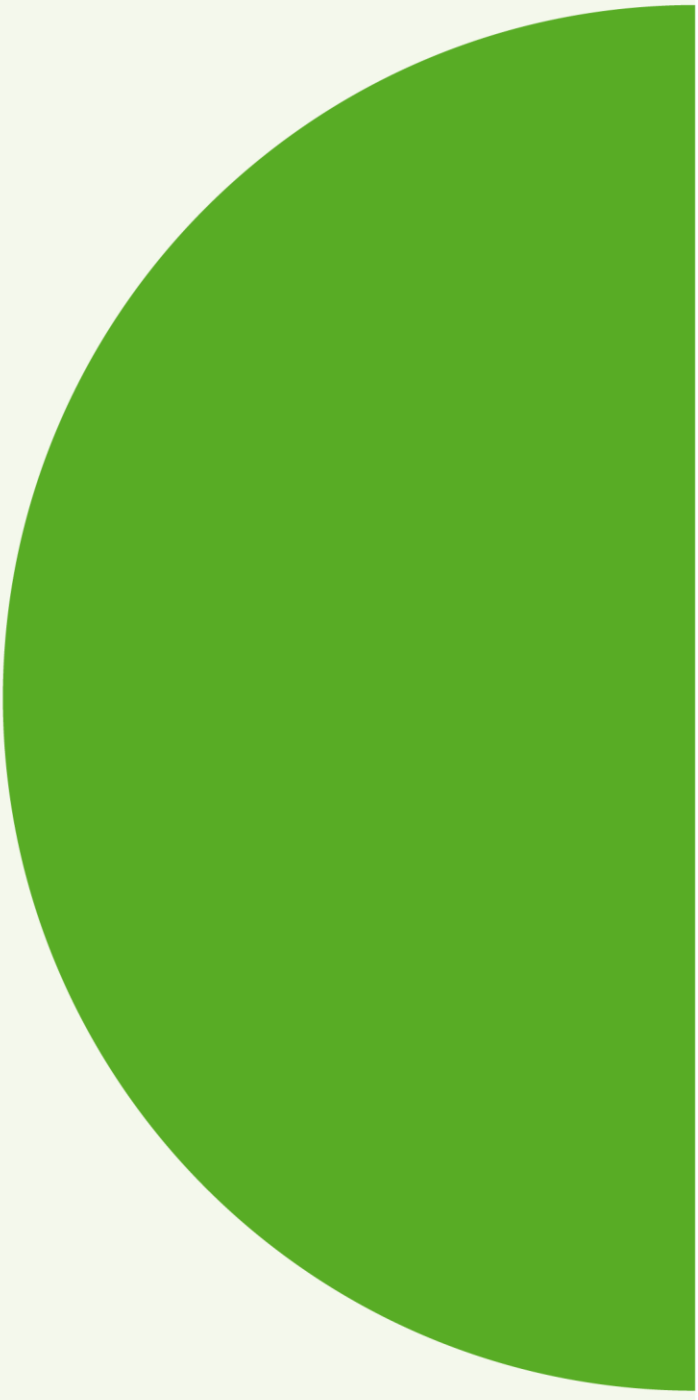
Veiledningsmateriellet

Internkontroll i praksis - informasjonssikkerhet

Grunnleggende begreper

Målgruppe: Fagansvarlig informasjonssikkerhet og virksomhetsledelsen

Oppdatert: 7.6.2017



Direktoratet for forvaltning og IKT

Internkontroll i praksis - informasjonssikkerhet

Grunnleggende begreper

Informasjonssikkerhet, risiko og internkontroll er grunnleggende begreper for å forstå og etablere en god internkontroll på informasjonssikkerhetsområdet. Her forklares de tre begrepene og sammenhengen mellom dem.

