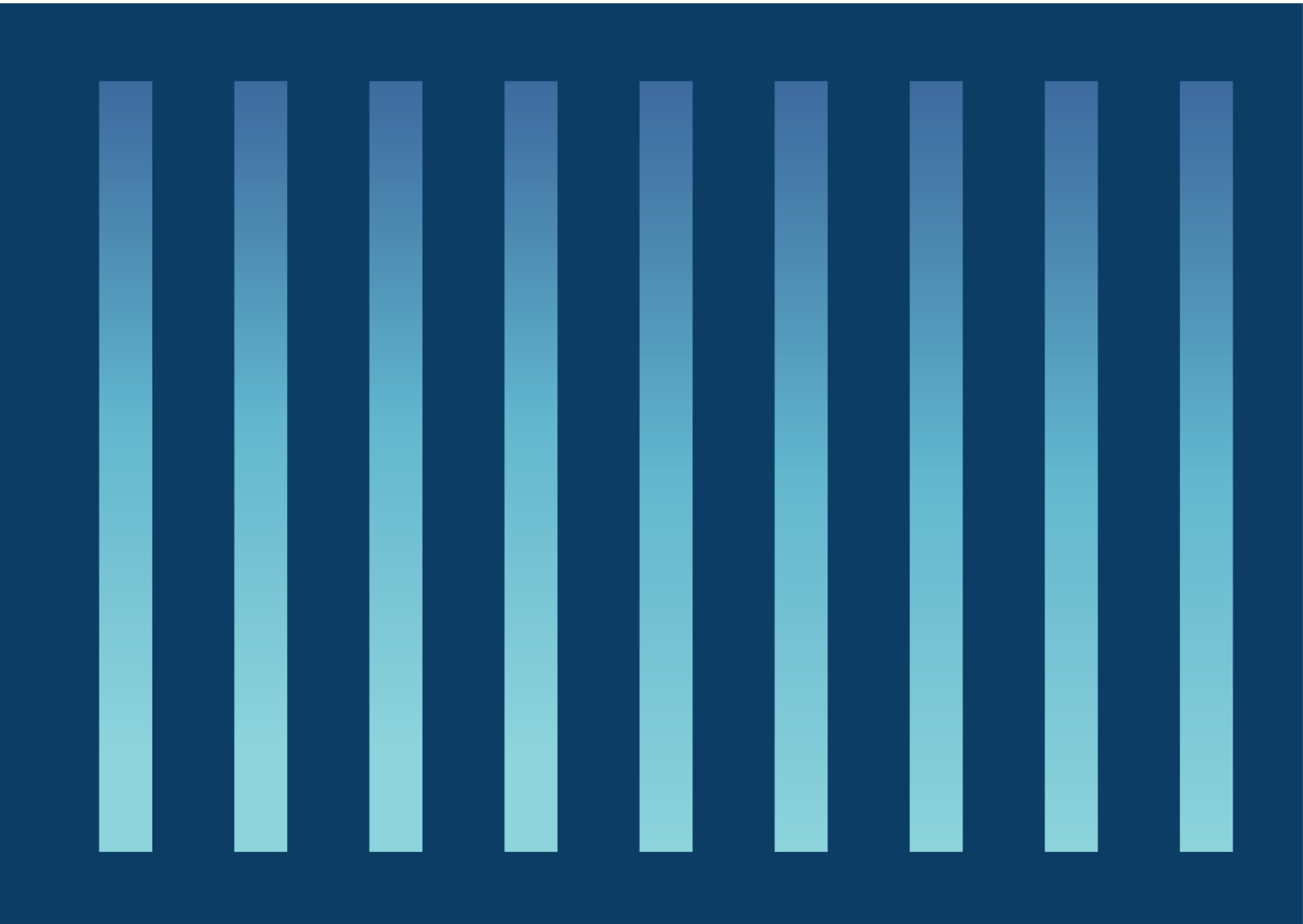
NASJONAL
SIKKERHETSMYNDIGHET

Risikovurdering av IKT-systemer

Ved hjelp av NSM grunnprinsipper for IKT-sikkerhet

Version: 1.0



INNHOLD

1. Bakgrunn og mål 3
2. Risiko og valg av tilnærming 4
3. Steg 1 - Planlegging 6
4. Steg 2 - Gjennomfør risikovurdering 7
4.1 Risikoidentifisering 7
4.2 Risikoanalyse og -evaluering 7
5. Steg 3 - Risikohåndtering 9
6. Referanser 11
Vedlegg A - Bruk av regnearkverktøy 12
Vedlegg B - Sjekkliste risikovurdering av IKT-systemer 13

