Difi
Direktoratet for
forvaltning og ikt

Kommunikasjon med ledelsen – hva kan Difi bidra med?

Katrine Aam Svendsen
Seniorrådgiver

NIFS 21.02.2018

Innhold

- Hvem er «ledelsen»?
- Innhold i Difis veiledningsmateriell «Internkontroll i praksis – informasjonssikkerhet»
- E-læring: Er det sikkert?
- Dilemmatrening for ledergruppen

«Ledelsen» - Hvem mener vi?

- Virksomhetsledelsen
  - «Toppledelsen», «ledergruppa», etc.

- «Operative ledere»
  - Linjeledere
  - Ansvarlig for mål og resultater i sin enhet
  - Oppgaveeier/prosesseier → Risikoeier

Virksomhetsledelsens viktigste rolle

- å få gjennomført nødvendige etableringsaktiviteter i virksomheten
- å gi de overordnede føringene for det kontinuerlige internkontrollarbeidet
- å tilføre nødvendige ressurser
- å følge opp at føringer blir etterlevd og fungerer som forutsatt
- å gjøre nødvendige endringer ved behov

Ledelsens styring og oppfølging

- Virksomhetsledelsens gjennomgang
  - Minimum en gang årlig

- Ledere på alle nivå
  - Delegere og følge opp gjennom linjen
  - Sikre finansielle rammer
  - Kommunisere viktighet
  - Løfte og håndtere problemstillinger gjennom linjen
  - Beredskap og krisehåndtering

Innhold i Difis veiledningsmateriell

INTERNKONTROLL I PRAKSIS - INFORMASJONSSIKKERHET

Hjelpemidler i «Internkontroll i praksis»

- Sammendrag for toppleder
- Foredrag for toppledergruppe
- Beslutningspunkter for ledergruppen ved etablering/forbedring av internkontroll
- Virksomhetsledelsen gjennomgang
- For «viderekomne»

- http://internkontroll.infosikkerhet.difi.no/

Sammendrag for toppleder

1. Hvordan få til internkontroll for informasjonssikkerhet?
2. Internkontroll, risiko og informasjonssikkerhet
3. Krav og anbefalinger
4. Sjekkliste for toppledere

- http://internkontroll.infosikkerhet.difi.no/sites/sikkerhet/files/for_toppledere_-_internkontroll_informasjonssikkerhet.pdf

Sammendrag for toppleder

1. Hvordan få til internkontroll for informasjonssikkerhet?
2. Internkontroll, risiko og informasjonssikkerhet
3. Krav og anbefalinger
4. Sjekkliste for toppledere

- http://internkontroll.infosikkerhet.difi.no/sites/sikkerhet/files/for_toppledere_-_internkontroll_informasjonssikkerhet.pdf

1. Hvordan få til internkontroll for informasjonssikkerhet?

- Analyse av status og plan for etablering og forbedring
- Tydelige føringer for aktivitetene
- En ledelse som bryr seg
- Fagansvarlig informasjonssikkerhet som rådgiver og pådriver

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.

Difi

Foredrag for toppledergruppen

- Ligger tilgjengelig under «Presentasjoner» på maler og eksempler-siden
- Presentasjonen kan brukes fritt

- Ønsker du at vi skal komme og holde foredrag for «din» ledergruppe? Send en e-post på infosikkerhet@difi.no

Topplederforedrag - innhold

- Bakgrunnskunnskap:
  - Hva er informasjonssikkerhet
  - Potensielle konsekvenser ved brudd på informasjonssikkerheten
  - Krav og anbefalinger til virksomhetene
- Difis veiledningsmateriell «Internkontroll i praksis – informasjonssikkerhet»
  - Viktige aktører i virksomheten
  - Systematiske aktiviteter
- Hvordan jobbe for å få på plass god internkontroll
  - Etablering/forbedring
  - Difis anbefaling for overordnede styrende dokumenter
  - Sammenhenger mellom systematisk og god internkontroll, og etablering/vedlikehold av konkrete sikkerhetstiltak

