NSM

Risikovurdering av IKT-systemer

Ved hjelp av NSMs Grunnprinsipper for IKT-sikkerhet v2.1

tirsdag 18. juni 2024

Om Nasjonal sikkerhetsmyndighet
Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for nasjonal forebyggende sikkerhet. NSMs hovedoppgave er å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler.

Risikovurdering av IKT-systemer og etterlevelse av lovverk
Risikovurderingsmetoden beskrevet i dokumentet kan benyttes på informasjonssystem (IKT), industrielle kontrollsystemer (OT) eller andre støttesystemer som inngår i virksomhetens IKT-portefølje. Metoden kan benyttes av alle virksomheter med IKT-systemer. Ved å benytte metoden vil virksomheter få et godt fundament for risiko i IKT-systemene, men metoden må vurderes og tilpasses hver enkelt virksomhet. *Merk at ulike lovverk kan ha andre krav risikovurdering enn hva som anbefales i dette dokumentet*. Et eksempel på dette er «Lov om nasjonal sikkerhet» (sikkerhetsloven), som har flere og strengere krav enn hva som anbefales her.

Innhold

1 Bakgrunn og formål

IKT-systemer er ofte avgjørende for en virksomhets eksistens og gir kritisk støtte til forretningsprosesser. Vi opplever at **risikovurderinger** av IKT-systemer ofte er mangelfulle, spesielt i små og mellomstore bedrifter (SMB) og hos virksomheter som ikke har avsatt dedikerte ressurser til sikkerhetsarbeid.

Den pågående digitaliseringen fører til at stadig flere IKT-systemer bli etablert og eksponert i det digitale rom. Det er derfor avgjørende at virksomheter tar ansvar for IKT-sikkerhet, beskytter sine verdier og øker egen robusthet i et stadig skiftende trussellandskap.

Risikovurderinger er et nødvendig hjelpemiddel for styringen av en virksomhet og bidrar til at virksomhetens ledelse får økt bevissthet rundt risikoer og kan benytte dette i beslutningsprosesser. Det bidrar også til at utviklings-, implementasjons- og driftspersonell kan synliggjøre risikoer i egne IKT-systemer og at personell får økt kunnskap og forståelser for IKT-systemenes verdier, sårbarheter og avhengigheter.

1.1 Formål

Formålet med dette dokumentet, og tilhørende verktøy, er å støtte virksomheter med risikovurdering av ugraderte IKT-systemer. Risikovurderingsmetoden beskrevet i dokumentet kan benyttes på informasjonssystem (IKT), industrielle kontrollsystemer (OT) eller andre støttesystemer som inngår i virksomhetens IKT-portefølje. Metoden kan benyttes av alle virksomheter med IKT-systemer.

Risikovurdering av IKT-systemer må sees på som en del av den totale risikostyringen i virksomheten hvor ansvar, utførelse og rapportering er forankret i virksomhetens ledelse. Målet med risikovurderingen er å avdekke, analysere og evaluere risikoer som kan påvirke virksomhetens IKT-systemer. Dokumentet skal være til hjelp for å kunne utføre risikovurdering og gi anbefalinger om hvilke tiltak som bør implementeres for å håndtere avdekket risiko i IKT-systemene.

Metoden kan benyttes selv om risikostyring er mangelfull i virksomheten, men den anbefales primært som et tillegg til etablerte metoder for risikostyring og risikovurdering og ikke som eneste metode.

1.2 Avgrensning

Dokumentet tar ikke for seg prosesser for risikostyring i virksomheten og er ikke ment å erstatte allerede etablerte metoder eller prosesser innen risikovurdering.

Sektorer og virksomheter kan være underlagt krav til risikostyring og risikovurdering i ulike regelverk. «Lov om nasjonal sikkerhet» (sikkerhetsloven) fastsetter for eksempel krav til vurdering og håndtering av risiko og at risikovurderinger skal utføres regelmessig.

Dokumentet er avgrenset til risikovurdering for ugraderte IKT-systemer og benytter tiltak i *NSMs grunnprinsipper for IKT-sikkerhet* som utgangspunkt for vurderingen.

1.3 Oppbygning

Dokumentet bygger på standarden *NS-ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks* (ISO) og *NSM grunnprinsipper for IKT-sikkerhet v2.1*.

