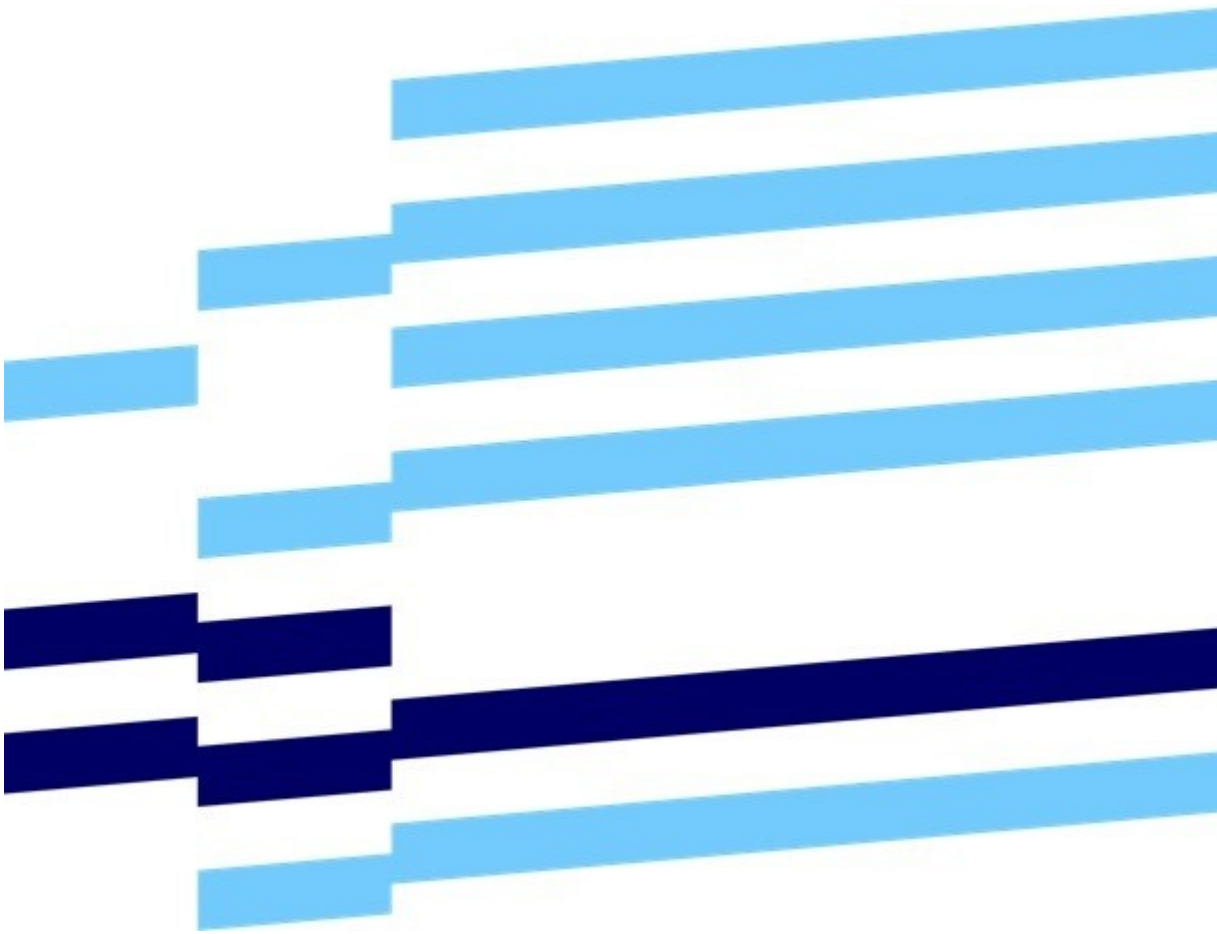
Difi
Direktoratet for
forvaltning og ikt

Internkontroll i praksis – informasjonssikkerhet
Grunnleggende innføring



Difi
Direktoratet for forvaltning og ikt

Interkontroll i praksis - informasjonssikkerhet

Grunnleggende innføring

Denne grunnleggende innføringen er et sammendrag av Difis veiledningsmateriell *Internkontroll i praksis – informasjonssikkerhet*. Formål, forankring og bruksområde blir presisert. Behov for og krav til internkontroll blir synliggjort. Sentrale aktiviteter i gjennomføring, etablering og forbedring av systematisk internkontroll blir beskrevet. Anbefalte kilder til støtte ved implementering av sikkerhetstiltak blir nevnt. Til slutt gis en kort oversikt over hele veiledningsmateriellet.

Målgruppe
Fagansvarlig informasjonssikkerhet og virksomhetsledelsen

Innhold

1 Bakgrunn og bruksområde

1.1 Formål med og forankring av veiledningsmateriellet

Internkontroll i praksis – informasjonssikkerhet er et veiledningsmateriell utviklet av Direktoratet for forvaltning og IKT (Difi). Målgruppen er offentlige virksomheter. Formålet er å gi hjelp til etablering/forbedring av internkontroll i samsvar med kravene i eForvaltningsforskriften § 15 *Internkontroll på informasjonssikkerhetsområdet*.

Materiellet er basert på den anbefalte anerkjente standarden ISO/IEC 27001. Materiellet støtter seg også sterkt på ISO 31000 og anerkjente forskningsmiljø innen risikostyring.

Rammeverkene i COSO, andre rammeverk og standarder samt veiledninger, eksempler og råd fra en rekke kilder er benyttet som kunnskapsgrunnlag og støtte. Blant kildene er Datatilsynet, Nasjonal sikkerhetsmyndighet (NSM), Direktoratet for e-helse, Direktoratet for samfunnssikkerhet og beredskap (DSB), Direktoratet for økonomistyring (DFØ) og Arbeidstilsynet.

De nevnte virksomhetene har også deltatt i en referansegruppe for veiledningsaktører. Interesserte fra en rekke statlige virksomheter og kommuner har deltatt i en annen referansegruppe for brukere.

1.2 Tilpasset bruk av ISO/IEC 27001

Veiledningsmateriellet konkretiserer det vi mener er de mest sentrale delene av standarden ISO/IEC 27001. Det inneholder samtidig pragmatiske tilpasninger til norske offentlige virksomheter.

Det er anbefalt å bruke dette veiledningsmateriellet som referanse og støtte ved analyse av status, og ved etablering og forbedring av internkontroll på informasjonssikkerhetsområdet, jf. Referansekatalogen over anbefalte og obligatoriske IT-standarder i offentlig sektor.

Materiellet dekker ikke alle krav i ISO/IEC 27001. Ønsker man å sertifisere seg, må man lese standarden og implementere alle kravene. Etter vår vurdering er dette normalt ikke nødvendig for offentlige virksomheter.

Kravet i eForvaltningsforskriften § 15 er at man skal **basere seg på** slike standarder. Det gir større handlingsrom enn krav om full etterlevelse og sertifisering. Det vil for de fleste være tilstrekkelig å basere seg på konkretiseringene i dette veiledningsmateriellet. De er basert på standarden.

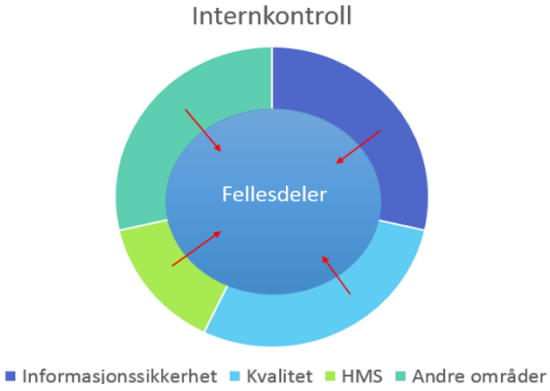
Den enkelte virksomhet må avgjøre om den i tillegg vil implementere alle kravene i standarden og eventuelt sertifisere hele eller deler av virksomheten.

1.3 Helhetlig internkontroll i virksomheten

Veiledningsmateriellet omfatter helhetlig internkontroll på **informasjonssikkerhetsområdet**. Det dekker de grunnleggende kravene om internkontroll, styringssystem og sikkerhetsstyring i eForvaltningsforskriften, personopplysningsloven og sikkerhetsloven.

Virksomheter kan også integrere andre internkontroll-områder i samme tilnærming. Dette kan være HMS, kvalitetskrav, personvernregelverket utover informasjonssikkerhet, objektsikkerhet mv.

Sentrale deler kan være felles for flere områder. Virksomheten kan da få bedre sammenheng og effektivitet i den samlede internkontrollen. Materiellet inneholder flere eksempler på helhetlig tilnærming.



Helhetlig internkontroll består av fellesdeler og områdespesifikke deler

Kjernen i materiellet og internkontrollen er et sett av systematiske aktiviteter. Disse er strukturert etter Difis forklaringsmodell. De kan omstruktureres og inngå i andre forklaringsmodeller til internkontroll dersom virksomheter ønsker det.

2 Hvorfor er internkontroll viktig?

2.1 Virksomhetenes behov

Formålet med internkontroll

Internkontroll betyr intern styring og kontroll. Det er også kalt styringssystem, ledelsessystem og sikkerhetsadministrasjon. 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

Internkontroll = intern styring og kontroll

Risikostyring er kjernen i internkontrollen

Det er risikostyring som er kjernen i internkontrollen. Hendelser som kan medføre uønskede konsekvenser må systematisk identifiseres, vurderes og håndteres rundt om i hele virksomheten.

Risiko er mulige konsekvenser og tilhørende sannsynligheter – oftest av uønskede hendelser som kan inntreffe eller av valg som blir gjort. Uønskede konsekvenser er avvik fra virksomhetens mål. Det er ved å etablere og følge opp en helhetlig systematikk i det samlede risikoarbeidet at virksomhetens ledelse og de ansatte forøvrig kan få tilstrekkelig sikkerhet om at man har kontroll på risikoene og vil nå virksomhetens mål.

Hva er informasjonssikkerhet?

Behandling av informasjon er både kjerneaktivitet og viktig støtteaktivitet i alle virksomheter. Effektiv og pålitelig informasjonsbehandling er avgjørende for at virksomheten skal 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 konfidensialitet, integritet og tilgjengelighet på informasjonen vi behandler;

- 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.

Konsekvenser ved brudd på informasjonssikkerheten

Brudd på konfidensialitet, integritet eller tilgjengelighet er brudd på informasjonssikkerheten. Slike brudd 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 og tilhørende sannsynligheter som er risikoene.

Når et informasjonssikkerhetsbrudd, dvs. brudd på konfidensialitet, integritet eller tilgjengelighet, er **en del av hendelsesforløpet** frem mot en uønsket konsekvens, kalles risikoen en **informasjons-sikkerhetsrisiko**. Dette er en delmengde av virksomhetens samlede risikoer.