Difi

Topplederforedrag - innhold

- Bakgrunnskunnskap:
  - Hva er informasjonssikkerhet
  - Potensielle konsekvenser ved brudd på informasjonssikkerheten
  - Krav og anbefalinger til virksomhetene
- Difis veiledningsmateriell «Internkontroll i praksis – informasjonssikkerhet»
  - Viktige aktører i virksomheten
  - Systematiske aktiviteter
- Hvordan jobbe for å få på plass god internkontroll
  - Etablering/forbedring
  - Difis anbefaling for overordnede styrende dokumenter
  - Sammenhenger mellom systematisk og god internkontroll, og etablering/vedlikehold av konkrete sikkerhetstiltak

Potensielle konsekvenser ved brudd på informasjonssikkerheten

Vår egen jobb

- feil beslutninger
- brudd på rettssikkerhet
- feil i øk. transaksjoner
- ikke korrekt og forsvarlig saksbehandling
- økonomiske tap
- ineffektivt arbeid
- tapt arbeidstid
- …

Personer og virksomheter

- tap av anseelse, integritet og rettigheter
- økonomiske tap
- ødelagte muligheter, arbeidsforhold, livssituasjon og eksistensgrunnlag
- bedriftshemmeligheter
- rikets sikkerhet
- liv og helse
- ikke korrekt og forsvarlig saksbehandling
- …

Difi

Etablering/forbedring av internkontroll

Difis anbefaling:

1. Analyse av status
   - Med Difis mal
2. Plan for etablering / forbedring
3. Ledelsens føringer for aktivitetene
   - Hvordan skal ting fungere hos oss?
   - → Styrende dokumenter

Difis mal for analyse av status

Systematiske aktiviteter	I hvilken grad gjennomføres dette? 0	1	2	3	Behov for endring (kan merke flere)	Prioritet Ress.beh
1 Ledelsens styring og oppfølging						
1.1 Virksomhetsledelsens gjennomgang						
Kommentarfelt….						
1.2 Delegere og følge opp gjennom linjen						
Kommentarfelt….						
1.3 Sikre finansielle rammer for internkontroll- og sikkerhetsarbeidet						
1.4 Kommunisere viktighet						
1.5 Håndtere problemstillinger løftet gjennom linjen						
1.6 Beredskap og krisehåndtering						
2 Risikovurdering						
2.1 Få oversikt og prioritere						
2.2 Analysere eksterne krav						
2.3 Planlegge risikovurdering						

Støtteark

1.3 Sikre finansielle rammer for internkontroll- og sikkerhetsarbeidet

- Ledere på alle relevante nivå må sørge for at økonomiske erfaringer og behov rundt internkontrollaktiviteter og sikkerhetstiltak systematisk er tema når budsjettrammer vurderes og diskuteres i virksomheten.

Anbefalt dokumentasjon:

- Budsjetter og virksomhetsplaner inneholder tydelig nødvendige ressurser til internkontrollarbeid og sikkerhetstiltak.
- Budsjettene er så fleksible at de kan dekke sikkerhetsmessige behov som dukker opp.

1.4 Kommunisere viktighet

- Ledere på alle nivå må systematisk kommunisere viktigheten av både informasjonssikkerhet, de iverksatte sikkerhetstiltakene og de systematiske aktivitetene i internkontrollarbeidet.
- Ledelsens holdning kommer til uttrykk gjennom det ledelsen sier og gjør. Kommunikasjonen bør derfor skje både muntlig, skriftlig og gjennom synlig handling.

1.5 Håndtere problemstillinger løftet gjennom linjen

- Dersom problemstillinger i internkontrollarbeidet ikke kan løses på det organisatoriske nivå de oppstår, skal de løftes gjennom linjen og håndteres på et høyere ledernivå.
- De skal løftes gjennom linjen til man når et ledernivå som har økonomisk handlingsrom eller myndighet til å finne budsjettdekning, akseptere aktuelle risikoer eller ta andre nødvendige beslutninger.
- Årsaken kan bl.a. være manglende finansiering, at akseptkriteriene sier at kun ledere på et visst nivå kan akseptere store restrisikoer, uenighet mellom ulike oppgaveeiere som benytter samme IKT-system, arbeidslokaler e.l., uenighet i virksomheten om hvilke tiltak som skal inngå i virksomhetens fellessikring og gjelde alle, og hvilke som bør være tilleggssikring for de som har ekstra behov.