1. Bakgrunn og mål

De fleste virksomheter er i dag avhengig av IKT-systemer for å støtte sine forretningsprosesser. Dessverre erfarer NSM for ofte at risikovurderinger er mangelfulle eller fraværende, spesielt hos små og mellomstore bedrifter (SMB) og virksomheter som ikke har dedikerte ressurser til sikkerhetsarbeid.

Den pågående digitaliseringen vil føre til at stadig flere IKT-systemer bli introdusert og eksponert i det digitale rom. Det er derfor avgjørende at virksomheter tar IKT-sikkerhet på alvor for å beskytte sine verdier og øke egen robusthet i et stadig skiftende trussellandskap. Risikovurderinger er et viktig hjelpemiddel for virksomhetens ledelse for å bevisstgjøre og ta informerte beslutninger, og for at utviklings- og driftspersonell skal kunne synliggjøre risikoer i egne IKT-systemer.

Bakgrunn og mål
Målet med dette dokumentet og tilhørende verktøy er å kunne hjelpe virksomheter i gang med risikovurdering av ugraderte IKT-systemer. Risikovurderingsmetoden beskrevet i dette dokumentet kan benyttes på informasjonssystem (IKT), industrielle kontrollsystemer (OT) eller andre støttesystemer som inngår i IKT-system porteføljen.

Risikovurdering av IKT-systemer må sees på som en del av den totale risikostyringen i virksomheten hvor IKT-sikkerhet inngår som et ansvarsområde som er forankret i virksomhetens ledelse. Sikkerhetsloven setter krav om vurdering av risiko og at det utføres regelmessig. Målet med en risikovurdering er å avdekke relevante sårbarheter og trusler mot virksomhetens IKT-systemer. Dokumentet skal være til hjelp for deg som risikooppgaveleder i egen virksomhet for å kunne utføre risikovurdering, og gi anbefalinger om hvilke tiltak som bør implementeres for å håndtere risiko i IKT-systemene.

Metoden som beskrives i dette dokument kan benyttes der hvor risikostyring forøvrig er mangelfull eller fraværende i virksomheten, eller som et tillegg til etablert risikostyring spisset mot IKT-systemer.

Avgrensing
Dokumentet vil ikke erstatte allerede etablerte metoder eller konsepter innen risikovurdering, og kan benyttes av alle virksomheter som har IKT-systemer. Utover dette kan enkelte virksomheter og sektorer i tillegg ha føringer fra annet regelverk og standarder innen risikostyring. Dokumentet er avgrenset til risikovurdering for ugraderte IKT-systemer med utgangspunkt i tekniske og organisatoriske tiltak ved bruk av *NSM grunnprinsipper for IKT-sikkerhet* [1] som risikovurderingsmetode.

Beslektede risikoområder er beskrevet i *NSM Veiledning i sikkerhetsstyring* [2], *NSM Sikkerhetsfaglige anbefalinger ved tjenesteutsetting* [3] og *NSM grunnprinsipper for sikkerhetsstyring* [4].