Målgruppe

- Fagansvarlig informasjonssikkerhet og virksomhetsledelsen

Innhold

1. Informasjonssikkerhet 1
   1.1 Hva handler informasjonssikkerhet om? 1
   1.2 Konfidensialitet og offentlige virksomheter 2
   1.3 Informasjonssikkerhetsrisiko 2
   1.4 Konsekvenser ved brudd på informasjonssikkerheten 3
2. Risiko 3
   2.1 Hva er risiko? 3
   2.2 Sannsynlighet og kunnskapsstyrke 4
   2.3 En hendelse kan ha flere konsekvenser med forskjellig sannsynlighet 4
   2.4 Risikobeskrivelser 5
   2.5 Forenkle, men vite hva man gjør 5
   2.6 Misforståelser rundt risiko 6
   2.7 Prosessledere er ofte viktig støtte 6
   2.8 Positiv risiko eller muligheter? 6
   2.9 Risikovurderinger på ulike styringsnivå 7
3. Internkontroll 7
   3.1 Hva betyr begrepet internkontroll? 7
   3.2 Omfang og formål med internkontroll 7
   3.3 Internkontroll er risikostyring, systematikk og formalisering 8
   3.4 Etablering av sikkerhetstiltak er en del av risikohåndteringen 9
   3.5 Felles tiltaksleverandører skal gi støtte, ikke beslutte 9
   3.6 Ulike internkontrollområder 10

1. Informasjonssikkerhet

1.1 Hva handler informasjonssikkerhet om?

Behandling av informasjon er både kjerneaktivitet og en viktig støtteaktivitet i alle virksomheter. Det er en sentral del av alle arbeidsoppgaver. Effektiv og pålitelig informasjonsbehandling er avgjørende for at virksomheter skal kunne nå sine mål. Det er da viktig at man kan stole på informasjonen, at den er tilgjengelig og at man følger lover og regler.

Informasjonssikkerhet handler om å ivareta dette. Vi kaller det 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

Informasjonssikkerhet **omfatter både muntlig, papirbasert og digital behandling av informasjon**. Det omfatter også **alle typer informasjon**, ikke bare enkelte typer som for eksempel personopplysninger og regnskapsinformasjon.

1.2 Konfidensialitet og offentlige virksomheter

Hovedregelen er at informasjonen som offentlige virksomheter behandler er offentlig. Dette er både grunnlovsfestet[1] og hovedregelen i offentleglova[2]. Målet er blant annet å legge til rette for at offentlig virksomhet er åpen og gjennomsiktig, og å legge til rette for viderebruk av offentlig informasjon[3].

Behov for konfidensialitet i offentlig sektor må derfor ha forankring i en lovbestemmelse[4]. De vanligste unntaksbestemmelsene fremgår av offentleglova kapittel 3 *Unntak frå innsynsretten* og forvaltningsloven § 13 (*taushetsplikt*).

Konfidensialitet er viktig også i offentlig sektor, men kun relevant for informasjon som er underlagt lovpålagt taushetsplikt, er unntatt offentlighet etter offentleglova av andre begrunnede årsaker eller har unntak hjemlet i annen lov. Det er heller ikke nok at noe *kan* unntas offentlighet etter offentleglova. Man skal alltid vurdere å gi helt eller delvis innsyn, det som kalles merinnsyn eller meroffentlighet[5].