Informasjonssikkerhet og mulige konsekvenser ved brudd på informasjonssikkerheten **angår alle arbeidsoppgaver, tjenester og mål i virksomhetene**. Det er derfor spesielt viktig for en virksomhet å ha kontroll på informasjonssikkerheten. Vi kaller det internkontroll på informasjonssikkerhetsområdet.

En lønnsom investering
Alle virksomheter, herunder kommunene, bør ut fra ovennevnte ha **en stor egeninteresse** i å etablere, gjennomføre og holde vedlike en systematisk internkontroll. Det er det som gir dem

- intern styring og kontroll
- tilstrekkelig sikkerhet om at de når sine samlede mål

Etablering av internkontroll kan kreve investering i noe tid og penger, spesielt den første tiden. Det er imidlertid en investering som lønner seg. Man

- blir oppmerksom på og får bedre kontroll på risikoene
- reduserer sannsynligheten for tap av penger, ineffektivt arbeid og lovbrudd
- sikrer bedre måloppnåelse for øvrig

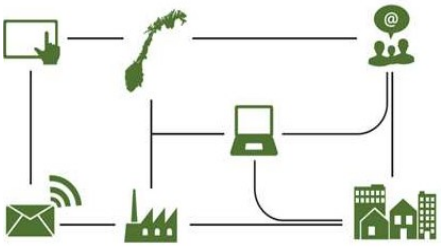
2.2 Myndighetenes behov

I tillegg er internkontroll i virksomhetene viktig for offentlige myndigheter. Offentlige midler skal brukes målrettet og effektivt innenfor lov- og regelverk. Da må vesentlige risikoer identifiseres, analyseres og håndteres på en systematisk måte i alle virksomheter.

Internkontroll sikrer målrettet og effektiv bruk av offentlige midler

Systematikken blir ekstra viktig i en digital verden. Uten tilstrekkelig internkontroll vil risikoer knyttet til informasjonssikkerhet øke i omfang og størrelse. Risikoene vil lett komme ut av kontroll. Kanskje vet ikke ledere og ansatte hva som faktisk skjer og hvilke konsekvenser det får.

Samtidig øker krav og forventninger til offentlige virksomheter. Man må få flere og pålitelige digitale tjenester og sørge for mer effektiv utføring av arbeidet.



Risikoer øker i en digital verden uten internkontroll

Dersom staten og kommunene skal nå sine mål, er de derfor avhengig av at virksomhetene, herunder kommunene, har tilstrekkelig internkontroll på informasjonssikkerhetsområdet.

Offentlige virksomheter er derfor pålagt internkontroll i regelverket. Det er virksomhetsleders ansvar at virksomheten etterlever dette.

2.3 Sentrale regelverkskrav

Generelle krav

Statlige virksomheter har et generelt krav om internkontroll i økonomiregelverket i staten. Kommuner har tilsvarende i kommuneloven.

eForvaltningsforskriften § 15

Forvaltningsorgan skal i tillegg ha en internkontroll (styring og kontroll) på informasjonssikkerhets-området **som baserer seg på anerkjente standarder for** styringssystem for informasjonssikkerhet, jf. eForvaltningsforskriften § 15.

Dette gir strammere føringer for arbeidet med internkontroll innen informasjonssikkerhet, enn de generelle kravene i økonomiregelverket i staten og i kommuneloven. Det henger sammen med risikoenes egenart innen informasjonssikkerhet.

eForvaltningsforskriften § 15 sier også at:

- Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks
- Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem
- Omfang og innretning på internkontrollen skal være tilpasset risiko

De to første er tydelige signal om at man bør samordne internkontrollarbeidet på tvers av regelverk og områder, så langt det er hensiktsmessig. Det siste innebærer at internkontrollarbeid og sikkerhetstiltak skal være tilpasset risiko og vesentlighet.

Samlet handler dette om effektivitet, kvalitet og riktig ressursbruk i arbeidet med internkontroll. Det er virksomhetsleders ansvar at virksomheten har en tilfredsstillende internkontroll.

3 Systematiske aktiviteter

Internkontroll er systematisk arbeid som involverer hele virksomheten. Systematikken er illustrert i figuren under. Figuren er Difis forklaringsmodell for internkontroll på informasjonssikkerhetsområdet. Den er en gjennomgående referanse i dette veiledningsmateriellet.

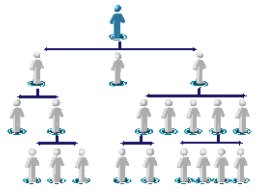
Difis forklaringsmodell for internkontroll

Figuren viser hovedaktivitetene i et systematisk internkontrollarbeid samt hvordan målrettet kommunikasjon binder de øvrige aktivitetene sammen.

Hver av hovedaktivitetene består av et sett **delaktiviteter**. De er kjernen i internkontrollarbeidet og må gjennomføres systematisk. Delaktivitetene må utføres av ulike aktører rundt om i virksomheten.

Overordnede styrende dokumenter

Skal internkontrollen fungere, er det avgjørende at virksomheten har gode overordnede styrende dokumenter. Disse må klargjøre hvem som skal gjøre hva, og gi føringer for arbeidet.



Klarhet i roller og ansvar er en avgjørende del av internkontrollen

Dette er en forutsetning for at de systematiske aktivitetene skal bli gjennomført i tilstrekkelig omfang og på riktig måte. Dokumentene er **fundamentet** i internkontrollen.

Virksomhetsleder bør eie dokumentene. Han må sørge for at de blir etablert og forbedret ved behov.

Fagansvarlig informasjonssikkerhet

En annen avgjørende faktor er å ha eller tidlig få på plass en støttefunksjon som fagansvarlig informasjonssikkerhet eller lignende. Dette er virksomhetsledelsens ansvar. Personen må ha tilstrekkelige ressurser, kompetanse og personlige egenskaper. De viktigste oppgavene er å

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

Både etablering av dokumentene og å få på plass nøkkelpersoner er nærmere omtalt i kapittel 4 Etableringsaktiviteter.

Hovedfokus på operativ risiko

Risikovurderinger bør normalt gjennomføres på flere nivå i virksomhetsstyringen. 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 virksomhetsstyringen

I internkontroll på informasjonssikkerhetsområdet har man i hovedsak blikket rettet mot operativ risiko. Det samme gjelder de fleste andre internkontrollområder.

Det er derfor operative risikoer som er dekket i hovedaktiviteten *Risikovurdering* i dette veiledningsmateriellet. Det er også håndtering av slike risikoer det er fokusert på i veiledningsmateriellet for øvrig.

Materiellet har imidlertid noen eksempler i de overordnede styrende dokumentene som viser hvordan man enkelt kan integrere arbeidet med strategisk og taktisk risiko i en helhetlig internkontroll.

Innhold i hoved- og delaktivitetene

De neste underkapitlene gir en innføring i de systematiske aktivitetene i internkontrollarbeidet. Strukturen følger hovedaktivitetene i forklaringsmodellen vår. Alle aktivitetene er mer utførlig beskrevet i andre deler av veiledningsmateriellet.

3.1 Ledelsens styring og oppfølging

Ledelsens styring og oppfølging er avgjørende for utforming og gjennomføring av internkontrollen. Vi kaller den «hjernen» i internkontrollen.

Ledelsens styring og oppfølging kan kalles hjernen i internkontrollen

Ledelsens styring og oppfølging involverer både virksomhetsleder og ledere på øvrige nivå.

3.1.1 Virksomhetsledelsens gjennomgang

Virksomhetsledelsens gjennomgang er den overordnede styrende og kontrollerende delen av internkontrollen i en virksomhet. Gjennomføring bør skje minimum en gang årlig. Hele toppledergruppa bør delta. Virksomhetsleder er selv ansvarlig for aktiviteten. Den gjennomføres best i et toppledermøte.

Formålet er å

- avklare status på virksomhetens samlede internkontrollarbeid innen informasjonssikkerhet
- avklare status på områder og tjenester der toppledelsen er spesielt opptatt av informasjonssikkerheten
- reagere og følge opp der det er nødvendig

Virksomhetsledelsens gjennomgang bør skje minimum en gang årlig

Fagansvarlig informasjonssikkerhet må lage et godt saksnotat til møtet og gjennomgangen. Det er en forutsetning for en vellykket gjennomføring.

Gjennomgangen bør ha klare konklusjoner og ansvarlige for oppfølgingspunkter. **Ved behov** bør virksomhetsleder

- sørge for at det skjer en forbedring av de overordnede styrende dokumentene
- gi tilleggsføringer for internkontroll- og sikkerhetsarbeidet
- stille og følge opp spesifikke krav til enkelte ledere og enheter
- vurdere om man skal måle tilstanden på enkelte indikatorer over tid
- vurdere om man skal få gjennomført evalueringer på større eller mindre deler av internkontrollen
- vurdere om man skal få gjennomført formell internrevisjon

Dersom noen av de tre siste velges, blir de en del av internkontrollens måling, evaluering og revisjon, jf. kapittel 3.5.

3.1.2 Øvrige aktiviteter

Ledere på alle nivå har også en viktig rolle i hovedaktiviteten *Ledelsens styring og oppfølging*. De er ansvarlig for systematisk gjennomføring av følgende aktiviteter:

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

Ordinære lederoppgaver må også omfatte informasjons-sikkerhet

Dette er normalt ledernes ordinære oppgaver som linjeledere på andre områder. Poenget her er at aktivitetene også må omfatte informasjonssikkerhet. Dette er avgjørende for å få internkontrollen til å fungere på informasjonssikkerhetsområdet.

3.2 Risikovurdering

Internkontroll handler om risikostyring. Risikovurdering er den grunnleggende aktiviteten i risikostyringen. Uten risikovurderinger får man ingen risikostyring eller internkontroll. Vi kaller risikovurdering «hjertet» i internkontrollen.

Risikovurdering kan kalles hjertet i internkontrollen

Risikovurderinger må skje rundt om i hele virksomheten av de som har ansvaret for gjennomføring av arbeidet, målene som skal nås og konsekvensene dersom risikoer blir en realitet. Det er ikke bare «tradisjonelle risikovurderinger» som må gjennomføres. Det er også behov for å gjennomføre en del støtteaktiviteter rundt disse.

Hovedaktiviteten *Risikovurdering* involverer risikoeiere og systemeiere fellessystem.

Risikoeier

Begrepet risikoeier brukes her om alle ledere med ansvar for konkrete arbeidsoppgaver og tjenester rundt om i virksomheten. De er ansvarlig for utføring av arbeidet og de mål som skal nås. De bør da også eie og være ansvarlig for å identifisere, vurdere og håndtere risikoer innen eget ansvarsområde.

Ansvaret som risikoeier for operative risikoer vil normalt bli delegert til laveste ledernivå. Det gjelder både kjerneoppgaver, de man gjør for å nå virksomhetens primære mål, og støtteoppgaver, typisk administrative oppgaver.