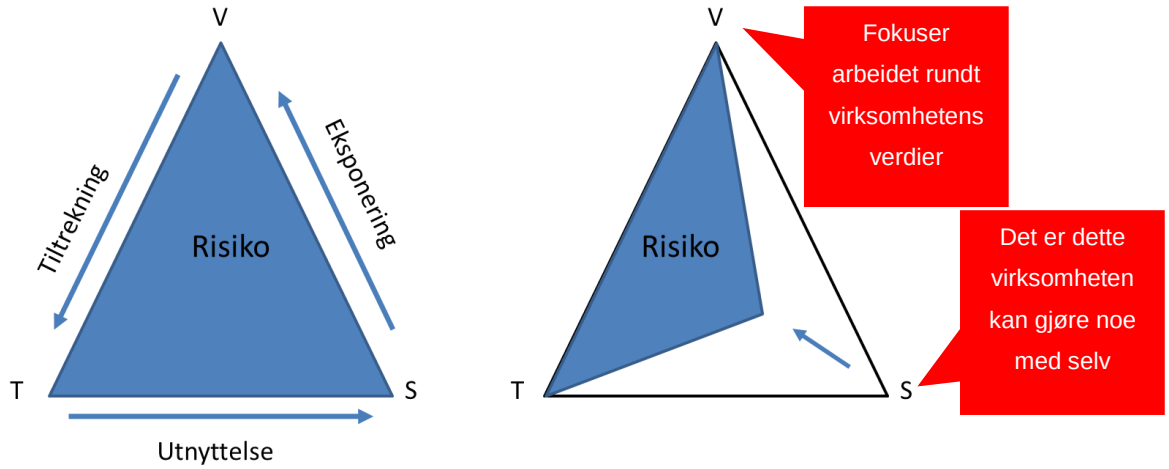
Oppbygning
Dokumentet bygger på standarden *NS-ISO/IEC 27005:2018 Informasjonsteknologi - Sikringsteknikker - Risikostyring for informasjonssikkerhet* [5] og *NSM grunnprinsipper for IKT-sikkerhet* [1].

2. Risiko og valg av tilnærming

Risiko er usikkerhet rundt måloppnåelse. Formålet med **risikostyring** er å sikre at virksomheten når sine mål og retter fokus mot de aktiviteter som er mest kritisk for å nå målene. **Risikovurdering** er et begrep som dekker de tre stegene risiko*identifisering*, risiko*analyse* og risiko*evaluering*. **Risikohåndtering** er å iverksette tiltak for å agere på risikovurderingen. Manglende styringsstrukturer og prosesser for risikovurdering kan føre til at ledelsen ikke får tilstrekkelig informasjon til å prioritere og styre virksomhetens IKT-sikkerhetsarbeid. Et IKT-system kan være en del av en større verdikjede hvor flere systemer inngår. Da er det viktig å ha kontroll og oversikt på risiko og sårbarheter både internt i virksomhetens systemer men også potensielle risikoer fra verdikjeden.

Det finnes forskjellige tilnærminger til risikovurderinger. Norsk Standard 5814:2008 definerer (IKT) risiko som et «uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse». En slik metode kan være utfordrende å anvende siden det skal settes en tallverdi for sannsynlighet og konsekvens hvor virksomhetens empiriske data og måltall er mangelfull eller er basert på et svakt datagrunnlag.

En annen tilnærmingen er basert på NS 5832:2014 der (IKT) risiko er omtalt som «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen. Vurdering av sannsynlighet for at scenario inntreffer er med hensikt utelatt da dette kan vise seg utfordrende å tallfeste. I stedet fokuseres det på å redusere sårbarheter som igjen reduserer IKT-systemets samlede risiko. Denne tilnærmingen kalles trefaktormodellen (også kalt «risikotrekanten») hvor verdi (V), trusler (T) og sårbarheter (S) er faktorene. Modellen er foretrukket av NSM.



Figur 1: I trefaktormodellen er IKT-systemets risiko et forholdet mellom verdi (V), trusler (T) og sårbarheter (S). Ved å bruke NSMs grunnprinsipper for IKT-sikkerhet reduseres sårbarheter og dermed IKT-systemets samlede risiko.

Det kan være ytre eller indre faktorer som påvirker risiko. Risiko endrer seg når:

1. **Verdier** endres. Når virksomhetens verdier endres, må dette reflekteres i risikovurderingen. Eksempelvis innføring av nye IKT-systemer, utvidet bruksområdet på eksisterende IKT-systemer med mer ved å justere verdi.
2. **Sårbarheter** endres. Nye sårbarheter kan gjøres kjent, ny teknologi innføres, nye angrepsmetoder introduseres.
3. **Trusler** endres. Forenklet kan vi si at trussellandskap er i kontinuerlig endring og at de digitale truslene er konstant økende. Det er lite virksomheten kan gjøre med dette, og arbeidet bør fokusere på å redusere sårbarhetene på egne verdier.

Sikkerhetsloven fordrer virksomheter til å utføre risikovurdering regelmessig. Vi har forenklet tilnærming til risiko og delt inn i de tre stegene planlegging, risikovurdering og risikohåndtering. Hver av stegene er beskrevet i de påfølgende kapitler, se Tabell 1 for detaljer.

