Nasjonal sikkerhetsmyndighet

Håndbok

Mars 2016

Risikovurdering for sikring

Risikovurderinger er en viktig del av virksomhetens sikkerhetsstyring.

Håndboken beskriver en metode for gjennomføring av risikovurderinger med fokus på tilsiktede uønskete handlinger (sikring).

Håndboken gir råd til virksomheter om hvordan slike risikovurderinger kan planlegges og gjennomføres.

Håndboken er resultat av en delleveranse i Prosjekt SÅKOV (Sikkerhetstilstanden – Årsaker, konsekvenser og virkemidler), på oppdrag fra og finansiert av Forsvarsdepartementet. NSM har ledet prosjektet. FFI har på oppdrag fra NSM gitt vesentlige bidrag i form av metodefaglig og administrativ støtte. I tillegg har representanter for en rekke virksomheter med kompetanse i sikringsrisikovurderinger gitt verdifulle innspill i referansegruppen for prosjektet samt gitt skriftlige bidrag til deler av håndboken.

Mars 2016

Innholdsfortegnelse

Vedlegg til elektronisk utgave

1. Mal for rapportering etter risikovurdering
2. Skjemasamling til bruk i gjennomføring av risikovurdering

1 Om håndboken

Hensikten med håndboken er å bedre sikkerhetstilstanden gjennom å øke sikkerhetsbevisstheten i virksomhetene. Håndboken skal herunder bidra til å bedre situasjonsforståelsen og erkjennelsen om risiko i egen virksomhet, egenevnen til å foreta risikovurderinger og bestillerkompetansen ved bruk av tjenesteleverandører på området.

Håndboken kan i utgangspunktet brukes av alle virksomheter, offentlige og private, store og små. Tilpasninger er imidlertid nødvendig fordi virksomheter har ulik kompetanse, forskjellige typer verdier og ulikt trusselbilde. I tillegg har virksomheter ulike regelverk å forholde seg til, slik som sikkerhetsloven, personopplysningsloven, sektorregelverk mv.
Enkelte har også avtaler med andre virksomheter der sikkerhetskrav inngår.

Håndboken beskriver hvordan risikovurderinger av tilsiktede uønskede handlinger kan planlegges, gjennomføres og dokumenteres.

Håndbokens kapittel 2 gir en forklaring av risikomodellen som benyttes i denne håndboken.

Kapittel 3 omhandler planlegging og igangsetting av en risikovurdering. Dette omfatter forutsetninger for å kunne arbeide effektivt med risikovurderinger, samt forberedelser som må gjøres hver gang man gjennomfører en risikovurdering.

I kapittel 4 beskrives selve gjennomføringen av en risikovurdering. Her er det beskrevet en stegvis gjennomgang av prosessen som omfatter verdivurdering, sikringsmål, trusselvurdering, scenariobeskrivelser og sårbarhetsvurdering. Når alle disse trinnene er gjennomført bør virksomheten ha et godt grunnlag for å gjøre en helhetsvurdering av sin risiko knyttet til tilsiktede uønskede handlinger, og kanskje også noen utilsiktede uønskede hendelser. Skjemaene skal vise hvilken informasjon som behandles i hvert trinn. I noen tilfeller kan skjemaene brukes direkte, men i de fleste tilfellene vil de bare tjene som maler for virksomhetene egen måte å gjøre det på.

2 Risikometodikken

2.1 Sikringsrisiko

Risikobasert sikkerhetsarbeid innebærer at risikovurderingen knyttes til virksomhetens primære mål og leveranser. Det handler om å utvikle et beslutningsunderlag om riktige tiltak for fremtiden basert på best tilgjengelig informasjon, fremfor statiske sikringstiltak som ikke er tilpasset et risikobilde i endring.

Det er viktig å velge en tilnærming for risikovurdering som passer virksomheten og formålet. I mange tilfeller bruker man sannsynlighet og konsekvens for å beskrive risiko. I risikovurderinger med fokus på *tilsiktede uønskede handlinger*, er det ofte mer nyttig å beskrive risiko som en funksjon av verdi, trussel og sårbarhet. I slike sammenhenger kan denne risikomodellen bidra til å få frem et risikobilde som ikke kommer frem gjennom andre modeller. Håndboken er imidlertid laget slik at det i risikovurderingen også skal være mulig å inkludere *utilsiktede uønskede hendelser* som naturkatastrofer og ulykker.

Denne håndboken baserer seg på NS 5832 "*Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse*". NS 5832 beskriver sikringsrisikoanalysen som bestående av tre faser: 1) sikringsrisikovurdering, 2) vurdering av strategi, og 3) vurdering av tiltak. Denne håndboken utdyper prosessbeskrivelsene under 1) sikringsrisikovurdering – heretter benevnt «risikovurdering». I andre standarder, fagområder og miljøer kan begrepet «risiko» forstås, defineres og presenteres annerledes. Mye av arbeidet og suksesskriteriene er imidlertid det samme uavhengig av hvilken modell man bruker; gode forberedelser, ledelsesforankring, sammensatte team, sporbarhet i arbeidet, samt kompetanse om arbeidsform og om det som risikovurderingen omfatter.

2.2 Usikkerhet

Det vil alltid være usikkerhet knyttet til risikovurderinger og analyse. Usikkerheten ligger i informasjons- og datagrunnlaget, organiseringen, kompetanse hos deltakende, bruk av metoder, vurderinger underveis i analysen, presentasjon av resultater, valg av og effekt av tiltak, med mer. Mange av skjemaene presentert i denne håndboken har rubrikker der virksomheten skal beskrive usikkerheten knyttet til vurderingene. Det er viktig å forstå usikkerheten knyttet til risikovurderingen, slik at det blir et mer troverdig beslutningsgrunnlag.

Der hvor det er knyttet stor usikkerhet til konsekvensene av en uønsket handling eller man anser kunnskapen man besitter som mangelfull, kan det være nødvendig å avgrense omfanget av vurderingen. Det kan også være riktig å gjøre vurderingen i flere trinn, ved at man først gjør en overordnet vurdering, og deretter går i dybden der det fremkommer behov for å gjøre det.

Når det gjelder beskyttelse mot tilsiktede uønskede handlinger er det usikkerhet ved for eksempel hva som kan ramme virksomheten, hvilke skader det gir, effekten av tiltakene (beskyttelsen) og hva som blir situasjonen til virksomheten under og etter hendelsen. Det har vært en praksis på flere områder å benytte ulike forståelser av sannsynlighet til å rangere forhold innen kjente eller antatte usikkerhetsområder. Man benytter da dette til en rangering av eksempelvis utvelgelse av scenarioer, der man gjør en bedømmelse av hva som er mulig og gir en relativ rangering. Det samme gjelder for hvilke aktører man bedømmer er mer eller mindre aktuelle, i hvilken grad man mener de kan lykkes, hvor stor skade et angrep kan få, med mer. NSM legger til grunn at man innenfor sikring mot tilsiktede handlinger, med sannsynlighet mener «mulighet for». Dette samsvarer med engelsk der «probability» benyttes om statistisk sannsynlighet, mens «likelihood» kan oversettes til «mulighet for».

Det kan være ulike sannsynlighetsbegreper som benyttes i ulike sammenhenger. I noen sammenhenger har man historiske data med tallmateriale som oppfyller kriteriene for å benytte matematiske metoder. I andre sammenhenger har man ikke tallmateriale i det hele tatt, som grunnlag for vurderingene, og da må man benytte ren bedømmelse. I overgangen mellom statistiske metoder og ren bedømmelse vil det opereres med en blanding av faglige metoder og bedømmelse – det vil si estimert sannsynlighet. Estimert sannsynlighet benyttes typisk der det er noe tallmateriale, men fordi det er begrenset i omfang eller kvalitet, oppfylles ikke kvalitetskravene for å utelukkende benytte statistiske metoder. I de enkelte trinn i en risikovurdering må man velge faglige metoder som er tilpasset det data-/informasjonsgrunnlaget man har.

