Oslo

Byrådsavdeling for finans

Veileder for risikovurdering

Informasjonssikkerhet

Versjon 1.5

Foto: Thomas Ekström

Innhold

Veileder for risikovurdering av informasjonssikkerhet

1 Introduksjon

1.1 Formål

Formålet med veilederen er å gi en innføring i anbefalt fremgangsmåte for risikovurdering av informasjonssikkerhet i virksomheter i Oslo kommune. Veilederen kan benyttes til å gjennomføre risikovurderinger av ulike aktiviteter, og andre informasjonsverdier som informasjon, systemer, prosesser, tjenester og personell. Veilederen refererer til risikovurderingsverktøyet som er utgitt av Byrådsavdeling for finans.

En risikovurdering gjennomføres for å analysere risikoer mot verdier og beskytte verdiene i henhold til behov. En risikovurdering består av flere trinn; verdivurdering, trusselvurdering, sårbarhetsvurdering, og vurdering av risiko ved uønskede hendelser i forhold til akseptabel risiko. Forslag til og gjennomføring av tiltak for håndtere risikoene inngår i aktiviteten risikohåndtering men det er også vanlig å ta med forslag til tiltak i en risikovurdering.

En verdi vil kunne utsettes for to ulike kategorier av trusler. En trussel kan enten være en villet handling gjennomført av en trusselaktør, med ønske om for eksempel å få uautorisert innsyn i informasjon eller forhindre tilgang til denne, eller et trusselfenomen som tekniske feil, naturkatastrofe, menneskelige feil etc.

God håndtering av risiko er nødvendig for å bidra til tilfredsstillende og sikker ivaretakelse av informasjon, systemer, prosesser, tjenester og personell.

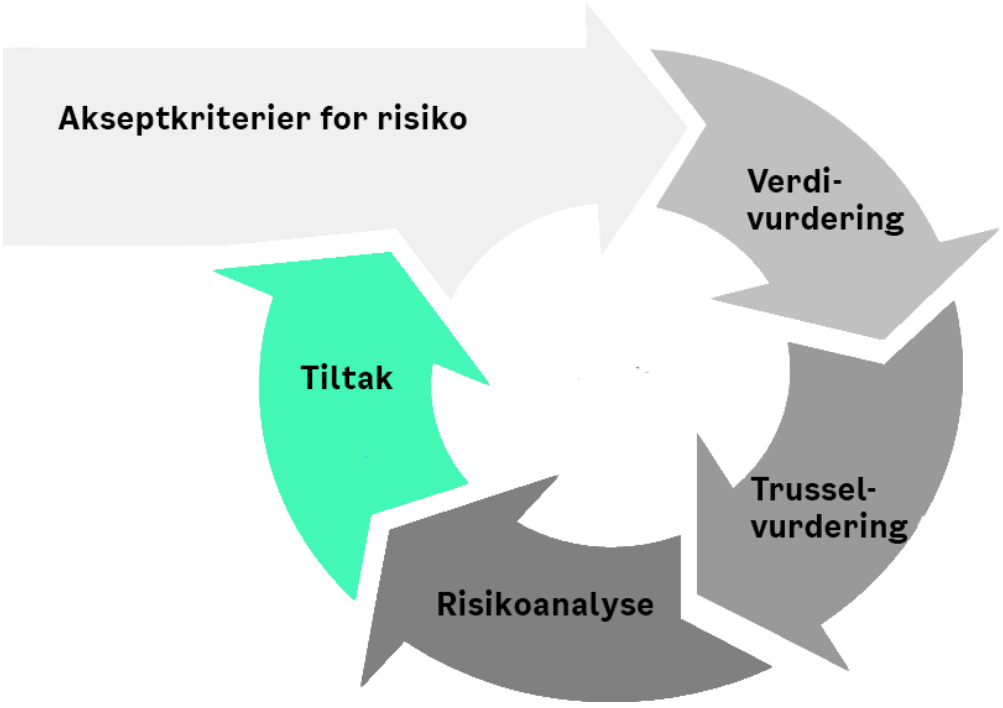
Risikovurdering er en del av virksomhetsstyringen i Oslo kommune. Resultatene skal dokumentere at virksomheten driver egne aktiviteter innenfor akseptabelt risikonivå, alternativt beskrive tiltak for å redusere risiko til akseptabelt nivå.

1.2 Målgruppe

Målgruppen er ansatte og andre som leder risikovurdering og/eller har ansvar for å gjennomføre risikovurdering innen informasjonssikkerhet i sin virksomhet. De bør ha gjennomført kurs i risikovurdering og/eller ha kunnskap om eller erfaring fra gjennomføring av risikovurderinger fra tidligere.