1.4 Versjonshistorikk

Tabell 1 - versjonshistorikk

Versjon	Produkt	Filnavn	Kommentar	Dato
1.0	Risikovurdering av IKT-systemer	Risikovurdering av IKT-systemer.pdf	Nytt dokument	Juni 2021
1.0	Regnearkverktøy	Vedlegg- Mal for risikovurdering IKT-systemer.xlsx	Nytt regnearkverktøy, basert på grunnprinsipp for IKT-sikkerhet versjon 2.0.	Juni 2021
2.1	Risikovurdering av IKT-systemer	Risikovurdering av IKT-systemer vha NSMs Grunnprinsipper for IKT-sikkerhet 2.1.pdf	Endring av enkelte formuleringer og retting av skrivefeil. Endret referanse til oppdaterte ISO-standarder og oppdatert versjon av GP-IKT. Endret verktøy til versjon 2.1 for å harmonere med versjonsnr. i GP-IKT 2.1.	Juni 2024
2.1	Regnearkverktøy	Vedlegg - Mal for risikovurdering av IKT-systemer_2.1.xlsx	Oppdateringa av enkelte tiltak for å harmonere med GP-IKT 2.1. Rettet skrivefeil.	Juni 2024

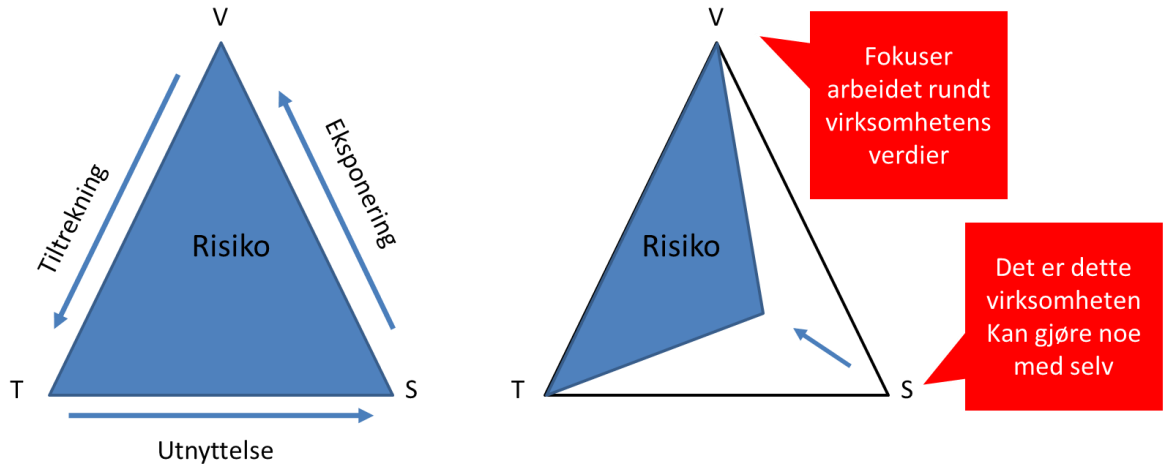
2 Risiko og valg av tilnærming

2.1 Risikometode

Risiko er usikkerhet rundt måloppnåelse. **Risikostyring** innebærer å etablere systematiske aktiviteter i virksomheten for å ha kontroll med risiko. **Risikovurdering** er et begrep som dekker de tre stegene **risikoidentifisering**, **risikoanalyse** og **risikoevaluering**. **Risikohåndtering** innebærer 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 styre virksomheten og 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 sårbarheter og risiko både internt i virksomhetens systemer men også potensielle risikoer fra verdikjeden.

Det finnes forskjellige tilnærminger til risikovurderinger. En vanlig måte er å se på 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 og virksomhetens måltall og empiriske data kan være mangelfull og er ofte basert på et svakt datagrunnlag.

En annen tilnærmingen, blant annet beskrevet i NS 5832:2014, omtaler (IKT) risiko 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.



Figur 1 - I trefaktormodellen er IKT-systemets risiko et forhold 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.

Risikovurderinger bør gjøres regelmessig, noe blant annet sikkerhetsloven stiller krav til. Metoden vi har tatt frem i dette dokumentet er en forenklet tilnærmingen til risikovurdering, delt inn i de tre stegene planlegging, risikovurdering og risikohåndtering. Hvert av stegene er beskrevet i de påfølgende kapitler. Metoden bygger på NS-ISO/IEC 27005:2022 og benytter seg av en GAP-analyse opp imot tiltakene i NSMs grunnprinsipper for IKT-sikkerhet. Hvert tiltak blir vurdert med tanke på etterlevelse og ved å vurdere sårbarheter knyttet til hvert tiltak, som vist i trefaktormodellen i Figur 1.