Tabell 1: De tre stegene i risikovurderingsprosessen.

1. **Planlegging** Involver og planlegg	**2.** **Risikovurdering** Identifiser, analyser og evaluer	**3.** **Risikohåndtering** Effekter og videre oppfølging
• Sørg for å få ledelsesaksept. • Avgrens og sett et mål for arbeidet. • Identifisere hvilke relevante ressurser som er nødvendig. • Lag en plan for risikovurderingen med estimater og datoer.	• Identifiser hvilke IKT-systemer som skal vurderes. • Identifisere sårbarheter og eventuelle trusler. • Identifisere eksisterende sikkerhetsmekanismer. • Identifisere konsekvenser ved brudd på tilgjengelighet, integritet og konfidensialitet.	• Lag en plan for oppfølging av risikoreduserende tiltak. • Vurder effekten av sikkerhetstiltak ved bruk av styringsparameter (KPI). • Vurder restrisikoaksept. • Involver ledelsen i beslutninger og oppfølging av risikotiltak.

3. Steg 1 - Planlegging

En risikovurdering sentreres rundt virksomhetens verdier. Før risikovurderingen kan utføres må det gjøres en kartlegging av virksomhetens verdier. Verdier kan grupperes i primærverdier og støtteverdier, men vi erfarer at skillet mellom disse kan oppleves som teoretiske for mange.

Primærverdier er **forretningsprosesser og informasjon**, og støtteverdier er de **verdier som muliggjør og er avgjørende for primærverdiene**. Eksempler på sekundærverdi er: Maskinvare, programvare, nettverk, personell og lokaler. Risikovurdering i dette dokumentet er sentrert rundt virksomhetens IKT-systemer (sekundærverdi), og verdibegrepet er derfor avgrenset til disse. Et IKT-system kan være database-servere, CRM, ERP, regnskapssystem, nettverksutstyr, klientmaskiner, m.m. Både IKT-systemer som virksomheten har selv («on-premise») eller er tjenesteutsatt (som skytjenester) bør behandles som verdigrunnlag.

Hvor starter jeg?
Planlegg og identifiser IKT-systemet som skal vurderes. Lag en plan for gjennomføring av risikovurderingen.
Hvordan tenke og vurdere risiko?
Enhver trussel, sårbarheter, scenario eller andre uønskede hendelser som kan skade integritet, tilgjengelighet og/eller konfidensialiteten til IKT-systemet utgjør en risiko.
Hva skal vurderes?
Virksomhetens IKT-systemer.
Eksempel: Klienter og servere enten fysisk eller virtuelle og tilhørende tjenester, lagret informasjon, kundedata, dokumentasjon om virksomheten m.m.
Hvordan vurdere?
Risikovurdering ved hjelp av NSM grunnprinsipper for IKT-sikkerhet med tilhørende sikkerhetstiltak.
Hvem skal vurdere?
Virksomheten selv med involverte ressurser som har kunnskap om virksomhetens IKT-systemer samt ledere.

Risikovurdering krever både tid og ressurser, sørg for å **få aksept fra ledelsen før du begynner**. Estimer tid og hvilket relevant personell som må involveres. Avgrens risikovurderingen til noe som er håndterbart gitt tilgjengelige ressurser og kompetanse.

Lag en plan for gjennomføring av arbeidet. Denne planen kan være en tekstlig beskrivelse av hva som skal vurderes (hvilke IKT-systemer), hva som kreves av virksomheten (ledelsesforankring og involvering av personell), estimert tidsforbruk, og hvordan risikovurderingen skal gjennomføres (beskrevet i dette dokumentet). Virksomheten bør gjøre justeringer i gjennomføringen basert på: Kompetanse, tidsperspektiv, plan for risikogjennomføring, etterarbeid med risikoreduserende tiltak og evaluering av risikoakseptkriterier. Det er bedre å starte i det små enn å ha ambisiøse planer som ikke lar seg gjennomføre. Avgrens risikovurderingen til for eksempel en av virksomhetens mest kritiske IKT-system fremfor å ta alle IKT-systemer.

Husk at dokumentasjon om virksomhetens risikovurderinger bør behandles som sensitiv informasjon, da vurderingene beskriver virksomhetskritisk informasjon. Selve risikovurderingen bør det gis begrenset tilgang til, og involvert personell informeres om hvordan de skal behandle sensitiv informasjon.