2 Prosess for risikovurdering

Risikovurdering gjennomføres i følgende steg:



Figur 1 Prosess for risikostyring innen informasjonssikkerhet

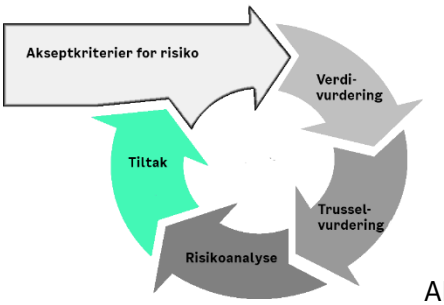
Steg	Kort beskrivelse
Verdivurdering	En vurdering av hvor kritisk informasjonen og prosess/system er for konfidensialitet, integritet og tilgjengelighet.
Trusselvurdering	En vurdering av trusselfenomener og -aktører som kan forårsake uønskede hendelser.
Risikoanalyse	En identifisering av uønskede hendelser, og en vurdering av konsekvenser av og sannsynlighet for de ulike hendelsene.
Tiltak	Identifisering av tiltak for å redusere risikoer som er høyere enn det som er akseptabelt.

Tabell 1 Prosess for risikostyring av informasjonssikkerhet

Figur 1 viser prosessen som et hjul for **jevnlig** risikovurdering. Etter førstegangs risikovurdering, vil senere risikovurderinger av samme prosess/system normalt være en oppdatering som tar utgangspunkt i endringer i forutsetninger siden sist. Dette kan være endringer i trusselbilde, teknologi, organisasjon, bruksmønster mm. I tillegg kommer risikovurdering i forbindelse med endringer i systemet eller prosessen.

Risikovurderingsarbeidet støttes av et regnearkbasert verktøy med flere faner, basert på stegene i metoden.

2.1 Akseptkriterier



Akseptkriterier brukes for å uttrykke et akseptabelt og et uakseptabelt risikonivå fastsatt av ledelsen for en virksomhet, eventuelt av en byrådsavdeling, for alle virksomheter i en sektor. Se også matrisen i Figur 4 i kap. 5.4. Målet er å redusere konsekvensen av og sannsynligheten for hendelser gjennom ulike tiltak, slik at alle risikoer er akseptable.

Denne metoden bruker tre risikonivåer som er beskrevet i Tabell 2:

Risikonivå	Beskrivelse	Kriterier for å akseptere risiko
Lav	**Tiltak er ikke nødvendig**	Risiko kan aksepteres uten å lete etter eller vurdere nytten av flere tiltak. Tiltak kan allikevel vurderes dersom de er kostnadseffektive. Risikoen kan aksepteres av ledere på alle beslutningsnivå.
Middels	**Tiltak skal vurderes. Risiko må følges opp.**	Det er gjennomført et systematisk arbeid for å identifisere tiltak. Alternativ risikohåndtering er mindre effektiv, gir høyere risiko på andre områder, og/eller er dyrere. Risikoen kan kun aksepteres av virksomhetsleder, eventuelt delegert til systemeier for systemer.
Høy	**Tiltak skal iverksettes snarest**	Det er gjennomført et systematisk og grundig arbeid for å identifisere risikoreduserende tiltak. Alternativ risikohåndtering er svært uhensiktsmessig, gir høyere risiko på dette eller andre områder, eller er svært kostbar. Risikoen kan kun aksepteres av virksomhetsleder og skal rapporteres til overordnet byrådsavdeling.

Tabell 2: Beskrivelse av risikonivåer og kriterier for å akseptere risiko

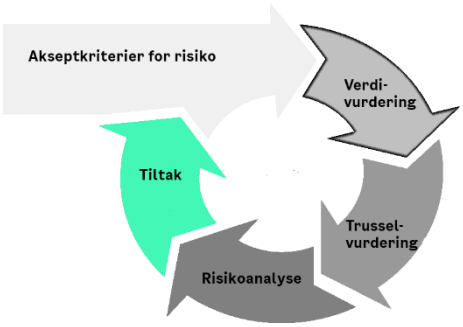
2.2 Omfang og avgrensninger

Det er viktig å klargjøre omfanget av risikovurderingen slik at alle som deltar har samme «bilde» av hva som skal vurderes og for å unngå for omfattende omfang å arbeide med. Avgrensninger og omfang skal dokumenteres. Det er viktig for tydelig å forstå hvilke komponenter, grensesnitt og/eller virksomhetsprosesser som har vært risikovurdert og hvilke som ikke har inngått. Dette gjelder for eksempel ved oppdatering av vurderingen eller

endringer i personell involvert i arbeidet. Det er også viktig for å legge planer for risikovurderinger som ikke er en del av denne.