Risikoeier = leder for operativ oppgave

For styringsoppgaver vil ansvaret som risikoeier ligge på ulike ledernivå, avhengig av styringsoppgavens egenart og de involverte ledernes rolle.

Når system, herunder digitale tjenester, understøtter kun én risikoeiers mål og arbeidsoppgaver, bør risikoeieren selv være systemeiere for disse systemene. Dette bør være en del av en risikoeier sitt samlede ansvarsområde.

Systemeiere fellessystem

Fellessystem er system, herunder digitale tjenester, som støtter arbeidsoppgaver hos flere risikoeiere. Eksempler er arkivsystem, e-post, den grunnleggende IKT-infrastrukturen og et felles system eller en felles digital tjeneste for tilskuddsforvaltning.

Begrepet systemeier fellessystem brukes her om leder for enheter som er utpekt til å forvalte ett eller flere fellessystem. Lederen vil ofte peke ut en person som systemforvalter eller lignende. Denne har det daglige ansvaret for enkeltsystem eller en digital tjeneste, og rapporterer til systemeier.

Systemeiere fellessystem er fellesfunksjoner i virksomheten

Systemeiere fellessystem skal ivareta interessene til risikoeierne som benytter systemene. Risikoeierne er likevel ansvarlig for egen bruk av fellessystem og risikoene det medfører. Risikoeierne må derfor på hensiktsmessig måte informeres og involveres i internkontrollarbeid knyttet til fellessystemene.

Aktiviteter

Risikoeiere og systemeiere fellessystem må systematisk få gjennomført følgende aktiviteter under *Risikovurdering:*

- Få oversikt og prioritere
- Analysere eksterne krav
- Planlegge risikovurdering

- Gjennomføre risikovurdering
- Vurdere risiko i hendelseshåndteringen
- Vurdere risiko ved anskaffelser og utvikling

3.2.1 Få oversikt og prioritere

Lederne må først få oversikt for å prioritere riktig

Risikoeiere og systemeiere fellessystem må tidlig få oversikt over eget ansvarsområde, gruppere det i hensiktsmessige delområder, og systematisk prioriterer hvor og når de bør få gjennomført nye eller oppdaterte risikovurderinger innen informasjonssikkerhet.

Aktiviteten omfatter bl.a. kartlegging av arbeidsoppgaver, informasjonstyper, regelverk, IKT-system som benyttes, hvilke konsekvensnivå brudd på informasjonssikkerheten kan gi, mv. Dette veiledningsmateriellet har flere maler og støttedokument som forenkler arbeidet. Vi anbefaler at man benytter en prosessleder med litt erfaring i gjennomføringen av sentrale deler.

Aktiviteten kan ofte med fordel gjennomføres i ledergruppen over operativt nivå. Når grunnarbeidet først er gjort, handler aktiviteten mest om avstemming og jevnlige oppdateringer.

3.2.2 Analysere eksterne krav

Målet med aktiviteten er å identifisere krav om sikkerhetstiltak eller typer tiltak som ligger i regelverk og avtaler som gjelder eget ansvarsområde.

Konkrete krav i regelverk og avtaler må identifiseres

En lignende aktivitet anbefales som fellesaktivitet på virksomhetsnivå, jf. kapittel *4 Etableringsaktiviteter*. Er etableringsaktiviteten gjennomført, kan man i hovedsak sjekke ut og benytte resultatet derfra. I tillegg må man analysere det som eventuelt er spesielt for eget ansvarsområde.

Også her ligger mesteparten av arbeidet i å gjennomføre aktiviteten første gang. Senere handler det om å holde seg oppdatert ved endringer i regelverk og avtaler samt når man får nye arbeidsoppgaver.

3.2.3 Planlegge og gjennomføre risikovurderinger

Risikovurderinger med ulik innretning

De øvrige aktivitetene under *Risikovurdering* handler om å planlegge og gjennomføre risikovurderinger. Hvilke områder det bør gjennomføres nye eller oppdaterte risikovurderinger på, bør i hovedsak bli styrt av resultatene fra aktiviteten *Få oversikt og prioritere* - jf. kapittel 3.2.1.

I tillegg bør man alltid vurdere om det er behov for avgrensede risikovurderinger i tilknytning til hendelseshåndteringen. Man kan da unngå å bare drive brannslukking. Man bør også alltid gjennomføre risikovurderinger som en del av anskaffelse og utvikling av IKT-system.

Hovedtrinnene i en risikovurdering

Risikovurdering = identifisere, analysere og evaluere risikoer

En risikovurdering består av trinnene identifisere, analysere og evaluere risikoer. Under evaluering skal risikoene vurderes opp mot virksomhetens kriterier for å akseptere risiko. Man vil da avdekke om det er behov for videre risikohåndtering. Det er beskrevet i neste hovedaktivitet. Kriteriene for å akseptere risiko bør fremgå i ett av de overordnede styrende dokumentene.

Planlegge og gjennomføre risikovurderinger
Risikovurderinger bør planlegges før de gjennomføres. Det er blant annet viktig at de som kjenner arbeidsoppgavene og bruken av systemene blir involvert i vurderingene. Det er de som har best kunnskap om mulige konsekvenser. De vet også mye om hva som går og kan gå galt underveis.

For risikovurderinger ut over det helt enkle, vil en prosessleder med litt erfaring være viktig støtte. Det bidrar til effektiv gjennomføring og tilstrekkelig kvalitet.

Gjennomføringen bør følge en systematisk fremgangsmåte. Den bør være fleksibel, slik at den kan tilpasses området som skal vurderes. Dette veiledningsmateriellet inneholder en slik fremgangsmåte.

3.3 Risikohåndtering

Trinnet evaluere i en risikovurdering, jf. kapittel 3.2.3, vil vise hvilke risikoer som må håndteres. Vi kaller risikohåndtering «hendene» i internkontrollen.


Risikohåndtering kan kalles hendene i internkontrollen

Hovedaktiviteten *Risikohåndtering* involverer risikoeiere, systemeiere fellessystem og tiltaksleverandører. Rollene risikoeier og systemeiere fellessystem er beskrevet i kapittel 3.2.

Tiltaksleverandører
Tiltaksleverandører leverer sikkerhetstiltak som skal dekke behovene til risikoeiere og systemeiere fellessystem. Dette vil normalt inkludere utforming, iverksetting, oppfølging og vedlikehold av sikkerhetstiltakene. Den formelle tiltaksleverandøren er leder for den enheten som leverer tiltakene.

Flere tiltaksleverandører er ansvarlige for sikkerhetstiltak til en rekke ulike risikoeiere og systemeiere. Disse kan kalles felles tiltaksleverandører. Eksempler er IKT-drift, systemleverandører, bygningsansvarlig og personalenhet.

Felles tiltaks-leverandører er fellesfunksjoner i virksomheten

Tiltaksleverandører kan være både interne og eksterne. Tiltakene de leverer kan ha flere formål enn informasjonssikkerhet. De kan også dekke risikoer innen HMS, verdisikring, kvalitet mv.

Risikoeiere og systemeiere fellessystem kan også være tiltaksleverandører til egne arbeidsoppgaver og system. Tiltakene vil da ofte være rutinebeskrivelser, opplæring og krav til gjennomføring av arbeidet eller bruk av systemene.

Aktiviteter
Risikoeiere og systemeiere fellessystem må systematisk få gjennomført følgende aktiviteter under *Risikohåndtering:*

- Foreslå håndtering av risikoer
- Godkjenne forslag til risikohåndtering
- Iverksette godkjente tiltak

Tiltaksleverandørene må gjennomføre følgende aktiviteter som oppfølging av dette:

- Utforme og implementere tiltakene
- Oppdatere fellessikring og tilleggssikring

3.3.1 Foreslå håndtering av risikoer

Aktiviteten *Foreslå håndtering av risikoer* er en direkte oppfølging av konkrete risikovurderinger i forrige hovedaktivitet *Risikovurdering*. De to delaktivitetene slås ofte sammen til en oppgave. Dette er ofte mest hensiktsmessig i praksis.

Hovedvalg i risikohåndtering = unngå, dele, redusere eller akseptere risiko

Håndtering av risiko gjør man ved å unngå, dele, redusere eller akseptere risikoen. Sikkerhetstiltak kan redusere risiko. Valg av håndtering bør være basert på virksomhetsleders føringer i de overordnede styrende dokumentene.

Som fremgangsmåte bør man også her benytte en systematisk metode. Dette veiledningsmateriellet inneholder en slik. Den er direkte koblet til metoden for gjennomføring av risikovurderinger.

3.3.2 Godkjenne forslag til risikohåndtering

Både risikovurderinger og forslag til håndtering av risikoer er beslutningsgrunnlag for ledere. Arbeidet utføres på oppdrag fra en risikoeier eller systemeier fellessystem.

Forslag til risikohåndtering må godkjennes av leder

Lederen bør alltid ta selvstendig stilling til arbeidet som er utført, og forslagene man er kommet frem til. Det er lederen som kan akseptere risikoer. Det er også hun som må sikre finansiering av tiltakene.

Systemeiere fellessystem må avstemme sin aksept av risiko og valg av tiltak med de risikoeierne som benytter fellessystemene.

Spesielle problemstillinger må løftes gjennom linjen. Det kan for eksempel være aktuelt dersom

- lederen ikke har myndighet til å akseptere visse risikoer
- lederen ikke har dekning på budsjettet til å finansiere nødvendige tiltak
- det er uenighet mellom risikoeiere og systemeier fellessystem om aksept av risiko eller innføring av tiltak som gir negative sideeffekter for en eller flere

3.3.3 Iverksette godkjente tiltak

Når tiltak er godkjent må den aktuelle lederen sørge for at beslutningen blir iverksatt. Dette kan omfatte leveranser fra flere tiltaksleverandører.

Iverksetting innebærer avtaler og oppfølging

Det vil ofte være hensiktsmessig å peke ut en person i egen enhet med ansvar for iverksettingen. Denne kan kalles håndteringsansvarlig. Hun må rapportere fremdrift til aktuell risikoeier eller systemeier fellessystem. Ved enkle tiltak kan lederen selv være håndteringsansvarlig.

Det vil ofte være nyttig å lage en plan for arbeidet. Man bør inngå klare avtaler med tiltaksleverandørene, slik at planen kan konkretiseres og følges opp. Formalisering bør tilpasses risiko og vesentlighet.

Tiltaksleverandører utformer og implementerer tiltakene

3.3.4 Utforme og implementere tiltakene

Tiltaksleverandører skal utforme og implementere tiltak i samsvar med avtaler gjort med ulike håndteringsansvarlige. Tiltakene må testes slik det er avtalt.