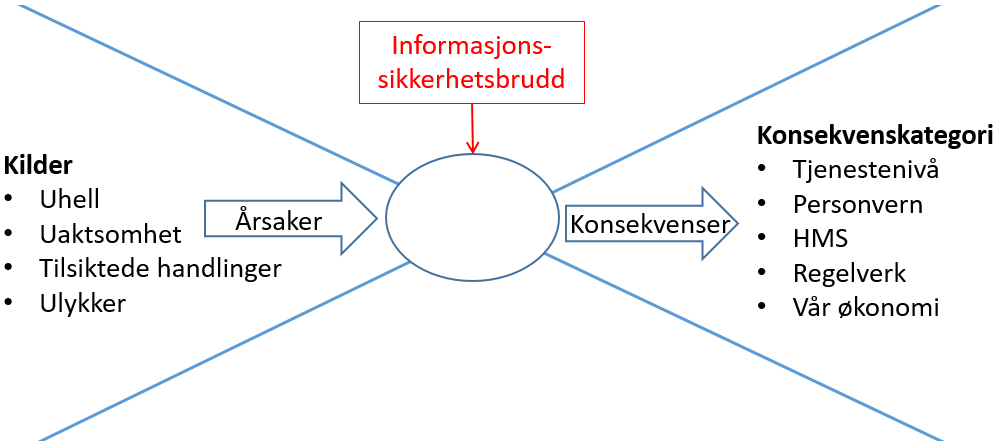
Det er viktig å være tydelig på dette internt i offentlige virksomheter. Det er nødvendig for å forstå hva **konfidensialitet** handler om i offentlig sektor, og hva vi skal bruke ressurser på å ivareta. Ellers kan vi bryte både Grunnlova og offentleglova, og hindre den **tilgjengelighet** disse er opptatt av.

Begrepet «sensitivt» som ofte benyttes i dagligtale er misvisende og skaper mange misforståelser. Det bør derfor unngås. Offentlige virksomheter bør i stedet benytte begrepene taushetsplikt og unntatt offentlighet når man snakker om behov for konfidensialitet. Man må også huske at åpenhet og tilgjengelighet på offentlig informasjon er lovpålagte krav som skal understøttes og ikke hindres.

1.3 Informasjonssikkerhetsrisiko

For å beskrive risikoer beskriver vi ofte en uønsket hendelse som kan medføre visse konsekvenser. Brudd på konfidensialitet, integritet eller tilgjengelighet på informasjonen som behandles er brudd på informasjonssikkerheten. Det kalles **informasjonssikkerhetsbrudd**. Når et informasjonssikkerhets-brudd er **en del av hendelsesforløpet** ved en risiko, er risikoen en **informasjonssikkerhetsrisiko**.

[1] Jf. Grunnloven § 100, 5. ledd
[2] Jf. offentleglova § 3
[3] Jf. offentleglova § 1
[4] Jf. offentleglova § 3 første punktum.
[5] Jf. offentleglova § 11



Informasjonssikkerhetsrisiko fra kilde, via årsaker og informasjonssikkerhetsbrudd til konsekvenser i ulike kategorier og nivå. Et informasjonssikkerhetsbrudd er et brudd på konfidensialitet, integritet eller tilgjengelighet på informasjonene som behandles.

Begrepene informasjonssikkerhetsbrudd og informasjonssikkerhetsrisiko er ikke nødvendig å bruke i hverdagen. De klargjør imidlertid hva informasjonssikkerhet handler om, og hva som er den kritiske faktoren i mange risikoer – informasjonssikkerheten.

1.4 Konsekvenser ved brudd på informasjonssikkerheten

Informasjonssikkerhetsbrudd 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

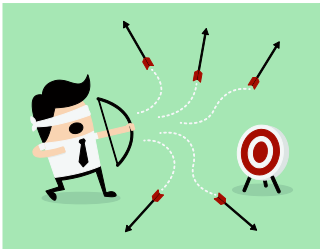
Det er slike **mulige konsekvenser kombinert med tilhørende sannsynligheter som er risikoene ved behandling av informasjon**. Kombinasjonen konsekvenser og tilhørende sannsynligheter brukes også som uttrykk for størrelsen på en risiko.

2. Risiko

2.1 Hva er risiko?

Risiko handler om mulige avvik fra våre mål. Noen sier mulige avvik fra ønskede resultater eller ønskede tilstander. Det er det samme.

Risiko kobles oftest til uønskede hendelser som har uønskede konsekvenser. Det er disse konsekvensene som er avvik fra det vi ønsker. For virksomheter vil det si avvik fra mål.



Risiko handler om mulige avvik fra våre mål

Det er alltid usikkerhet rundt hva som kan skje i fremtiden. Denne usikkerheten gjelder også hvorvidt hendelser med konsekvenser vil inntreffe.