- Beskriv om risikovurderingen dekker hele eller deler av et IKT-system og hvilke grensesnitt den omfatter.
- Beskriv prosesser/delprosesser. Beskriv funksjonelle, tekniske og/eller organisasjonsmessige avgrensninger.
- Benytt gjerne figurer for å illustrere avgrensninger og omfang.
- Hvis det er enklere å beskrive hva som ikke inngår i omfang enn å beskrive alle elementer som inngår, kan man gjøre dette.

3 Verdivurdering



Verdivurderingen er en kvalitativ vurdering av hvor viktig informasjonen er for virksomheten. Dette omfatter informasjon som lagres og behandles elektronisk, på papir eller som ikke er nedskrevet. Verdivurderingen skal omfatte all informasjon som skal beskyttes, av hensyn til de skadefølger som kan påføres verdien dersom informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.

Så hva betyr brudd på konfidensialitet, integritet og tilgjengelighet?

Konfidensialitet: Dersom det kan få skadefølger om informasjonen blir kjent for uvedkommende, så må informasjonens konfidensialitet beskyttes. Med uvedkommende menes alle som ikke er autorisert for informasjonen, og som ikke har et tjenstlig behov for å være kjent med informasjonen. Om uvedkommende blir kjent med informasjonen anses det som et konfidensialitetsbrudd.

Integritet: Dersom det kan få skadefølger om informasjonen blir endret, så må informasjonens integritet beskyttes. Med integritet menes at informasjonen er korrekt og fullstendig sett i sammenheng med emnet og omfanget som informasjonen har til hensikt å omfatte. Integritetsbeskyttelse innebærer å sørge for at det ikke lar seg gjøre urettmessig å endre innholdet i informasjonen, eventuelt sikre at det blir oppdaget og korrigert om informasjonen er urettmessig endret.

Tilgjengelighet: Dersom det kan få skadefølger om informasjonen går tapt eller blir utilgjengelig, så må informasjonens tilgjengelighet beskyttes. Med tilgjengelighet menes at informasjonen er tilgjengelig for virksomheten innenfor det tidsrommet som virksomheten har behov for å bruke den. Dersom slik informasjon går tapt, eller blir gjort utilgjengelig, anses det som et tilgjengelighetsbrudd. Virksomheten må vurdere tilgjengelighetsbehovene til informasjonen den besitter.

Det er viktig å merke seg at en verdivurdering gjøres for å kunne identifisere behovene for å beskytte informasjonens konfidensialitet, og/eller tilgjengelighet og integritet, og at verdivurderingen i seg selv ikke er tilstrekkelig for å kunne vurdere hvilke konsekvenser brudd eller manglende tiltak på disse vil ha. Resultatene av vurderingen tas derfor med videre i risikovurderingen og inngår i grunnlaget for å bestemme konsekvens av hendelser og valg av tiltak. Forholdet mellom informasjonens behov for konfidensialitet, integritet, og tilgjengelighet vil kunne endres etter omstendighetene. Når det gjelder informasjon av betydning for virksomheten/funksjoner/systemer/mennesker mm, vil slike endringer som oftest være forårsaket av endringer i trusselnivået. Virksomheten må derfor kunne avveie hvilket behov som totalt sett er viktigst å ivareta ifm. sikkerheten til verdien man ønsker å beskytte, eksempelvis informasjon, system, funksjon, og/eller tjeneste. Formålet med verdivurderingen er å vurdere og beskrive hvilken konsekvens tap av konfidensialitet, integritet og tilgjengelighet for informasjonsverdiene i verste fall kan medføre.

Verdivurderingen er et viktig grunnlag i risikovurderingen av en prosess eller et system. Verdivurderingene skal imidlertid også benyttes i sektor/virksomhet for å prioritere hvilke prosesser, systemer og informasjon som virksomheten skal gjøre videre risikovurdering av.