Tabell 2: 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. • Identifiser hvilke relevante ressurser som er nødvendig. • Lag en plan for risikovurderingen med estimater og datoer.	• Identifiser hvilke IKT-systemer som skal vurderes. • Identifiser sårbarheter og eventuelle trusler. • Identifiser eksisterende sikkerhetsmekanismer. • Identifiser 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.

Relevant risikodokumenter:

- ISO 31000:2018 Risk Management Guidelines
- NS 5814:2021 – Krav til risikovurderinger
- NS 5831:2014 – Samfunnssikkerhet – Beskyttelse mot utilsiktede handlinger – Krav til sikringsrisikostyring
- NS 5832:2014 – Samfunnssikkerhet – Beskyttelse mot utilsiktede handlinger – Krav til sikringsrisikoanalyser
- US NIST SP 800-30 – Guide for Conducting Risk Assessments
- Carnegie Mellon - Octave Allegro: Operationally Critical Threat, Asset, and Vulnerability Evaluation methodology

2.2 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 med en gang.

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.

2.3 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 går ut på å vurdere i hvor stor grad sikkerhetstiltakene i *NSMs grunnprinsipper for IKT-sikkerhet* er fulgt for hvert IKT-system. Metoden er forsøkt laget enkel og overkommelig, og vil gi virksomheten et godt utgangspunkt for å få oversikt over risikoer for hvert vurderte IKT-system.

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

2.3.1 Risikoidentifisering

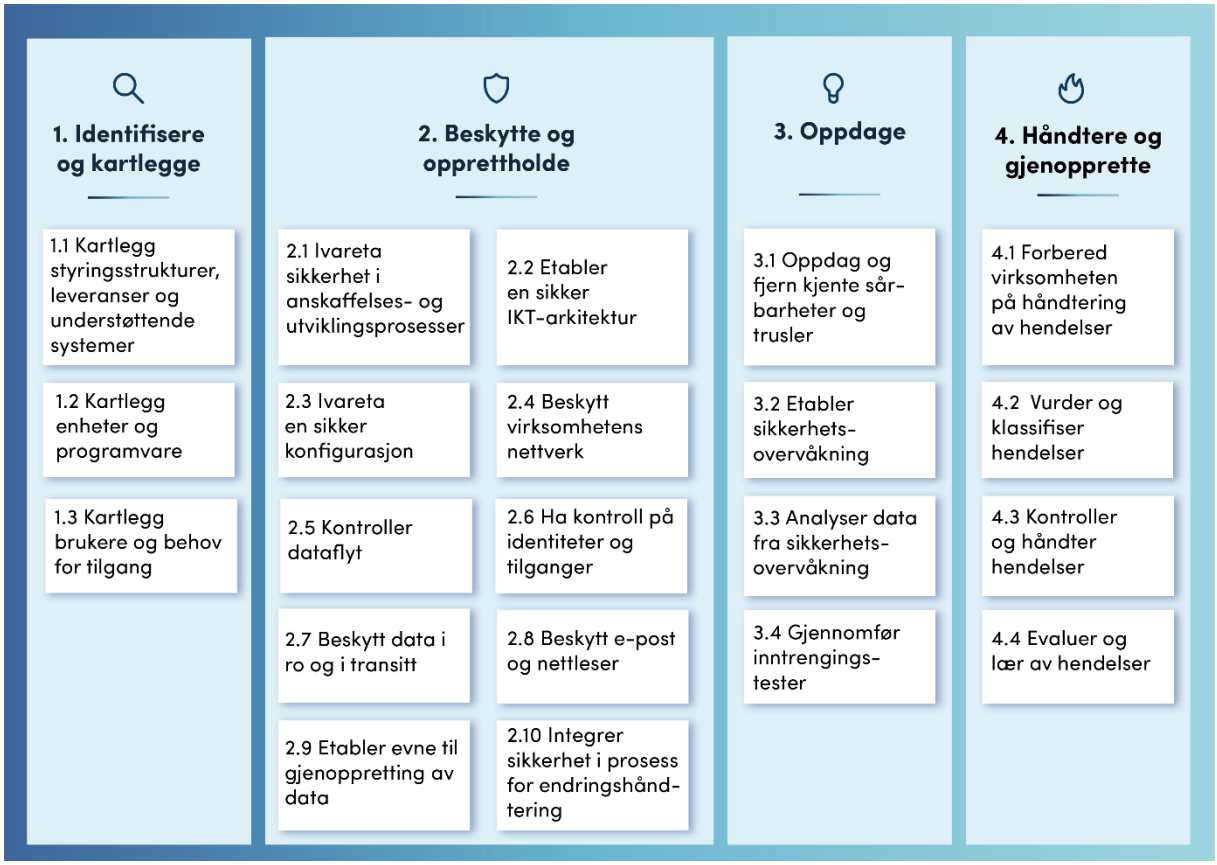
Det første som må gjøres, hvis det ikke allerede er på plass, er å **identifisere og kartlegge alle IKT-systemer for virksomheten**. Hvis det er utfordrende å få oversikt kan man starte med IKT-systemer innenfor ett forretningsområdet/ansvarsområde. For hvert IKT-system bør sårbarheter kartlegges så godt det lar seg gjøre. Det bør også beskrives hvilke konsekvenser et utfall av IKT-systemet kan ha, dvs dersom dette blir utilgjengelig.

