**Nasjonal sikkerhetsmyndighet**

Veiledning

Sist oppdatert: 2006-12-05

# Veiledning i risiko- og sårbarhetsanalyse

Del I i denne veiledningen beskriver risikohåndtering som en kontinuerlig forbedringsprosess. Den er tilpasset virksomheter som er underlagt sikkerhetsloven.

Del II presenterer en metode for planlegging, gjennomføring og oppfølging av risiko- og sårbarhetsanalyser (ROS-analyser).



# Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet er tverrsektoriell fag- og tilsynsmyndighet innenfor forebyggende sikkerhetstjeneste i Norge og forvalter lov om forebyggende sikkerhet av 20 mars 1998. Hensikten med forebyggende sikkerhet er å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, primært spionasje, sabotasje og terrorhandlinger. Forebyggende sikkerhetstiltak skal ikke være mer inngripende enn strengt nødvendig, og skal bidra til et robust og sikkert samfunn.

## Hensikt med veiledning

NSM sin veiledningsvirksomhet skal bygge kompetanse og øke sikkerhetsnivået i virksomhetene, gjennom økt motivasjon, evne og vilje til å gjennomføre sikkerhetstiltak. NSM gir jevnlig ut veiledninger til hjelp for implementering av de krav sikkerhetsloven stiller. NSM publiserer også veiledninger innen andre fagområder relatert til forebyggende sikkerhetsarbeid.

**Postadresse**
Postboks 14
1306 BÆRUM
POSTTERMINAL

**Sivil telefon/telefax**
+47 67 86 40 00/+47 67 86 40 09
**E-postadresse**
post@nsm.stat.no

**Militær telefon/telefaks**
515 40 00/515 40 09

**Internettadresse**
www.nsm.stat.no

# Innhold

Veiledning i risiko- og sårbarhetsanalyse ..... 1
1 Innledning ..... 4
1.1 Bakgrunn ..... 4
1.2 Hensikt ..... 4
1.3 Referanser ..... 4
1.4 Definisjoner ..... 4
2 Del I - Risikohåndtering ..... 6
2.1 Sammendrag ..... 6
2.2 Innledning om risikohåndtering ..... 6
2.3 Trinn 1: Planlegging og organisering ..... 8
2.3.1 Planlegging ..... 8
2.3.2 Organisering av arbeidet ..... 9
2.3.3 Identifisering av verdier ..... 9
2.3.4 Kartlegging av risikobildet ..... 10
2.4 Trinn 2: Gjennomføring av ROS-analyse ..... 10
2.4.1 Identifisering av uønskede hendelser ..... 11
2.4.2 Fastsetting av sannsynlighet og konsekvens ..... 12
2.4.3 Fastsetting av risiko ..... 13
2.4.4 Risikoevaluering og akseptabel risiko ..... 13
2.5 Trinn 3: Utarbeiding og implementering av tiltak ..... 14
2.5.1 Kartlegging av eksisterende tiltak ..... 14
2.5.2 Utarbeiding av sikringstiltak ..... 14
2.5.3 Vurdering av nytte og kostnad ..... 15
2.5.4 Kommunikasjon med beslutningstakere ..... 15
2.5.5 Implementering av tiltak ..... 15
2.6 Trinn 4: Kontroll og revisjon ..... 16
2.6.1 Oppfølging og kontroll av sikkerhetsarbeidet ..... 16
2.6.2 Ledelsens evaluering av sikkerhetstilstanden ..... 16
3 Del II Risiko- og sårbarhetsanalyse ..... 17
3.1 Sammendrag ..... 17
3.2 Innledning ..... 17
3.3 Bruk av metoden ..... 18
3.4 Dokumentasjon av arbeidet ..... 20
3.5 Trinn 1: Planlegging og organisering ..... 21
3.5.1 Skjema 1: Planlegging og organisering ..... 21
3.5.2 Skjema 2: Beskrivelse av virksomheten ..... 22
3.5.3 Skjema 3: Beskrivelse av kritiske objekt og informasjonsverdier ..... 22
3.6 Trinn 2: Gjennomføring av ROS-analyse ..... 23
3.6.1 Oversikt over farekilder ..... 23
3.6.2 Skjema 4: Uønsket hendelse ..... 24
3.7 Trinn 3: Utarbeiding og implementering av tiltak ..... 27
3.7.1 Skjema 5: Utarbeiding av tiltak ..... 27
3.7.2 Skjema 6: Prioritert tiltaksliste ..... 28
3.7.3 Skjema 7: Handlingsplan ..... 28
3.8 Trinn 4: Kontroll og revisjon ..... 29
3.8.1 Overvåking av risikobildet, intern revisjon ..... 29
3.8.2 Årlig evaluering av sikkerhetstilstanden ..... 29
Vedlegg A Dokumenthistorie ..... 29
Vedlegg B: Beskrivelse av delsystemer ..... 30
Vedlegg C: Skjemaer for bruk i virksomheten ..... 30

# 1 Innledning

## 1.1 Bakgrunn

Nasjonal sikkerhetsmyndighet (NSM) har i flere år hatt et samarbeid med Norges teknisk-naturvitenskaplige universitet (NTNU) for å utvikle en metode for risiko- og sårbarhetsanalyser (ROS). Dette samarbeidet har resultert i rapportene *"Objekt- og informasjonssikkerhet. Metode for risiko- og sårbarhetsanalyser"* (ROS 2000), og *"Risikohåndtering. Bruk av risiko- og sårbarhetsanalyser i det kontinuerlige sikkerhetsarbeidet",* (ROS 2004).

Denne veiledningen bygger i all hovedsak på ROS 2004, og består av to deler. Den første delen omhandler risikohåndtering generelt, og andre delen omhandler metode for risiko- og sårbarhetsanalyse. Begrepsapparat og definisjoner i veiledningen er tilpasset ROS 2000. På denne måten håper vi på en entydig bruk av begrepene.

## 1.2 Hensikt

Veiledningen er ment som en hjelp for virksomheter til å bruke risiko- og sårbarhetsanalyser, og på den måten bedre kunne håndtere risiko i egen virksomhet.

## 1.3 Referanser

Sikkerhetsloven, med forskrifter (2001): *Lov om forebyggende sikkerhetstjeneste*, Cappelen Akademisk Forlag.

Skavland, E.I. og Ø.M. Jakobsen (2000): *Objekt- og informasjonssikkerhet: Metode for risiko- og sårbarhetsanalyse*, ROSS (NTNU) 2000.

Øksne, A. og Furuseth, H.R. (2004): *Risikohåndtering. Bruk av risiko- og sårbarhetsanalysr i det kontinuerlige sikkerhetsarbeidet,* NTNU 2004.

## 1.4 Definisjoner

**Forebyggende sikkerhetstjeneste:** Med forebyggende sikkerhetstjeneste menes planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet.

**Informasjon:** Enhver form for opplysninger i materiell eller immateriell form.

**Integritet:** Informasjon og objekters nøyaktighet og fullstendighet, samt pålitelighet av transaksjoner.

**Kompromittering:** Tap eller mistanke om tap av konfidensialitet, integritet eller tilgjengelighet for skjermingsverdig informasjon, herunder uønsket avhending, modifisering eller ødeleggelse.

**Konfidensialitet:** Det forhold at informasjon ikke er tilgjengelig for uautoriserte personer eller ikke-godkjente systemer.

**Risiko:** Uttrykk for den fare som uønskede hendelser representerer for informasjon/objekter. Risikoen uttrykkes ved sannsynligheten for og konsekvensene av den uønskede hendelsen.

**Risikobildet:** Forstås her som alle interne og eksterne trusler, samt sårbarheter og svakheter i interne systemer og rutiner.

**Sikkerhetsgradert informasjon/objekt:** Informasjon/objekt som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser,

og som er merket med sikkerhetsgrad i henhold til Sikkerhetsloven (STRENGT HEMMELIG – HEMMELIG – KONFIDENSIELT - BEGRENSET).

**Sikkerhetstruende virksomhet:** Med sikkerhetstruende virksomhet menes forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet

**Sårbarhet**

En svakhet som reduserer eller begrenser et systems evne til å motstå en uønsket hendelse, eller til å gjenopprette en ny stabil tilstand etter hendelsen har inntruffet.

**Tilgjengelighet**

Tilgang til objekter, tjenester og informasjon ved behov og uten unødvendig forsinkelse.

# 2 Del I - Risikohåndtering

## 2.1 Sammendrag

Del I i denne veiledningen beskriver risikohåndtering som en kontinuerlig forbedringsprosess, og er tilpasset virksomheter som er underlagt sikkerhetsloven. Del I er ment å fungere som et utdypende tillegg til metode for risiko- og sårbarhetsanalyser (del II), for å bedre kunne sette slike analyser i sammenheng med det kontinuerlige sikkerhetsarbeidet i virksomhetene.

Innledningsvis blir styringssløyfen for risikohåndtering presentert. Denne viser trinnene man må igjennom i forbindelse med kontinuerlig risikohåndtering og viser sammenhengen mellom disse. De fire trinnene blir presentert hver for seg med forklaringer og utdypinger rundt hvordan de skal gjennomføres og bakgrunnen for dette. Trinn 1 består i planlegging og organisering hvor forarbeid blir utført, inkludert kartlegging av risikobilde og identifisering av verdier. Trinn 2 er gjennomføring av selve ROS-analysen, som blir beskrevet som det viktigste i arbeidet. Denne går igjennom identifisering av uønskede hendelser, fastsetting av sannsynlighet og konsekvens, samt resulterende risikonivå. I trinn 3 beskrives utarbeiding og implementering av tiltak som omfatter kartlegging av tiltak og kost- nytte vurdering. Kommunikasjon med beslutningstakere blir behandlet som eget punkt da dette er vesentlig for å gjennomføre tiltakene. Kontroll og revisjon blir beskrevet i trinn 4.

## 2.2 Innledning om risikohåndtering

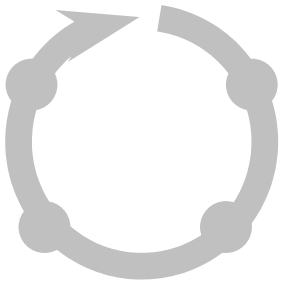
Sikkerhetsloven med forskrifter trådte i kraft i 2001, og gir bestemmelser om hvilke minimumskrav som stilles til virksomheter med gradert informasjon, og/eller skjermingsverdige objekt. Forskriftene til loven omhandler fagområdene sikkerhetsadministrasjon (internkontroll), personellsikkerhet, informasjonssikkerhet[1], og sikkerhetsgraderte anskaffelser. Pr dags dato er det ikke utarbeidet forskrift for objektsikkerhet.

Forebyggende sikkerhetstjeneste skal forhindre at informasjon og objekter blir kompromittert. Med kompromittering av informasjon menes her tap av kravene om konfidensialitet, integritet og tilgjengelighet. Kompromittering av objekter innbefatter også disse kravene til beskyttelse, -opprettholdelse av objektenes funksjonalitet og yteevne er ofte en mer forståelig beskrivelse av formålet med beskyttelsen.

Kravene om å utøve risikohåndtering og risikovurdering er gitt i forskrift om sikkerhetsadministrasjon. Forskriften setter krav til gjennomføring av systematiske tiltak for å sikre at den enkelte virksomhet planlegger, organiserer, utfører og reviderer sine aktiviteter, og er å betrakte som en internkontrollforskrift.