Verdi	Prosess/system	Konfidensialitet	Integritet	Tilgjengelighet
Personalia - ansattopplysninger	Timeregistrerings-system	Lav	Moderat	Moderat
Helseopplysninger - pasienter	Elektronisk pasient - journalsystem	Alvorlig	Svært alvorlig	Svært alvorlig
Tilbudsinformasjon fra tilbyder	Anskaffelses-prosess	Alvorlig	Alvorlig	Moderat

Tabell 3 Eksempel på verdivurdering

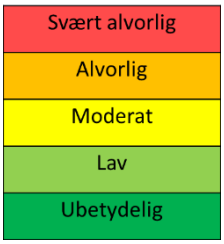
	Hjelpespørsmål til verdivurderingen
Tilgjengelighet	Hvor viktig er det at informasjonen er tilgjengelig? Hva er konsekvensene om informasjonen er utilgjengelig? Hvor lang er kritisk tid for reetablering av prosessen/systemet?
Integritet	Hvor viktig er det at informasjonen er korrekt og til å stole på? Hva er konsekvensene om informasjonen er manipulert – eller har feil? Brukes informasjonen som beslutningsgrunnlag i virksomhetens prosesser?
Konfidensialitet	Er informasjonen underlagt lover, forskrifter eller regelverk som personopplysningsloven, sikkerhetsloven eller offentleglova? Hva er konsekvensene dersom informasjonen blir kjent av uvedkommende?

Tabell 4 Hjelpespørsmål for verdivurdering

Vurderingen benytter en skala med fem konsekvensnivåer (se Figur 2). Konsekvensnivåene beskriver mulig tap eller skade og angir øvre grense for hvor alvorlige en hendelse kan bli. Konsekvens vurderes innenfor følgende kategorier (se også Vedlegg 1):

- Liv og helse
- Økonomi
- Tillit
- Etterlevelse av lover, forskrifter og avtaler
- Måloppnåelse

Konsekvensnivået bestemmes ut fra kategorien som gir mest alvorlig konsekvens.



Figur 2 Konsekvensnivåer

3.1 Konsekvens av utilgjengelighet

Utilgjengelighet av ulike prosesser eller systemer kan gi svært forskjellig konsekvens for tjenestene som prosessene eller systemene skal støtte. For eksempel kan prosesser/systemer som benyttes i medisinsk behandling raskt medføre alvorlige konsekvenser ved utilgjengelighet, mens det ved nedetid for administrative systemer kan ta lengre tid før konsekvensen kommer opp i for eksempel «Alvorlig».

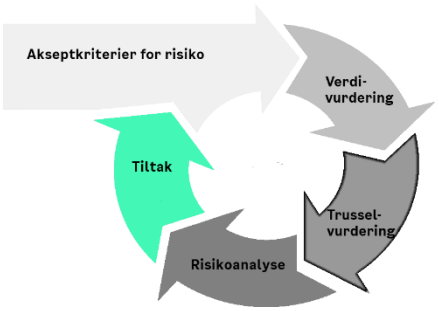
Stopp i en prosess eller nedetid for et system har ikke noen konsekvens i seg selv, men fører til andre konsekvenser som for eksempel tap av liv og helse, økonomisk tap eller tap av tillit til virksomheten eller til Oslo kommune som helhet. Eksempler på hendelser som kan få prosesser til å stoppe, er nøkkelpersonell som blir syke eller utilgjengelige, brukere som glemmer passord og forsinket autorisering av brukere pga. at leder er utilgjengelig. Kostnader til tiltak for å sikre høy tilgjengelighet øker vanligvis ikke lineært men blir relativt sett dyrere når man nærmer seg 100 % tilgjengelighet. Det er derfor viktig å kartlegge hvor lenge en prosess kan stoppe eller et system kan være utilgjengelig før det får alvorlige konsekvenser.

		Konsekvens iht. konsekvensmatrise				Eksisterende tiltak	Kommentar
		Lav	Moderat	Alvorlig	Svært alvorlig		
Bydel							
Hjemme-tjeneste (privat og kommunale utførere, boliger uten bemanning)	Uten tiltak	1 time	2 timer	3 timer	4 timer		Ingen papirbaserte backup-rutiner
	Med eksisterende tiltak	4 timer	8 timer	16 timer	1 dag	Papirutskrift av oppgaver med helseopplysninger om tjenestemottakere, medisinlister	
Saksbehandler	Uten tiltak	3 timer	1 dag	2 dager	3 dager		Hvis man uten tiltak mener uten reserverutiner mot sykehus vil det bli dyrt (overliggerdøgn) men ikke kritisk.
	Med eksisterende tiltak	1 dag	2 dager	3 dager	4 dager	Kan benytte telefon og notere på papir, reserverutiner ved samhandling med sykehus	
Sykehjemsetaten							
Sykehjem	Uten tiltak	4 timer	6 timer	8 timer	1 dag		Ingen papirbaserte backup-rutiner
	Med eksisterende tiltak	6 timer	8 timer	1 dag	2 dager	Papirutskrifter av beboeropplysninger	

Tabell 5 Eksempel på konsekvens av nedetid for et elektronisk pasientjournalsystem

Konsekvens av nedetid skal utarbeides for alle systemer som gjennomgår risikovurdering og kan utarbeides for prosesser. Resultatet skal dokumenteres i regnearket.