4. Steg 2 - Gjennomfør risikovurdering

Når det foreligger en plan for gjennomføring og det er forankret hos ledelsen, kan risikovurderingen utføres. Metoden som ligger til grunn er å se på i hvor stor grad sikkerhetstiltakene i *NSMs grunnprinsipper for IKT-sikkerhet* er fulgt for hvert IKT-system. Metoden er enkel og overkommelig, og vil gi virksomheten en god oversikt over samlet risiko for hvert vurderte IKT-system. Se eget regnearkverktøy på NSM.no for mer informasjon og anvendelse.

Rasjonale for gjennomføring
Risikovurdering kan gjennomføres ved bruk av ulike tilnærminger og verktøy. Det er viktig å etablere en plan og gjennomføre denne systematisk, samtidig som det dokumenteres gjennom hele vurderingsprosessen. Det er virksomhetens egne ressurser som kjenner informasjonssikkerhetstilstanden best, og som kan identifisere risiko samt bidra med forslag på mulige sikkerhetstiltak. Dette medfører at det kreves ulike virksomhetsressurser ved gjennomføringen av en risikovurdering.

4.1 Risikoidentifisering

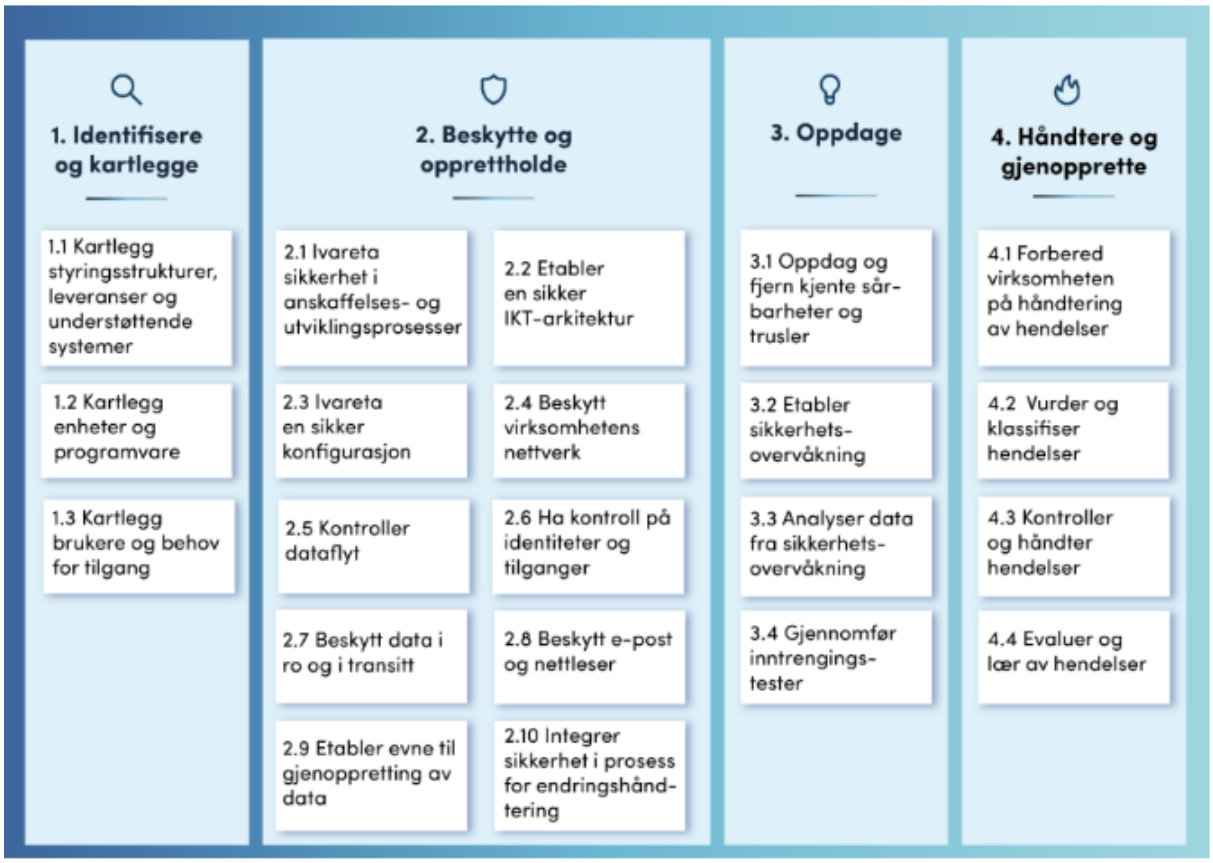
Det første som må gjøres, hvis det ikke allerede er på plass, er å **identifisere og kartlegge alle IKT-systemer for virksomheten**. Hvis det er utfordrende så kan du avgrense og begynne med de IKT-systemene som er sentral og har størst verdi for ditt forretningsområdet/ansvarsområde. For hvert IKT-system bør sårbarheter kartlegges så godt det lar seg gjøre. Hvilke konsekvenser kan en uønsket hendelse mot eller utfall av IKT-systemet ha? Det bør beskrives.