Modellen for risikohåndtering er i denne veiledningen beskrevet som en *kontinuerlig prosess*, delt inn i fire hovedtrinn, og minner i stor grad om styringssløyfen for internkontroll (IK) som vi kjenner fra det tradisjonelle safety-arbeidet HMS (helse-miljø-sikkerhet). I denne veiledningen omtales prosessen som ***styringssløyfe for risikohåndtering***:

[1] Fagområdet består av feltene sikkerhetsgradering/verdivurdering, dokumentsikkerhet, informasjonssystemer, fysisk sikring, kryptosikkerhet, sikring av konferanserom, tekniske sikkerhetsundersøkelser, og monitoring.



*Figur 1: Styringssløyfe for risikohåndtering*

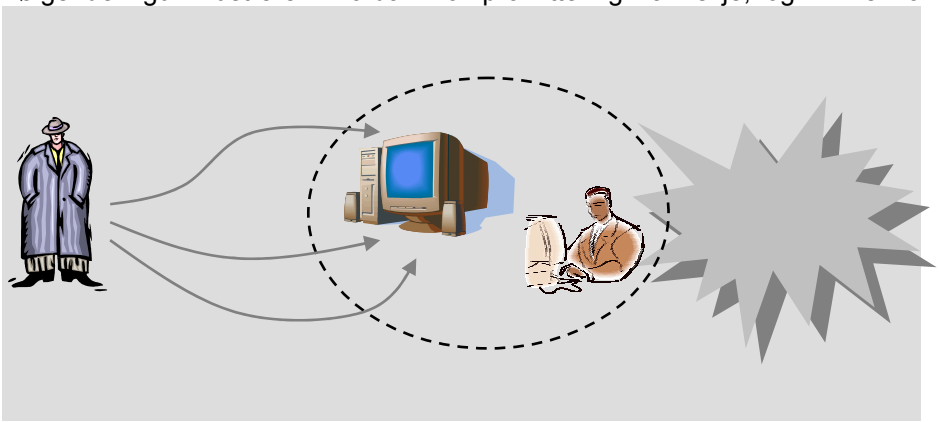
Loven med forskrifter stiller krav til virksomheter om å utøve risikohåndtering. Dette innebærer at virksomhetene skal fastsette og gjennomføre sikkerhetstiltak etter en risikovurdering. NSM har foretatt en generell risikovurdering på nasjonalt nivå. Minimumskravene i lov og forskrift er satt med bakgrunn i denne risikovurderingen.

I tillegg plikter virksomheter å utføre risikovurdering med bakgrunn i lokale forhold. Risikovurderingen i den enkelte virksomhet skal ta hensyn til forhold med betydning for å

1. avdekke behov for tiltak *utover* minimumskravene i sikkerhetsloven med forskrifter,
2. avdekke *overflødige* og *unødvendig overlappende* sikkerhetstiltak, og
3. finne frem til mer *kosteffektive tiltak* som kan erstatte eksisterende tiltak.

Virksomheten må kartlegge de trusler som finnes, både internt og eksternt, slik at den videre kan iverksette tiltak for å redusere trusler med *uakseptabel risiko*. Dette forutsetter at det finnes kriterier å styre i forhold til: Det må være mulig å ha holdepunkter for å si når en risiko øker ut over et nivå som på forhånd er definert som akseptabelt. Å fastlegge et nivå for hvilken risiko virksomheten kan akseptere er en beslutning som tas av virksomhetens leder. Dette resulterende nivået skal være dokumentert i virksomhetens *grunnlagsdokument for sikkerhet.* Forskrift om sikkerhetsadministrasjon § 3-3 gir bestemmelser om hva grunnlagsdokumentet skal inneholde.

Følgende figur illustrerer hvordan kompromittering kan skje, og hvilke konsekvenser det kan få:



*Figur 2: Trusselbildet og konsekvenser*

Som figuren viser, er truslene en funksjon av både eksterne og interne forhold. Dårlige holdninger og rutiner, menneskelig feil og slurv samt manglende sikkerhetstiltak (sammen definert som *egeneksponering*) øker sannsynligheten for at *eksterne trusselaktører* vil lykkes med et eventuelt angrep. I de fleste tilfeller vil slike aktører bevisst lete etter slike sårbarheter av ulike slag for å nå sitt mål. I tillegg kan det også være personer innenfor virksomheten (*utro tjenere*) som bevisst – eller under press – forsøker å volde skade eller få tak i f eks sensitiv informasjon. Hensikten kan være å ødelegge eller få tak i virksomhetens verdier, eller sette funksjoner ut av spill.

Utfordring for sikkerhetsarbeidet er å rette fokus mot alle trusler – både eksterne og interne. Aktivitet fra trusselaktører skal forsøkes vanskeliggjort gjennom situasjonstilpassede sikkerhetstiltak. Egeneksponeringen skal forsøkes minimalisert gjennom en riktig og målbevisst gjennomføring av sikkerhetstiltakene. Risikoproblematikk knyttet til utro tjenere skal forsøkes avverget gjennom gode interne kontroll- og personellrutiner, samt sikkerhetsklarering og autorisasjonsprosessen.

En god huskeregel kan være å tenke på det forebyggende sikkerhetsarbeidet som en stol med tre bein; et bein representerer teknologi, et representerer policy og formelle retningsliner og det siste representerer holdninger og kultur relatert til sikkerhet i virksomheten. Alle de tre beina er like viktig og må være på plass for å kunne opprettholde et tilfredsstillende sikkerhetsnivå.



*Figur 3: Forebyggende sikkerhet som en stol med tre bein.*

**I det følgende vil trinnene i styringssløyfen bli beskrevet.**

## 2.3 Trinn 1: Planlegging og organisering

Trinn 1 i risikostyringsprosessen har til hensikt å legge forholdene til rette for å kunne gjennomføre en risiko- og sårbarhetsanalyse (ROS-analyse). En rekke aktiviteter bør gjennomføres i forkant av selve ROS-analysen for å sikre at den blir gjort på en hensiktsmessig måte uten unødvendig bruk av ressurser. Disse aktivitetene blir beskrevet i dette kapitlet.

### 2.3.1 Planlegging

En ROS-analyse kan være både en situasjonsbetinget og en regelmessig aktivitet. Flytting, større ombygginger og innføring av nye IT-systemer er eksempler på aktiviteter som bør medføre gjennomføring eller revisjon av en ROS-analyse. Store endringer i trusselbildet kan også være grunnlag for å gjennomføre en slik analyse.

I tillegg til å gjennomføre ROS-analyser på bakgrunn av slike kriterier, bør virksomheten foreta en overordnet analyse av virksomheten med jevne mellomrom. Dette kan for eksempel være årlig eller hvert andre år.

*Dersom virksomheten ikke har gjennomført en risiko- og sårbarhetsanalyse tidligere, er det i seg selv grunn god nok for å iverksette dette arbeidet.*

Forberedelse til risiko- og sårbarhetsanalysen omfatter innledningsvis en beskrivelse av mål (dvs. beskrivelse av hva man vil oppnå/finne ut gjennom analysen), og eventuelle delmål. Eventuelle avgrensninger skal angis. Dette kan være avgrensning i omfang, spesielle forutsetninger eller antagelser, samt ressursbegrensning (knyttet til tid, bemanning, utstyr, datagrunnlag osv.).

For å sikre at risiko- og sårbarhetsanalysen gjennomføres til riktig tid, kan det være nødvendig å utarbeide kriterier for igangsetting. Disse kriteriene må gi informasjon om vilkår for igangsetting, og retningslinjer for overvåkning av interne og eksterne forhold som kan gjøre det nødvendig å gjennomføre en risikovurdering.

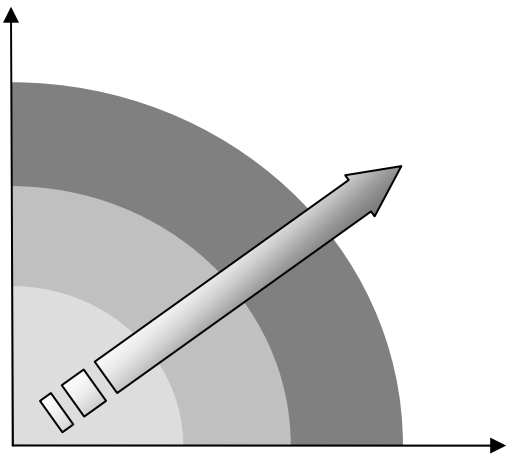
### 2.3.2 Organisering av arbeidet

En risiko- og sårbarhetsanalyse kan organiseres som et prosjekt, og gjennomføres i henhold til prosjektplan. En slik plan skal angi start- og sluttidspunkt, samt alle aktiviteter som skal utføres med ansvar for utførelse. Prosjektet bør ha en prosjektleder som har ansvar for å lede/koordinere analysearbeidet.

I små organisasjoner er det ikke sikkert det er nødvendig å definere arbeidet som et formelt prosjekt. Det holder da å definere en arbeidsgruppe som skal gjennomføre analysen.

Arbeidsgruppen/prosjektgruppen bør bestå av personer med kunnskap og erfaring fra arbeid med slike analyser. Arbeidsgruppen bør i tillegg ha nødvendig kjennskap de aktiva og systemer som skal undersøkes. Gruppemedlemmene bør ha god kjennskap til metodikken som skal benyttes.

Å definere omfang og detaljeringsgrad for analysen kan være vanskelig. Arbeidet må tilpasses forholdene i virksomheten. Risikobildet vil være avhengig av flere faktorer, som f eks størrelse på virksomheten (antall ansatte), risikonivå i virksomheten (verdifulle objekter, sensitiv informasjon), grad av kompleksitet/uoversiktlighet (mange lokasjoner, komplekse IT-systemer osv.) og risikobildet i omgivelsene. Generelt vil behovet for dokumentasjon og styring øke ettersom disse faktorene øker. Dette er illustrert i følgende figur:



*Figur 4: Sammenheng mellom kompleksitet og behov for dokumentasjon og styring*

### 2.3.3 Identifisering av verdier

I forkant av selve risiko- og sårbarhetsanalysen bør en del faktorer kartlegges for å lette det videre arbeidet.

Et viktig punkt er å kartlegge virksomhetens *verdier*. Begrepet *verdi* benyttes for det objektet eller den informasjonen virksomheten må sikre konfidensialitet, tilgjengelighet eller integritet for. I denne

sammenheng kan det være fornuftig å visualisere systemet ved hjelp av en eller flere representasjonsteknikker. Hierarkisk nedbryting, kart over fysisk beliggenhet, prosesstegninger og organisasjonskart er eksempler på slike teknikker.

Videre må man identifisere de objekter/informasjonsverdier som er av en kritisk verdi for virksomheten. Hensikten er å kunne utelate eiendeler med lav verdi fra den videre analysen, og på denne måten forenkle det videre arbeidet.

Kritiske verdier identifiseres ved å anslå taps- eller skadepotensialet – i form av kostnad for gjenanskaffelse, indirekte kostnader som tap av goodwill osv. Kartlegging av verdier resulterer i en oversikt hvor antatt sikkerhetsbehov knyttes til den enkelte verdi. Verdier av høy betydning (kroneverdi, kritikalitet, sårbarhet osv.) bør prioriteres i den videre risiko- og sårbarhetsanalysen. Å angi kroneverdi på skjermingsverdig informasjon kan være vanskelig, men kan samtidig lette det videre analysearbeidet.

### 2.3.4 Kartlegging av risikobildet

I forkant av selve risiko- og sårbarhetsanalysen vil det være fornuftig å identifisere mulige kilder til risiko. Hensikten med dette er å få en oversikt over trusselbildet virksomheten står overfor.

Dette kan være en vanskelig oppgave, men er et viktig bakteppe for senere å kunne identifisere uønskede hendelser. Som beskrevet innledningsvis vil det eksistere både eksterne og interne kilder til risiko. Begge disse aspektene må vurderes.