4 Trusselvurdering



Formålet med trusselvurderingen er å identifisere og vurdere trusler som kan føre til uønskede hendelser. Vi skiller mellom trusselaktører, altså mennesker eller grupper av mennesker, som med overlegg utfører ondsinnede handlinger, og trusselfenomener som skjer tilfeldig og uten intensjon om å påføre skade.

Under trusselvurderingen vil aktuelle trusselaktører og -fenomener identifiseres og egenskapene ved truslene beskrives. Regnearket beregner et foreslått trusselnivå av fem mulige nivåer, hvor nivåene er vist i Figur 3. Mer detaljer om denne beregningen kan finnes i vedlegg 3. Hvis de som utfører trusselvurderingen er uenig i beregningsresultatet, går det an å overstyre det med en manuell vurdering.

5 - Svært høyt
4 – Høyt
3 – Middels
2 – Lavt
1 – Ubetydelig

Figur 3 Trusselnivåer

4.1 Trusselaktører

En trusselaktør er et individ eller en gruppe individer med en mulig intensjon som gjennom bevisste handlinger ønsker å ramme virksomhetens funksjon og verdier.

Eksempler på trusselaktører kan være:

- fremmed etterretning,
- ressurssterke organiserte kriminelle,
- vinningskriminelle som opererer enkeltvis,
- utro ansatte,
- aktivister.

Vurdering av trusselnivået skjer ut fra egenskaper ved aktøren, som avgjør i hvilken grad aktøren utgjør en reell fare eller ikke. Tabell 6 viser indikatorene som vurderes for å fastsette trusselnivået.

Indikator	Beskrivelse
Tilstedeværelse	Aktøren antas å være i stand til å nå virksomheten og ansatte, enten fysisk eller via elektroniske nettverk
Kapasitet	Tilegnet, antatt eller demonstrert evne til å utføre uønskede handlinger
Intensjon	Aktøren har, eller kan antas å ha en vilje til og/eller ønske om å utføre uønskede handlinger
Historikk	Aktøren har stått bak påviselig aktivitet over tid
Målvalg	Virksomheten antas å være et utsatt og attraktivt mål for aktøren

Tabell 6 Indikatorer for trusselaktører

4.2 Trusselfenomener

Trusselfenomener oppstår naturlig eller som resultat av tilfeldigheter, og kan for eksempel være:

- menneskelige feil/vanvare,
- systemfeil,
- brann,
- vannskade, ekstremvær.

Indikatorene for trusselfenomener er litt annerledes enn for trusselaktører, se vedlegg 3.

Indikator	Beskrivelse
Potensial	Fenomenet kan gi betydelige skader på virksomhetens verdier
Forutsetninger	Alle forutsetninger er til stede for at fenomenet kan inntreffe
Utbredelse	Fenomenet er velkjent og vanlig i virksomheten eller i miljøer som kan sammenliknes med virksomheten
Historikk	Fenomenet har inntruffet tidligere i virksomheten
Omstendigheter	Virksomheten er spesielt utsatt for fenomenet

Tabell 7 Indikatorer for trusselfenomener

Trusselnivået for de enkelte trusselaktører og trusselfenomener blir brukt som støtte i senere steg i risikovurderingen, men inngår ikke i automatisk beregning av risiko i risikovurderingsverktøyet.

4.3 Eksempel

Tabell 8 viser et eksempel på trusselvurderinger av fenomen (brann, syk nøkkelmedarbeider) og en aktør (organiserte vinningskriminelle). De ulike områdene (tilstedeværelse, potensial, etc.) er nærmere forklart i regnearkverktøyet.

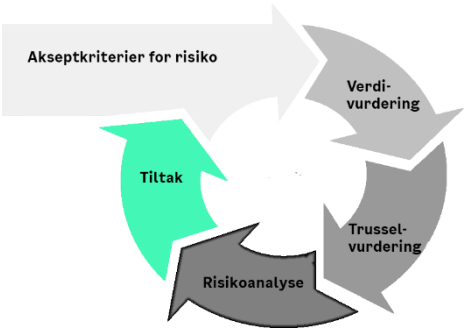
Brannfaren blir i eksempelet beregnet til en lav trussel da det er krysset av for kun potensial og forutsetninger for å inntreffe. I eksemplet tenker vi oss at det ikke er utbredelse, historikk eller andre omstendigheter som gjør at virksomheten er spesielt utsatt for brann.