3 Planlegging og igangsetting

3.1 Risikovurdering som del av sikkerhetsstyringen

NSMs veileder i sikkerhetsstyring beskriver blant annet hvordan virksomheten kan etablere en sikkerhetsorganisasjon, sikre lederforankring og oppfylle kravene om sikkerhetsdokumentasjon.

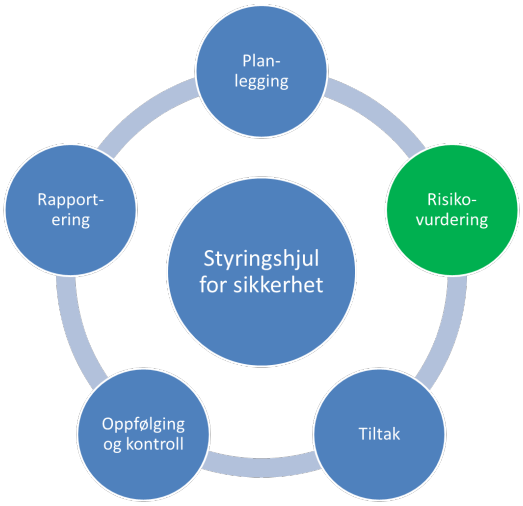
Fra NSMs veileder i sikkerhetsstyring:

3.3.1 Generelt om sikringsrisikovurderinger
Sikringsrisikovurderinger er en viktig del av sikkerhetsstyringsprosessen. Gjennom sikringsrisikovurderinger blir virksomheten klar over hvilke utfordringer man står overfor. Dette bidrar til økt bevissthet om hvilke områder som krever iverksetting av tiltak. Sikringsrisikovurderinger gjennomføres i forlengelsen av planleggingsfasen. Samtidig må det gjennomføres sikringsrisikovurderinger når det skjer endringer som påvirker risikobildet. For eksempel kan endringer i trusselbildet, sårbarheter, verdier, organisering eller virksomhetens overordnede føringer påvirke risikobildet.
Sikringsrisikovurderinger får frem virksomhetens viktigste risikoer innen sikkerhetsområdet, og disse må være styrende for sikkerhetsarbeidet.

Det er virksomhetens leder som formelt bestemmer og fastsetter hvordan sikkerhetsarbeidet skal organiseres og gjennomføres. For å ha et styringssystem som fungerer er det avgjørende at det er forankret hos virksomhetens ledelse. Myndighet kan delegeres, og oppgaver fordeles, men ansvaret vil forbli hos virksomhetens leder.

For å få en effektiv styring av den forebyggende sikkerheten må leder på riktig ansvarsnivå fastsette virksomhetens *risikoaksept*. For å gjøre dette kan man benytte konsekvensskjemaet i denne håndboken, som vil være et grunnlag for en policy om ulike grader av tap[1]. Konsekvensskjemaet i håndboken brukes til å klassifisere konsekvenser som er relevante for virksomheten.

Resultatet fra risikovurderinger er sammen med eksterne krav og interne overordnede føringer premissgivende for sikkerhetsstyringen, og inngår som en viktig del av styringsprosessen. Figuren viser hvordan risikovurdering inngår i styringshjulet for sikkerhet[2]. Virksomheten vil få en mer bevisst og målrettet styring av det forebyggende sikkerhetsarbeidet når det er samspill mellom risikovurderingene og sikkerhetsstyringen.



[1] Dette innebærer å si noe om hva som er ønsket eller akseptabel tilstand for verdiene under og etter en uønsket hendelse.
[2] For mer informasjon om styringshjulet for sikkerhet, se NSMs veileder i sikkerhetsstyring.

Risikovurderinger må gjennomføres og oppdateres med jevne mellomrom. For hver enkelt risikovurdering må det utvikles et overordnet mål, og eventuelle delmål. Dette må forankres hos leder på riktig ansvarsnivå.

3.2 Risikovurdering som en del av prosjektstyring

Risikovurderinger i *store prosjekter* kan skje mer isolert fra den operasjonelle sikkerhetsstyringen i virksomheten. I prosjekter vil vurderingen ofte ha mer preg av utredning som et grunnlag for endringshåndteringen, enn operasjonell styring. Det kan for eksempel gjelde byggeprosjekter, etablering av ny virksomhet, utvikling av informasjonssystemer eller andre større endringer. Merk at slike sikringsrisikovurderinger er noe annet enn risikostyring av prosjekter som sådan (gjennomføringsrisiko).

3.3 Vurderingens omfang

Som en del av planleggingen må det tas stilling til omfang, ressursbruk og tidsbruk for risikovurderingen. Med omfang menes at avgrensninger i analysen skal tydeliggjøres, eksempelvis om det er hele virksomheten, eller en organisasjonsenhet, aktivitet, lokaler eller system som skal risikovurderes. Involverte parter må være omforent om hva det er som skal risikovurderes og hva som er formålet med vurderingen.

3.4 Ledelsens involvering

Ledere på riktig ansvarsnivå må involveres på riktig måte før risikovurderingen starter. Beslutningspunkter og forutsetninger for arbeidet må identifiseres og avklares, herunder organisering, ressursramme, hovedmilepæler og rapportering. Forankring innebærer også at beslutningstaker gjør seg opp en mening om hvilke verdier virksomheten eier og forvalter som er viktigst.

3.5 Dokumentasjon

Vurderinger og resultater fra risikovurderingen skal dokumenteres. Skjemaer og vedlegg som blir fylt ut tjener som dokumentasjon av arbeidet og må arkiveres. I noen tilfeller kan skjemaene brukes som de er, mens de i andre tilfeller bare er en illustrasjon på hva som hører hjemme i det aktuelle trinnet.

Allerede før oppstart av arbeidet må det foretas en vurdering av skjermingsverdien på informasjonen som vil bli utarbeidet. For eksempel vil identifiserte sårbarheter i virksomheten ofte måtte anses som skjermingsverdig eller sensitiv informasjon. Det kan ha betydning for hvilke informasjonssystemer dokumentasjonen kan utarbeides på. Dersom vurderingen er at informasjonen er skjermingsverdig etter sikkerhetsloven, beskyttelsesinstruksen eller sektorregelverk med graderingsbestemmelser, må dokumentene graderes og sikres i samsvar med aktuelle bestemmelser. For dokumenter som er sensitive av andre grunner, f. eks. virksomhetens egne interne behov eller der det ikke finnes graderingsbestemmelser, må virksomheten selv vurdere hva som vil være god nok beskyttelse.

3.6 Kompetanse

Erfaring med metoder for risikovurdering er viktig for en effektiv og god kvalitativ gjennomføring. Dersom virksomheten mangler kompetanse må denne gjøres tilgjengelig, enten ved tilstrekkelig kompetanseheving eller ved innleid assistanse. Ved kjøp av risikovurderingstjenester må virksomheten ha tilstrekkelig bestillerkompetanse for å kunne styre anskaffelsen og selve utredningsarbeidet på en god måte.

Valg av deltakere avhenger av hva som skal risikovurderes. Gruppens sammensetning kan derfor variere i de ulike trinn i prosessen. Det vil være behov for informasjon og kunnskap om verdiene, trusler mot verdiene og verdienes sårbarheter mot truslene. Det er ikke nødvendigvis de samme personene som har relevant informasjon og kunnskap om henholdsvis verdier, trusler og sårbarheter. Det må derfor planlegges med informasjonsinnhenting.