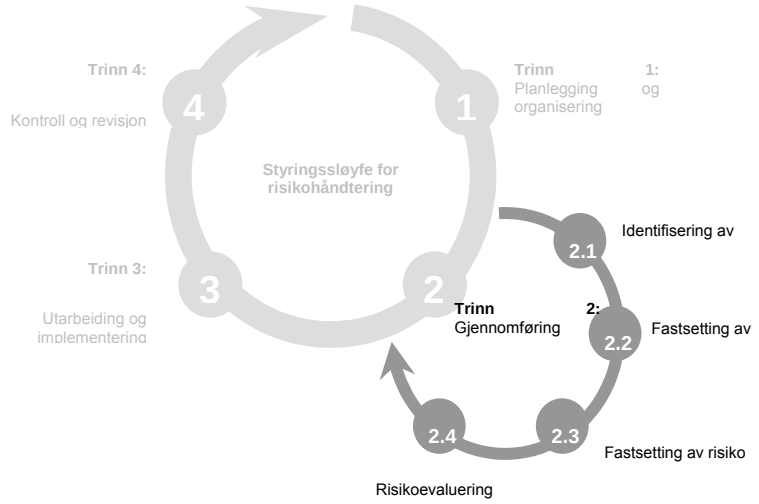
NSM gir årlig ut en risikovurdering som kan være til hjelp i denne sammenhengen. I tillegg utgis kortere sikkerhetsvurderinger med jevne mellomrom. Disse er gjerne temabasert og kan være nyttige støttekilder. Risikovurderingen formidler et oppdatert, overordnet nasjonal sikkerhetstilstand, og omhandler blant annet potensielle trusselaktører, deres fokus, metoder og virkemidler.[2] Denne type kilder kan gi nyttig informasjon til komplekse virksomheter. Det vil imidlertid være vel så viktig å kjenne lokale forhold i virksomhetens nærmiljø som kan ha betydning for risikobildet.

## 2.4 Trinn 2: Gjennomføring av ROS-analyse

I trinn 2 gjennomføres selve risiko- og sårbarhetsanalysen (ROS-analysen). Hensikten med analysen er å kartlegge hvilket risikobilde virksomheten står overfor. Analysen brukes som et grunnlag for planlegging og implementering av sikringstiltak.

ROS-analysen består av fire trinn, som vist i figur 5. En utfyllende veiledning til gjennomføring av analysen er beskrevet i del II i denne veiledningen.

[2] Risiko- og sikkerhetsvurderingene er graderte og distribueres etter egen adresseliste. Vurderingene kan distribueres på etterspørsel til virksomheter ikke er oppført på adresselisten. Det legges i tillegg ut en ugradert versjon av risikovurderingen på NSMs hjemmesider på internett: www.nsm.stat.no




*Figur 5: Gjennomføring av ROS-analyse*

## 2.4.1 Identifisering av uønskede hendelser

Første punkt i analysen er å identifisere uønskede hendelser. En uønsket hendelse inntreffer når informasjon og objekter blir *kompromittert*. Med kompromittering av informasjon menes her tap av konfidensialitet, integritet og tilgjengelighet. For objekter er opprettholdelse av objektenes funksjonalitet og yteevne i mange sammenhenger en mer forståelig beskrivelse av formålet med beskyttelsen.

Kompromittering av informasjon og objekter kan noe forenklet skje på tre måter:

1) **Eksterne trusselaktører** – eksterne trusselaktører som gjennom bevisste handlinger prøver å få innsyn i sikkerhetsgradert informasjon, alternativt manipulere eller gjøre den utilgjengelig. For objekter vil en aktiv trusselaktører gjennom bevisste handlinger prøve å påvirke objekters funksjons- og yteevne. En trusselaktør vil alltid prøve å finne sårbare punkter som forsøkes utnyttet.
2) **Egeneksponering** – en virksomhet gjør seg selv mer sårbar dersom egensikringen ikke fungerer tilfredsstillende. Mangelfullt sikkerhetsarbeid vil kunne medføre at skjermingsverdig informasjon og skjermingsverdige objekter blir eksponert for omverdenen. Dette vil eksempelvis ofte bli resultatet dersom regelverket som regulerer sikkerhetstjenesten fravikes. Egeneksponeringen kan utløses både gjennom bevisste og ubevisste handlinger.
3) **Utro tjenere –** egne ansatte kan utgjøre en risiko og kan under visse omstendigheter bevisst bidra til at informasjon kompromitteres. Drivkreftene kan være egen vinning eller komme som et resultat av press fra eksterne aktører.

Arbeidet med å identifisere uønskede hendelser bør gjennomføres som en workshop, og inkludere alle som er med i prosjektgruppen/arbeidsgruppen. Hendelsene finnes konkret ved å se på hvilke trusler som kan påvirke de verdiene som er identifisert i virksomheten.

Hendelser som antas representere lav risiko utelates fra det videre arbeidet. Risikobildet vil samtidig være dynamisk, og hendelser som anses som uviktige kan senere bli viktige. Derfor bør også disse hendelsene dokumenteres for eventuell senere gjennomgang/revisjon.

I mange tilfeller vil man finne at ulike verdier kan bli utsatt for samme type uønskede hendelse. Det er likevel viktig å være oppmerksom på at konsekvensene av hendelsen kan bli svært forskjellige for de ulike verdiene.

### 2.4.2 Fastsetting av sannsynlighet og konsekvens

Risiko kan uttrykkes ved sannsynligheten for og konsekvensen av en uønsket hendelse. For å kunne si noe om risiko, må vi altså kunne sette et mål på både sannsynligheten og konsekvensen for den uønskede hendelsen.

**Konsekvensvurdering** er en vurdering av hvilke følger en hendelse kan få for virksomhetens verdier. Konsekvens angis kvalitativt som en beskrivelse av de følger en hendelse kan få. Samtidig vil det være nødvendig å angi konsekvens som en kvantitativ størrelse. Som beskrevet under innledning til risikostyring, kan følgende kvantitative konsekvensgradering benyttes:

- K=4; Katastrofalt
- K=3; Kritisk
- K=2; Farlig
- K=1; Lite farlig

Denne kvantitative angivelsen av konsekvens er et middel for å synliggjøre og oppsummere resultater fra risikovurderingen, og for senere å sammenligne vurderinger fra forskjellige hendelser. Det vil også være til hjelp i arbeidet med å avdekke restrisiko.

I konsekvensvurderingen må det tas hensyn til eiendel(er)/objekt(er) som påvirkes, mulighet for erstatning, eventuelle reserveløsninger og eksisterende tiltak.

Spesielt i kompliserte systemer kan det være vanskelig å forutsi hvilke konsekvenser som kan inntreffe. Hvis systemet er tett sammenkoblet, kan for eksempel en hendelse utløse en annen hendelse som man ikke tenkte på i utgangspunktet. Det er derfor viktig å være kreativ og holde alle muligheter åpne når man identifiserer uønskede hendelser.

**Vurdering av sannsynlighet** for at en hendelse inntreffer har som mål å finne svar på spørsmålet ”*hvor ofte…?*”. Dette svaret må angis kvalitativt som beskrivelse av hyppighet. Som for konsekvensvurderingen er det nødvendig å kunne representere graden av sannsynlighet kvantitativt:

- S=4; Svært sannsynlig
  (hendelsen inntreffer flere ganger hvert år)
- S=3; Meget sannsynlig
  (hendelsen inntreffer årlig eller sjeldnere)
- S=2; Sannsynlig
  (hendelsen inntreffer en gang pr 10 år eller sjeldnere)
- S=1; Lite sannsynlig
  (hendelsen inntreffer en gang per 50 år eller sjeldnere)

I de tilfeller hvor man har løpende statistikk over visse typer hendelser, kan dette benyttes som utgangspunkt for å si noe om sannsynlighet. Det må likevel gjøres med forsiktighet. At noe har inntruffet i fortiden betyr ikke nødvendigvis at dette kommer til å skje i fremtiden. Her må man se på dynamikken i trusselbildet og eventuelle sikringstiltak som allerede er implementert og som kan påvirke sannsynligheten. Et viktig hjelpemiddel i dette arbeidet kan være virksomhetens egne rapporter om sikkerhetstruende hendelser.

Andre måter å vurdere sannsynlighet på, kan være ut fra letthetsbetraktning (”*Hva skal til for at hendelse x inntreffer?*”) eller med utgangspunkt i motivering (”*Hvordan kan andre nyttegjøre seg…?*” eller ”*Hvorfor vil noen…?*”). Dette kan også være nyttige hjelpemidler i arbeidet med å fastsette sannsynlighet.

### 2.4.3 Fastsetting av risiko

Når konsekvens og sannsynlighet er bestemt, kan vi fastsette hendelsens risiko. Begrepet risiko uttrykker en hypotese om den fare hendelsen representerer for verdiene i virksomheten.

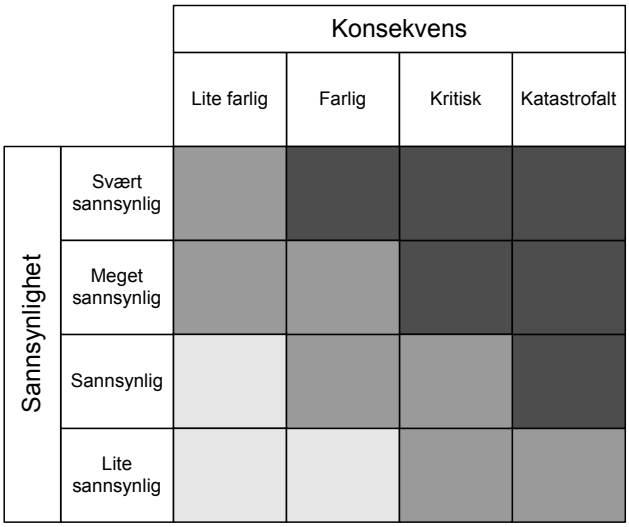
Som nevnt kan konsekvens og sannsynlighet angis som kvantitative størrelser. Risiko kan da avmerkes i en *risikomatrise*, som vist i figur 6. En hendelse med en estimert konsekvens og sannsynlighet vil da høre til en bestemt rute i risikomatrisen. **Risiko for uønskede hendelser som er med i ROS-analysen skal dokumenteres i risikomatrisen**.

På bakgrunn av matrisen kan risiko deles inn i tre hovedområder:

*Høy risiko* :risikoreduserende tiltak skal iverksettes umiddelbart (mørk grå felt i risikomatrisen)

*Middels risiko* :risikoreduserende tiltak skal vurderes (mellomgrå felt i risikomatrisen)

*Lav risiko* :ikke nødvendig å iverksette risikoreduserende tiltak, så fremt krav i lov og forskrift er oppfylt (lys grå felt i risikomatrisen)




*Figur 6: Risikomatrise.* ***Figuren er hentet fra rapporten,*** **Objekt- og informasjonssikkerhet. Metode for risiko- og sårbarhetsanalyse*****, Skavland Idsø og Mejdell Jakobsen, 2000, side 44.***

### 2.4.4 Risikoevaluering og akseptabel risiko

Hensikten med å fastsette risiko er å få en oversikt over virksomhetens trusselbilde, og bruke dette som grunnlag for å redusere de risikoer man ikke kan akseptere.