Håndteringsansvarlig må informeres om fremdrift og testresultat. Hun er bindeleddet mot aktuell risikoeier eller systemeier fellessystem.

3.3.5 Oppdatere fellessikring og tilleggssikring

Alle tiltaksleverandører må systematisk vurdere hvilke tiltak som bør etableres som henholdsvis fellessikring og tilleggssikring.

Fellessikring er sikkerhetstiltak som gjelder for alle oppgaver, systemer og ansatte i virksomheten. Tilleggssikring er sikkerhetstiltak som gjelder for de med spesielle risikoer og ekstra behov for tiltak.

Fordelingen mellom fellessikring og tilleggssikring bør styres av hva som gir best nytte/kost for virksomheten samlet. Man bør ta hensyn til

- hvor mange som har vesentlig nytte av sikkerhetstiltaket
- omfanget av negative sideeffekter av tiltaket for risikoeiere med lav nytteverdi
- behovet for kostnadseffektiv drift av det samlede sikkerhetsarbeidet

Nytte/kost for virksomheten samlet bør avgjøre om tiltak blir fellessikring eller tilleggssikring

Forslag om økning eller reduksjon av fellessikringen kan komme fra både tiltaksleverandører og risikoeiere. Fagansvarlig informasjonssikkerhet bør lede og koordinere arbeid med å avgjøre endringer i fellessikringen. Beslutning bør tas av virksomhetsleder eller den hun har pekt ut.

3.4 Overvåking og hendelseshåndtering

Man må akseptere og leve med noe risiko. Det er hverken er mulig eller kostnadseffektivt å identifisere og fjerne alle. Man må derfor systematisk overvåke der det er nødvendig, og identifisere, følge opp og lære av uønskede hendelser. Vi kaller overvåking og hendelseshåndtering «vakta» i internkontrollen.

Overvåking og hendelseshåndtering kan kalles vakta i internkontrollen

Hovedaktiviteten *Overvåking og hendelseshåndtering* involverer risikoeiere, systemeiere fellessystem, tiltaksleverandører og øvrige ansatte.

Aktiviteter

Tiltaksleverandører må systematisk få gjennomført aktiviteten:

- Overvåke i henhold til avtale

Alle ansatte må systematisk:

- Rapportere hendelser, avvik og informasjonssikkerhetsbrudd

Tiltaksleverandører, systemeiere fellessystem, risikoeiere og øvrige ledere må systematisk:

- Følge opp hendelser, avvik og informasjonssikkerhetsbrudd

3.4.1 Overvåke i henhold til avtale

Overvåking er sikkerhetstiltak som velges på bakgrunn av risikovurderinger. Det kan være overvåking av fysiske områder, tekniske komponenter, logger mv. Hva som skal overvåkes og hvordan, er en del av det aktuelle tiltakets utforming. Det samme gjelder krav til når og hvordan man skal rapportere det man oppdager av uønskede hendelser.

Overvåking må utføres som avtalt

For eksterne tiltaks- eller tjenesteleverandører bør omfang og krav være nedfelt i en tjenestenivåavtale (SLA). For interne tiltaksleverandører vil det ofte være nok at det fremkommer tydelig i beskrivelsen av tiltaket.

3.4.2 Rapportere hendelser, avvik og informasjonssikkerhetsbrudd

Alle ansatte må rapportere i samsvar med klare krav. Det gjelder også tiltaksleverandører og eksterne som arbeider i eller for virksomheten.

Hva som skal rapporteres, hvem som skal rapportere og når og hvordan det skal skje, bør fremgå tydelig av inngåtte avtaler og av virksomhetens system for hendelses- og avvikshåndtering. Etablering av det siste er omtalt i kapittel 4 *Etableringsaktiviteter*.

For at kravene skal bli etterlevd, er det viktig at

- omfanget er på et hensiktsmessig nivå
- at selve gjennomføringen er enkel
- at det er synlig at rapporteringen blir tatt positivt imot og fulgt opp systematisk

Uønskede hendelser mv. må rapporteres systematisk og enkelt

Ellers vil det ofte utvikles en negativ kultur som hemmer nødvendig rapportering.

3.4.3 Følge opp hendelser, avvik og informasjonssikkerhetsbrudd

Hvem som skal informeres og hvem som skal følge opp ulike typer hendelser, avvik og informasjonssikkerhetsbrudd, bør fremgå tydelig av inngåtte avtaler og av virksomhetens system for hendelses- og avvikshåndtering. Informasjonsflyten for ulike hovedtyper bør være klart definert.

For effektiv håndtering av alvorlige sikkerhetsbrudd, kan det være viktig med rask reaksjon. Rapporterings- og oppfølgingsrutinene må sikre dette.

Oppfølging bør stå i forhold til risikoens størrelse samt hendelsen, avviket og informasjonssikkerhetsbruddet egenart. Aktuelle responser kan være en eller flere av følgende:

- Iverksette krise- og beredskapsplaner
- Iverksette andre prosedyrer for konsekvensreduserende tiltak
- Iverksette akutte konsekvensreduserende tiltak
- Rette opp feil i eller forbedre utformingen av avtalte sikkerhetstiltak
- Styrke kompetanse og kultur hos ansatte
- Oppdatere risikovurderinger og forslag til håndtering av risiko
- Akseptere risikoen ved at det kan skje igjen

Uønskede hendelser mv. må følges opp systematisk med relevant håndtering

Oppfølging kan dermed involvere flere aktører og alle hovedaktiviteter i internkontrollen.

3.5 Måling, evaluering og revisjon

Man må systematisk vurdere om sikkerhetstiltak fungerer, om regelverk etterleves og om internkontrollarbeidet rundt om i virksomheten blir gjennomført som forutsatt. Ellers kommer risikoene ut av kontroll. Vi kaller måling, evaluering og revisjon for «kontrolløren» i internkontrollen.

Måling, evaluering og revisjon kan kalles kontrolløren i internkontrollen

Hovedaktivitetene *Måling, evaluering og revisjon* involverer ledere på alle nivå samt spesialfunksjoner og enkelte ansatte.

Aktiviteter
Ledere på alle nivå må systematisk:

- Vurdere status på eget ansvarsområde

Ved regelverkskrav eller krav fra ledelsen må ulike aktører:

- Måle tilstanden på definerte indikatorer
- Gjennomføre evalueringer
- Gjennomføre internrevisjon

3.5.1 Vurdere status på eget ansvarsområde

Ledere på alle nivå bør minst en gang årlig systematisk vurdere status innen eget ansvarsområde. Det omfatter en reell vurdering av

- om sikkerhetstiltak de har ansvaret for fungerer som forutsatt
- om de selv og de personer de har ansvaret for
  - følger gjeldende lov- og regelverk
  - gjennomfører pålagte oppgaver i internkontroll- og sikkerhetsarbeidet på en tilfredsstillende måte
  - etablerer og følger opp vedtatte eller avtalte sikkerhetstiltak
  - etterlever innførte sikkerhetstiltak

Lederne bør minst en gang årlig systematisk vurdere status på eget ansvarsområde

Viktige grunnlag er

- egne observasjoner
- formelle og uformelle medarbeidersamtaler
- tilbakemelding fra andre
- rapportering eller indikasjoner fra avviks- og hendelseshåndteringen

Er lederen usikker på om status er tilfredsstillende, bør hun gjennomføre nærmere undersøkelser. Dette kan være enkle undersøkelser eller mer omfattende evalueringer, avhengig av hva det gjelder. Ved vesentlige avvik og mangler må tiltak iverksettes for å rette opp forholdene.

3.5.2 Måle tilstanden på definerte indikatorer

Ønsker ledelsen å følge tilstanden i virksomheten over tid, kan det være hensiktsmessig å etablere et system med relevante indikatorer som kan måles og analyseres jevnlig. Beslutning om å iverksette aktiviteten, tas normalt i tilknytning til virksomhetsledelsens gjennomgang, jf. kapittel 3.1.

Måling av indikatorer må skje systematisk

Man må da først peke ut noen som skal lage et forslag til målinger. Hvem som skal gjøre hva når målinger skal gjennomføres, er avhengig av ledelsens beslutning på bakgrunn av forslaget.

Det er viktig med et edruelig ambisjonsnivå. Man bør i første omgang velge ut noen få indikatorer på noen nøkkelområder. Da kan man også bedre se og vurdere ressursbruken i forhold til nytten.

3.5.3 Gjennomføre evalueringer

Evaluering er systematiske undersøkelser av et visst omfang

Evalueringer er systematiske undersøkelser av et visst omfang. Man ser normalt på status innen et definert område. Evalueringer kan gjennomføres på oppdrag fra ledere på alle nivå. Det er også de som mottar evalueringsrapporten, og er ansvarlig for nødvendig oppfølging.

Et evalueringsoppdrag bør være spesifisert og avgrenset. Evalueringer kan ledes og utføres av både interne og eksterne. Tilgjengelige ressurser og behov for uavhengighet til det som skal evalueres, er viktige kriterier når man velger hvem som skal utføre oppdraget.

Evalueringer kan for eksempel være:

- Analyse av status på internkontrollområdet informasjonssikkerhet generelt, eller på et spesifikt delområde, utført på oppdrag fra virksomhetsledelsen, jf. kapittel 3.1.1.
- Gjennomføring av lovpålagte eller avtalte systemgjennomganger, systemrevisjoner o.l., utført på oppdrag fra risikoeiere eller systemeiere fellessystem
- En grundig undersøkelse som oppfølging av en leders usikkerhet i aktiviteten *Vurdere status på eget ansvarsområde*, jf. kapittel 3.5.1.

3.5.4 Gjennomføre internrevisjon

Formålet med internrevisjon er å få en formell vurdering av om virksomheten følger bestemte krav, og om kravene er implementert og vedlikeholdt på en formåls- og kostnadseffektiv måte. Kravene kan være både eksterne og interne.

Internrevisjon bør følge anerkjente standarder

Det er normalt virksomhetsleder som avgjør behovet, og bestiller en eventuell internrevisjon. Det er også hun som mottar og må følge opp revisjonsrapporten.

Internrevisjon har klare likhetstrekk med evalueringer. For å kalle det internrevisjon, bør gjennomføringen følge anerkjente standarder. Disse kan ha egne deler for ulike revisjonsområder, eksempelvis internkontroll eller styringssystem for informasjonssikkerhet.

Ofte vil evalueringer, med et tydelig mandat og tilstrekkelig uavhengige utførere, være gode alternativ til formelle internrevisjoner.

3.6 Kompetanse- og kulturutvikling

Kompetanse- og kulturutvikling kan kalles læreren i internkontrollen

Man er avhengig av god kompetanse hos de ansatte og en understøttende organisasjonskultur. Det må følges opp systematisk. Vi kaller kompetanse- og kulturutvikling «læreren» i internkontrollen.