Normalt bør det i en virksomhet være en kjernegruppe med kompetanse i risikometodikk og prosjektledelse som står for prosessledelsen og dokumenterer ulike risikovurderinger. Gruppen bør så suppleres med personell fra ulike fagmiljøer i kjernevirksomheten og støttefunksjonene som har bedre innsikt i leveransene og de ressurser som er relevante for den enkelte risikovurdering.

3.7 Klassifisering av konsekvenser

Før risikovurderingen begynner bør virksomheten ha klassifisert mulige konsekvenser av tapt konfidensialitet, integritet eller tilgjengelighet, som følge av tilsiktede uønskede handlinger.

Konfidensialitet: Beskyttelse mot uvedkommendes tilgang til en verdi.

Integritet: Beskyttelse mot uønsket endring av en verdi.

Tilgjengelighet: Beskyttelse mot uønsket tap, reduksjon eller stans av en verdi.

Det forutsettes at virksomhetens behov og natur ligger til grunn for vurderingene. Resultatet av vurderingene skal brukes når sikringsmål skal bestemmes senere i prosessen.

Skjema A er et eksempel på en visuell fremstilling av disse vurderingene.

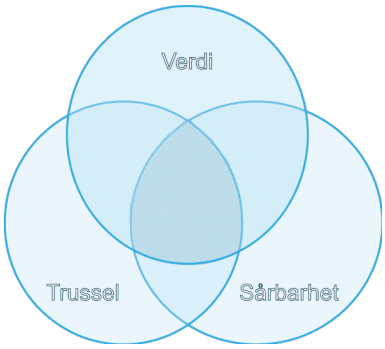
A	Klassifisering av konsekvener					
		Lav	Moderat	Høy	Svært høy	Ikke relevant
Virksomhet	**Liv og helse for eget personell**	*Xx lettere skade på personell.*	*Xx alvorlig skade på personell.*	*xx-xx dødsfall og alvorlig skade på personell.*	*Mer enn xx-xx dødsfall og alvorlig skade på personell.*	
	Liv og helse for andre	*Xx lettere skade på personer.*	*Xx alvorlig skade på personer.*	*xx-xx dødsfall og alvorlig skade på personer.*	*Mer enn xx-xx dødsfall og alvorlig skade på personer.*	
	Omdømme	*Ingen fare for omdømmetap og liten innvirkning på tillit.*	*Omdømme kan skades. Mediedekning begrenset til nasjonal eller regional presse. Kan redusere tillit.*	*Overhengende omdømmerisiko.Internasjonal mediedekning i store aviser.Kan alvorlige redusere tillit.*	*Omdømme vil skades.XX antall internasjonale medieoppslag. Svært alvorlig redusert tillit.*	
	Økonomi	*Over xx kr.*	*Over xx kr.*	*Over xx kr.*	*Over xx kr.*	
	Operativ drift	*Oppgaver eller mål kan fortsatt oppnås, men det må påregnes forsinkelser eller dårligere kvalitet.*	*Utilfredsstillende kvalitet eller store forsinkelser av leveranser eller kun delvis oppfyllelse av forretningsmål.*	*Delvis manglende evne til å levere oppgaver eller nå mål for kjernevirksomheten.*	*Ikke evne til å levere kritiske oppgaver eller nå mål for kjernevirksomheten.*	
Samfunn	**Nasjonal sikkerhet og suverenitet**	*Kan i noen grad medføre skadefølge.*	*Kan skade.*	*Alvorlig kan skade.*	*Helt avgjørende skadefølger.*	
	Klima og miljø	*Xx skade på klima og miljø.*	*Xx skade på klima og miljø.*	*Xx skade på klima og miljø.*	*Xx skade på klima og miljø.*	
	Kritisk infrastruktur og kritiske samfunnsfunksjoner	*Oppgaver eller mål kan fortsatt oppnås, men det må påregnes forsinkelser eller dårligere kvalitet.*	*Utilfredsstillende kvalitet eller store forsinkelser av leveranser eller kun delvis oppfyllelse av forretningsmål.*	*Delvis manglende evne til å levere oppgaver eller nå mål for kjernevirksomheten.*	*Ikke evne til å levere kritiske oppgaver eller nå mål for kjernevirksomheten.*	

4 Gjennomføring av risikovurderinger

4.1 Oversikt over hovedfaktorene for risiko

Sikkerhet bygger på at du har noe av verdi som må beskyttes. Det er ikke mulig å beskytte alt like godt, og prioritering er nødvendig. Ikke alle typer hendelser eller trusler er like aktuelle eller relevante. Derfor er en risikovurdering som tar utgangspunkt i verdiene et godt verktøy for sikkerhetsstyring.

Når *verdiene* er kategorisert, er det nødvendig å vurdere *truslene* mot verdiene, og *sårbarhetene* mot truslene. Trusler omfatter ulike former for kriminalitet, herunder (informasjons)tyveri og skadeverk – i sin ytterste konsekvens spionasje, sabotasje, terrorhandlinger og organisert kriminalitet. Sårbarheter er ofte er resultat av mangelfull eller uhensiktsmessig sikring av verdier. Virksomhetene kan i liten grad selv påvirke truslene, og har størst påvirkning på egen risiko ved å redusere sårbarhetene.



Det innbyrdes styrkeforholdet mellom verdier, trusler og sårbarheter brukes for å beskrive den aktuelle risikoen. I figuren er risiko representert ved det skraverte området.

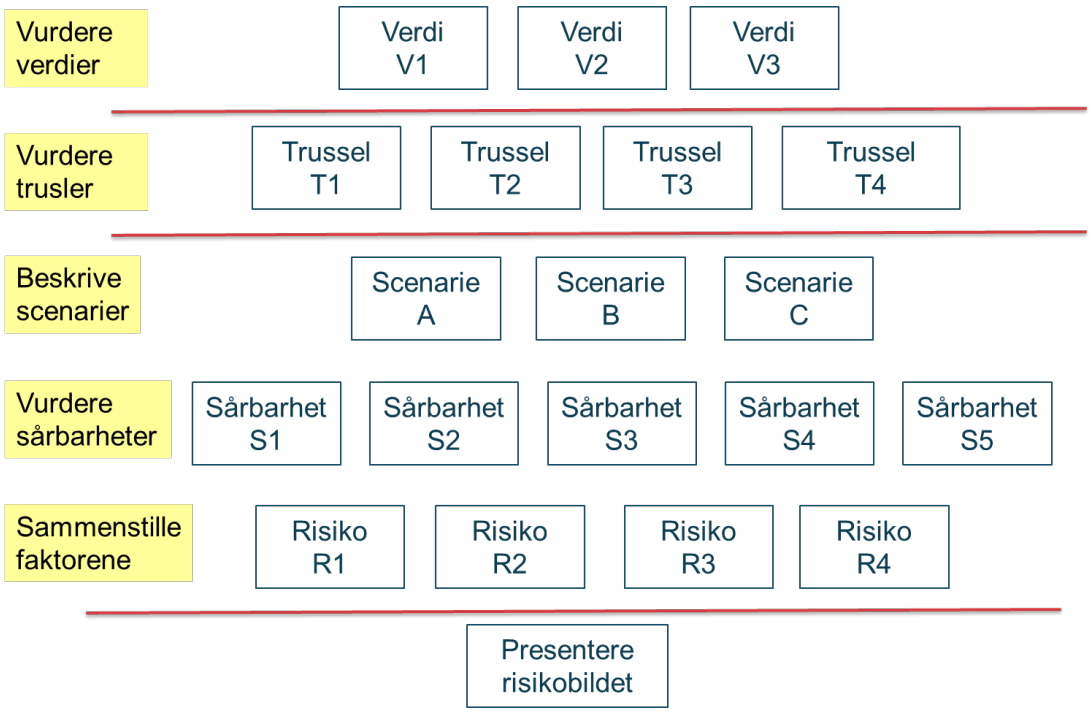
4.2 Oversikt over prosessen

Virksomheten skal identifisere og rangere verdier, fastsette sikringsmål, gjennomføre en trusselvurdering, utvikle scenarioer, kartlegge allerede innførte sikringstiltak og gjennomføre en sårbarhetsvurdering. Når alle skjemaene er fylt ut sammenstilles faktorene verdi, trussel og sårbarhet, og sammenfattes så til et helhetlig risikobilde.