Virksomhetenes utøvelse av forebyggende sikkerhetstjeneste skal ta utgangspunkt i sikkerhetsloven med forskrifter. Bestemmelsene i forskriftene er likevel bare å regne som minimumskrav. Virksomheten plikter løpende å vurdere om skjermingsverdig objekt/informasjon er godt nok sikret i forhold til risikobildet og kjente sårbarheter. Gjennom utøvelse av risikohåndtering skal virksomhetene avdekke behov for å iverksette ytterligere tiltak utover minimumskravene. Dette systemet skal sikre en tilpasset og fleksibel grunnsikring innenfor hver virksomhet og innenfor hver samfunnssektor - summen av dette bidrar til samfunnets totale sikkerhet.

## 2.5 Trinn 3: Utarbeiding og implementering av tiltak

I trinn 3 utarbeides og implementeres risikoreduserende tiltak på bakgrunn av risikoevalueringen i trinn 2.

### 2.5.1 Kartlegging av eksisterende tiltak

Før nye tiltak kan vurderes, må eksisterende sikkerhetsfunksjoner kartlegges. Slike sikringsmekanismer kan være fysiske (låser, brannmurer), operative (vakthold) eller organisatoriske (prosedyrer, rutiner, organisasjonsstrukturer). Kartleggingen har to hensikter:

1. Unngå overlapping og unødvendig bruk av ressurser
2. Finne ut om de eksisterende mekanismer er tilfredsstillende

Eksisterende tiltak skal dokumenteres i de relevante planer og instrukser. Planer og instrukser skal videre listes opp i *grunnlagsdokument for sikkerhet*. **Etter hvert som nye tiltak blir implementert, skal de inkluderes i de riktige planer og instrukser**.

Ved revisjon av prosessen bør eksisterende tiltak vurderes for å finne ut om de er hensiktsmessige.

### 2.5.2 Utarbeiding av sikringstiltak

Sikringstiltak utarbeides i hovedsak på bakgrunn av resultatene fra risiko- og sårbarhetsanalysen i trinn 2. De forebyggende mottiltak kan, uavhengig av de ulike sikkerhetsfaglige områdene, deles inn i tre kategorier;

- Barrierer
- Deteksjon
- Reaksjon

Når den enkelte virksomhet skal utøve forebyggende sikkerhetstjeneste, er det viktig at det foreligger en forståelse for innholdet i disse kategoriene av tiltak.

**Barrierer** er her å forstå som de faktiske sikkerhetstiltakene som omgir skjermingsverdig informasjon og objekt. Barrierene skal helst forhindre, eller i hvert fall redusere muligheten for, at trusselaktører kan utnytte sårbarheter i virksomheten. Det er vesentlig at de ulike tiltakene er samstemte og utgjør en helhetlig sikring av informasjonen og objektene.

De ulike tiltakene kan videre deles inn i ulike underkategorier. Dette kan være:

- **fysiske** - som f eks gjerder, vegger/dører/vinduer, oppbevaringsenheter, alarmsystemer
- **psykologiske** - som f eks normer, sanksjoner og informasjon
- **personellmessige** – som f eks sikkerhetsklarering og autorisasjon
- **elektroniske** - som f eks strålingshindring, systemtekniske krav
- **logiske** – som f eks kryptologi
- **administrative** – som f eks organisering, rapportering, adgangskontroll og håndteringsprosedyrer, plan- og regelverk, revisjoner og risikohåndtering

Barrierene fastsettes mer spesifikt innenfor de ulike fagområdene innenfor forebyggende sikkerhet.

**Deteksjon** forstås som virksomhetenes fysiske eller elektroniske evne til å avdekke sikkerhetstruende hendelser. Dette kan være egenforskyldt kompromittering av informasjon eller sikkerhetstruende aktivitet fra en trusselaktør. Dette kan eksempelvis omhandle hvilke personer eller metoder en trusselaktør nyttiggjør seg for å forberede eller gjennomføre et anslag.

**Reaksjon** er her å forstå som virksomhetens handlemåte etter at kompromittering eller annen sikkerhetstruende virksomhet er avdekket. Reaksjonen kan være av elektronisk, fysisk eller administrativ karakter.

### 2.5.3 Vurdering av nytte og kostnad

De aller fleste sikringstiltak har en kostnad – både ved implementering og drift. Det er derfor ikke sikkert at høyest mulig sikkerhet alltid er ønskelig eller fornuftig. Investeringskostnadene for sikringstiltak må veies mot det potensielle tapet som et sikkerhetsbrudd kan forårsake. I § 4-2 i forskrift om sikkerhetsadministrasjon fremgår at virksomheten skal vurdere kostnadseffektivitet ved implementering av nye tiltak.

Samtidig må en slik tilnærming brukes med fornuft. I visse tilfeller kan det være vanskelig å kvantifisere kostnadene ved et sikkerhetsbrudd, og for objekter som er av høy betydning bør man ofte investere mer for sikkerheten.

I mange tilfeller vil det også være vanskeligere å fastsette nytte i kroner og øre ved de tiltak man ønsker å implementere. En slik vurdering vil likevel ofte være etterspurt i forbindelse med å forsvare de aktuelle investeringsutgiftene.

En må være klar over at de færreste investeringer i forebyggende sikkerhet genererer nytte i form av *inntekter*. En alternativ måte for å vurdere nytte vil heller være å se på nytte som *unngåtte utgifter*. Utover dette må nytte begrunnes kvalitativt.

### 2.5.4 Kommunikasjon med beslutningstakere

Etter at tiltak er identifisert, og prioritert i forhold til kostnader og egnethet, skal de dokumenters i en tiltaksplan. Denne tiltaksplanen skal overleveres virksomhetens beslutningstaker(e) på området.

I de fleste tilfeller vil det ikke være arbeidsgruppens oppgave å avgjøre hvilke tiltak som faktisk skal implementeres. Dette er ofte en ledelsesbeslutning, tatt på grunnlag av den prioriteringen som arbeidsgruppen gjør.

Dette krever at arbeidsgruppen kan kommunisere på en enkel og lettfattelig måte. Tiltaksplanen må være oversiktlig og lett forståelig for personer som ikke jobber med sikkerhet i det daglige. Prioriteringen må være klar, med begrunnelse for de valg som er gjort og en vurdering av kost/nytte. Dette er essensielt for å skaffe til veie et underlag som gir beslutninger i tråd med hva arbeidsgruppen mener er de rette prioriteringer.

### 2.5.5 Implementering av tiltak

Når tiltak er godkjent (eller endret/omprioritert) av virksomhetens beslutningstager(e), kan de implementeres.

Det er viktig at ansvar for implementering blir bestemt for alle tiltak. Ansvaret kan ligge hos en enkeltperson, en gruppe eller avdeling. Noen tiltak kan også kreve eksterne ressurser (leverandører, spesialister osv.). I slike tilfeller bør det også eksistere et internt ansvar for gjennomføring.

For alle tiltak skal det settes en frist for gjennomføring. Når tiltaket er implementert, bør den/de ansvarlige registrere dette i et skjema (evt. et dataprogram/database).

Når tiltak er implementert, skal dette oppdateres i de riktige planer og instrukser.

## 2.6 Trinn 4: Kontroll og revisjon

Trinn 4 i prosessen sikrer kontinuitet i sikkerhetsarbeidet gjennom løpende kontroll av de implementerte sikringstiltakene samt overvåking av trusselbildet.

### 2.6.1 Oppfølging og kontroll av sikkerhetsarbeidet

Risikohåndtering er ikke en enkeltstående aktivitet, men en kontinuerlig prosess. Dette betyr at risikobildet[3] må overvåkes og vurderes kontinuerlig. Dette tjener som et grunnlag for å vurdere om nye ROS-analyser må gjennomføres.

I tillegg skal virksomheten løpende kontrollere at sikringstiltakene som er pålagt eller besluttet etablert faktisk er iverksatt og fungerer etter sin hensikt. Dette fungerer som den interne *sikkerhetsrevisjonen* og skal brukes som ett av grunnlagene i ledelsens årlige evaluering av sikkerhetstilstanden.

Tidligere ble det presisert at en ROS-analyse kan være en situasjonsbetinget aktivitet. Samtidig bør en overordnet analyse av virksomheten gjennomføres med faste intervaller, f eks årlig eller hvert andre år, avhengig av virksomhetens objekter/informasjon og trusselbilde. Det er virksomhetens eget ansvar å sørge for at sikkerheten er tilfredsstillende, med bakgrunn i en risikovurdering.

### 2.6.2 Ledelsens evaluering av sikkerhetstilstanden

Virksomhetens leder skal minst en gang i året evaluere den generelle sikkerhetstilstanden i virksomheten. Resultatet av sikkerhetsrevisjonen skal benyttes som et av grunnlagene for evalueringen. I henhold til bestemmelsen i § 4-4 i forskrift om sikkerhetsadministrasjon skal resultatet av sikkerhetsrevisjon og ledelsens evaluering dokumenteres.

[3] Risikobildet forstås her som alle interne og eksterne trusler, samt sårbarheter og svakheter i interne systemer og rutiner.

# 3 Del II Risiko- og sårbarhetsanalyse

## 3.1 Sammendrag

Del II i denne veiledningen presenterer en metode for planlegging, gjennomføring og oppfølging av risiko- og sårbarhetsanalyser (ROS-analyser).

Metoden skiller ikke eksplisitt mellom de tradisjonelle safety-, og security fagområdene. Grunnen til dette er at mange trusler påvirker de to fagområdene gjensidig. Hensikten med å gjennomføre en analyse vil bl.a være å finne sårbarhetene og iverksette tiltak for disse, uavhengig av om de er forårsaket av en tilfeldig eller tilsiktet handling.

Metoden er skjemabasert, og er plassert inn i en helhetlig styringssløyfe for risikohåndtering. Utfylling av skjemaene er beskrevet sammen med hvordan man skal gå fram for å hente inn data. Metoden leder brukeren først gjennom planleggings- og organiseringstrinnet hvor virksomheten, delsystemer, verdier og farekilder skal kartlegges. Med utgangspunkt i dette vil man i neste trinn, som er risiko- og sårbarhetsanalysen, kartlegge uønskede hendelser, fastsette risiko og vurdere dette opp mot akseptabel risiko. Dette leder frem til en prioritert tiltaksliste og handlingsplan. Metoden avslutter med beskrivelse av hvordan kontroll og revisjon bør utføres. Alle skjemaer til bruk i metoden finnes til slutt i rapporten

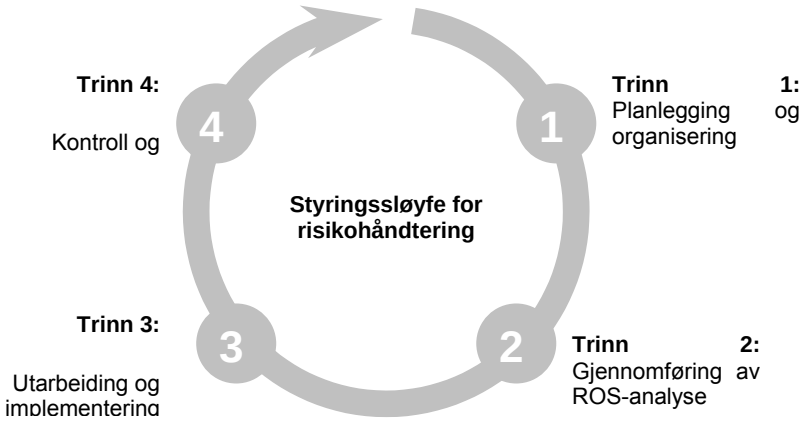
## 3.2 Innledning

Risiko- og sårbarhetsanalyser (ROS-analyser) er et viktig hjelpemiddel for å kunne utøve risikohåndtering. Figuren nedenfor illustrerer at risikohåndtering er en løpende aktivitet som består av fire trinn, hvor ROS-analysen er gitt en sentral plass i styringssløyfen.