Trusselen «organiserte vinningskriminelle» er til stede da virksomhetens systemer kan nås via Internett. Det er observert andre angrep via epost mot liknende systemer og det antas at aktøren har kapasitet, for eksempel med løsepengevirus, direktørsvindel eller annet. Det antas videre at intensjonen er til stede siden vinningskriminelle ønsker å utnytte sårbarheter som kan føre til økonomisk gevinst. Eksempelsystemet er ikke et mer opplagt mål enn andre systemer, slik at det ikke krysses av for «Målvalg». Denne trusselen blir derfor beregnet til høy.

Trussel	Type	Tilstede-værelse	Kapasitet	Intensjon	Historikk	Målvalg	Trussel-nivå
		Potensial	Forut-setninger	Utbredelse	Historikk	Omstendig-heter	
Brann	**Fenomen**	**X**	**X**				**2 – Lavt**
Organiserte vinnings-kriminelle	**Aktør**	**X**	**X**	**X**			**4 – Høyt**
Syk nøkkel-medarbeider	**Fenomen**	**X**	**X**	**X**	**X**		**4 – Høyt**

Tabell 8 Eksempel på trusselvurdering

5 Risikoanalyse



I risikoanalysen vurderes hvor stor konsekvensen blir dersom ulike uønskede hendelser inntreffer - og hvor sannsynlig det er at hendelsene inntreffer. Dette dokumenteres i regnearket og det beregnes automatisk en risikoverdi for hver hendelse.

Det kan være greit å ha i bakhodet når man arbeider med risikoanalyse:

- Hvis verdien er lav, blir risikoen lav (på grunn av lav konsekvens)
- Hvis truslene og/eller sårbarhetene er små, blir risikoen lav (på grunn av lav sannsynlighet)

Identifisere uønskede hendelser

Først identifiseres uønskede hendelser - dette gjøres vanligvis i et arbeidsmøte (workshop) for risikoanalyse. Til dette møtet bør man invitere relevante deltakere med førstehåndskjennskap til prosessen eller systemet som vurderes – systemeier, systemforvalter, linjeleder, ulike grupper av ansatte eller brukere og/eller driftsansvarlige.

De enkelte deltakere tar utgangspunkt i

- sine erfaringer fra bruk/forvaltning/drift,
- kjennskap til sårbarheter ved prosessen, systemet eller omgivelsene,
- nylige endringer av aktiviteter eller funksjonalitet etc.

Det kan være lurt å begynne med uønskede hendelser for verdiene med størst taps-/skadepotensial og de største truslene.

Hendelsene som trusselaktørene og -fenomenene kan forårsake, kan påvirke konfidensialitet, integritet og/eller tilgjengelighet (se også Tabell 5). Tenk derfor gjennom på hvilken måte ulike trusler kan føre til konsekvenser for verdiene på disse tre områdene, for eksempel:

- En vinningskriminell kan tenkes å skaffe seg innsyn om kjendiser i pasientjournaler eller om tilbydere i en anbudsprosess (konfidensialitet)
- En misfornøyd tjenestemottaker kan ønske å gjøre hærverk med å endre informasjon i et pasientjournalsystem (integritet)
- En oppdatering av programvare for en applikasjon som feiler, kan føre til utilgjengelighet av applikasjonen (tilgjengelighet)

Husk å begrense hendelsene til det beskrevne omfanget av risikovurderingen. Det skjer lett at engasjerte deltakere kommer på uønskede hendelser rundt prosess eller system som ligger utenfor definert omfang – og tar med disse videre i risikovurderingen.

5.1 Beskrivelse av hendelsene

Å formulere hendelser på en god måte krever en viss trening. Her er noen eksempelbeskrivelser;