Denne prosessen er delt i trinn og til hvert trinn er det utviklet skjemaer, og i noen tilfeller også kontrollspørsmål og sjekklister.

Rekkefølgen på skjemaene er ment å være til hjelp for en strukturert fremgangsmåte. Brukerne kan ved behov tilpasse de enkelte skjemaene, kontrollspørsmålene og sjekklistene til sin virksomhet.

Figuren nedenfor viser hvordan faktorene i prosessen henger sammen. Det er ikke tegnet inn tråder mellom de enkelte boksene i figuren fordi det ikke nødvendigvis er et en-til-en forhold mellom boksene. For eksempel kan én og samme trussel være relevant for flere verdier, og flere trusler kan være relevant for én og samme verdi. Også forholdet mellom sårbarheter og scenarioer kan være slik.



En risiko kan presenteres slik: *«Risiko 1 er at verdi V1 kan rammes ved at trusselaktør T3 utnytter sårbarhet S1 og S5. Denne risikoen betegnes som R1 og er på nivå MODERAT»*.

4.3 Verdivurdering

4.3.1 Formål

Verdivurderingen er en kartlegging av virksomhetens verdier. Formålet med vurderingen er å identifisere hvilke verdier som er de viktigste for virksomhetens oppdrag og leveranser. Virksomheten skal utføre verdivurderingen på en systematisk måte ved å vurdere hvilke konsekvenser det kan få dersom verdiene skulle rammes. Disse verdiene kan være av materiell eller ikke-materiell art.

Det er ikke alle verdier en virksomhet besitter som det bare er opp til virksomheten å avgjøre om skal beskyttes. Også verdier som må sikres pga. f. eks. offentlige krav, avtaler med andre eller symbolverdier som kan være attraktive terrormål, må derfor identifiseres. Virksomheter som har informasjon eller objekter som f. eks. er skjermingsverdige etter sikkerhetsloven eller sektorregelverk, er pliktig å sikre informasjonen og objektene i samsvar med reglene. Ofte vil slik informasjon være gradert av og mottatt fra andre virksomheter, mens objekter vil være klassifisert av myndighetene på området. Slike verdier skal sikres i samsvar med offentlige krav.

Verdivurderingen er en viktig bevisstgjøringsprosess om hvilke verdier virksomheten besitter som kan være eller bli et mål for en potensiell trusselaktør.

Leveransene skapes gjennom virksomhetens verdiskapende prosesser og aktiva. Disse prosessene er avhengig av ulike ressurser (innsatsfaktorer) for å virke. Det er ressursene* som i denne sammenheng utgjør verdiene og som er gjenstand for sikringstiltak.

4.3.2 Hovedelementer i en verdivurdering

Hvis risikovurderingens omfang er omfattende som for eksempel en hel virksomhet, vil det første steget i verdivurderingen være å bryte ned virksomheten i mindre deler som avdelinger eller prosesser. Verdivurderingen må ferdigstilles før gruppen starter med scenarioutvikling, sårbarhetsvurdering og risikovurdering.

4.3.3 Gjennomføring

Verdivurderingen kan gjøres på flere måter. NSM anbefaler her å gå frem slik :

Trinn	Aktiviteter	Skjema
1	Avgrens oppdraget eller leveransen som skal vurderes og de verdikjedene som inngår.	**B**
2	Identifiser prosessene som er nødvendige for oppdraget eller leveransen. Vurder konsekvens ved bortfall av disse prosessene.	**B**
3	Identifiser ressursene* (innsatsfaktorer) som understøtter prosessene, og derved leveransene.	**B**
4	Sammenfatt identifiserte ressurser i en samlet liste	**C**
5	Klassifiser verdiene slik som skjema viser. Begrunn klassifiseringen ved hjelp av konsekvensskjema (A), og på en slik måte at det er mulig for andre å forstå grunnlaget for vurderingene og en senere revidering blir enklere.	**C**

*) Ressurser kan være Informasjon, utstyr, programvare, nettverk, objekter, personell og organisasjonsstrukturer. Disse kan igjen være avhengig av vann, strøm eller tele-kommunikasjon for å virke. Noen av ressursene er avhengigheter som virksomheten ikke selv har direkte kontroll over, som f. eks. kjøpte tjenester. Også slike ressurser må tas med i vurderingen. Enkelte ressurser kan understøtte flere prosesser (typisk IKT-systemer).

Skjema B under kan benyttes til å dokumentere trinn 1 til 3 i verdivurderingen:

B	Identifisere verdier			
Leveranser (kapasiteter, tjenester, varer)	**Prosesser** som styrer leveransene	**Verdier** som inngår i prosessene	**Verdiansvarlig** (den som har daglig ansvar for verdiene)	**Lokalisering** (hvor befinner verdiene seg)

Skjema C under kan benyttes til å dokumentere trinn 4 og 5 i verdivurderingen:

C	Klassifisere verdier				
nr	**Verdi beskrivelse**	**Klassifisering**			
		Lav	Moderat	Høy	Svært høy
Verdi 1					
Verdi 2					
Verdi 3					
Verdi 4					
Ta utgangspunkt i konsekvens for virksomheten ved tap av Konfidensialitet, Integritert eller Tilgjengelighet					

4.4 Fastsettelse av sikringsmål

4.4.1 Formål

I trinnet om fastsettelse av sikringsmål skal virksomheten bestemme hva de aksepterer av skade og bortfall av kritiske verdier. Vurderingen gjøres på grunnlag av den klassifiseringen av konsekvenser som er gjort tidligere. Hvilke sikringsmål virksomheten setter vil ha betydning for hvor mye ressurser som må settes av for å beskytte virksomhetens kritiske verdier.

Sikringsmålene som settes i dette trinnet er bare et utgangspunkt som skal revideres senere i prosessen. Det er nemlig først etter at resultatet av risikovurderingen er klart, at en kost-nytte vurdering av mulige konkrete sikringstiltak kan foretas. En slik kost-nytte vurdering har betydning for strategien som velges for å håndtere risikoen, herunder akseptering av risiko. Prosessen med revidering av sikringsmålene omhandles imidlertid ikke av denne håndboken, da det skjer etter at sikringsrisikovurderingen er gjort (er en del av tiltaksvurderingen).

4.4.2 Gjennomføring

Fastsettelse av sikringsmål kan gjøres på flere måter. NSM anbefaler her følgende fremgangsmåte:

Trinn	Aktiviteter	Skjema
1	Vurder sikringsmål for hver av verdiene som er dokumentert i forrige trinn, for å komme frem til et forslag. Forklar vurderingen.	**C + A**
2	Før forslaget til sikringsmål opp i skjemaet.	**D**
3	Gjennomgå utfylt skjema med ansvarlig leder og få aksept for konklusjonene.	**D**

Sikringsmål kan være negativt eller positivt formulert. Et eksempel er «bortfall av produksjonssystem X skal *ikke* overstige 15 minutter i døgnet». Et annet eksempel er «ved en hendelse som kan true sikkerheten i IKT-system Y skal responstiden være under 1 time».