Definisjonen av risiko er blitt tydeligere forankret rundt usikkerhet de siste årene. Det er fra sterke forskningsmiljø presisert at risiko er kombinasjonen av mulige konsekvenser og tilhørende usikkerhet. Dette tilsvarer definisjonen i ISO-standardene.

Usikkerhet uttrykkes i hovedsak som sannsynlighet. Vi sier derfor ofte at **risiko er kombinasjonen av mulige konsekvenser og tilhørende sannsynligheter**.

2.2 Sannsynlighet og kunnskapsstyrke

Med sannsynlighet mener vi her vår grad av tro på om noe vil inntreffe. Det kalles kunnskapsbasert eller subjektiv sannsynlighet.

Når vi skal estimere eller anslå sannsynligheten for en konsekvens, er det flere faktorer vi bør vurdere skjønnsmessig i sammenheng. De viktigste er:

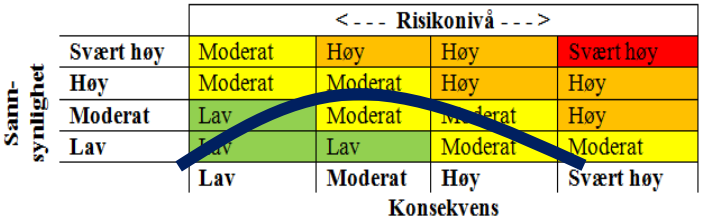
- hvor ofte vi vet eller tror at hendelsen med denne konsekvensen har skjedd tidligere
- motivasjon, vilje og kapasitet hos trusselaktører, dersom det handler om tilsiktede handlinger
- hvor lett det er at uhell, uaktsomhet, tilsiktede handlinger eller ulykker som gir denne konsekvensen, kan skje. Dette er et uttrykk for våre sårbarheter

Det er også nyttig å synliggjøre hvor god bakgrunnskunnskap og kvalitet man har hatt i arbeidet med estimat som dette. Det kalles ofte **kunnskapsstyrke**. Kunnskapsstyrken kan nevnes i enkle stikkord eller korte beskrivelser for enkeltrisikoer, en risikovurdering samlet eller i kombinasjoner.

Ved å supplere med kunnskapsstyrke får man synliggjort litt mer om usikkerheten enn bare sannsynlighetsstørrelser. Det kan være viktig for beslutningstakere og andre, som skal forstå resultatene i etterkant av gjennomførte risikovurderinger, og bruke resultatet videre.

2.3 En hendelse kan ha flere konsekvenser med forskjellig sannsynlighet

Det er viktig å forstå at en innledende hendelse kan få flere forskjellige konsekvenser av ulik alvorlighetsgrad. Hver av disse vil normalt ha forskjellig sannsynlighet. Dette er illustrert med sannsynlighetsfordelingen i den blå buen i figuren til høyre. Sannsynlighets-fordelingen vil variere fra hendelse til hendelse.



Risikomatrise med eksempel på sannsynlighetsfordeling mellom ulike konsekvensnivå

Konsekvenser kan også virke inn på flere mål. I risikovurderinger grupperer vi ofte målene i konsekvenskategorier, eksempelvis tjenestenivå, økonomi, personvern og HMS. Sannsynligheten på ulike konsekvensnivå vil normalt være forskjellig mellom ulike konsekvenskategorier.

Vi må også merke oss at **sannsynligheten gjelder konsekvensene**, og ikke ett eller annet tidlig i hendelsesforløpet. Dette er viktig for å forstå risiko. Sannsynligheten for at noe tidlig i

hendelsesforløpet kan skje, vil likevel være nyttig støtte ved estimat av sannsynligheten for aktuelle konsekvenser.

2.4 Risikobeskrivelser

Risikoer bør beskrives i en risikobeskrivelse, også kalt hendelsesbeskrivelse, scenario eller lignende. Hvor detaljert vi beskriver konsekvensdelen av hendelsen, påvirker omfanget av mulige konsekvenser. Det gir mulighet for å spisse risikovurderinger mot det vi er spesielt redd for eller opptatt av.