A	B	C	D	E	F	G
RiskID	**Scenariobeskrivelse**	**Konsekvensbeskrivelse (Eksisterende tiltak/sårbarhet, konsekvens og hhv. KIT)**	***Konse-kvens***	**Beskrivelse av estimert sannsynlighet (Eksisterende tiltak/sårbarhet og sannsynlighet) '**	***Sannsyn-lighet***	***Risiko (låst)***
1	Feil i EPJ-applikasjonen fører til at systemet er utilgjengelig for alle brukere	De ansatte får ikke utført arbeidsprosesser i EPJ. Papirbasert nødrutine fungerer tilfredsstillende når systemet er utilgjengelig. Ved nedetid utenfor arbeidstid kan varsling ta lengre tid. Nødrutine krever ekstra ressurser, og øker sannsynligheten for at uønskede hendelser oppstår.	Moderat	Frekvens: Dette er forventet å inntreffe sjeldnere enn en gang per år. Det er knyttet noe usikkerhet rundt hvorvidt det er feil i applikasjonen som forårsaker slike feil.	Meget liten	Middels
2	Uforutsette feil etter planlagt endring eller oppgradering i driftsmiljøet fører til nedetid i EPJ. Dette oppstår som følge av systemfeil, mangelfull testing eller andre menneskelige feil.	De ansatte får ikke utført arbeidsprosesser i EPJ. Papirbasert nødrutine fungerer tilfredsstillende når systemet er utilgjengelig. Ved nedetid utenfor arbeidstid kan varsling ta lengre tid. Nødrutine krever ekstra ressurser, og øker sannsynligheten for at uønskede hendelser oppstår.	Moderat	Frekvens: Basert på tidligere erfaring, inntreffer dette tilnærmet månedlig. Skjedd flere ganger at oppgraderinger ikke feiler under test, men fører til store feil i produksjonsmiljø.	Stor	Middels
3	Personopplysninger og helseopplysninger skrevet på papir kommer på avveier grunnet utstrakt bruk av papirbasert reserveløsning.	Sensitive personopplyninger kan leses av uvedkommende. Større mengder opplysninger på avveie krever en villet handling der sikkerhetsinnstillinger reduseres eller omgås.	Alvorlig	Papirbaserte nødrutiner er innarbeidet og implementert. Det antas at det varierer mellom bydelene hvor godt rutinene er implementert.	Moderat	Høy
4	Mangelfullt utfylling av autorisasjonskjema for applikasjon fører til urettmessig utdeling av tilganger	Ansatte og private tjenesteleverandører får for vide tilganger. Brudd på intern instruks og muligens lovbrudd.	Moderat	Det er flere kjente tilfeller, forventes månedlig	Stor	Middels
5	Konfigureringsfeil hos leverandør fører til at uvedkommende klarer å logge inn i systemet	Her kan sensitive opplysninger kan komme på avveier, også informasjon fra andre kommuner	Alvorlig	Et kjent tilfelle der sertifikat på webserver var feilkonfigurert. Ikke kjent hvor godt leverandøren er rustet mot slike hendelser	Moderat	Høy
6	Ansatt logger på systemet og uvedkommende kan se (også se skulderen)	Sensitiv informasjon kommer på avveie, men er begrenset til kun det som er aktivt på skjerm.	Lav	Presentasjon av plan på storskjerm kan føre til eksponering av informasjon.	Liten	Lav
7	Mangelfull rutine for internkontroll fører til at urettmessig bruk av og tilgang til informasjon i applikasjon ikke oppdages	Redusert sporbarhet. Brudd på etterlevelse av internt regelverk. Kan også føre til at man ikke oppdager brudd	Moderat	Mangler rutine for å avdekke brudd. Høy grad av usikkerhet. SIkkerhetstiltak er ikke etablert.	Svært stor	Høy

Utfordringen er å utarbeide beskrivelser av uønskede hendelser som er passe generelle;

- Ikke så generelle at de blir lite konkrete og alt for mange tiltak er aktuelle
- Ikke så spesifikke at det blir veldig mange nesten like hendelser

Hvis man ender opp med mange hendelser som likner på hverandre, kan man med fordel velge en med høy sannsynlighet og/eller hendelsen med høyest konsekvens (men prøv å unngå ekstreme hendelser med svært lav sannsynlighet).

5.2 Risikoanalyse

5.2.1 Sårbarhetsvurdering

Sårbarhet vurderes i forbindelse med analyse av konsekvens av og sannsynlighet for hver enkelt hendelse. I en sårbarhetsvurdering vurderer man om prosessen/systemet mangler tiltak som kan stå imot truslene eller tiltak som reduserer konsekvensene.

En sårbarhet er altså noe som gjør at informasjonsverdien er mer utsatt for hendelsen, eller at konsekvensen blir større enn nødvendig. F eks er en virksomhet mer utsatt for stopp i en prosess hvor bare en person innehar en viktig kompetanse, mer utsatt for virusangrep på systemer som ikke har antivirusprogram og mer utsatt for datatap over lang tid dersom det ikke utføres sikkerhetsovervåking.