Anbefalt dokumentasjon:

- Problemstillinger av vesentlig betydning og tilhørende beslutninger journalføres og arkiveres.

http://internkontroll.infosikkerhet.difi.no/maler-og-eksempler

Hvordan få til «ledelsesforankring»

- Husk! Internkontroll er ledelsens verktøy for å ha styring og kontroll
  - En virksomhet kan ikke ha et «styringssystem» på siden, forankret noe annet sted
- Topplederbeslutning: gjennomføre analyse av status
- Topplederbeslutning: plan for etablering | forbedring
  - eller å være fornøyd med det dere har

1

- **Analysere** status
- **Planlegge** etablering/forbedring
- Gjennomføre andre **etableringsaktiviteter**

Gjennomføre aktivitetene systematisk

2

Internkontroll-aktiviteter

Sikkerhetstiltak

3

Tilleggssikring

Fellessikring

- Instrukser og rutiner
- Avtaler
- Retningslinje for fysisk sikkerhet
- Tilgangsstyring IT-systemer
- Sikkerhetskopiering og gjenoppretting
- Osv.

Difi

Virksomhetsledelsens gjennomgang

- Sentrale temaer over tid:
  - Status på vedtatte tiltak
  - Bakgrunnskunnskap
    - Trender
    - Sammenhenger, konflikter, balanse K-I-T
    - Betydning i virksomheten
  - Status på det helhetlige internkontrollarbeidet
  - Tilbakemeldinger på informasjonssikkerhetsnivået
  - Status på spesielle risikoer/risikoområder
  - Muligheter for forbedring

Saksnotat – virksomhetsledelsens gjennomgang

- Virkemiddel for en effektiv virksomhetsledelsens gjennomgang
- Utarbeides av fagansvarlig informasjonssikkerhet
- Tydelige og begrunnede anbefalinger
- Innhold tilpasset virksomhetens behov og situasjon, og hva som vil være tema i virksomhetsledelsens gjennomgang.
- Bør alltid inneholde:
  - status i oppfølgingspunkter fra forrige gjennomgang
  - sentrale trender i risikobildet både for virksomheten, nasjonalt og internasjonalt
  - omtale av særskilte risikoer av strategisk betydning for virksomheten
  - oppsummering av vesentlige avvik i internkontrollarbeidet og i informasjonssikkerheten
  - vurdering av årsaker til vesentlige avvik
  - anbefalte tiltak for forbedring

For «viderekommende»

- Sammendrag:
  - «Grunnleggende innføring»
  - «Grunnleggende begreper»
  - http://internkontroll.infosikkerhet.difi.no/sammendrag

- Godt å vite – Ledelsens styring og oppfølging
  - Hvorfor internkontroll informasjonssikkerhet?
  - Suksessfaktor – Tonen på toppen
  - Suksessfaktor – Støtte til ledelsen
  - Krav og anbefalinger
  - http://internkontroll.infosikkerhet.difi.no/ledelsens-styring-og-oppfolging/godt-vite

Difi

E-læring

ER DET SIKKERT?

Difi

Er det sikkert?

- E-læring med toppleder som målgruppe
- Fokus:
  - Lederansvar
  - Positivitet
  - Lønnsomhet
  - Mer enn konfidensialitet