ROS-analysen må integreres i styringssløyfen for å kunne ha nytte.

De anbefalinger om iverksetting av tiltak som fremgår av en analyse må implementeres følges opp av virksomheten på lik linje med andre aktiviteter virksomheten jobber med.

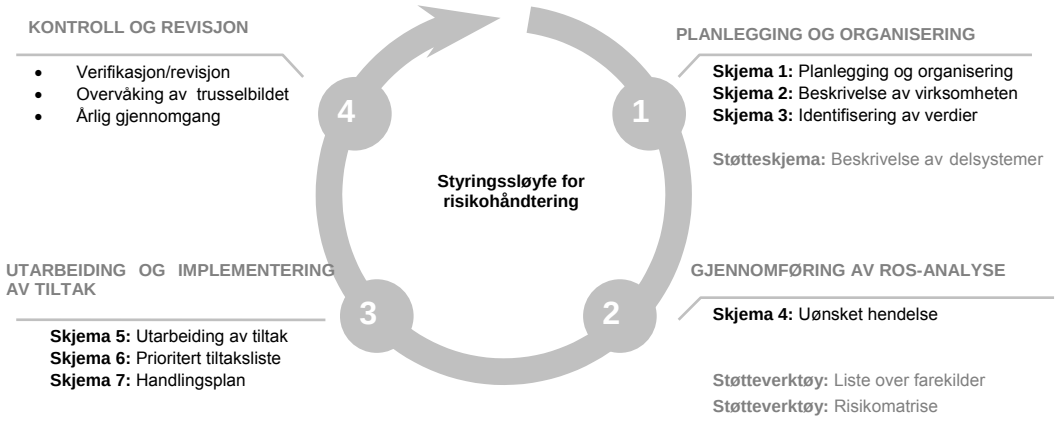
Planlegging og organisering av arbeidet er en viktig forutsetning for å kunne gjennomføre en effektiv ROS-analyse. Videre er utarbeiding og implementering av tiltak i etterkant av analysen essensielt; det hjelper lite å avdekke risikoer dersom man ikke gjør noe for å redusere dem. Trinn 4 – Kontroll og revisjon – er viktig for å sikre kontinuitet i sikkerhetsarbeidet og oppfølging/verifikasjon av implementerte tiltak.




*Figur 7: Styringssløyfe for risikohåndtering*

## 3.3 Bruk av metoden

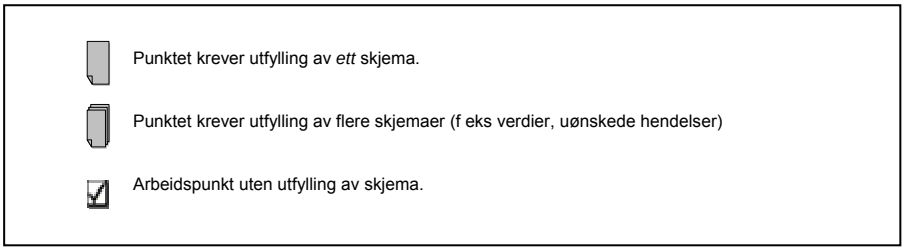
Metoden i denne veiledningen følger styringssløyfens fire trinn for risikohåndtering. Metoden består av sju skjemaer som skal fylles ut i bestemt rekkefølge. Alle skjemaer som beskrives finnes som vedlegg bak i denne veiledningen. Fra side 5 i del II her gis en veiledning til hvordan skjemaene kan fylles ut.

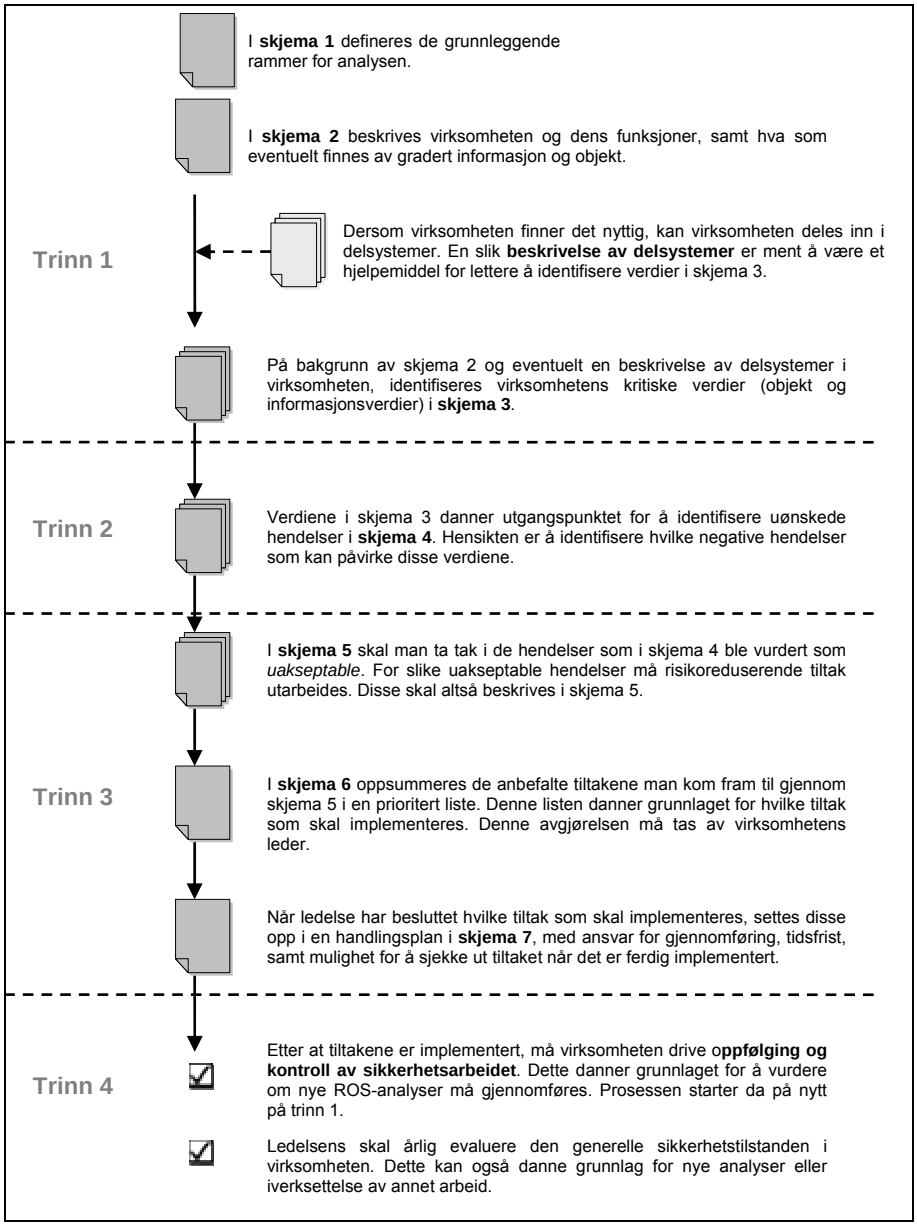



*Figur 8: Metodens hovedtrinn og skjemaer*

Figur 8 viser hvordan metoden er relatert til trinnene i styringssløyfen. Tre skjemaer er relatert til planlegging og organisering av arbeidet. Selve ROS-analysen er oppsummert i ett skjema, mens utarbeiding og implementering av tiltak støttes av tre skjemaer. Kontroll og revisjon gjennomføres ikke ved bruk av skjemaer, men består likefullt av tre viktige arbeidspunkter.

Sammenhengen mellom skjemaer og arbeidspunkter i metoden, samt hvordan de skal brukes, er vist i skjema 3 på neste side. Følgende symboler er benyttet:






*Figur 9: Sammenheng mellom metodens skjemaer og arbeidspunkter*

## 3.4 Dokumentasjon av arbeidet

Alle skjemaer og vedlegg som blir fylt ut gjennom denne metoden, tjener som dokumentasjon av ROS-arbeidet, og bør derfor arkiveres etter at analysen er gjennomført. Det anbefales i tillegg at arbeidsgruppen skriver en oppsummerende rapport til ledelsen i etterkant av arbeidet. Denne bør inneholde de viktigste resultatene av analysen. I tillegg bør arbeidsgruppen drøfte problemer og svakheter og komme med eventuelle råd for senere analyser/revisjoner. Rapporten bør være konkret på hvilke tiltak arbeidsgruppen anbefaler at iverksettes i virksomheten.

Under arbeidet må det foretas en verdivurdering av informasjonen. Dersom verdivurderingen viser at informasjonen er skjermingsverdig må gradering påføres relevant informasjon. Særlig viktig her er at informasjonssystemer/pcer som brukes i arbeidet er godkjent for aktuelt graderingsnivå.

## 3.5 Trinn 1: Planlegging og organisering

Hensikten med trinn 1 i styringssløyfen er å legge forholdene til rette for å kunne gjennomføre en effektiv ROS-analyse. Først skal arbeidsgruppen definere de grunnleggende rammene for analysen i skjema 1. I skjema 2 skal arbeidsgruppen gå nærmere inn på virksomheten, og se på input, output, kritiske funksjoner og hva virksomheten har av gradert informasjon og objekt dersom dette er relevant. I skjema 3 skal virksomhetens mest kritiske verdier (informasjon og/eller objekt) identifiseres. Disse skal videre brukes som utgangspunkt for å identifisere uønskede hendelser i selve ROS-analysen i trinn 2.

### 3.5.1 Skjema 1: Planlegging og organisering

I skjema 1 defineres de grunnleggende rammene for analysearbeidet. Hensikten er å danne en oversikt over hensikten med og omfanget av analysearbeidet, hvem som skal delta i arbeidet og hvilken tidsbegrensning som er satt.

**a)** **Virksomhetens navn:** I punkt a definerer man hvilken virksomhet analysen gjelder.

**b)** **Målsetting for analysen:** I punkt b skal målsettingen for analysen beskrives kort.

**c)** **Bakgrunn for analysen:** Bakgrunnen for analysen skal spesifiseres gjennom sjekkboksene i punkt c. ROS-analyser bør gjennomføres jevnlig (rutinemessig kontroll/revisjon) for å sikre kontinuitet i sikkerhetsarbeidet. Videre kan endringer i lovverk være en god grunn for å gjøre en analyse og kontrollere at kravene er oppfylt. Større endringer i virksomheten (f eks flytting, større ombygging) eller i omgivelsene (nye trusler, økt nasjonalt risikonivå) vil også kunne være gode grunner for å gjøre en analyse. Dersom analysen gjennomføres av andre årsaker, skal dette spesifiseres på skjemaet.

**d)** **Eventuelle avgrensninger/spesielle forutsetninger:** Dersom spesielle avgrensinger/ forutsetninger ligger til grunn for analysen, skal dette bemerkes i punkt d. Dette kan være avgrensinger i omfang, antagelser, samt ressursbegrensinger knyttet til tid, bemanning, utstyr, datagrunnlag osv.

**e)** **Analyseleder:** I punkt e spesifiseres det hvem som er leder for analysearbeidet. Analyselederen bør ha god kjennskap til virksomheten, og bør helst ha gjennomført slike analyser tidligere.

**f)** **Analysedeltakere:** Arbeidet med risikoanalysen skal gjennomføres av en arbeidsgruppe. Denne skal omfatte personer med nødvendig kjennskap til virksomheten og til gjennomføring av risikoanalyser. I punkt f skal det spesifiseres hvem som er med i gruppen. Gruppens størrelse kan variere noe med virksomhetens størrelse og analyseomfang, men bør ikke overstige sju til åtte personer, inkludert analyseleder

**g)** A**ntatt tidsbruk:** I punkt g angis start- og sluttidspunkt for analysen. Dette er viktig for å kunne planlegge hvor mye ressurser arbeidet krever.