Konsekvensen bør alltid nevnes som en del av risikobeskrivelsen. Det gir forståelse for hva vi snakker om når vi angir størrelsen på risikoer.

2.5 Forenkle, men vite hva man gjør

Matematisk utregning av risiko
På spesielle områder regner man ut viktige risikoer i kroner. For en gitt hendelse omfatter regnestykket da alle mulige konsekvenser og tilhørende sannsynligheter. Dette blir komplekst og ressurskrevende i de fleste sammenhenger. Man velger derfor som regel å forenkle.

Bruk av risikomatrise og konsekvenskategorier
En vanlig forenkling er å dele både konsekvensene og sannsynligheten opp i nivå i en risikomatrise, som i figuren over. I tillegg grupperer man som nevnt over gjerne virksomhetens mål i noen konsekvenskategorier.

Uttrykke kun én kombinasjon av konsekvens og sannsynlighet
Videre forenkler man ofte ved å uttrykke risikoen ved en hendelse kun som én kombinasjon av konsekvens og sannsynlighet, selv om den egentlig består av flere kombinasjoner, jf. sannsynlighetsfordelingen i figuren over.

Man velger da oftest det **mest forventede konsekvensnivået og tilhørende sannsynlighet**. Når man gjør det, bør man være oppmerksom på at dette ikke alltid er den største risikoen, og eventuelt justere hva man velger.

Forstå sammenhengene og tydeliggjøre ved behov
Forenklinger som dette er ofte nødvendig for å få effektive risikovurderinger og effektiv kommunikasjon. Det er likevel viktig å forstå de grunnleggende sammenhengene og tydeliggjøre disse for beslutningstakerne både for risikovurderinger generelt og for spesielle risikoer ved behov. Eksempler:

- Risikoer utenfor den ene kombinasjonen av konsekvens og sannsynlighet som man velger å uttrykke, kan kreve særskilt håndtering. Dette må fanges opp.
- Dersom beslutningstaker skal få den forståelse og det beslutningsgrunnlag hun trenger, vil komplekse eller spesielle risikoer kunne ha behov for mer tekstlig utdypning enn det som vises i en forenklet fremstilling. Dette må da utdypes spesielt, f.eks. i vedlegg til et risikonotat.

Forenkle, men vite hva man gjør

Utfordringer om man ikke vet at man forenkler
Man bør generelt være tydelig i kommunikasjonen om at man forenkler, og hva som skjuler seg utenfor en forenklet fremstilling. Dersom man ikke forstår at man forenkler og hva man forenkler kan man

- snakke forbi hverandre

- overse viktige risikoer
- gi og få et misvisende risikobilde
- ta feil beslutninger
- kaste bort tiden på risikoarbeid der man ikke forstår hva man gjør

2.6 Misforståelser rundt risiko

Det eksisterer en del misforståelser rundt både sannsynlighet, risiko, sårbarhet mv. Mye skyldes at man benytter talemåter, forenklinger og upresise teknikker og støtteverktøy ukritisk. Flere IKT-system og støtteverktøy, både fra leverandører og «hjemmelagde» løsninger, stimulerer til misvisende fremgangsmåter, risikobilder og forståelse av risiko.

Dette er det viktig å være oppmerksom på

- ved anskaffelser og bruk av system og støtteverktøy
- i intern informasjon og opplæring
- i praktisk gjennomføring av risikovurdering og risikohåndtering

2.7 Prosessledere er ofte viktig støtte

Risikovurderinger bør gjennomføres rundt om i hele virksomheten. Nøkkelpersoner i utføring av arbeidsoppgavene må involveres.

Å bruke trente prosessledere i det som går utover det helt enkle, vil for de fleste virksomheter være en god investering. Det bidrar til tilstrekkelig kvalitet og effektivitet. Prosesslederne kan gjerne være internt ansatte. Det er grunnleggende forståelse, personlige egenskaper og litt trening som skal til. Eksperter kan man hente inn ved spesielle behov, f.eks. ved spesielt tekniske problemstillinger.