Hovedaktivitetene *Kompetanse- og kulturutvikling* involverer ledere på alle nivå samt fagansvarlig informasjonssikkerhet.

En avgjørende del av internkontrollen

Både kompetanse og kultur er en avgjørende del av internkontrollen. Organisasjonskultur er den uoffisielle påvirkningen som skjer mellom ansatte. Den blir ofte omtalt som «slik gjør vi det hos oss».

Alle ansatte må kjenne til, være bevisst og i stand til å etterleve sitt ansvar. Organisasjonskulturen må understøtte forståelse, kompetanse samt etterlevelse og forbedring av krav og sikkerhetstiltak. Det

innebærer også identifisering, justering og fjerning av krav og tiltak som har liten nytte, eller som gir negative sideeffekter for alle eller deler av organisasjonen.

Å sørge for tilstrekkelig informasjon, opplæring og kulturutvikling er tiltak for å redusere risiko.

Lokale sikkerhetskoordinatorer
I virksomheter av en viss størrelse kan det være behov for lokale ressurspersoner innen informasjons-sikkerhet. De kan kalles lokale sikkerhetskoordinatorer. Oppgavene vil naturlig være lokal lederstøtte, ressursperson og pådriver.

Hvem som peker dem ut og hvor mange organisatoriske enheter de skal dekke, er avhengig av virksomhetens størrelse og organisering. Funksjonen kan legges til en ordinær fagstilling.

Sikkerhetskoordinator er lokal lederstøtte, ressurs-person og pådriver

Funksjonen vil ofte ha stor betydning for de lokale ledernes kompetanse, og det praktiske arbeidet med internkontroll og informasjonssikkerhet rundt om i virksomheten.

Aktiviteter
Ledere på alle nivå må systematisk gjennomføre følgende aktiviteter under *Kompetanse- og kulturutvikling*:

- Identifisere behov løpende
- Følge opp behovene systematisk

Fagansvarlig informasjonssikkerhet må systematisk gjennomføre aktiviteten:

- Følge opp lokale sikkerhetskoordinatorer

3.6.1 Identifisere behov løpende

Å identifisere behov for kompetanse- og kulturutvikling er en ordinær og kontinuerlig aktivitet i lederarbeid på alle nivå. Det må også omfatte behov innen informasjonssikkerhet, dvs.:

- Forståelse av hva informasjonssikkerhet handler om
- Forståelse og gjennomføring av internkontrollaktivitetene
- Forståelse og etterlevelse av krav, prosedyrer, rutiner og andre sikkerhetstiltak

Behov for kompetanse- og kulturutvikling bør identifiseres som en del av det løpende arbeidet

Behov kan identifiseres under gjennomføring av flere aktiviteter i internkontrollen. Formelle og uformelle medarbeidersamtaler samt observasjoner i gjennomføring av arbeidet, er også viktige kilder.

3.6.2 Følge opp behovene systematisk

Når man har identifisert et behov som bør dekkes, må lederne sørge for å få gjennomført hensiktsmessige tiltak.

Kompetanse- og kulturutvikling bør skje systematisk med ulike virkemidler

For mindre ting kan det være nok å gi bedre informasjon. Ved mer omfattende behov bør tiltak planlegges. Tiltakene bør være målrettede, bestå av hensiktsmessige virkemidler og være tilstrekkelig varierte.

Man bør alltid vurdere hva som bør gjennomføres på virksomhetsnivå, i enkelte organisatoriske enheter, for mindre grupper eller enkeltpersoner.

Fagansvarlig informasjonssikkerhet vil være en naturlig støtte og koordinator på virksomhetsnivå. Lokale sikkerhetskoordinatorer vil være naturlig støtte lokalt.

3.6.3 Følge opp lokale sikkerhetskoordinatorer

For å sikre god effekt av lokale sikkerhetskoordinatorer, bør fagansvarlig informasjonssikkerhet systematisk følge opp disse. Hun bør gjennomføre jevnlige samlinger og være lett tilgjengelig for råd. Målet er å

- formidle kunnskap
- dele erfaringer
- få bedre innsikt i virksomhetens utfordringer
- lære av hverandre.

Lokale sikkerhets-koordinatorer må følges opp systematisk

3.7 Kommunikasjon

Kommunikasjon binder sammen de andre hoved- og delaktivitetene samt aktørene som utfører disse. Vi kaller kommunikasjon for «limet» i internkontrollen. Kommunikasjon involverer alle aktørene i internkontrollarbeidet.

Aktiviteter

Ledere på alle nivå må systematisk:

- Formidle nye føringer
- Dokumentere gjennomførte internkontrollaktiviteter

Kommunikasjon kan kalles limet i internkontrollen

Fagansvarlig informasjonssikkerhet må systematisk

- Utarbeide statusrapporter som grunnlag for risikovurderinger
- Utarbeide saksnotat til virksomhetsledelsens gjennomgang

Ulike aktører må ut fra definerte krav:

- Dokumentere etterlevelse av tiltak
- Utføre sin del av ekstern kommunikasjon

Alle ansatte må systematisk bidra til:

- Kommunikasjon mellom aktiviteter og aktører

3.7.1 Formidle nye føringer

Nye føringer for arbeidet må formidles raskt og effektivt til de som har eller kan få bruk for dem. Føringene må være enkelt tilgjengelig over tid. Det krever normalt at de er dokumenterte, lagret og tilgjengeliggjort på en systematisk måte.

Føringer for arbeidet må formidles raskt og effektivt og nå målgruppen

Ansvaret ligger hos de som gir føringene. Lagrings- og formidlingskanalene bør være koordinert på virksomhetsnivå, slik at man får en helhet i virksomhetens dokumentasjon av internkontroll.

Den ansvarlige bør alltid vurdere om det i tillegg er behov for informasjonsmøter, opplæringstiltak og lignende. Man må forsikre seg om at føringene når frem til rette mottakere, er forstått samt at mottakeren har tilstrekkelig kompetanse til å etterleve føringene.

3.7.2 Dokumentere gjennomførte internkontrollaktiviteter

Gjennomføring av de systematiske aktivitetene i internkontrollen bør som hovedregel dokumenteres skriftlig. Dette kan oftest gjøres enkelt som en del av gjennomføringen. Ansvaret ligger hos de som er ansvarlig for aktiviteten, men hvor ting skal lagres bør være samordnet på virksomhetsnivå.

Ved bruk av gode maler, ved å ha fokus på å dokumentere det viktigste, og ved å integrere dokumentasjonsarbeidet i virksomhetens ordinære arkiverings- og journalføringsrutiner, vil slik dokumentasjon i liten grad representere vesentlig merarbeid.

Gjennomførte internkontrollaktiviteter bør alltid dokumenteres

Samtidig vil systematisk dokumentering sikre at det som er gjort og bakgrunnen for beslutninger og selve beslutningene, blir en del av virksomhetens hukommelse. Dette vil være viktig og nyttig både som kontrollgrunnlag, og ved behov for etterlevelse, opplæring og oppdateringer.

3.7.3 Dokumentere etterlevelse av tiltak

Etterlevelse av prosedyrer, rutiner og andre sikkerhetstiltak må dokumenteres skriftlig dersom tiltakene stiller konkrete krav om det. Hvem som har ansvaret må fremgå av tiltaket.

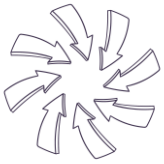
Dokumentasjonskrav bør være risikobaserte og klart forankret i behov. Behovene vil variere, avhengig av hvilke risikoer tiltaket skal dekke, type tiltak, kompetanse og kultur blant de ansatte samt behov for å kontrollere etterlevelse.

Etterlevelse av tiltak må dokumenteres når det er nødvendig, og på enkel måte

Dokumentasjonskrav må utformes slik at de ikke oppleves unødvendig eller vesentlig hemmende for annet viktig arbeid. Gjør de det, må man justere formen eller styrke forståelsen for hvorfor dokumentasjonen er viktig.

3.7.4 Utarbeide statusrapporter som grunnlag for risikovurderinger

Risikoeiere og systemeiere fellessystem skal systematisk vurdere behovet for og eventuelt få gjennomført nye eller oppdaterte risikovurderinger innen eget ansvarsområde, jf. kapittel 3.2. For å gjøre gode vurderinger og ta de riktige valgene, trenger de relevant informasjon som supplerer egne observasjoner og mottatte tilbakemeldinger.



Statusrapporter sammenstiller nyttig informasjon til risikovurderinger

Fagansvarlig informasjonssikkerhet bør derfor systematisk utarbeide statusrapporter som grunnlag for risikovurderinger. Dette krever en vurdering og oppsummering av relevante forhold og trender både internt i virksomheten, i sammenlignbare virksomheter og nasjonalt.

Virksomhetens system for hendelses- og avvikshåndtering vil være en viktig kilde. Ulike aktører rundt om i virksomheten vil også være viktige informasjonskilder. Både samarbeidspartnere og offisielle rapporter kan være eksterne kilder.

3.7.5 Utarbeide saksnotat til virksomhetsledelsens gjennomgang

Virksomhetsledelsen gjennomgang er avhengig av et godt forberedende saksnotat, jf. kapittel 3.1. Det er en forutsetning for en vellykket gjennomføring og reell styring og kontroll. Fagansvarlig informasjonssikkerhet bør utarbeide notatet i samsvar med føringer fra virksomhetsleder.

Virksomhetsledelsens gjennomgang er avhengig av et godt saksnotat

Dokumentasjon av gjennomførte internkontrollaktiviteter vil være en viktig kilde. Det samme vil virksomhetens system for hendelses- og avvikshåndtering, evalueringer og revisjoner. Både samarbeidspartnere og offisielle rapporter kan være eksterne kilder.

Innretningen er avhengig av hvor langt virksomheten er kommet i etablering av systematisk internkontroll på informasjonssikkerhetsområdet.

Notatet 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

3.7.6 Kommunikasjon mellom aktiviteter og aktører

Alle aktiviteter i internkontrollen er avhengig av effektiv kommunikasjon med andre aktiviteter og mellom ulike aktører.

Ansatte, støttesystem og kultur må bidra til effektiv kommunikasjon internt

Alle ansatte bør ha et klart ansvar for å bidra til at riktig informasjon kommer frem til riktig person til riktig tid. Ivaretagelse av lovpålagt taushetsplikt og etterlevelse av krav om unntatt offentlighet, ligger i begrepet riktig informasjon til riktig person.

Virksomheten må ha gode støttesystemer som understøtter effektiv kommunikasjon. I tillegg må organisasjonskulturen også understøtte dette.

3.7.7 Ekstern kommunikasjon

Kommunikasjon med personer utenfor virksomheten om risikoer, tiltak, internkontroll, informasjonssikkerhet, mv., må skje i samsvar med virksomhetens policy og retningslinjer for ekstern kommunikasjon generelt.