**h)** A**nsvarlig for kvalitetssikring:** Hvis mulig, bør kvaliteten på arbeidet kontrolleres av en kompetent person som ikke deltar aktivt i selve analysearbeidet. Avhengig av omfanget kan slik kontroll gjennomføres fortløpende eller som sluttkontroll.

### 3.5.2 Skjema 2: Beskrivelse av virksomheten

Gjennom skjema 2 skal arbeidsgruppen komme fram til hva som er de mest kritiske funksjonene og avhengighetene i virksomheten, samt beskrive hva virksomheten eventuelt har av gradert informasjon og graderte objekt. Hensikten er å gjøre deltakerne i analysen bevisste på hva som er de mest kritiske funksjonene/verdiene i virksomheten, og som følgelig har størst behov for beskyttelse.

a) **Hvilke tjenester/produkter (output) leverer virksomheten?** Formålet med en virksomhet er å utføre oppgaver, eller å levere tjenester eller produkter til et marked. Dette kan defineres som virksomhetens *output*. Dersom virksomheten ikke klarer å levere sin output, vil det økonomiske grunnlaget for driften kunne falle bort.

b) **Hva er virksomhetens mest kritiske funksjoner?** Virksomhetens mest kritiske funksjoner er de interne systemer og prosesser som sørger for at man klarer å levere rett tjeneste/produkt til rett tid. Dersom disse blir satt ut av spill, vil virksomheten ikke kunne produsere det den skal.

c) **Hvilke innsatsfaktorer er virksomheten avhengig av for å fungere?** Alle virksomheter er avhengige av ulike *innsatsfaktorer* i form av varer, tjenester, arbeidskraft osv. Disse er essensielle for å kunne utføre kritiske funksjoner og levere de ønskede tjenester og produkter.

d) **Hva har virksomheten av gradert informasjon/graderte objekt?** Gradert informasjon og objekt er sårbare verdier for en virksomhet. Sikkerhetsloven krever spesifikt at virksomheten med gradert informasjon og graderte objekt, skal sikre disse verdiene gjennom implementering av sikringstiltak. Å ha oversikt over denne typen verdier er derfor viktig i det videre analysearbeidet.

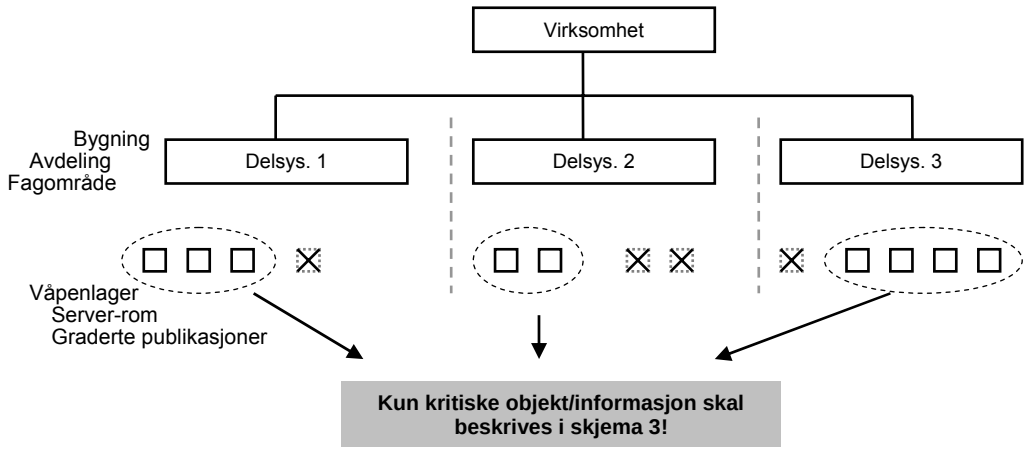
### 3.5.3 Skjema 3: Beskrivelse av kritiske objekt og informasjonsverdier

En virksomhet vil til enhver tid ha informasjon og objekt av varierende verdi. Det faktum at man anser noe for å ha en verdi, innebærer at det eksisterer et skadepotensiale – det vil si at informasjonen/objektet kan bli utsatt for en hendelse med negative konsekvenser. Potensialet i forbindelse med en reduksjon eller et tap av sikkerhetsmessig verdi kan være knyttet til flere forhold. – Informasjon og/eller objekter med betyding for rikets sikkerhet er gitt beskyttelse gjennom minimumskravene i lov og forskrift på bakgrunn av dets kritiske funksjon. Å fastslå disse verdiene i penger er ikke så enkelt eller interessant, derfor er kravene til risikohåndtering strenge.

Andre verdier i virksomheten kan måles i forhold til potensielt økonomisk tap, tap av anseelse og integritet, samt økt sårbarhet på virksomhetsnivå. Dess høyere tapspotensial, dess høyere verdi.

Det er lite hensiktsmessig å bruke ressurser på å analysere informasjon/eiendeler av lav verdi siden tapspotensialet for disse er tilsvarende lite. **I skjema 3 skal derfor arbeidsgruppen kun beskrive de informasjonsverdier og objekt som har et høyt skadepotensial.** Videre i analysen er det kun disse verdiene som skal analyseres med hensyn på hvilke trusler de kan bli utsatt for.

Det første leddet i det å identifisere verdier, er å bryte ned virksomheten i passende deler. Videre må man gå systematisk gjennom disse delene for å sikre at man identifiserer alle verdier med høyt skadepotensial. For små virksomheter hvor man har god oversikt, kan det hende at denne nedbrytingen er unødvendig. For større virksomheter anbefales det at virksomheten deles opp i *delsystemer* før man identifiserer verdiene. Sammenhengen mellom virksomhet, delsystemer og verdier er illustrert med eksempler i følgende figur:




Denne metoden tilbyr et støtteskjema for kartlegging av delsystemer. Dette er beskrevet i *vedlegg B*. Selve skjemaet finnes sammen med de andre skjemaene bakerst i denne veiledningen. Dersom virksomheten finner det nyttig å beskrive delsystemer, må dette gjøres før man her går videre og bruker skjema 3, som blir beskrevet under.

*For skjema 3 skal det fylles ut ett skjema per objekt eller informasjonsverdien som er identifisert. Disse nummereres da 3.1, 3.2, osv.*

**a) Beskrivelse av verdi:** I dette feltet beskrives kort det aktuelle objektet eller den aktuelle informasjonsverdienen.

**b) Begrunnelse for kritikalitet:** I punkt b skal verdiens kritikalitet begrunnes.

c) **Ytterste konsekvens ved kompromittering:** I punkt c skal arbeidsgruppen beskrive den ytterste konsekvensen ved kompromittering av objektet/informasjon. Dette innebærer å beskrive de verste konsekvensene som kan inntreffe ved brudd på *konfidensialitet*, *integritet* eller *tilgjengelighet* for informasjon, samt brudd på *funksjonalitet* og *yteevne* for objekt.

**d) Mulighet for erstatning ved kompromittering:** I dette punktet skal arbeidsgruppen kartlegge muligheten for erstatning dersom objektet/informasjonene blir kompromittert.

e) **Eventuelt økonomisk tap ved kompromittering (ytterste konsekvens):** Dersom det er relevant og mulig, skal arbeidsgruppen i punkt d anslå det potensielle økonomiske tapet ved kompromittering. Dette tapet er relatert til ytterste konsekvens ved kompromittering, og kan ofte anslås ved å se på erstatningskostnaden for objektet/informasjonene, jfr. punkt d.

## 3.6 Trinn 2: Gjennomføring av ROS-analyse

I trinn 2 gjennomføres selve ROS-analysen. Hensikten med analysen er å danne et bilde av risikoen virksomheten står overfor, slik at man kan benytte dette som et grunnlag for planlegging og implementering av sikringstiltak. Gjennomføring av ROS-analysen er derfor på mange måter det viktigste elementet i risikohåndteringen. Samtidig er det viktig å presisere at analysen har liten hensikt dersom den ikke benyttes som grunnlag for det videre arbeidet.

### 3.6.1 Oversikt over farekilder

Gjennom skjema 3 ble kritiske informasjonsverdier og objekt identifisert. Dersom disse verdiene blir utsatt for trusler, kan dette resultere i *uønskede hendelser*.

I det følgende presenteres en oversikt over mulige farekilder som kan true disse verdiene på ulike måter. **Dette er ikke en komplett oversikt over alle mulige farekilder**. En komplett oversikt vil være umulig å utarbeide på grunn av de dynamiske forholdene både internt i virksomheten samt i omgivelsene. Oversikten er derimot et utgangspunkt som må kompletteres og tilpasses den enkelte virksomheten.

Oversikten skal brukes sammen med å se på de verdier som ble identifisert i skjema 3. Ved å se på relevante trusler mot kritiske verdier antas det at arbeidsgruppen vil være i stand til å identifisere relevante hendelser (scenarioer) i neste trinn.

Oversikten over farekilder er delt inn i *trusler* og *påvirkende faktorer*.

| **Trusler** | **Påvirkende faktorer** |
|---|---|
| ▪ Spionasje<br>▪ Sabotasje<br>▪ Terrorhandlinger<br>▪ Hacking<br>▪ Tyveri<br>▪ Informasjonslekk<br>▪ Rutinesvikt<br>▪ Brudd på infrastruktur<br>▪ Brann/brannstifting<br>▪ Eksplosjon/gassutslipp<br>▪ Flom/ras/storm<br>▪ Strømbrudd (påført, eller tilfeldig)<br>▪ Vannlekkasje | ▪ Omorganisering<br>▪ Outsourcing<br>▪ Bruk av eksterne konsulenter, leverandører eller underleverandører<br>▪ Iverksetting av nye lover og/eller forskrifter<br>▪ Uklare ansvarsforhold<br>▪ Manglende/dårlig oppfølging av rutiner og instruksverk<br>▪ Stor turnover i arbeidsstokken<br>▪ Indisponibelt nøkkelpersonell<br>▪ Installering av ny teknologi<br>▪ Manglende redundans<br>▪ Manglede barrierer |

### 3.6.2 Skjema 4: Uønsket hendelse

En uønsket hendelse er en handling som kan utsette verdier for risiko. Identifisering av slike hendelser er derfor kjernepunktet i risikoanalysen. Gjennom skjema 4 skal arbeidsgruppen dokumentere disse hendelsene.

De uønskede hendelsene identifiseres ved å gå systematisk igjennom verdiene kartlagt i skjema 3, og benytte oversikten over farekilder for å se hvilke potensielle trusler hver enkelt verdi står overfor.

Det er selvsagt mulig å identifisere flere hendelser relatert til samme verdi.

*Ett skjema skal fylles ut for hver hendelse som identifiseres. Disse nummereres 4.1, 4.2 osv.*

**a) Beskrivelse av uønsket hendelse:** I punkt a skal den uønskede hendelsen beskrives. Her bør man få med hva som kan skje, hvilken verdi (verdier) som berøres, samt en beskrivelse av de mulige konsekvensene.

