerheten.

2.4 Konsekvenser ved brudd på informasjonssikkerheten

Brudd på informasjonssikkerheten kan få konsekvenser for både virksomheten selv, innbyggerne og andre offentlige og private virksomheter. Det kan for eksempel medføre

- feil beslutninger
- brudd på rettigheter og rettssikkerhet
- omdømmetap og økonomiske tap for innbyggere, næringsliv og virksomheten selv
- ødeleggende livssituasjon
- effektivitetstap for virksomheten selv og andre
- tap av liv og helse

Informasjonsbehandling, informasjonssikkerhet og mulige konsekvenser ved brudd på informasjonssikkerheten angår alle arbeidsoppgaver og mål i virksomheten. Derfor er det spesielt viktig at virksomheten har tilfredsstillende internkontroll på informasjonssikkerhetsområdet.

3. Krav og anbefalinger

3.1 Basere seg på anerkjente standarder

Internkontroll er ikke bare viktig for god virksomhetsstyring. Det er også pålagt i regelverket. Kravene er strengere på informasjonssikkerhetsområdet enn for internkontroll generelt. Internkontrollen på informasjonssikkerhetsområdet skal i henhold til eForvaltningsforskriften §15 være basert på anerkjente standarder.

Standarden ISO/IEC 27001 er den anbefalte anerkjente standarden for offentlige virksomheter. Difis veiledningsmateriell "Internkontroll i praksis - informasjonssikkerhet" er basert på og konkretiserer denne standarden, og dekker det Difi anser som de viktigste kravene.

Det er i offentlig sektor anbefalt å benytte Difis veiledningsmateriell for å tilfredsstille kravene i eForvaltningsforskriften §15 – som referanse og støtte ved analyse av status, og ved etablering og forbedring av internkontroll på informasjonssikkerhetsområdet.

3.2 Difis veiledningsmateriell har konkrete anbefalinger, eksempler og støttemateriell

Difis veiledningsmateriell har konkrete anbefalinger om hvilke aktiviteter som bør inngå i internkontrollen, hvem som bør ha ansvar for hva, hvordan føringer for risikohåndtering og aksept av risiko bør utformes samt hvilke aktiviteter som er sentrale ved etablering og forbedring.

Materiellet har eksempler på overordnede styrende dokumenter, maler og støttedokument. Eksemplene viser også hvordan man på en enkel måte kan inkludere andre områder enn informasjonssikkerhet. Da får virksomheten en helhetlig internkontroll.

Difis forslag kan tilpasses andre tilnærminger til internkontroll. Systematikken og den helhetlige virksomhetstilnærmingen i Difis veiledning bør alltid ivaretas for området informasjonssikkerhet.

Hele veiledningsmateriellet fra Difi er nettbasert og tilgjengelig på internkontroll.infosikkerhet.difi.no

4. Sjekkliste for toppledere

	Ja	Nei	Vet ikke
1. Har din virksomhet en systematisk internkontroll som dekker informasjonssikkerhetsområdet?			
2. Har virksomhetsledelsen gitt klare krav og føringer for roller og ansvar og innhold i de systematiske aktivitetene i internkontrollarbeidet?			
3. Dekker kravene og føringene alle organisatoriske enheter i virksomheten?			
4. Er kravene og føringene basert på anerkjente standarder på informasjonssikkerhetsområdet eller på Difis veiledningsmateriell?			
5. Gir kravene og føringene et godt grunnlag for at risikoer blir identifisert og håndtert rundt om i hele virksomheten?			
6. Gir kravene og føringene et godt grunnlag for at virksomhetens samlede mål blir nådd rundt om i hele virksomheten?			
7. Følger du og dine ledere systematisk opp at internkontrollaktivitetene blir utført rundt om i hele virksomheten i samsvar med krav og føringer?			

Dersom du som toppleder er usikker, eller svarer nei, på noen av spørsmålene over, bør du få gjennomført en analyse av status (jf. pkt. 1.2). Når analysen foreligger bør du ved behov få laget en plan for etablering eller forbedring av internkontrollen og få gjennomført planen. Fagansvarlig informasjonssikkerhet bør være en ressursperson, pådriver og tilrettelegger. Difis veiledningsmateriell har konkrete anbefalinger, eksempler og støttemateriell.

Direktoratet for
forvaltning og IKT (Difi)
Postboks 8115 Dep, 0032 Oslo
Telefon: 22 45 10 00
postmottak@difi.no
www.difi.no