Ekstern kommunikasjon må skje i samsvar med policy og retningslinjer

Lovpålagt taushetsplikt og interne føringer om unntatt offentlighet og meroffentlighet etter offentleglova, må ligge til grunn for all ekstern kommunikasjon.

4 Etableringsaktiviteter

Etableringsaktiviteter er sentrale støtteaktiviteter under etablering og forbedring av internkontrollen. Av pragmatiske grunner er de her kun kalt etableringsaktiviteter. De kan gjennomføres når som helst, ved behov. Som samlet gruppe har de størst relevans under etablering av internkontrollen.

Etableringsaktiviteter støtter etablering og vesentlig forbedring av internkontrollen

4.1 Avklare behov og lage en plan

Aktiviteter

- Analysere status
- Planlegge etablering/forbedring

4.1.1 Analysere status

Er omfang og kvalitet på det vi har godt nok?

Man må vite noe om hvor man er for å vite om status er tilfredsstillende, eller om noe bør gjøres. Dersom virksomhetsledelsen er usikker på om omfang og kvalitet i internkontrollarbeidet på informasjonssikkerhetsområdet er godt nok, bør de få gjennomført en analyse av status.

Benchmarking opp mot Difis veiledningsmateriell

En mal og et støttedokument til hjelp i en analyse av status, er tilgjengelig i dette veiledningsmateriellet. Man vurderer da status i virksomheten opp mot veiledningsmateriellets anbefalte aktiviteter og dokumentasjon. Det tilsvarer benchmarking med Difis veiledningsmateriell som referanse.

Analyse av status opp mot veiledningsmateriellet = Benchmarking

Organisering av arbeidet

Analysen bør gjennomføres av en liten arbeidsgruppe med god innsikt i virksomhetens organisering, aktiviteter og eksisterende internkontroll. Gruppen må normalt snakke med flere interne aktører.

Det er viktig at deltakerne i arbeidsgruppen ikke er opptatt av å forsvare det som er gjort tidligere. Følelsesmessig uavhengighet til det som skal analyseres, er en forutsetning for et pålitelig resultat.

4.1.2 Planlegge etablering/forbedring

Hvordan komme videre?

En analyse av status er grunnlaget for valg av veien videre. Beslutter virksomhetsledelsen at man skal etablere eller vesentlig forbedre internkontrollen, bør de peke ut noen som skal lage og følge opp en plan for arbeidet.

Et langsiktig arbeid

Etablering av internkontroll handler om både utforming av styrende dokumenter, andre etableringsaktiviteter samt det man anser som nødvendig for å få de systematiske aktivitetene i gang i hele virksomheten. Det siste innebærer informasjon, opplæring og de første rundene i gjennomføringen. Samtidig må man tilpasse tidsbruken til virksomhetens løpende aktiviteter.

Planen vil derfor ofte gå over flere år. Den kan med fordel grovplanlegges for hele planperioden, og detaljplanlegges for avgrensede perioder underveis. Det bør være en ordinær prosjektplan med klare aktiviteter og ansvarlige utførere.

Etablering kan kreve en langsiktig plan

Forankring i virksomhetsstyringen

For å sikre gjennomføring og fremdrift, bør planen forankres og følges opp i den ordinære virksomhetsplanen med tilhørende rapportering. Den bør i tillegg følges opp i virksomhetsledelsens gjennomgang, jf. kapittel 3.1.

4.2 Få på plass det viktigste

Aktiviteter

- Utforme/forbedre overordnede styrende dokumenter
- Få på plass nøkkelpersoner og aktivere sikkerhetsorganisasjonen
- Utforme og gjennomføre grunnopplæring
- Etablere system for hendelses- og avvikshåndtering

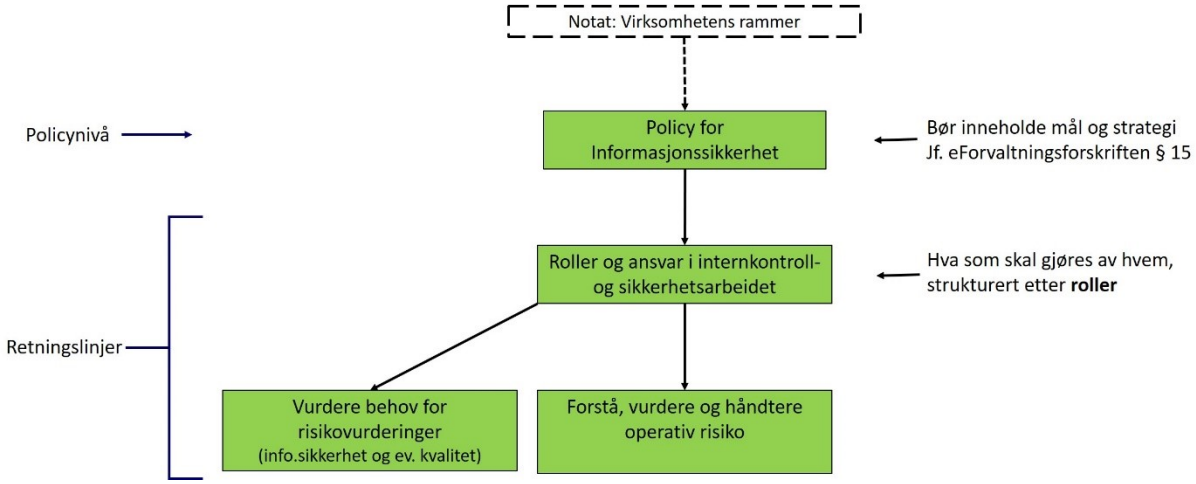
4.2.1 Utforme/forbedre overordnede styrende dokumenter

Fundamentet i internkontrollen

De overordnede styrende dokumentene er fundamentet i internkontrollen. De klargjør hvem som skal gjøre hva, og gir føringer for arbeidet. De er en forutsetning for at de systematiske aktivitetene i internkontrollen skal bli gjennomført i tilstrekkelig omfang og på riktig måte.

Arbeidet med dokumentene bør organiseres som et prosjekt. Arbeidet vil involvere ulike aktører, avhengig av hva man arbeider med i de enkelte dokumentene.

Hvilke dokumenter bør man etablere?



Vi anbefaler følgende overordnede styrende dokumenter for informasjonssikkerhetsområdet:

1. Policy for informasjonssikkerhet (kort og overordnet)
2. Roller og ansvar i internkontroll- og sikkerhetsarbeidet
3. Forstå, vurdere og håndtere operativ risiko
4. Vurdere behov for risikovurderinger

I tillegg bør man vurdere om det kan være nødvendig med en retningslinje eller veiledning som utdyper dokument nr. 2 for aktiviteter og ansvar for informasjonssikkerhetsområdet. Et innledende notat som klargjør utgangspunkt og rammer, vil alltid være nyttig.

Felles dokumenter for flere internkontrollområder

Dokument nr. 2 og 3 bør utformes slik at de på kort eller lengre sikt kan dekke alle internkontrollområder dersom det er ønskelig. Dette er vår primære anbefaling, men noe virksomhetsleder må avgjøre.

På policynivå vil virksomheten da kunne ha forskjellige toppdokument som dekker mål og sentrale retningsvalg for de enkelte internkontrollområdene. Videre kan dokument nr. 2 og 3 være felles for flere eller alle områdene.

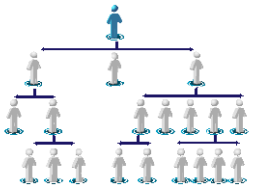
Nr. 4 vil gjelde for informasjonssikkerhet og eventuelt kvalitet. Andre områder kan få egne dokument tilsvarende nr. 4, avhengig av områdenes egenart og behov. De kan også få egne utdypende

retningslinjer eller veiledninger for hele eller deler av det aktuelle området, slik det er nevnt over for informasjonssikkerhetsområdet.

Eksempler er tilgjengelig fra Difi
Dette veiledningsmateriellet har konkrete eksempler på alle dokumentene nevnt over. De viser også hvordan flere internkontrollområder kan integreres på en enkel måte. Eksemplene kan benyttes som inspirasjon eller utgangspunkt, og tilpasses den enkelte virksomhet.

4.2.2 Få på plass nøkkelpersoner og aktivere sikkerhetsorganisasjonen

Linjen som hovedføring i internkontrollarbeidet
Ansvaret for informasjonssikkerhet og tilhørende internkontrollarbeid bør som hovedregel følge linjen. Det er sikring av måloppnåelse som er formålet med internkontrollen. Ansvaret for det ligger i linjen.



Ansvaret for internkontroll og informasjonssikkerhet bør følge linjen

Støtte fra ulike funksjoner
For å understøtte både virksomhetsleder og linjen, må virksomheten etablere tilstrekkelige fellesfunksjoner, støttefunksjoner og samarbeidsgrupper. Sammen med linjen utgjør dette det man kan kalle sikkerhetsorganisasjonen i virksomheten.

Roller og ansvar må være tydelige
De fleste virksomheter har allerede en del fellesfunksjoner, støttefunksjoner og samarbeidsgrupper som dekker noen behov. Andre behov kan være delvis dekket. Det vil da mest være snakk om å tydeliggjøre ansvar, og eventuelt foreta justeringer. Det man har behov for og mangler, må man etablere.

Både hovedføringen, hvilke funksjoner og grupper man har behov for og deres rolle og ansvar, bør komme tydelig frem av de overordnede styrende dokumentene, jf. kapittel 4.2.1.

Det er viktig å få frem hvordan fellesfunksjonene skal støtte linjen. Sikkerhetsarbeidet i virksomheten skal være en integrert del av virksomhetens internkontroll. Det bør ikke leve sitt eget liv ved siden av. Da får man ikke sammenheng i virksomhetens styring og kontroll.

Få på plass personer og få arbeidet i gang
Etablering av nye funksjoner og grupper, og utpeking av hvilke personer som skal dekke funksjonene eller inngå i gruppene, bør legges inn i planene for etablering/forbedring av internkontrollen. Da kan aktivering av sikkerhetsorganisasjonen følges opp systematisk.

Utpeking av personer som skal dekke funksjoner eller inngå i grupper er normalt et ansvar for ulike ledere.

Fagansvarlig informasjons-sikkerhet er en nøkkelperson

Det er svært viktig å ha eller tidlig få på plass en støttefunksjon som fagansvarlig informasjonssikkerhet eller lignende. Dette er virksomhetsledelsens ansvar. Funksjonen fagansvarlig informasjonssikkerhet er kort omtalt i kapittel 3.