2.8 Positiv risiko eller muligheter?

ISO-standardene

ISO-standardene sier at risikoer kan være både negative og positive, på samme måte som avvik fra mål. Risikovurderinger kan da gi både negative og positive konsekvenser.

Andre rammeverk

Flere andre rammeverk bruker begrepet risiko kun om negative avvik. De kaller positive avvik for muligheter. En vurdering som dekker både risiko og muligheter, kalles da en usikkerhetsvurdering. En risikovurdering er i denne sammenheng en avgrenset del av dette. Den dekker da kun negative avvik, oftest kalt negative konsekvenser.

Negative og positive konsekvenser

Liten betydning, men vær tydelig i kommunikasjonen

Forskjellen viser ulike tradisjoner i forskjellige fagmiljø. Det har liten praktisk betydning. Det viktige er at virksomheter velger egne begreper bevisst, vet hva man mener med begrepene og bruker fremgangsmåter og støtteverktøy ut fra det.

Siden begrepsforståelsen varierer, bør man være tydelig på innholdet i begrepet når man kommuniserer med andre virksomheter om risiko og risikovurderinger.

Difis veiledningsmateriell bruker risiko kun om negative avvik

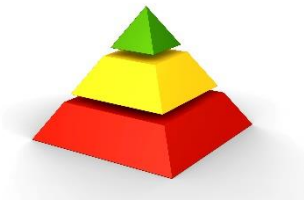
I dette veiledningsmateriellet brukes risiko kun om negative avvik. Dette er et pragmatisk valg. Difis forståelse er at dette er mest vanlig i offentlig sektor. Samtidig er det brudd på informasjons-

sikkerheten og mulige negative konsekvenser man normalt har blikket på i arbeidet med informasjonssikkerhet.

2.9 Risikovurderinger på ulike styringsnivå

Risikovurderinger med påfølgende håndtering bør normalt gjennomføres på flere styringsnivå i virksomheter. Man har da ulikt fokus, og gjerne litt forskjellige støtteverktøy og tilnærminger:

- Strategisk: Overordnede mål og langsiktige retningsvalg
- Taktisk: Hva som bør gjøres av oppgaver, tjenester o.l. for å nå virksomhetens mål samt organisering av arbeidet
- Operativt: Hvordan oppgaver og tjenester utføres



Strategisk, taktisk og operativt nivå er som en pyramide i virksomheten

Operativt nivå

På operativt nivå handler det om å identifisere, analysere og håndtere uønskede hendelser og konsekvenser i utføringen av oppgaver og tjenester, det vi kaller det operative arbeidet. Dette bør skje rundt om i hele virksomheten der arbeidet utføres. Det bør dekke både kjerneoppgaver, støtteoppgaver og styringsoppgaver.

Hovedfokus i internkontroll informasjonssikkerhet

Selv om risikovurderinger og valg på strategisk og taktisk nivå gir viktige rammevilkår for informasjonssikkerheten, handler de i hovedsak om styring og organisering generelt i virksomheten.

Innen internkontroll på informasjonssikkerhetsområdet er det operativt nivå og de operative risikoene man i hovedsak retter blikket mot. Tilsvarende gjelder de fleste andre internkontrollområder.

Risikostyring på strategisk og taktisk nivå er mest relevant i andre deler av virksomhetsstyringen. Å gå nærmere inn på dette, herunder hva som er hensiktsmessige fremgangsmåter og støtteverktøy, faller utenfor formålet med dette veiledningsmateriellet.

3. Internkontroll

3.1 Hva betyr begrepet internkontroll?

Begrepet internkontroll er en forenklet oversettelse fra engelsk, og betyr **intern styring og kontroll**. Noen fagmiljø og regelverk bruker begreper som internkontrollsystem, styringssystem, ledelsessystem og sikkerhetsadministrasjon. Begrepene betyr det samme som internkontroll når de er brukt i konteksten intern styring og kontroll.