Deretter bør **eksisterende sikkerhetstiltak for hvert IKT-system identifiseres og kartlegges**. Dette er viktig da eksisterende sikkerhetstiltak må vurderes opp tiltakene i grunnprinsippene for IKT-sikkerhet som er neste steg.

4.2 Risikoanalyse og -evaluering

Metoden for risikoanalyse og –evaluering legger til grunn de sikkerhetstiltak som er beskrevet i *NSM grunnprinsipper for IKT-sikkerhet* og hvorvidt virksomheten har implementert disse.

NSM grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene med tilhørende sikkerhetstiltak er gruppert i fire kategorier. Les mer om grunnprinsippene her.



Figur 2: NSM grunnprinsipper for IKT-sikkerhet 2.0 med fire kategorier, 21 prinsipper og 118 sikkerhetstiltak som brukes i risikovurderingen. Hvert prinsipp med tilhørende sikringstiltak evalueres opp mot hvert IKT-system.

Det identifiserte IKT-system vurderes opp mot hvert (relevant) grunnprinsipp og det settes vekting på i hvor stor grad IKT-systemet følger tiltakene i grunnprinsippet (se Tabell 2). Vektingen («måltallet») vil gi en indikasjon på i hvor stor grad IKT-systemet er beskyttet av et eller flere sikkerhetstiltak. Vurderingen vil gi en indikator på etterlevelse i henhold til grunnprinsippene for de vurderte IKT-systemer, samt oversikt over mangler (risikoer). Tabell 2 viser vektingen som skal gjøres for hvert sikkerhetstiltak.

Tabell 2: Vurderingsskala som benyttes ved vekting på i hvor stor grad IKT-systemet følger sikkerhetstiltak

Grad av implementasjon	Beskrivelse
Høy grad	Alle / de fleste sikkerhetstiltak fra grunnprinsippet er implementert / hensyntatt for IKT-systemet.
Moderat grad	Flere sikkerhetstiltak fra grunnprinsippet er implementert / hensyntatt for IKT-systemet, men flere burde være implementert / hensyntatt.
Liten grad	Få eller ingen sikkerhetstiltak fra grunnprinsippet er implementert / hensyntatt for IKT-systemet.
Ikke relevant	Sikkerhetstiltakene fra grunnprinsippet er ikke relevant for IKT-systemet.

Når regnearket er utfylt for hvert IKT-system vil virksomheten ha en oversikt over den samlede risiko som IKT-systemet bærer, men og hvilke områder som krever risikoreduksjon. Tilhørende risikovurderingsregneark finnes NSM.no som kan anvendes ved dokumentering og risikovurdering.

5. Steg 3 - Risikohåndtering

Når risikoer er identifisert og evaluert (steg 2) 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 blant annet legale, økonomiske og praktiske rammer. En vanlig strategi for å håndtere risiko for IKT-systemer er at risikoen *reduseres* ved at sikkerhetstiltak iverksettes.

Hvordan håndtere risikoreduserende tiltak
Det er ulike sikkerhetstiltak virksomheten kan innføre for å redusere risiko. En balanse mellom menneskelige, tekniske og organisatoriske tiltak er viktig for å redusere risiko. Hensikten er å komme frem til tiltak som er formålstjenlig og relevant for å redusere den aktuelle risikoen tilstrekkelig. Metoden beskrevet i dette dokumentet fokuserer på tekniske tiltak og benytter sikkerhetstiltak som er beskrevet i *NSMs grunnprinsippene for IKT-sikkerhet*.