Skjema D under kan benyttes til å dokumentere fastsettelsen av sikringsmål:

D	Sikringsmål for hver enkelt verdi	
Verdi nr.	**Verdi**	**Virksomhetens sikringsmål for den aktuelle verdi:**
Verdi 1		
Verdi 2		
Verdi 3		
Verdi 4		
Verdi 5		
Gjennomgått med leder navn / dato		

4.5 Trusselvurdering

4.5.1 Formål

Trusselvurderingen beskriver det gjeldende trusselbildet for det som ønskes beskyttet, og gir en vurdering av hvordan trusselbildet kan utvikle seg. Hovedfokuset er på reelle og potensielle trusselaktørers intensjon om og kapasitet til å ramme virksomheten.

4.5.2 Trusselkategorier

NSM anbefaler å dele truslene opp i kategoriene spionasje, sabotasje, terrorhandlinger og annen alvorlig kriminalitet.

Spionasje[3] er målrettet informasjonstyveri ved bruk av fordekte metoder. Tyveriet kan skje ved fysisk eller menneskebasert innhenting, ved å utnytte IKT-systemer, eller en kombinasjon av disse. Fysisk innhenting kan skje ved å skaffe seg direkte adgang til dokumenter og lagringsmedier. Menneskebasert innhenting består ofte av sosial manipulasjon, bruk av innsidere i virksomheter eller plassering av personer utenfra i virksomheten (infiltrasjon). Infiltrering av IKT-systemer omtales gjerne som hacking, datainnbrudd, digital spionasje eller cyberspionasje. Spionasje kan også benyttes til å planlegge sabotasje, terrorhandlinger eller annen alvorlig kriminalitet.

Sabotasje[4] er målrettet skade på store datamengder eller infrastruktur, herunder lokaler og informasjonssystemer. Sabotasje rammer tilgjengelighet og integritet til informasjon og infrastruktur.

Terrorhandlinger[5] omfatter å sette menneskers liv eller helse i fare, ødeleggelse av eller alvorlig skade på eiendom, å forstyrre prosesser eller systemer som opprettholder et demokratisk styre eller samfunnets økonomiske velferd og virkemåte.

Også annen alvorlig kriminalitet er ofte relevante trusler. Med alvorlig kriminalitet menes straffbare handlinger med alvorlige konsekvenser for personer, virksomheten eller samfunnet. Denne kategorien kan igjen deles opp i underkategorier av ulike typer handlinger, som f. eks. vold, skadeverk, frihetsberøvelse og ulike typer vinningskriminalitet. En annen måte å kategorisere på er å skille mellom organisert kriminalitet og «alminnelig» kriminalitet, der førstnevnte anses som mest alvorlig. Virksomheten bør vurdere hvilke underkategorier som er mest relevante for sine verdier og sin situasjon.

[3] Spionasje er i sikkerhetsloven § 3 definert som innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt.
[4] Sabotasje er i sikkerhetsloven § 3 definert som tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg eller aktivitet, eller tilsiktet uskadeliggjøring av personer, utført av eller for en fremmed stat, organisasjon eller gruppering
[5] Terrorhandlinger er i sikkerhetsloven § 3 definert som ulovlig bruk av, eller trusler om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål.

Til støtte ved vurdering av trusselaktørers intensjon og kapasitet anbefaler NSM bruk av trusselmatrise som et verktøy for å kunne klassifisere trusselen. Under er en forenklet matrise med fire klassifiseringsnivåer, A til D. Matrisen må passe for virksomheten.

E1	Matrise for virksomhetens vurdering av trussel - Intensjon			
	Trusselnivå			
	A1	B1	C1	D1
Intensjon	Enkeltpersoners personlige motiv, ideologisk eller kommersiell.	Del av gruppering med felles mål, ideologisk eller kommersiell.	Del av internasjonalt nettverk med overordnet målsetting, ideologisk eller kommersiell.	Svært målrettet og systematisk organisasjon, kan være tilknyttet andre stater. Utenrikspolitiske mål.
			Målrettet angrep for å ramme sentral utvalgt virksomhet.	Målet er å skade vitale nasjonale interesser.
	Kan være hevnmotiv eller leilighetshandling	Planlagt handling. Mer tilfeldig hvem som blir offer.	Planlagt handling. Planlagt offer	Planlagt handling.Planlagt offer
	Målet søkes nådd gjennom :	Målet søkes nådd gjennom	Målet søkes nådd gjennom :	Målet søkes nådd gjennom :
	• Spionasje mot offentlig eller privat aktør, informasjonstyveri	• Spionasje mot offentlig eller privat aktør, informasjonstyveri	• Spionasje mot offentlig eller privat aktør, informasjonstyveri	• Spionasje mot offentlig aktør, informasjonstyveri
	• Sabotasje mot nettverk, nettside, samfunnsfunksjon, for eksempel ta ned nettsteder	• Sabotasje mot kritisk infrastruktur	• Sabotasje mot kritisk infrastruktur	• Sabotasje mot kritisk infrastruktur, logisk eller fysisk
	• Terrorhandling mot person eller virksomhet	• Terrorhandling mot person eller virksomhet	• Terrorhandling mot symbolmål	• Terrorhandling mot symbolmål eller kritisk infrastruktur.
			• Systematisk påvirkning av nyhetsbildet for å fremme egen sak	• Systematisk påvirkning av nyhetsbildet og myndigheter for å fremme egen sak

E2	Matrise for virksomhetens vurdering av trussel - Kapasitet			
	Trusselnivå			
	A2	B2	C2	D2
Kapasitet	Oftest enkeltpersoner med lite ressurser	Grupper med begrensete ressurser	Grupperinger med mye ressurser	Godt organiserte grupperinger med store ressurser, statlig aktører.
	Liten kompetanse, enkle og tilgjengelige metoder og verktøy,liten utholdenhet, kort horisont	God kompetanse hos flere enkeltpersoner,enkle og tilgjengelige metoder og verktøy, noe utholdenhet	God kompetanse hos flere,avanserte metoder og verktøy,	Godt trente grupper med evne til å utnytte avanserte metoder og verktøy.Kapasitet til systematisk arbeid over lang tid.
				Kapasitet til systematisk arbeid over lang tid.
			Grundig planlegging og god utholdenhet.	Egne eller andre aktører vil ha kartlagt mål på forhånd. Bruk av innsidere sannsynlig.
				Sammensatte operasjoner
	Potensial for liten / kortvarig skade som følge av	Potensial for betydelig skade som følge av	Potensial for alvorlig skade som følge av	Potensial for svært alvorlig skade som følge av
	Spionasje	Spionasje	Spionasje	Spionasje
	Sabotasje	Sabotasje	Sabotasje	Sabotasje
	Terrorhandling	Terrorhandling	Terrorhandling	Terrorhandling

Hvis det i risikovurderingen også skal inkluderes *utilsiktede uønskede hendelser* (ofte kalt farer), som for eksempel naturkatastrofer og ulykker, kan virksomheten lage en matrise for det også. Da er imidlertid inndelingen i intensjon og kapasitet ikke relevant.