Innen informasjonssikkerhet var det tidligere tradisjon for å bruke begrepet styringssystem. Både eForvaltningsforskriften § 15 og Difi benytter imidlertid begrepet internkontroll. Dette er det vanligste begrepet på andre fagområder, og det er viktig å forstå at det handler om det samme.

Internkontroll på informasjonssikkerhetsområdet er det samme som et styringssystem eller ledelsessystem for informasjonssikkerhet.

3.2 Omfang og formål med internkontroll

Internkontrollen skal etableres av virksomhetsledelsen, og den bør omfatte hele virksomheten.

Formålet er at ledere på alle nivå skal få tilstrekkelig (eller rimelig) sikkerhet om at man når virksomhetens samlede mål. Det vil si at man i alle enheter i virksomheten

- når mål- og resultatkrav
- arbeider effektivt
- etterlever lover og regler
- har pålitelig rapportering

Formålet med internkontroll er å sikre måloppnåelse

Dette forutsetter at lederne har tilstrekkelig kontroll på risikoene innen de mål og arbeidsoppgaver de og deres organisatoriske enhet har ansvaret for. Det skal lederne få ved at alle i virksomheten følger de krav og føringer som virksomhetsledelsen har gitt for internkontrollen.

Kulepunktene over kan kalles de samlede målene for en virksomhet. Det er viktig å merke seg at disse kan komme i konflikt med hverandre. Tiltak på ett område må derfor sees i sammenheng med de øvrige.

Formålet over er også formålet med internkontroll på informasjonssikkerhetsområdet. Forskjellen er bare en avgrensning til ett internkontrollområde – informasjonssikkerhet. Det vil si til brudd på konfidensialitet, integritet eller tilgjengelighet som en medvirkende årsak til at vi kanskje ikke når målene våre.

Tilsvarende gjelder for andre internkontrollområder som har sine avgrensninger, eksempelvis HMS og kvalitet.

3.3 Internkontroll er risikostyring, systematikk og formalisering

Risikostyring er kjernen i internkontrollen

Det er virksomhetens risikoer vi er opptatt av å identifisere, vurdere og håndtere i et internkontrollarbeid. Det er på den måten vi opprettholder tilstrekkelig sikkerhet om at vi når virksomhetens mål.

Risikostyring er kjernen i internkontrollarbeidet

Systematisk tilnærming

Risikostyring krever en systematisk tilnærming rundt om i hele virksomheten. Det er der virksomhetens arbeid utføres, og det er der man er ansvarlig for mål og mulige avvik og konsekvenser.

Risikoer må identifiseres, vurderes og håndteres både jevnlig og når uønskede hendelser inntreffer. Risikoer er ikke statiske. De forandrer seg over tid.

Risikohåndtering bør baseres på virksomhetsleders føringer

Håndtering av risiko gjør man ved å unngå, dele, redusere eller akseptere risikoen. Det bør være bevisste valg basert på virksomhetsleders føringer. Internkontroll handler om å nå virksomhetens samlede mål. Da må man ha en felles forståelse og et felles grunnlag for å akseptere risiko og prioritere ressurser.

Overvåking og hendelseshåndtering

Vi må akseptere og leve med noe risiko. Det er hverken mulig eller kostnadseffektivt å identifisere og fjerne alle risikoer. Vi må derfor ha en systematikk for å overvåke der det er nødvendig, og for å identifisere, følge opp og lære av uønskede hendelser.

Kontrollere om internkontrollen fungerer
De som er ansvarlig for ulike deler må systematisk vurdere eller kontrollere om de ansatte har tilstrekkelig kompetanse, om etablerte sikkerhetstiltak fungerer som forventet, og om internkontrollarbeidet rundt om i virksomheten blir gjennomført som forutsatt. Ellers kommer risikoene ut av kontroll.