**b)**

**c) Gradering av sannsynlighet og konsekvens:** I punkt b og c skal sannsynlighet og konsekvens fastsettes for den aktuelle hendelsen. Dette gjøres kvalitativt på en skala med fire alternativer. Prosessen med å bestemme sannsynlighet og konsekvens gjøres gjennom en

diskusjon innad i analysegruppen. Om nødvendig kan eksterne ressurspersoner trekkes inn for å hjelpe til i dette arbeidet.
Generelt kan de følgende retningslinjer benyttes for graderingen av sannsynlighet:

- *Svært sannsynlig*: hendelsen inntreffer flere ganger hvert år
- *Meget sannsynlig*: hendelsen inntreffer årlig eller sjeldnere
- *Sannsynlig*: hendelsen inntreffer en gang pr 10 år eller sjeldnere
- *Lite sannsynlig*: hendelsen inntreffer en gang per 50 år eller sjeldnere

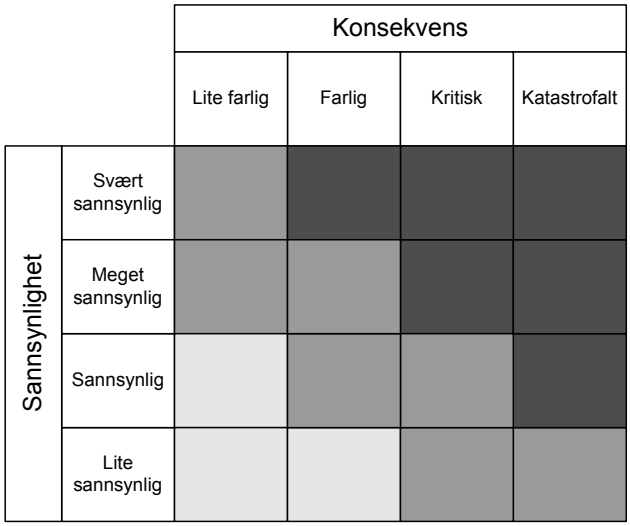
Ved vurdering av konsekvens er det naturlig å ta utgangspunkt i målet med den forebyggende sikkerhetstjenesten – nemlig å opprettholde konfidensialitet, integritet og tilgjengelighet for virksomhetens informasjon og objekt. Klarer man ikke å opprettholde dette, vil det kunne få ulike konsekvenser for virksomheten, og i ytterste konsekvens for rikets sikkerhet. Følgende retningslinjer kan benyttes for gradering av konsekvens:

- *Katastrofalt*: Hendelsen fører til konsekvenser som påvirker nasjonen som helhet, i form av betydelig/uopprettelig økonomisk tap, eller tap av anseelse og integritet. Tap av skjermingsverdig informasjon kan føre til vesentlig økt sårbarhet for nasjonen.
- *Kritisk*: Hendelsen fører til betydelig eller uopprettelig økonomisk tap for virksomheten (og eventuelle samarbeidspartnere), og kan føre til alvorlig tap av anseelse og integritet. Tap av skjermingsverdig informasjon kan føre til vesentlig økt sårbarhet for virksomheten.
- *Farlig*: Hendelsen kan medføre betydelig økonomisk tap for virksomheten (men som kan gjenopprettes) samt vesentlig tap av anseelse og integritet. Tap av skjermingsverdig informasjon kan være skadelig for virksomheten.
- *Lite farlig*: Hendelsen kan medføre økonomisk tap for virksomheten (men som kan gjenopprettes) eller kan føre til mindre tap av anseelse og integritet.

**d) Resulterende risikonivå:** Når arbeidsgruppen har fastsatt sannsynlighet og konsekvens, kan man finne *risikoen* for hendelsen. Dette gjøres ved å bruke *risikomatrisen* som er illustrert i figur 4 på neste side. Risikomatrisen finnes sammen med skjemaene bak i denne veiledningen.

Risikomatrisen er delt inn i tre områder – lys grå (lav risiko), mellomgrå (middels risiko) og mørk grå (høy risiko). Ved å kombinere sannsynligheten og konsekvensen for en bestemt hendelse, vil man kunne sette et kryss i en bestemt rute i matrisen. Hendelsen vil da havne innenfor en av de tre definerte områdene.

Som eksempel kan vi tenke oss en uønsket hendelse, f eks nr. 4.3 ”*sabotasje av hovedkraftstasjon*”, hos virksomheten Kraftnett AS. Sannsynligheten for denne hendelsen er *liten*, men skulle den inntreffe vil konsekvensene kunne bli *kritisk* – både for virksomheten, men også for andre kraftleverandører som transporterer kraft via virksomhetens hovednett. I dette eksemplet er altså sannsynligheten liten og konsekvensen kritisk. Når vi setter inn disse vurderingene i risikomatrisen, vil resulterende risikonivå havne i det mellomgrå feltet i matrisen.




Figur 10: Risikomatrise. **Figuren er hentet fra Skavland Idsø og Mejdell Jakobsen, *Objekt- og informasjonssikkerhet*, NTNU 2000, side 44.**

Etter å ha funnet det resulterende risikonivået fra matrisen, går man tilbake og krysser av for resulterende risikonivå i punkt d på skjemaet. I eksemplet med Kraftnett AS, fant vi at hendelse 4.3 har middels risiko:

| | | |
|---|---|---|
| d. | Resulterende risikonivå (fra risikomatrise): | ☐ Høy risiko<br>☐ Middels risiko<br>☐ Lav risiko |

**e) Akseptabel risiko?** Etter at man har funnet det resulterende risikonivået for hendelsen, skal man vurdere om risikoen (for hendelsen) er akseptabel eller ikke. For å kunne gjøre dette må man ha definert hva som er et *akseptabelt risikonivå*.

Sikkerhetsloven med forskrifter er minimumskrav for alle virksomheter underlagt loven. Minimumskravene er basert på en generell risikovurdering, og sikkerhetstrusselen på nasjonalt nivå. Utover minimumskravene er virksomhetene selv ansvarlige for å iverksette nødvendige tiltak med bakgrunn i trusselbildet mot egen virksomhet.

Der hvor man ikke kan benytte lovkrav eller virksomhetskrav for å avgjøre om risikoen er akseptabel eller ikke, kan arbeidsgruppen se på det resulterende risikonivået (se figur 2, risikomatrise). Dersom risikoen er høy bør den trolig ikke aksepteres, da konsekvensene trolig kan gi vesentlige økonomiske (og andre) konsekvenser for virksomheten. Dersom risikoen havner i det midtre området må man se på kostnaden versus nytten av å reduseres den aktuelle risikoen. Dersom kostnadene overstiger den antatte nytten (i kroner) av å redusere risikoen, er det lite hensiktsmessig å gjøre noe (→ hendelsen aksepteres). Motsatt, dersom nytten av å redusere risikoen antas å være høyere enn kostnadene, bør risikoen reduseres (→ hendelsen er uakseptabel).

Dersom resulterende risiko for en hendelse befinner seg i det laveste området, anses det som

lite hensiktsmessig å redusere denne ytterligere.

Når avgjørelsen om akseptabel/ikke akseptabel er tatt, gjelder følgende regel for det videre arbeidet:

| |
|---|
| Dersom hendelsen er *akseptabel*, avsluttes arbeidet for denne hendelsen med skjema 4. |
| Dersom hendelsen er *uakseptabel*, må tiltak iverksettes for å redusere risikoen, og uakseptable hendelser benyttes som utgangspunkt for neste trinn. |

## 3.7 Trinn 3: Utarbeiding og implementering av tiltak

I trinn 2 ble mulige uønskede hendelser identifisert. Videre kom man fram til et resulterende risikonivå for hver hendelse, og man vurderte om hendelsen var akseptabel eller ikke.

Hendelser som ble vurdert som akseptable trenger ingen videre analyse. Hensikten i trinn 3 er å ta tak i de *uakseptable hendelsene*. For disse må risikoen reduseres ned til et akseptabelt nivå, slik at man i det minste tilfredsstiller lovpålagte og virksomhetsdefinerte krav. Dette gjøres gjennom å utarbeide og implementere *risikoreduserende tiltak*.

### 3.7.1 Skjema 5: Utarbeiding av tiltak

Hensikten med skjema 5 er å utarbeide risikoreduserende tiltak for de uakseptable hendelsene, med det mål at de *ikke skal inntreffe*.

Ett skjema skal fylles ut for hver uakseptable hendelse som ble identifisert i skjema 4, punkt e.

**a) Uakseptabel hendelse:** I dette punktet nedtegnes den uakseptable hendelsen.

**b) Eksisterende tiltak:** For en del hendelser kan det hende at tiltak allerede eksisterer. Dette skal avdekkes i punkt b. Eventuelle eksisterende tiltak skal beskrives, og deres egnethet skal vurderes.

Dersom det eksisterende tiltaket er tilstrekkelig, stoppes analysen ved punkt b for den aktuelle hendelsen. Dersom eksisterende tiltak må forbedres, eller helt nye tiltak må implementeres, fortsetter man til punkt c.

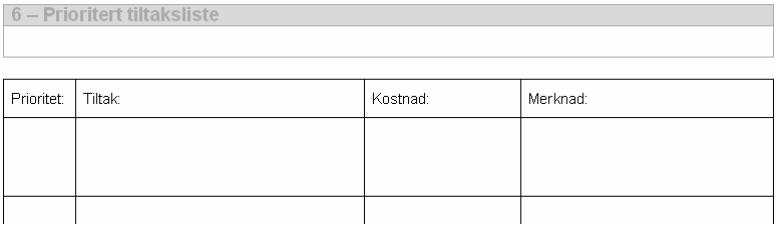
**c) Forslag til nye tiltak:** I punkt c skal nye risikoreduserende tiltak foreslås. Det er lagt opp til at tre ulike tiltak kan foreslås for hver hendelse. Hensikten er at det skal være mulig å vurdere ulike tiltak opp mot hverandre dersom flere identifiseres.

Hvert tiltak skal beskrives, og det skal angis om tiltaket er konsekvens- og/eller sannsynlighetsreduserende. I tillegg skal en enkel vurdering av kostnad og nytteverdi gjøres for hvert tiltak. Dersom flere tiltak er aktuelle, kan dette være til hjelp om man må velge mellom dem.I den høyre kolonnen i punkt c skal det krysses av for det tiltaket arbeidsgruppen

*anbefaler* å implementere/gjennomføre – forutsatt at man har identifisert mer enn ett alternativ.

### 3.7.2 Skjema 6: Prioritert tiltaksliste

Arbeidsgruppen gikk i forrige skjema gjennom alle uakseptable hendelser og foreslo tiltak der hvor de ikke eksisterte fra før, eller ikke var tilstrekkelige. I skjema 6 skal disse tiltakene settes opp i en prioritert liste. Den prioriterte listen skal danne grunnlaget for å fatte beslutninger om hvilke tiltak som faktisk skal *iverksettes*. Ideelt sett bør alle tiltak implementeres, men i realiteten vil ikke dette alltid være mulig. En prioritert liste vil derfor kommunisere hva som er viktigst å gjennomføre. Den utfylte listen vil være et hjelpemiddel for den eller de som skal ta *beslutningen* om hvilke tiltak som skal iverksettes. Dette vil som regel være virksomhetens leder, alternativt leder på et lavere nivå, eller sikkerhetsleder. Denne listen kan enten overleveres direkte som den er, eller danne grunnlaget for et mer fyldig bakgrunnsdokument fra arbeidsgruppen, eksempelvis en rapport.



6 – Prioritert tiltaksliste

| Prioritet: | Tiltak: | Kostnad: | Merknad: |
|---|---|---|---|
| | | | |
| | | | |

*Figur 11: Utsnitt av skjema 6 – prioritert tiltaksliste*

Hvert tiltak (i prioritert rekkefølge fra nr. 1 og oppover) skal beskrives kort, og et overslag over kostnadene skal settes opp.

Kostnadene vil avhenge av om man anser tiltaket som en engangsinvestering (som f eks et gjerde rundt eiendommen, brannmur), eller om tiltaket også medfører driftskostnader av ulikt slag (f eks vedlikehold av gjerdet og vakthold i tillegg, drift av brannmuren og oppdatering av software). Hva som er inkludert/ikke inkludert i kostnadene skal spesifiseres i ”merknad”-feltet, slik at man senere unngår overraskelser.