Mulige kilder til innhenting av informasjon om trusselbildet	
• Offentlige myndigheters publikasjoner om trusler og utviklingstrekk • Relevante bransjeorganisasjoners publikasjoner om trusler og utviklingstrekk • Internasjonale organisasjoners publikasjoner om trusler og utviklingstrekk (NATO, EU, sektorspesifikke organisasjoner, med mer) • Store konsulentselskapers og sikkerhetsleverandørers offentliggjorte publikasjoner om trusler og utviklingstrekk • Politidistriktet for området • Sikkerhetsorganisasjonen i virksomheter i samme etat eller bransje • Sikkerhetsorganisasjonen i virksomheter i samme geografiske område (nabovirksomheter) • Virksomhetens registre over interne sikkerhetsbrudd og sikkerhetstruende hendelser	• Politiets sikkerhetstjeneste (PST) (www.pst.politiet.no) • Lokalt politidistrikt (www.politiet.no) • Nasjonal sikkerhetsmyndighet (NSM) (www.nsm.stat.no) • Kripos (www.politiet.no/kripos) • Direktoratet for samfunnssikkerhet og beredskap (DSB) (www.dsb.no) • Norsk senter for informasjonssikring (NorSIS) (www.norsis.no) • Næringslivets sikkerhetsråd (NSR) (www.nsr-org.no)

For å utarbeide en trusselvurdering bør det innhentes informasjon fra flere kilder (se tekst-boks). En flerkildeanalyse gir et bedre informasjonsgrunnlag enn om analysen bare baseres på én kilde. Det er også viktig å reflektere over kildens og informasjonens troverdighet.

4.5.3 Gjennomføring

Trusselvurdering kan gjøres på flere måter. NSM anbefaler følgende fremgangsmåte:

Trinn	Aktiviteter	Skjema
1	Innhent informasjon om trusselbildet ved å bruke ulike kilder. Vurder kildens og informasjonens troverdighet.	-
2	Identifiser relevante trusselaktører som kan tenkes å true virksomhetens verdier og kategoriser disse.	F del 1
3	Vurder relevante trusselaktørers intensjon og kapasitet til å ramme virksomheten og verdiene.	F del 1
4	Fastsett trusselnivået for hver trusselaktør, basert på en vurdering av intensjon og kapasitet.	F del 2
5	Begrunn valg av trusselaktører og fastsettelse av trusselnivå.	F del 2
6	Kommenter usikkerhet i vurderingen.	F del 1 og 2

Skjema F under kan benyttes for å dokumentere resultatet av trusselvurderingen:

F		**Identifisere og klassifisere trusselaktører**						
nr	**i) Trusselkategori** **ii) Farekategori** (utilsiktet uønsket hendelse)	**Intensjon** (kun security)	**Kapasitet** (kun security)	**i) Trusselnivå** (security) **ii) Farenivå** (safety) Lav	Moderat	Høy	Svært høy	**Begrunnelse og beskriv usikkerhet**
Trussel 1								
Trussel 2								
Trussel 3								
Trusselkategorier er terror, spionasje, sabotasje og annen alvorlig kriminalitet								

4.6 Identifisering og valg av scenarioer

4.6.1 Formål

Hensikten med å benytte scenarioer er å få frem sårbarheter som er relevante for analysen.

Verdivurderingene og trusselvurderingene er grunnlaget for å utarbeide scenarioer. Scenarioene beskriver hvordan trusselaktører kan gå fram for å skade verdiene, og som er relevante for videre analyse. En god scenariobeskrivelse forenkler sårbarhetsvurderingen og gjør det enklere for beslutningstakere å følge resonnementene.

4.6.2 Gjennomføring

Her er en sjekkliste for hva som bør tas med i en scenariobeskrivelse:

- Hendelsesforløpet: Hva som inntreffer, når det inntreffer, hvor det inntreffer, hvordan det inntreffer.
- Trusselaktørens intensjon og kapasitet (og eventuelt farer som ekstremvær, ulykker og teknisk eller menneskelig svikt).
- Hvordan verdiene rammes (f.eks. datainnbrudd, utilgjengelighet til data, korrupte data, bilbombe, avlytting, tyveri, osv.).
- Andre verdier som rammes indirekte (f.eks. liv og helse, miljø, økonomi eller omdømme).
- Mulig varsling av hendelsen i forkant (f. eks. fra etterretning, politiet utpressere eller terrororganisasjon).
- Tidspunktet når trusselen rammer (f.eks. tidspunkt på døgnet eller året, under et arrangement, osv.)
- Hendelsens varighet.

Forslag til hvordan scenariobeskrivelsene utarbeides:

Trinn	Aktiviteter	Skjema
1	Velg de mest relevante trusselaktørene fra trusselvurderingen. Begrunn hva som tas med og hva som ikke tas med.	**G**
2	Sett fra en potensiell trusselaktørs ståsted, hvilke verdier kan være attraktive? Tenk hvordan trusselaktøren kan skade verdiene. På grunnlag av dette utarbeides scenarioer.	**G**
3	Bruk det antall skjemaer som trengs – ett skjema for hvert scenario.	**G**
4	Scenarioene samles i skjemaet «liste over scenarioer» for oversikt.	**H**

Skjema G kan benyttes til å beskrive hvert enkelt scenario.

G	Beskrivelse av ett scenario		
Scenario nummer:	**Berørte verdier:**	**i) Trusselkategori (security)** **ii) Farekategori (safety)** Eksempel: innbrudd (security) og brann (safety)	**Trusselaktør:**
Scenariotittel:			
Scenariobeskrivelse:	Hva, når, hvordan,trusselaktør, konsekvens, varsling, varighet, kostnad		

Skjema H kan benyttes til å lage en oversikt over scenarioene.

H nr	**Scenariotittel** tittel, beskrivelse
Scenarie 1	
Scenarie 2	
Scenarie 3	
Scenarie 4	
Scenarie 5	

4.7 Sårbarhetsvurdering

4.7.1 Formål

Sårbarhet er manglende evne til å motstå en uønsket hendelse eller å opprette en ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning, jf. NS 5830. Sårbarhetsvurderingen skal vise eventuelle gap mellom innførte sikringstiltak og en trusselaktørs intensjon og kapasitet.

4.7.2 Gjennomføring

For å vurdere sårbarhet i en risikovurdering kan vi for hvert scenario se på eksisterende sikringstiltak, hvor godt de virker, og om de er dekkende. For utviklingsprosjekter, der det ikke finnes eksisterende forhold å vurdere, vil vurderingen fokusere på ønsket motstandsdyktighet mot scenarioene (sikringsnivået for å unngå fremtidig uakseptabel sårbarhet).

Sårbarheter (og sikringstiltak) kan inndeles i tre hovedkategorier:

- Organisatoriske (sikkerhetsstyring – av menneskelige og teknologiske tiltak)
- Menneskelige (personellsikkerhet)
- Teknologiske (IKT-sikkerhet og fysisk sikkerhet)

I det følgende er det gitt en rekke eksempler på sårbarheter som kan være aktuelle for hele eller deler av virksomheten.

4.7.3 Organisatoriske sårbarheter

Noen eksempler på organisatoriske sårbarheter:

- Virksomheten setter ikke av nødvendige ressurser til sikkerhet.
- Utydelige ansvars- og rapporteringslinjer for sikkerhetssaker.
- Ledere måles ikke på hvor godt de ivaretar sikkerheten.
- Mangelfulle (relevante) måleparametere for sikkerhet.
- Mangelfull oversikt over kompetansebehov innen sikkerhet.
- Mangelfulle krav til sikkerhetskompetanse.
- Mangelfull styring eller oppdatering av logiske og fysiske tilganger.
- Mangelfullt register over sikkerhetstruende hendelser.
- Manglende beredskapsplan for håndtering av sikkerhetshendelser.
- Manglende øving av beredskapsplaner.
- Manglende rutiner for sikkerhetsoppdatering av programvare.
- Kritiske komponenter eller funksjoner er avhengige av én ressurs med potensial for feil (innsatsfaktorer, personell eller leverandører).
- Manglende bestillerkompetanse innen sikkerhet i tekniske løsninger.
- Manglende system for avviks- og hendelseshåndtering.
- Mangelfull internrevisjon av sikkerheten.
- Mangelfull evaluering av sikkerhetstilstanden i virksomheten.