Nødvendig med formalisering og dokumentasjon
Behov for etterlevelse og kontroll krever en formalisering av hva som skal gjøres i internkontrollarbeidet, hvem som skal gjøre hva og dokumentasjon av at det blir gjort. Dokumentasjon av gjennomføring må samtidig ikke være mer omfattende enn nødvendig. Det går ut over effektiviteten.

Internkontroll er et systematisk arbeid rundt om i hele virksomheten

Internkontroll er et systematisk arbeid
Samlet krever dette et systematisk arbeid i hele virksomheten innenfor formelle rammer og føringer gitt av virksomhetsledelsen. Det er dette vi kaller internkontroll. Omfang og innretning bør være tilpasset risikoenes størrelse. Tiltak bør baseres på vesentlighet og nytte/kost.

3.4 Etablering av sikkerhetstiltak er en del av risikohåndteringen

Å etablere sikkerhetstiltak, som prosedyrer, rutiner, opplæring, fysiske tiltak og tekniske tiltak, samt å finne alternative måter å gjennomføre arbeidet på, er eksempler på risikohåndtering. Både sikkerhetstiltak og annen risikohåndtering blir ofte bare kalt tiltak. Noen bruker også begrepene sikringstiltak eller kontroller i stedet for sikkerhetstiltak.

Risikoreduserende tiltak må vurderes, etableres og gjennomføres som en integrert del av internkontrollen. Behov og alternativer må lederne rundt om i virksomheten få vurdert for sine ansvarsområder. Grunnlaget er risikovurderinger de får gjennomført, risikoers størrelse samt virksomhetsledelsens føringer for risikohåndtering og aksept av risiko.

Ved valg av tiltak bør man normalt ta hensyn til både risikoreduserende effekt, kostnader og negative sideeffekter. Det siste er viktig siden tiltak for å redusere en risiko kan øke en annen risiko. Dersom man lar sikkerhetstiltak omfatte områder og ansatte som i liten grad er omfattet av risikoen, kan det gå ut over både virksomhetens effektivitet og andre mål.

3.5 Felles tiltaksleverandører skal gi støtte, ikke beslutte

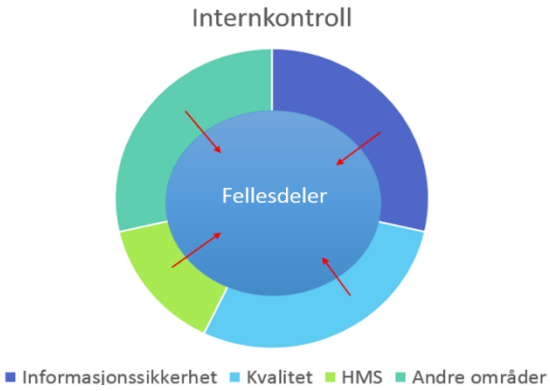
Mange sikkerhetstiltak vil naturlig tilbys og leveres av fellesfunksjoner som IT-drift, bygningsansvarlig og personalenhet. Disse aktørene kan kalles felles tiltaksleverandører i internkontrollen. Det tydeliggjør deres rolle.

Tiltak bør ikke være løsrevne beslutninger fra tiltaksleverandørene. Det vil kunne gi negative sideeffekter og økte risikoer på andre områder enn det tiltaksleverandørene arbeider med. Det kan hindre viktig måloppnåelse for en rekke linjeledere.

3.6 Ulike internkontrollområder

Det er vanlig å snakke om og rette blikket på ulike internkontrollområder som informasjonssikkerhet, HMS, kvalitet mv. Det finnes ulike eksterne krav og interne behov for internkontrollen innen de ulike områdene. Samtidig er en del ting felles.

Det er oftest anbefalt å integrere de ulike internkontrollområdene der det er hensiktsmessig. En helhetlig internkontroll i virksomheten bør bestå av både fellesdeler som gjelder alle internkontrollområder og områdespesifikke deler som gjelder enkelte internkontrollområder.



Helhetlig internkontroll består av fellesdeler og områdespesifikke deler

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