4.2.3 Utforme og gjennomføre grunnopplæring

Informasjon og kurs for ledere
Når nye overordnede styrende dokumenter er ferdig og godkjent, bør virksomheten

ha ferdig informasjonsmateriell til internt bruk. Ved større endringer bør man også ha klart et kort kurs for linjeledere. Behov, innretning og organisering er avhengig av virksomhetsstørrelse, status i internkontrollarbeidet samt kompetansen til lederne om internkontroll og informasjonssikkerhet.

Opplæring av andre aktører
Man bør i tillegg spesielt vurdere om og hvordan det eventuelt bør gjennomføres informasjon, opplæring og kulturutvikling for:

- Systemeiere fellessystem
- Felles tiltaksleverandører
- Prosessledere i aktivitetene *Få oversikt og prioritere*, *Gjennomføre risikovurdering* og *Foreslå håndtering av risikoer*
- Håndteringsansvarlige i aktiviteten *Iverksette godkjente tiltak*
- Alle ansatte

Tilpasset informasjon og opplæring må gis under etablering

Dette behøver ikke skje med en gang, men legges inn i planen for etablering/forbedring.

Organisering av arbeidet
Fagansvarlig informasjonssikkerhet vil naturlig være en sentral aktør i behovsvurdering, planlegging og gjennomføring av grunnopplæring. Arbeidet bør skje i samarbeid med eventuelle fellesfunksjoner i virksomheten med ansvar for intern informasjon og intern opplæring, og lederne for relevante områder.

Vedlikehold gjennom internkontrollen
Kompetanse- og kulturutvikling er en av de systematiske aktivitetene i internkontrollen, jf. kapittel 3.6. Den skal sørge for at nødvendig kompetanse- og kulturutvikling skjer også etter den grunnopplæring som ligger i denne etableringsaktiviteten.

4.2.4 Etablere system for hendelses- og avvikshåndtering

Hvorfor trenger vi et system for dette?
Risikoer må identifiseres, vurderes og håndteres både jevnlig og når de inntreffer. En viktig støtte er et hensiktsmessig system for hendelses- og avvikshåndtering.

Systemet må sikre forsvarlig rapportering, registrering og oppfølging av uønskede hendelser, avvik og informasjonssikkerhetsbrudd.

Uønskede hendelser mv. må rapporteres systematisk og enkelt

Hva er «systemet»?
Å ha et «system» vil si å ha hensiktsmessig systematikk for håndteringen. Det handler ikke bare om et IKT-system som understøtter hendelseshåndteringen. Det viktigste er klare føringer om

- hva som skal rapporteres
- hvem som skal rapportere og når det skal rapporteres
- hvordan rapporteringen skal skje
- hvem som skal håndtere hva
- hvem som skal informeres om hva

Dette må understøttes av enkle og effektive IKT-løsninger og eventuelt en egen støttefunksjon. Samlet må de sikre god informasjonsflyt, oppfølging og analysemuligheter.

Behovet gjelder flere områder

En virksomhet vil normalt trenge et system for avviks- og hendelseshåndtering innen flere internkontrollområder. Man må også være oppmerksom på at løsninger på enkelte funksjonsområder, som for eksempel «helpdesk» for IKT-drift, er en del av virksomhetens samlede avviks- og hendelseshåndtering. Mange glemmer dette.

Det er viktig å se ulike internkontrollområder, funksjoner og tilhørende IKT-løsninger i sammenheng. Det er en forutsetning for å få en helhet i avviks- og hendelseshåndteringen i virksomheten.

Ulike områder og støttesystem bør sees i sammenheng

Dette er også viktig for å kunne analysere hva som har skjedd av ulike typer hendelser, lære av erfaring samt rapportere relevant statistikk til virksomhetsledelsen, risikoeiere og systemeiere fellessystem.

Organisering av arbeidet
Virksomheten bør vurdere status på eksisterende system for avviks- og hendelseshåndtering. Ved vesentlige svakheter bør man starte et prosjekt for etablering eller forbedring. Innretning og omfang er avhengig av hva virksomheten har fra før, og i hvilken grad man vil samordne det som er nevnt over.

Behov for endring
For noen vil det være nok å få presisert føringene i eksisterende system slik at også informasjons-sikkerhetsområdet dekkes. Andre må sørge for ny og bedre informasjonsflyt mellom aktører for å sikre at informasjon om det som skjer kommer frem til relevante aktører og blir håndtert forsvarlig.

Noen må få tilrettelagt for nyttig statistikk også fra system som «helpdesker» og lignende. Andre må inkludere flere internkontrollområder i ett system. Noen må også utvikle eller anskaffe en ny IKT-løsning som understøtter et mer helhetlig system for flere eller alle områder.

4.3 Skap en god plattform for internkontrollen

Aktiviteter

- Etablere fellessikring og synliggjøre tilleggssikring
- Etablere rammeverk for dokumentasjon

4.3.1 Etablere fellessikring og synliggjøre tilleggssikring

Sikkerhetstiltak skal redusere risiko. Det gjør de ved å forebygge, redusere og/eller reagere på uønskede hendelser.

Negative sideeffekter av sikkerhetstiltak
Tiltak som ikke er tilpasset risikoer og ulike organisatoriske enheters behov, kan imidlertid gi negative sideeffekter og medføre nye risikoer. Det kan spesielt gå utover effektivitet, men også andre mål. Ressursene i virksomheten blir da ikke brukt riktig. De ansatte får unødvendige hindringer på mange arbeidsområder. De kan også miste respekten for sikkerhetstiltak generelt.

En risikobasert tilnærming
Virksomhetene bør derfor ha et bevisst og risikobasert forhold til hvilke sikkerhetstiltak de etablerer, hvor stramme de er og fordelingen mellom fellessikring og tilleggssikring. Fellessikring er sikkerhetstiltak som gjelder for alle oppgaver, systemer og ansatte i virksomheten. Tilleggssikring er sikkerhetstiltak som gjelder for de med spesielle risikoer og ekstra behov for tiltak.

Nytte/kost for virksomheten samlet bør avgjøre om tiltak blir fellessikring eller tilleggssikring. Man må da legge til grunn risikovurderinger og behov for sikkerhetstiltak hos risikoeierne rundt om i virksomheten. Man må samtidig være litt pragmatisk for å få en kostnadseffektiv drift av det samlede sikkerhetsarbeidet.

Nytte/kost for virksomheten samlet bør avgjøre om tiltak blir fellessikring eller tilleggssikring

Status og konskevenser
De fleste virksomheter har en rekke sikkerhetstiltak, men mange mangler et bevisst og systematisk forhold til hvilke risikoer tiltakene skal dekke, hvilke tiltak som bør være felles for alle i virksomheten og hvilke som bare bør gjelde for noen. Tiltakene er da ikke tilpasset risiko og nytte/kost for virksomheten samlet.

Gjennomføre en «ryddejobb»
For å finne den riktige balansen mellom fellessikring og tilleggssikring, må de fleste virksomheter gjennomføre en «ryddejobb» i sikkerhetstiltakene. Den bør gjennomføres som et prosjekt på virksomhetsnivå. Difis veiledningsmateriell har støtte for dette.

Arbeidet bør ledes av fagansvarlig informasjonssikkerhet. Alle felles tiltaksleverandører er sentrale deltakere. Representanter fra risikoeiere og systemeiere fellessystem må involveres underveis.

Nytte av «ryddejobben»
Resultatet har vesentlig betydning for virksomhetens effektivitet og samlede styring og kontroll. Det gir også risikoeiere og systemeiere fellessystem bedre oversikt over virksomhetens fellessikring samt hvilke muligheter de har til å velge tilleggssikring. Dette øker kvaliteten på gjennomføring og oppfølging av konkrete risikovurderinger.

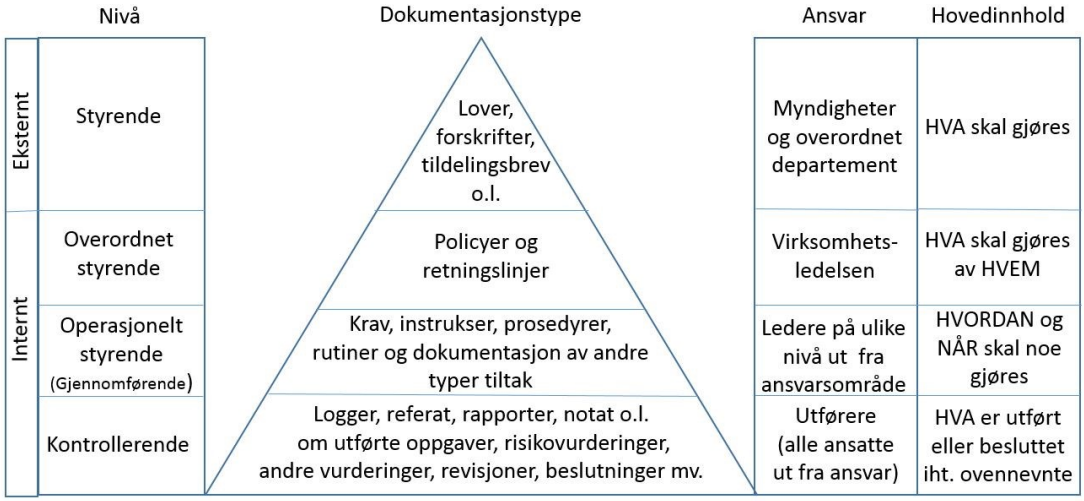
4.3.2 Etablere rammeverk for dokumentasjon

Dersom internkontrollen skal fungere, må nødvendig informasjon være tilgjengelig for de som har behov for den. Det må også være lett å utarbeide og fylle ut nødvendig dokumentasjon, og kontrollere etterlevelsen.

Dette sikres best ved at virksomheten har et tydelig rammeverk for dokumentasjon av internkontroll. Det kan også dekke virksomhetsstyring for øvrig. Et godt rammeverk vil blant annet skissere en variant av oversiktsfiguren under. Den er basert på en tilsvarende illustrasjon fra NSM.

Begrepene i figuren er ingen fasit, men typiske eksempler. Det er heller ikke nødvendig å ha med alle kolonnene. Man tilpasser og tar med det som gir nytte internt.

Sentralt innhold i rammeverket
Rammeverket bør konkretisere formål og bruksområde for de ulike dokumenttypene man har, vise til relevante maler, presisere arkiverings- og publiseringskrav, klargjøre forvaltningsansvar for rammeverket mv.



Eksempel på dokumentstruktur i et rammeverk for dokumentasjon

Det er spesielt viktig at man får tydeliggjort en god sammenheng mellom hva som skal journalføres og lagres på bestemte saker i virksomhetens sak-/arkivsystem, hva som skal publiseres på virksomhetens intranett, og hva som skal lagres og være tilgjengelig fra eventuelle spesialsystem for internkontroll eller lignende.

Det er også viktig å ha eller få utviklet hensiktsmessige maler for sentrale dokumenttyper. Da unngår man stor variasjon i lesbarhet, og mye oppdateringsarbeid senere.