4.7.4 Menneskelige sårbarheter

Noen eksempler på menneskelige sårbarheter:

- Utvisking av hva som er jobb og hva som er privat.
- Manglende retningslinjer for bruk av sosiale medier.
- Svake kontrollrutiner som tillater en medarbeider å gjøre stor skade uoppdaget.
- Bruk av privat utstyr i virksomhetens nettverk.
- Svak forståelse blant medarbeiderne om hvorfor sikkerhet er viktig for virksomheten.
- Linjelederes manglende motivering av medarbeidere om viktigheten av sikkerhet.
- Manglende kunnskap om hvordan den enkelte kan bidra til god sikkerhet.
- Manglende melding om avvik innen sikkerhet.

4.7.5 Teknologiske sårbarheter – IKT

Noen eksempler på IKT-sårbarheter:

- Manglende tilgangskontroll i systemer.
- Manglende oppgradering av program- og maskinvare.
- Manglende installasjon av sikkerhetsoppdateringer.
- Manglende registrering av datatrafikk og tiltak for å oppdage illegitime brukere.
- Sluttbrukere er tildelt administratorrettigheter.
- Brukere kan kjøre programvare som ikke er godkjent av virksomheten.
- Manglende herding av applikasjoner.
- Manglende bruk av klientbrannmurer.
- Manglende eller feil bruk av diskkryptering.
- Manglende oversikt over eget nettverk og egne systemer.
- Manglende bruk av sikkerhetssystemer og sikkerhetsprogrammer.
- Manglende evne til å oppdage uønsket aktivitet i nettverk.

4.7.6 Teknologiske sårbarheter – fysisk

Noen eksempler på fysiske sårbarheter:

- Manglende sikkerhetssoner og bygningsmessige skiller mellom disse.
- Rom for kritiske funksjoner er plassert i sone med for lavt sikringsnivå.
- Manglende sikring i bygningsskallet, dører, vinduer og låser mot innbrudd.
- Manglende inndragning av adgangskort til personell som ikke lenger skal ha adgang.
- Manglende bruk av kjøretøysperrer, vindussikring og bærende konstruksjoner mot virkningen av eksplosjoner.
- Manglende bruk av alarmsensorer og fjernsynsovervåking for avdekking av innbrudd.
- For lang reaksjonstid ved innbrudd og andre fysiske anslag.

Forslag til fremgangsmåte for vurdering av sårbarhet:

Trinn	Aktiviteter	Skjema
1	Beskriv de ulike sårbarhetene for ett scenario om gangen. Vurder hvor godt eventuelle sikringstiltak virker og om de er dekkende for scenarioet.	**I**
2	Klassifiser hver sårbarhet.	**I**
3	Vurder samlet sårbarhet for scenarioet.	**I**
4	Gå til neste scenario og gjenta trinn 1-3 for scenarioet.	
5	Beskriv usikkerhet i vurderingen.	**I**
6	Når alle scenarioene er vurdert, lag en liste over de viktigste sårbarhetene. Påfør referanse til hvilket scenario den enkelte sårbarhet er vurdert utfra.	**J**

Skjema I kan benyttes til å beskrive sårbarhetene ved hvert enkelt scenario (ett skjema for hvert scenario).

I	Identifisere sårbarheter for ett scenario				
Identifiser sårbarheter		**Klassifisering av sårbarheter**			
Scenario nr :					
Beskrivelse av sårbarheter for dette scenariet		Lav	Moderat	Høy	Svært høy
Menneskelige sårbarheter					
Teknologiske sårbarheter IKT					
Teknologiske sårbarheter fysisk					
Organisatoriske sårbarheter					
Samlet vurdering av sårbarhet for dette scenariet :		Lav	Moderat	Høy	Svært høy
Beskriv usikkerhet.					

Lav	Det finnes flere og gode overlappende sikringstiltak som beskytter verdiene.
Moderat	Det eksisterer sikringstiltak som beskytter verdien, men de er mangelfulle.
Høy	Det eksisterer få eller ingen sikringstiltak som beskytter verdien og / eller sikringstiltakene er mangelfulle.
Svært høy	Det eksisterer ingen sikringstiltak som beskytter verdien og/eller sikringstiltakene er svært mangelfulle.

Skjema J kan benyttes til å lage en liste over alle sårbarheter med klassifisering.

J	Oversikt alle sårbarheter for risikovurderingen				
		Klassifisering av sårbarheter			
Nr	**Betegnelse på sårbarhet**	**Lav**	**Moderat**	**Høy**	**Svært høy**
Sårbarhet 1					
Sårbarhet 2					
Sårbarhet 3					
Sårbarhet 4					
Sårbarhet 5					
Sårbarhet 6					
Sårbarhet 7					
Sårbarhet 8					
Sårbarhet 9					

4.8 Sammenstilling av faktorene

4.8.1 Formål

I dette trinnet sammenstiller virksomheten resultatene fra verdivurderingen, trusselvurderingen og sårbarhetsvurderingen. Hensikten er å beskrive hver enkelt risiko som virksomheten er eksponert for og klassifisere disse.

4.8.2 Gjennomføring

Risiko beskrives med utgangspunkt i et scenario med tilhørende sårbarheter: *«Risiko 1 er at verdi V1 kan rammes ved at trusselaktør T3 utnytter sårbarhet S1 og S5. Denne risikoen betegnes som R1 og er på nivå MODERAT»*.

For å komme frem til risikonivået for den enkelte risiko må det gjøres en bedømmelse. Hvilke faktorer som er dimensjonerende for virksomheten må tas hensyn til i bedømmelsen.

Følgende fremgangsmåte kan brukes for å få frem en beskrivelse av hver enkelt risiko og bestemme risikonivå.

Trinn	Aktiviteter	Skjema
1	Hent og sammenstill resultater fra verdivurderingen, trusselvurderingen og sårbarhetsvurderingen.	-
2	Basert på scenarier og sårbarheter, formuler hver enkelt risiko	**K**
3	Bestem risikonivå basert på klassifisering av verdi, trussel og sårbarhet som inngår i beskrivelsen av den aktuelle risiko.	**K**
4	Begrunn valgt risikonivå for hver risiko, herunder hvordan usikkerhet ved de enkelte faktorene er vurdert.	**K**

Skjema K kan benyttes til å beskrive hver risiko:

K	**Beskrivelse av en enkelt risiko**				
Risikonavn :					
	Verdi	**Trussel**	**Sårbarhet**		**Risikonivå**
Risikobeskrivelse :					
Begrunnelse for risikonivå og vekting av vurderingene. Beskriv usikkerhet.					

4.9 Beskrivelse av risikobildet

4.9.1 Formål

Hensikten er at beslutningstakere skal forstå hvilken risiko virksomheten er eksponert for, og deretter velge riktig strategi for håndtering av hver risiko og deretter utforme de mest effektive tiltak, som vil inngå i styringssystem for sikkerhet.

4.9.2 Gjennomføring

Presentasjon av risiko bør bestå av en visuell fremstilling som gir oversikt, supplert av en rapport som viser forutsetninger og detaljerte vurderinger av hver enkelt risiko.

Den visuelle fremstillingen kan gjøres på mange måter, ved hjelp av ulike diagrammer, figurer eller prosatekst. Det kan være hensiktsmessig at fremstillingen tilpasses til den måten beslutningstakere ellers er vant til å få presentert risikobildet på, f. eks. i den operasjonelle risikostyringen.