### 3.7.3 Skjema 7: Handlingsplan

Når ledelsen (eller andre beslutningstakere) har besluttet hvilke tiltak som skal implementeres i virksomheten, er det klart for å sette i gang dette arbeidet. Skjema 7 er i praksis en handlingsplan som har til hensikt å holde oversikt over de tiltak som skal iverksettes, og som til enhver tid *er* implementert.

Alle vedtatte tiltak føres opp i venstre kolonne i skjemaet. For hvert tiltak må arbeidsgruppen føre opp en *ansvarlig person* (kolonne 2). Dette er personen som har hovedansvaret for at tiltaket blir implementert innen en gitt *tidsfrist*. Denne fristen spesifiseres i neste kolonne.

I kolonnen lengst til høyre krysser man av ettersom tiltakene er implementert.


7 – Handlingsplan

| Tiltak | Ansvarlig person | Tidsfrist | Utført |
|---|---|---|---|
| | | | ☐ |
| | | | ☐ |
| | | | ☐ |

*Figur 12: Utsnitt av skjema 7 – Handlingsplan*

## 3.8 Trinn 4: Kontroll og revisjon

Trinn 4 i prosessen skal sikre kontinuitet i sikkerhetsarbeidet gjennom løpende kontroll av de implementerte sikringstiltakene samt overvåking av risikobildet. virksomheter underlagt sikkerhetsloven skal minst en gang i året evaluere den generelle sikkerhetstilstanden. Sikkerhetstilstanden bør for øvrig kontrolleres jevnlig. Hensikten er å sikre at tiltakene er implementert og fungerer som forventet.

### 3.8.1 Overvåking av risikobildet, intern revisjon

Virksomheten må kontinuerlig overvåke risikobildet den står overfor. Risikobildet forstås her som alle interne og eksterne trusler, samt sårbarheter og svakheter i interne systemer og rutiner. Dette tjener som et grunnlag for å vurdere om det er behov for planlegging og gjennomføring av nye ROS-analyser. Store omorganiseringer, flytting, økt konkurransesituasjon og økt terrortrussel er eksempler på situasjoner som kan medføre økt risiko for virksomheten.

I tillegg skal virksomheten løpende verifisere at sikringstiltakene som er pålagt eller besluttet etablert faktisk er iverksatt og fungerer etter sin hensikt. En slik intern *sikkerhetsrevisjon* er virksomhetens kontrollmekanisme, og i seg selv en viktig del av sikkerhetsarbeidet.

Tidligere ble det presisert at en ROS-analyse kan være en situasjonsbetinget aktivitet. Slike analyser vil kunne ta for seg spesielle fagområder. Samtidig bør en overordnet risikoanalyse av virksomheten gjennomføres med faste intervaller, f eks årlig eller hvert andre år, avhengig av trusselbilde og virksomhetens kompleksitet. Bakgrunnen for dette er at overordnete analyser gir et bedre helhetsbilde av de virksomhetens sårbarheter, og kan danne grunnlaget for mer fagspesifikke analyser.

### 3.8.2 Årlig evaluering av sikkerhetstilstanden

Virksomheter underlagt sikkerhetsloven, skal minst én gang i året evaluere sikkerhetstilstanden i virksomheten. Dette ansvaret ligger eksplisitt på virksomhetens leder. Resultatet av sikkerhetsrevisjonen skal benyttes som et av grunnlagene for evalueringen. I følge § 4-4 i forskrift om sikkerhetsadministrasjon skal resultatet av sikkerhetsrevisjon og ledelsens evaluering dokumenteres. ROS-analyser er ofte et godt underlag både for gjennomføring av en sikkerhetsrevisjon (dersom revisjonen ikke avdekker at analyse må gjennomføres), og som underlag for ledelsens evaluering.

# Vedlegg A Dokumenthistorie

2006-11-09 Dokumentet konvertert til ny mal

# Vedlegg B: Beskrivelse av delsystemer

Å dele virksomheten opp i passende deler, funksjoner eller fagområder kan gi arbeidsgruppen bedre oversikt over egen organisasjon. Dette vil i neste omgang gjøre det lettere å foreta en systematisk gjennomgang for å identifisere kritiske objekt og informasjonsverdier. Skjemaet "*Beskrivelse av delsystemer*" er utarbeidet for denne oppgaven, og finnes sammen med de andre skjemaene bakerst i denne veiledningen.

Denne oppdelingen vil trolig være mest relevant i større virksomheter. Det er lagt opp til en hierarkisk struktur med *ett* nivå av delsystemer, før man identifiserer verdien innenfor disse delsystemene.

Oppdelingen kan gjøres på ulike måter, avhengig av hva arbeidsgruppen finner mest hensiktsmessig. Eksempler kan være objektbasert oppdeling (i bygninger, områder, geografisk beliggenhet), oppdeling i avdelinger, fagområder eller andre funksjoner, samt oppdeling i virksomhetens arbeidsprosesser.

Hjelpemidler for å gjøre denne inndelingen kan være organisasjonskart, kart over virksomhetens områder, oversikt over virksomhetens hovedprosesser (samt eventuelt støttefunksjoner), tekniske spesifikasjoner på anlegg/systemer osv. Relevante hjelpemidler som viser hvordan man har gjort inndelingen, bør legges ved analysen som dokumentasjon.

*Det skal fylles ut ett skjema for hvert delsystem.*

**a) Navn på delsystem:** Først definerer arbeidsgruppen delsystemet. Avhengig av hvilken oppdeling man ønsker å gjøre, kan dette f eks være "Hovedkontor", "Ammunisjonslager", "Utviklingsavdelingen" eller "Faktureringsprosessen".

**b) Beskrivelse av delsystem:** Videre skal delsystemet beskrives. Dette gjøres i punkt b. Vekten skal her ligge på å beskrive delsystemets hovedfunksjoner og oppgaver. Dersom gradert informasjon/objekt faller inn under delsystemet, skal dette nevnes her.

**c) Avhengigheter til andre delsystemer:** I punkt c skal arbeidsgruppen se på hvilken input delsystemet er avhengig av, samt hvilken output delsystemet produserer for andre deler av virksomheten.

**d) Konsekvens ved bortfall av hele delsystemet:** I punkt d skal arbeidsgruppen beskrive hvilke konsekvensene bortfall av delsystemet kan få for virksomheten.

# Vedlegg C: Skjemaer for bruk i virksomheten

På de følgende sidene er alle skjemaer i denne metoden vedlagt. Skjemaene kan rives ut, kopieres eller skrives ut for bruk i den enkelte virksomhet.

## Planlegging og organisering

a. Virksomhetens navn:

b. Målsetting for analysen:

c. Bakgrunn for analysen:

- ☐ Rutinemessig gjennomgang/revisjon
- ☐ Lovpålagt krav
- ☐ Endringer i omgivelser/interne forhold
- ☐ Annet:

d. Eventuelle avgrensinger/spesielle forutsetninger:

e. Analyseleder:

f. Analysedeltakere:

g. Dato for oppstart: Dato for ferdigstilling:

h. Ansvarlig, kvalitetssikring:

## Beskrivelse av virksomheten

a. Hvilke tjenester/produkter (output) leverer virksomheten?

b. Hva er virksomhetens mest kritiske funksjoner?

c. Hvilke innsatsfaktorer er virksomheten avhengig av for å fungere?

d. Hva har virksomheten av gradert informasjon/graderte objekt?

Eventuelle vedlegg……..(Antall)

## Støtteskjema: Beskrivelse av delsystemer

a. Navn på delsystem:

b. Beskrivelse av delsystem:

c. Avhengigheter til andre delsystemer.

Inputs:

Outputs:

d. Konsekvens (for virksomheten og/eller andre delsystemer) ved bortfall av delsystem:

## Beskrivelse av kritiske objekt og informasjonsressurser (verdier)

a. Beskrivelse av verdi (objekt/informasjon):

b. Er kritisk pga

☐ objekt/informasjon er sikkerhetsgradert i henhold til sikkerhetsloven

☐ kompromittering av objekt/informasjon gir vesentlig økt sårbarhet for virksomheten, og *kan* føre til økonomisk tap, eller tap av anseelse og/eller integritet

☐ kompromittering av objekt/informasjon gir direkte økonomisk tap, tap av anseelse eller tap av integritet for virksomheten

☐ Annet:_____

c. Ytterste konsekvens ved kompromittering:

d. Mulighet for erstatning ved kompromittering:

e. Økonomisk tap ved kompromittering (ytterste konsekvens):

## Uønsket hendelse

a. Navn/beskrivelse av uønsket hendelse:

b. Gradering av sannsynlighet:
- ☐ Svært sannsynlig
- ☐ Meget sannsynlig
- ☐ Sannsynlig
- ☐ Lite sannsynlig

c. Gradering av konsekvens:
- ☐ Katastrofalt
- ☐ Kritisk
- ☐ Farlig
- ☐ Lite farlig

d. Resulterende risikonivå (fra risikomatrise):
- ☐ Høy risiko
- ☐ Middels risiko
- ☐ Lav risiko

e. Akseptabel risiko? ☐ Ja ☐ Nei

Begrunnelse:

# Risikomatrise

Alle hendelser fra skjema 4 noteres med nummer i korrekt celle risikomatrisen

| | | Konsekvens | | | |
|---|---|---|---|---|---|
| | | Lite farlig | Farlig | Kritisk | Katastrofalt |
| Sannsynlighet | Svært sannsynlig | | | | |
| | Meget sannsynlig | | | | |
| | Sannsynlig | | | | |
| | Lite sannsynlig | | | | |

Mørk grå : høy risiko

Mellomgrå : middels risiko

Lys grå : lav risiko

# Utarbeiding av tiltak (for uakseptable hendelser, skjema 4)

| | | |
|---|---|---|
| a. | Uakseptabel hendelse: | |
| b. | Eksisterende tiltak<br><br>☐ er tilstrekkelig<br><br>☐ finnes, men må forbedres<br><br>☐ finnes ikke– nytt tiltak må iverksettes | Beskrivelse av eksisterende tiltak:<br><br>(bruk eget ark) |
| c. | Forslag til nye tiltak | |

| | | | ANBEFALT TILTAK (kryss av for ett eller flere alternativer): Tiltak 1 | Tiltak 2 | Tiltak 3 |
|---|---|---|---|---|---|
| Tiltak 1: | | | | | |
| ☐ Konsekvensreduserende<br><br>☐ Sannsynlighetsreduserende | Kostnad ☐ ☐ ☐<br>Høy Middels Lav | Nytteverdi ☐ ☐ ☐<br>Høy Middels Lav | | | |
| Tiltak 2: | | | | | |
| ☐ Konsekvensreduserende<br><br>☐ Sannsynlighetsreduserende | Kostnad ☐ ☐ ☐<br>Høy Middels Lav | Nytteverdi ☐ ☐ ☐<br>Høy Middels Lav | | | |
| Tiltak 3: | | | | | |
| ☐ Konsekvensreduserende<br><br>☐ Sannsynlighetsreduserende | Kostnad ☐ ☐ ☐<br>Høy Middels Lav | Nytteverdi ☐ ☐ ☐<br>Høy Middels Lav | | | |

## Prioritert tiltaksliste

| Prioritet: | Tiltak: | Kostnad: | Merknad: |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Blank**

| Tiltak | Ansvarlig person | Tidsfrist | Utført |
|---|---|---|---|
| | | | ☐ |
| | | | ☐ |
| | | | ☐ |
| | | | ☐ |
| | | | ☐ |
| | | | ☐ |
| | | | ☐ |

**Blank**