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

2.3.2 Risikoanalyse og -evaluering

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

NSMs 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 - NSMs grunnprinsipper for IKT-sikkerhet 2.1 med fire kategorier, 21 prinsipper og 118 sikkerhetstiltak som brukes i risikovurderingen. Hvert prinsipp med tilhørende sikringstiltak evalueres opp mot hvert IKT-system

IKT-systemet vurderes opp mot hvert (relevante) tiltak som hører under de ulike grunnprinsippene og det vektes i hvor stor grad IKT-systemet følger tiltaket (se Tabell 3). 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 3: 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 vil virksomheten få ha en oversikt over kartlagt risiko i IKT-systemet og hvilke områder som krever risikoreduksjon.

2.4 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, de vanlige er: *unngå, overføre, akseptere eller redusere risiko*. Virksomheten står sjelden helt fritt til å velge strategi. Handlingsrommet avhenger av blant annet juridiske, økonomiske og praktiske rammer. En vanlig strategi for å håndtere risiko for IKT-systemer er å *reduseres* risiko ved at sikkerhetstiltak iverksettes.

Hvordan håndtere risikoreduserende tiltak
Virksomheten kan innføre ulike sikkerhetstiltak for å redusere risiko. En balanse mellom menneskelige, tekniske og organisatoriske tiltak er ofte nødvendig. 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 grunnprinsipper for IKT-sikkerhet*.

Kost/nyttevurdering
Virksomheten må ofte vurdere kost opp imot nytte med tanke på hvilke tiltak som kan iverksettes og/eller justeres. Identifiserte risikoreduserende tiltak bør 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 avdekt risiko bør det lages en plan for hvilke tiltak som bør implementeres, prioritet på disse, estimat på hva tiltaket vil koste, start- og ferdigstillelsesdato, og ansvarlig for tiltaket. Se forslag i Ledelsen må deretter involveres for å beslutte risikohåndteringsplanen.

Tabell 4. Ledelsen må deretter involveres for å beslutte risikohåndteringsplanen.

Tabell 4: Forslag på elementer som bør inngå i risikohåndteringsplanen

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

Lag tilpassede effektmål som beskriver 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?»).

Effektmåling av tiltak kan gjøres ved å stille enkelte spørsmål, for eksempel:

- Lukker sikkerhetstiltaket sårbarheter som er identifisert?
- Bidrar iverksatte sikkerhetstiltak til å forbedre virksomhetens sikkerhet og sikre virksomhetens verdier?
- Fungerer sikkerhetstiltaket etter hensikt?
- Er det riktig sikkerhetstiltak som er iverksatt opp imot aktuell trussel?
- Er sikkerhetstiltaket kostnadseffektivt?
- Er vedlikehold av IKT-system og sikkerhetstiltak innenfor budsjettert timeforbruk og kostnad? (Både internkostnad og kostnader ved tjenesteutsetting.)

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

Risikovurdering er en kontinuerlig prosess. Enhver endring og modifisering av IKT-systemer bør risikovurderes før de iverksettes. En endring i ett IKT-system kan påvirke andre deler av systemet og kan også påvirke risikoen i andre IKT-systemer. Tilpassing av sikkerhetstiltak og styringsparameter (KPI) er en løpende aktivitet som bør justeres basert på relevante trusler. 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.

3 Vedlegg A – Regnearkverktøy og sjekkliste

Risikovurdering av IKT-systemer kan utføres ved bruk av tilhørende regnearkverktøy (*Vedlegg - Mal for risikovurdering av IKT-systemer_2.1.xlsx*). 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. Regnearket kan lastes ned under «støtteprodukter» på nsm.no/gp-ikt.

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

3.1 Vedlegg A1 - 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).