Rapporten som dokumentasjon er viktig for at vurderingen skal kunne etterprøves, oppdateres eller videreutvikles. Resultatene av denne vurderingen blir grunnlag for neste trinn.

Vedlegg 1 gir et eksempel på hvordan en slik rapport kan utformes.

Tabellen viser et forslag til hvordan risikobildet utarbeides.

Trinn	Aktiviteter	Skjema
1	Finn frem dokumentasjon for hver risiko slik de er dokumentert i de foregående trinn. Gjør eventuelle justeringer utfra en mer overordnet vurdering.	B-K
2	Sorter risikoene etter risikonivå (rangering) for å kunne presentere risikoene for beslutningstaker og andre.	L
3	Lag en samlet dokumentasjon av prosessen, og hver enkelt risiko gjennom de faktorer som inngår. Vedlegg 1 er et forslag til en slik rapport.	

Skjema L viser en måte å visuelt fremstille det samlede risikobildet på.

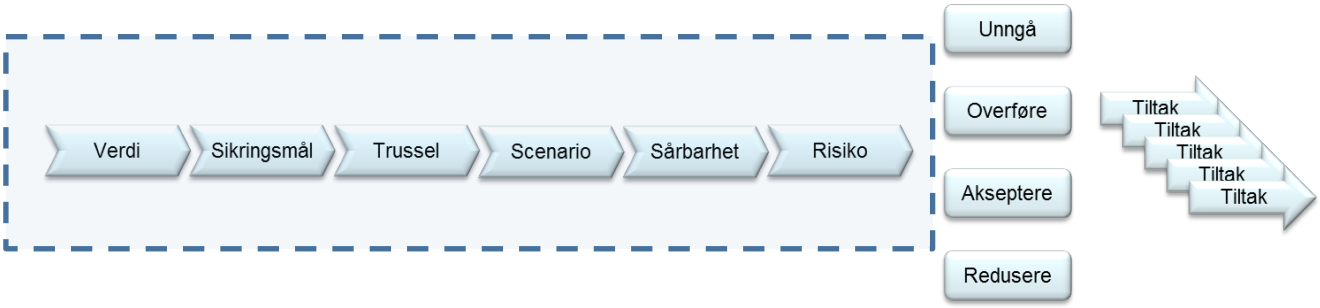
L	Risiko rangering
	Risiko tittel og evt stikkord
Svært høy	Risiko 4 tittel …
Høy	Risiko 1 tittel
Høy	Risiko 3 tittel
Moderat	Risiko 6 tittel
Lav	Risiko 2 tittel
Lav	Risiko 5 tittel
Lav	Risiko 7 tittel

5 Håndtering av risiko

Denne håndboken dekker sikringsrisikovurderingen. Det gis derfor her bare en kort introduksjon til håndtering av risiko.

Når risikoer er identifisert og vurdert må beslutningstaker velge strategi for håndtering av risikoene. Det finnes ulike strategier for håndtering av risiko; *unngå, overføre, akseptere* eller *redusere* risiko. Virksomheten står sjelden helt fritt til å velge strategi. Handlingsrommet avhenger av bl.a. legale, økonomiske og praktiske rammer. Det må avklares hvilket beslutningsnivå som er det riktige for valg av strategi og for hvilken risiko som aksepteres.

Dersom strategien for håndtering av en risiko er at risikoen skal *reduseres*, må det fastsettes og iverksettes *sikringstiltak*. Det finnes ulike typer publikasjoner som beskriver sikringstiltak av organisatorisk, menneskelig og teknologisk art. NSM har utgitt flere veiledere, håndbøker og lignende som kan brukes for å komme frem til hensiktsmessige tiltak. Også andre etablerte standarder om sikkerhet angir en del tiltak som bør vurderes. Innen informasjonssikkerhet er ISO 27001 Annex A og ISO 27002 mye brukt i så henseende. Hensikten er å komme frem til tiltak som er formålstjenlige og relevante for å redusere den aktuelle risikoen tilstrekkelig.



Denne veilederen dekker de første seks fasene (verdi til risiko).

Mange risikoreduserende tiltak er krevende å gjennomføre slik at de fører til ønsket effekt. Det er viktig at disse tiltakene inngår i styringssystemet slik at de følges opp over tid og sees i sammenheng med andre tiltak.

6 Definisjoner

I denne håndboken benyttes følgende definisjoner:

Begrep	Kilde	Definisjon
Sikkerhet	NS 5830	reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare
Sikring	NS 5830	bruk av sikringstiltak ved håndtering av risiko forbundet med tilsiktede uønskede handlinger
Risiko	NS 5830	uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen
Risikovurdering	NS 5830	helhetsvurdering basert på verdivurdering (eller konsekvensvurdering), trusselvurdering og sårbarhetsvurdering med mål om å angi en entitets risiko i en definert sikringsmessig kontekst
Verdi	NS 5830	ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen
Trussel	NS 5830	mulig uønsket handling som kan gi negativ konsekvens for en entitets sikkerhet
Intensjon	NS 5830	vilje og hensikt til å utføre en handling
Kapasitet	NS 5830	evne, herunder ressurser, kunnskap og ferdighet, til å utføre en handling
Sårbarhet	NS 5830	manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning
Menneskelige sikringstiltak	NS 5830	tiltak som påvirker persepsjon, vurderingsevne, kunnskap, adferd og reell evne til å bruke teknologiske sikringstiltak og følge organisatoriske sikringstiltak
Organisatoriske sikringstiltak	NS 5830	tiltak i form av skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, rutiner, adferd og/eller anvendelse av andre sikringstiltak
Teknologiske sikringstiltak	NS 5830	fysisk, elektronisk eller logisk sikringstiltak

7 Referanseliste

Nasjonal sikkerhetsmyndighet (NSM) Veileder i sikkerhetsstyring. (2015)
Nasjonal sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste Veileder i terrorsikring. (2015)
Direktoratet for sikkerhet og beredskap (DSB) Veileder for Fylkesros (2014) Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen (2014) Nasjonalt risikobilde (2014)
Direktoratet for økonomistyring (DFØ) Veileder i internkontroll Kort om internkontroll- for deg som er leder Hvordan få en god start på risikostyring i statlige virksomheter Risikostyring i staten- håndtering av risiko i mål- og resultatstyringen, metodedokument
Direktoratet for forvaltning og IKT (DIFI) Internkontroll i praksis - informasjonssikkerhet BETA (2015)
Kystverket Vurdering av sårbarhet for havner og havneterminaler.
Forsvarsbygg (FB) Sikringshåndboken
Forsvarets Forskningsinstitutt (FFI) Rapport: Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet (2014) Rapport: Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger (2014)
Standarder NS (2012). Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi. Norsk Standard NS 5830:2012. NS (2014). Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til risikostyring. Norsk Standard NS 5831:2014. NS (2014). Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til risikoanalyse. Norsk Standard NS 5832:2014. NS-ISO/IEC (2013). Norsk Standard NS-ISO/IEC 27001:2013 Informasjonsteknologi. Sikringsteknikker. Styringssystemer for informasjonssikkerhet. Krav. NS-ISO/IEC (2013). Norsk Standard NS-ISO/IEC 27002:2013 Informasjonsteknologi. Sikringsteknikker. Styringssystemer for informasjonssikkerhet. Tiltak for informasjonssikring. NS-ISO/IEC (2011). Norsk Standard NS-ISO/IEC 27005:2011 Informasjonsteknologi. Sikringsteknikker. Risikostyring av informasjonssikkerhet.
Aven, T. (2012). "The risk concept—historical and recent development trends", *Reliability Engineering and System Safety* **99** (2012) 33–44.
Aven, T (2010): On How to define, understand and describe risk. Reliability Engineering and System Safety 95 (2010) 623 – 631.