Kost/nyttevurdering vil kunne gjøre utfall i risikovurdering med hvilke tiltak som kan iverksettes og/eller justeres. Identifiserte risikoreduserende tiltak skal implementeres med mindre de står i vesentlig misforhold til kostnader og andre ulemper. Det er virksomhetens ledelse som må ta stilling til risiko sett opp mot kostnadene ved å iverksette risikoreduserende tiltak.

Hvilke sikkerhetstiltak bør iverksettes for å redusere risikoen tilstrekkelig til at vi kan akseptere den? Basert på vurderinger utført på avdekte risiko bør det lages en plan for hvilke tiltak som bør implementeres, prioritet, estimat på hva tiltaket vil koste, start- og ferdigstillelsesdato, og ansvarlig for tiltaket. Se forslag i Tabell 3.

Tabell 3: Forslag på elementer som bør inngå i risikohåndteringsplanen

Tiltak	Prioritet	Ressursbruk	Ansvarlig (risikoeier)	Start- og ferdigstillelsesdato	Vedlikehold / kommentar

Ledelsen må deretter involveres for å beslutte risikohåndteringsplanen.

Lag tilpassede effektmål som sier noe om sikkerhetstiltak
Nye eller endrede sikkerhetstiltak må vurderes etter iverksettelse for å se hvilken effekt dette har på avdekt risiko (effektmål). Her er det viktig å sette seg fornuftige effektmål og styringsparametere (KPI) som sier noe om hvor godt tiltaket fungerer og evnen det har til å redusere risiko. Både i et teknisk perspektiv («Fungerer sikkerhetstiltaket etter hensikt?») og i et kostnadsperspektiv («Hva er kostnadene ved implementering, drift og vedlikehold?»). Et eksempel på styringsparametere innen

deteksjon og analysearbeid som sier noe om effekten til sikkerhetstiltak og IKT-systemets evne til å motstå driftsforstyrrelser.

Effektmåling av risikoreduserende tiltak kan for eksempel gjøres ved å stille spørsmålene:

- Forhindrer sikkerhetstiltaket sårbarheter som er identifisert?
- Blir IKT-systemer vedlikeholdt med regelmessige sikkerhetsoppdateringer?
- I hvor stor grad utføres monitorering av unormal datatrafikk av IKT-systemene?
- Anvendes IKT-systemet av brukerne i henhold til avtalte prosedyrer?
- Er vedlikehold av IKT-system og sikkerhetstiltak innenfor budsjettert timeforbruk og kostnad? (Både internkostnad og kostnader ved tjenesteutsetting.)
- Bidrar iverksatte sikkerhetstiltak til å forbedre virksomhetens sikkerhet og sikre virksomhetens verdier?
- Øker virksomhetens evne til å reagere på varsler fra deteksjon for å kunne håndtere uønskede hendelser?

Slike effektmålinger bør gjøres over en lengre tidsperiode, for eksempel ett års tid, hvor de nye sikkerhetstiltakenes effektmål blir vurdert hvert kvartal.

Resultatet av den investerte kostnaden med risikoreduserende tiltak og oppfølging av effektmål vil være; redusert risiko, økt robusthet i IKT-systemer, økt kunnskap og forståelse for IKT-systemenes sårbarheter og avhengighet.

En beslutning kan være å *akseptere* risikoen og beholde IKT-systemet uforandret basert på kost/nytte-vurderinger. Husk også at der hvor IKT-systemer endres så kan risikoer og sårbarheter påvirke hverandre negativt ved risikovandring mellom systemer. Eksempel ved at en endring i funksjonalitet på en internetteksponert applikasjon/tjeneste kan føre til at uvedkommende kan få tilgang på virksomhetens interne systemer siden disse kan være tilkoblet hverandre i et nettverk. Da kan risikoen vandre fra den internetteksponerte applikasjonen/tjenesten og til andre deler av virksomhetens IKT-systemer.