Hensiktsmessig omfang
Man bør ikke gjøre rammeverket og arbeidet med det mer omfattende enn nødvendig. Formålet er at det skal støtte og effektivisere nødvendig dokumentasjon, samt gjenfinning, bruk og kontroll av dokumentasjonen. Det er også bedre å legge til rette for gradvis forbedring av rammeverket enn å skulle identifisere alle behov i forkant.

Dersom virksomheten allerede har et godt rammeverk, bør det benyttes også for informasjonssikkerhet. Slik blir informasjonssikkerhet en del av helheten.

Organisering av arbeidet
Etablering eller vesentlig forbedring av rammeverket bør organiseres som et fellesprosjekt i virksomheten. Det vil være naturlig at virksomhetens enhet for intern kommunikasjon leder arbeidet. Sentrale deltakere vil være virksomhetens arkivfunksjon, fagansvarlig informasjonssikkerhet og fagansvarlige for andre internkontrollområder.

4.4 Lag et godt grunnlag for sentrale systematiske aktiviteter

Aktiviteter

- Identifisere typiske oppgave- og informasjonstyper
- Felles analyse av eksterne krav

4.4.1 Identifisere typiske oppgave- og informasjonstyper

Støtte til den systematiske aktiviteten Få oversikt og prioritere

Få oversikt og prioritere under *Risikovurdering* er en grunnleggende og avgjørende aktivitet som bør gjennomføres på operativt nivå rundt om i hele virksomheten, jf. kapittel 3.2. Vesentlige deler bør ledes av en prosessleder ved første gangs gjennomføring.

Suksesskriterium

For å lykkes med aktiviteten, bør risikoeierne ta utgangspunkt i eksempler på typiske oppgave- og informasjonstyper som behandles i virksomheten. Dette veiledningsmateriellet har en samling av slike eksempler. Den dekker imidlertid ikke alle oppgavetyper og alle virksomheters behov.

Virksomheter av en viss størrelse, kan med fordel lage sin egen versjon av eksempelsamlingen. Man kan da avgrense og supplere eksemplene i dette materiellet. Områder som ikke er dekket, bør suppleres med flere typiske oppgaver og tilhørende informasjonstyper som er relevante i virksomheten.

Typiske eksempler på oppgave- og informasjonstyper vil være viktig støtte

Virksomhetsversjonen vil være en viktig støtteressurs

- når ulike organisatoriske enheter skal få oversikt og prioritere
- når nye oppgaver skal starte rundt om i virksomheten
- dersom virksomheten er stor med mange litt like organisatoriske enheter

Den vil dessuten ofte være mer oversiktlig i bruk i virksomheten enn den generelle eksempelsamlingen i dette veiledningsmateriellet.

Gradvis oppbygging

Virksomhetsversjonen kan bygges opp gradvis etter hvert som man får gjennomført aktiviteten *Få oversikt og prioritere* i stadig flere organisatoriske enheter.

De som pekes ut som prosessleder til aktiviteten bør være nøkkelpersoner i utarbeiding av virksomhetens egen eksempelsamling. Arbeidet bør koordineres av fagansvarlig informasjonssikkerhet. Med riktige egenskaper, vil også hun selv kunne være prosessleder i aktiviteten *Få oversikt og prioritere*.

4.4.2 Felles analyse av eksterne krav

Støtte til den systematiske aktiviteten *Analysere eksterne krav*

I aktiviteten *Analysere eksterne krav* under *Risikovurdering*, må risikoeiere og systemeiere fellessystem identifisere konkrete krav om sikkerhetstiltak eller typer tiltak i regelverk og avtaler innen eget ansvarsområde, jf. kapittel 3.2.

Et fellesprosjekt gir bedre effektivitet

Ofte vil de samme reglene og avtalene gjelde for arbeidsoppgaver og system i flere organisatoriske enheter. Det vil derfor være mest effektivt for virksomheten samlet å gjennomføre deler av arbeidet som et fellesprosjekt i virksomheten.

Konkrete krav i regelverk og avtaler må identifiseres

I fellesprosjektet analyserer man kravene i regelverk og avtaler som gjelder flere. Resultatet bør være en spesifisering av konkrete sikkerhetstiltak eller typer tiltak som kreves.

Risikoeiere og systemeiere fellessystem kan da primært kvalitetssikre at resultatet fra fellesprosjektet er dekkende for eget ansvarsområde, og eventuelt kun supplere med egne analyser på spesielle deler.

Krav til og gjenbruk av kompetanse
Det er viktig at gruppen som skal gjennomføre en slik felles analyse har kompetanse om både juss og informasjonssikkerhet. Deltakerne vil også kunne fungere som ressurspersoner senere for ulike risikoeiere og systemeiere fellessystem, når de skal analysere områder som ikke er dekket av fellesprosjektet.

5 Valg og implementering av sikkerhetstiltak

Risikobasert etablering
Sikkerhetstiltak skal redusere risikoer. Valg og implementering bør være basert på risikovurderinger og påfølgende risikohåndtering. Sikkerhetstiltak må ikke etableres ukritisk og tilfeldig. Mange tiltak kan gi negative sideeffekter. Det kan gå ut over effektivitet og annen måloppnåelse.

Sikkerhetstiltak bør fordeles systematisk og risikobasert mellom fellessikring og tilleggssikring. Fellessikring gjelder alle i virksomheten. Tilleggssikring er for dem med spesielle risikoer og behov. Veiledningsmateriellet understøtter at en slik fordeling etableres og gjennomføres systematisk.

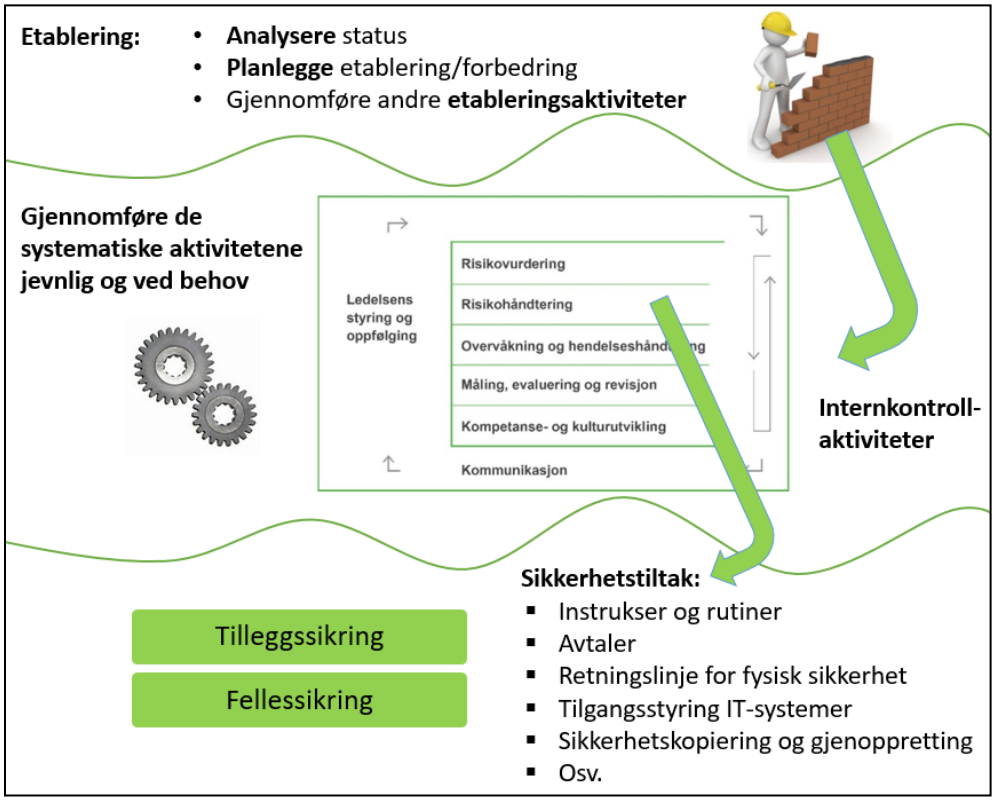
Støtte ved valg og implementering av sikkerhetstiltak
Ved valg og implementering av konkrete sikkerhetstiltak bør virksomhetene følge anbefalingene i Referansekatalogen over anbefalte og obligatoriske IT-standarder i offentlig sektor. Der heter det:

Ved valg og implementering av risikoreduserende tiltak er det anbefalt å søke støtte i anerkjente kilder. Dette kan for eksempel være ISO/IEC 27002, ulike rammeverk, faktaark og veiledere i Norm for informasjonssikkerhet Helse og omsorgstjenesten og veiledninger fra NSM, Difi og Datatilsynet. Tidsbruk bør tilpasses risikoen.

Man bør også merke seg at enkelte regelverk kan stille krav om spesifikke tiltak for enkelte typer informasjon eller informasjonsbehandlinger. Disse kravene må da identifiseres og følges. Veiledningsmateriellet understøtter dette gjennom aktivitetene:

- *Felles analyse av eksterne krav* under Etableringsaktiviteter, jf. kapittel 4.4.2
- *Analysere eksterne krav* under Risikovurdering, jf. kapittel 3.2.2

Sammenhenger
Det er i hovedaktiviteten risikohåndtering at sikkerhetstiltak blir etablert og justert. Dette er illustrert i figuren under. Den viser også sammenhengen mellom etableringsaktiviteter og de systematiske aktivitetene.



Etableringsaktiviteter får på plass de systematiske internkontrollaktivitetene. Når disse gjennomføres systematisk rundt om i virksomheten, vil sikkerhetstiltak bli etablert og justert gjennom hovedaktiviteten risikohåndtering.

6 Oversikt over hele veiledningsmateriellet

Dette veiledningsmateriellet er nettbasert. Sentrale deler er tilgjengelig som egne PDF-dokument. Veiledningsmateriellet har følgende innehold:

- Sammendrag
  - For toppledere
  - Grunnleggende innføring
  - Grunnleggende begreper
- Systematiske aktiviteter
  - Beskrivelser av de systematiske aktivitetene
- Etableringsaktiviteter
  - Beskrivelser av etableringsaktivitetene
- Utdypninger
  - Utdypende beskrivelser av litt omfattende eller komplekse aktiviteter
- Godt å vite – utdypende bakgrunnsstoff
- En rekke maler, eksempler og støttedokument til de ulike aktivitetene
- Nyttig tilleggsstoff som begrepsliste, endringslogg, kilder, hva sier ISO/IEC 27001, mv.

Målgruppen for de ulike delene fremgår innledningsvis i alle delene.

Hele veiledningsmateriellet er tilgjengelig på http://internkontroll.infosikkerhet.difi.no

Lykke til med etablering, forbedring og gjennomføring av en systematisk internkontroll!