- http://erdetsikkert.difi.no

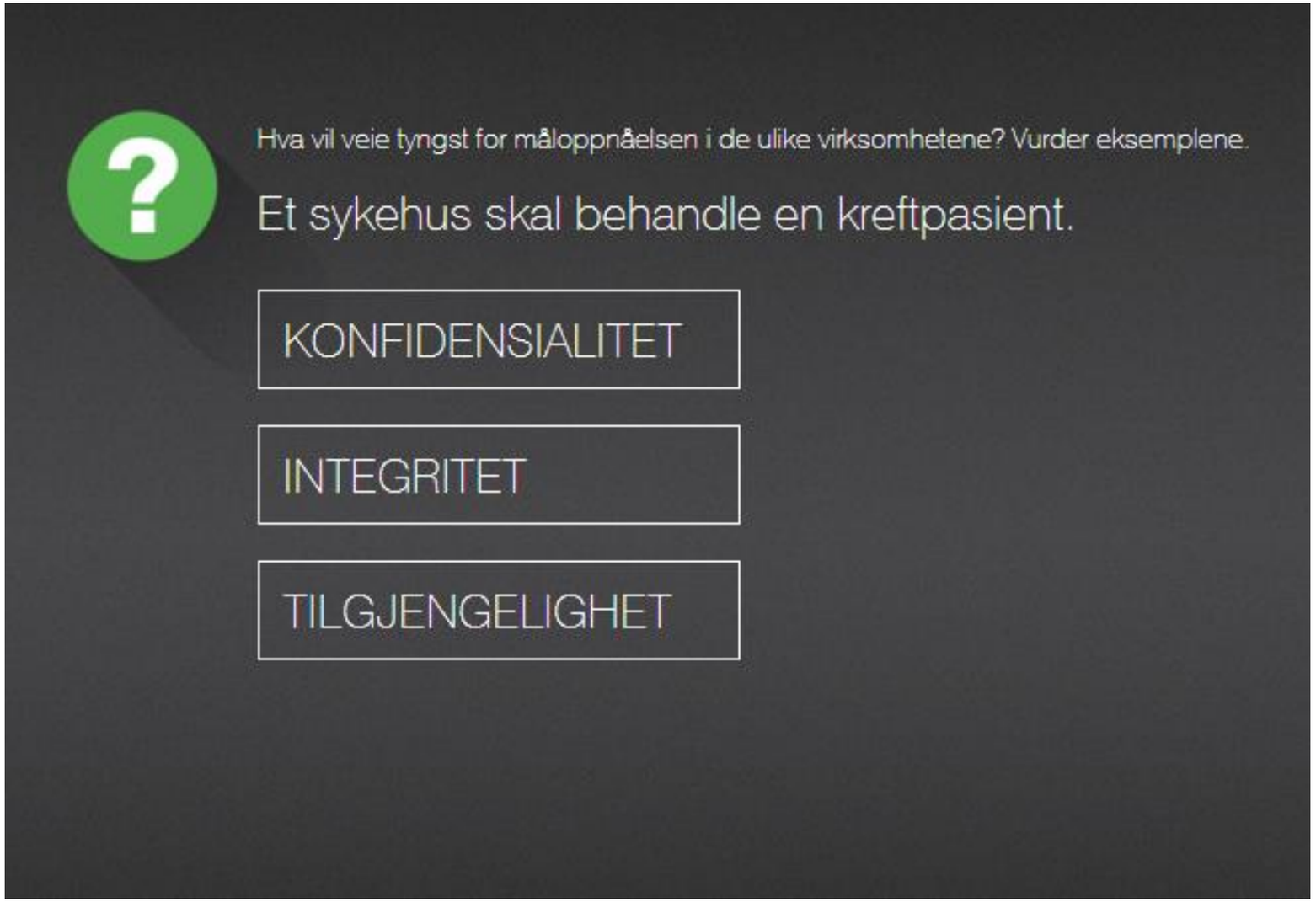
Modulene i programmet

- Informasjonssikkerhet lønner seg
- Jobb smart med informasjonssikkerhet
- God virksomhetsstyring
- Tonen på toppen
- Digitalisering og sikkerhet – ditt ansvar i digitaliseringsprosjekter
- Informasjonssikkerhet gir muligheter

Film fra «Er det sikkert» modul 2 – Internkontroll i praksis – informasjonssikkerhet

Film fra «Er det sikkert» modul 4 – Tonen på toppen

«Bevisstgjørende» spørsmål



De foregående spørsmålene har ingen riktige eller gale svar.

Målene for informasjonsbehandlingen kan være flere. For å nå enkelte av dem, vil tilgjengelighet være det viktigste, for andre er det helt essensielt at konfidensialitet eller integritet veier tyngst.

Virksomhetens mål og pålagte krav avgjør balansen mellom tilgjengelighet, konfidensialitet og integritet. Sikkerhetsmålene utledes fra virksomhetsmålene.

Virksomhetsstyring er de aktiviteter som ledelsen iverksetter for at virksomheten skal kunne realisere sine målsettinger. Informasjonssikkerhet **skal** være en av disse.

Difi

DILEMMATRENING FOR LEDERGRUPPEN

Difi

Dilemmatrening

Difi