Risikovurdering er en kontinuerlig prosess. Enhver endring og modifisering av IKT-systemer bør risikovurderes før de iverksettes. Tilpassing av sikkerhetstiltak og styringsparameter (KPI) er en løpende aktivitet som bør justeres basert på trusler i det digitale rom. Dette krever proaktiv oppfølging og god kommunikasjon i egen virksomhet mellom systemeiere, risikoeiere og ledelse. Virksomheten og ledelsen har alltid ansvaret for sikring av egne verdier. Risikovurdering og risikohåndtering er helt nødvendig for å kunne oppnå et forsvarlig sikkerhetsnivå i egen virksomhet.

6. Referanser

[1] NSM, «NSMs grunnprinsipper for IKT-sikkerhet 2.0,» [Internett]. Available: https://nsm.no/grunnprinsipper-ikt.

[2] NSM, «Veileder i sikkerhetsstyring,» [Internett]. Available: https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-sikkerhetsstyring/om-denne-veilederen/.

[3] NSM, «Sikkerhetsfaglige anbefaling ved tjenesteutsetting,» [Internett]. Available: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/introduksjon/.

[4] NSM, «NSM grunnprinsipper for sikkerhetsstyring,» [Internett]. Available: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/introduksjon/.

[5] ISO, NS-ISO/IEC 27005:2018 Informasjonsteknologi - Sikringsteknikker - Risikostyring for informasjonssikkerhet.

Vedlegg A - Bruk av regnearkverktøy

Risikovurdering av IKT-systemer ved bruk av regnearkverktøy og NSM grunnprinsipper for IKT-sikkerhet. Regnearket inneholder ulike faner som anvendes ved vurdering og dokumentering av stegene i risikovurderingen.

Samtlige 118 sikkerhetstiltak er med i regnearkverktøyet. For mindre IKT-systemer og/eller anlegg kan listen med «prioritet 1» og «prioritet 2» sikkerhetstiltak anvendes. Dette vil medføre at risikovurdering gjøres mot 35 tiltak i stedet for alle 118.

Fanetittel	Beskrivelse
Planlegging og deltagere	Planlegg og forankre risikovurdering.
Risikovurdering	Gjennomføring av vurderingen ved bruk av
Risikohåndtering	Oppfølging og håndtering av avdekt risiko
Plan og oppfølging	Plan og videre oppfølging
NSM grunnprinsipper for IKT-sikkerhet	Grunnprinsipp og sikkerhetstiltak versjon 2.0

Versjonshistorikk

Versjon	Dokument	Kommentar	Dato
1.0	Risikovurdering av IKT-systemer	Nytt dokument	Juni 2021
1.0	Regnearkverktøy	Nytt regnearkverktøy, basert på grunnprinsipp for IKT-sikkerhet versjon 2.0.	Juni 2021

Vedlegg B - Sjekkliste risikovurdering av IKT-systemer

Steg 1 Planlegging
1. Velg en oppgaveeier som har ansvaret for prosessen med risikovurderingen. Involver ledelsen og forankre risikovurderingen før den kan starte. 2. Lag en plan for gjennomføring som viser milepæler, delaktiviteter og tidsestimat for de ulike steg, avgrens vurderingen og forenkle prosess basert på kunnskap om systemer samt tildelt personell og tid. 3. Forbered risikovurdering. Involver personell, informer om plan for gjennomføring, del informasjon slik at de involverte og ledelsen er godt informert om veien videre før vurdering og ulike aktiviteter starter.
Steg 2 Risikovurdering
1. Få oversikt over risikoområder og identifiser disse i egnet verktøy som benyttes gjennom hele vurderingsprosessen. 2. Ikke gå i dybden med det første, det er oftest viktigere å avdekke risikoer i gråsoner i og mellom ulike IKT-systemer og spesielt i de nettverkssonene som er eksponert for ytre tjenester og internett. 3. Vurder og beskriv avdekt risiko opp mot virksomhetens krav til IKT-systemet, lovverk, standarder og retningslinjer, samt systemdokumentasjon. 4. Analyser og evaluer resultatene fra risikovurderingen.
Steg 3 Risikohåndtering
1. Prioriter de mest alvorligste risikoene til de mest sentrale (verdifulle) IKT-systemene. Risikoreduksjon bør utføres så snart som mulig og i henhold til risikohåndteringsplanen med involvering av rett personell og ledelse. 2. Etabler effektmål og styringsparameter for videre oppfølging. 3. Avklar og beslutt restrisikoaksept og veien videre (kontinuerlig forbedring).