Sårbarheter omfatter prosessuelle, tekniske, organisatoriske eller menneskelige sårbarheter. Tenk gjennom og dokumentèr hvilke sårbarheter som er aktuelle akkurat for denne hendelsen i denne prosessen eller dette IKT-systemet, som er under risikovurdering. Noen eksempler kan være:

- Mangel på opplæring
- Mangelfull planlegging og styring av sikkerhetsarbeidet
- Avtaler beskriver i liten grad roller og ansvar knyttet til informasjonssikkerhet
- Manglende sikkerhetsoppdatering av programvare
- Sikkerhetsmessige forhold logges ikke

Etter dette kan man også bruke standardiserte sjekklister. Tips til sårbarheter kan man få fra for eksempel

- Digdir: https://www.digdir.no/informasjonssikkerhet/trinn-3-vurder-trusler-farer-og-sarbarheter/2645 eller
- NSM (basert på mangel på tiltak): https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/nyheter-fra-ncsc/digital-beredskap-i-en-skjerpet-situasjon/

Det er også lurt å dokumentere viktige sikkerhetstiltak som allerede er iverksatt og reduserer risiko i prosessen eller IKT-systemet som er under risikovurdering, se eksempel i figuren på neste side. Dette reduserer faren for å utrede tiltak som allerede er innført, forbedrer muligheten til å se tiltak i sammenheng og forenkler arbeidet for eventuelt nye medarbeidere som skal vedlikeholde risikovurderingen i ettertid.

Trussel (nedtrekk)	Trusselnivå (beregnet)	Beskriv relevante sårbarheter (menneskelige, organisatoriske, tekniske) som reduserer evnen til å motstå en trussel	Eksisterende tiltak
Ekstern hacker - løsning blir hacket med ønske om økonomisk vinning av en kjent kriminell organisasjon.	4 - Stor	Tekniske sårbarheter i infrastruktur.	Patching av sårbarheter i programvare iht. alvorlighet/hast.
		Tekniske sårbarheter i applikasjon.	Periodisk sårbarhetsscanning av eksterne tjenester.
		Mangelfull kontroll av kontonummer før utbetaling.	

5.2.2 Konsekvens

Konsekvensen av en uønsket hendelse beskriver hvor alvorlig hendelsen vil være for verdier. Konsekvensnivået vurderes ut fra:

- Hvilke verdier som påvirkes av hendelsen med hensyn til konfidensialitet, integritet og/eller tilgjengelighet?
- Hvor alvorlig er hendelsen i henhold til konsekvenstabellen (Vedlegg 1)?
- Finnes det tiltak som er implementert for å begrense konsekvensen? Beskriv i så fall dette i kolonnen «Eksisterende tiltak», ref. også forrige underkapittel.
- Velg den konsekvensindikatoren i konsekvenstabellen som gir høyest verdi på konsekvens når det er tatt hensyn til tiltak som allerede er implementert. Legg så denne verdien inn i regnearket ved å velge tilsvarende verdi i nedtrekksmenyen for feltet «Konsekvens».

5.2.3 Sannsynlighet

Sannsynlighet beskriver hvor ofte og hvor lett en hendelse kan forventes å inntreffe i fremtiden. Sannsynlighet kan baseres på flere faktorer:

- Hvor reell er trusselen som utløser den uønskede hendelsen? Svar på det finnes i trusselvurderingen.
- Hvor sårbar er virksomheten overfor hendelsen? Hvilke tiltak er allerede implementert for å begrense sannsynligheten? Skriv i tilfelle en begrunnelse om slike tiltak i feltet «Begrunnelse for sannsynlighet» i regnearket.
- Tabell for sannsynlighet (se Vedlegg 2) kan hjelpe ved å se på frekvens og letthet ("hvor ofte kan det skje, og hvor lett skjer det"?)
- Velg den sannsynlighetsindikatoren som gir størst sannsynlighet når det er tatt hensyn til tiltak som allerede er implementert. Legg så denne verdien inn i regnearket ved å velge tilsvarende verdi i nedtrekksmenyen for feltet «Sannsynlighet».

I sannsynlighetstabellen er de to første kolonnene (Forventning og Estimert sannsynlighet) mest hensiktsmessig å benytte dersom det finnes statistikk på området eller personell har erfaring med prosessen/systemet som man kan ta utgangspunkt i.

De tre siste kolonnene, under «Hvor lett skjer det?» er mer hensiktsmessige å bruke dersom man ikke har statistikk fra eller erfaring med en prosess eller et system, f.eks. ved risikovurdering av nyetablerte systemer.

5.3 Resultat av risikoanalyse

Etter gjennomføring av risikoanalysen vil hver uønsket hendelse ha fått en risikoverdi i regnearket. Risikoen er beregnet ut fra konsekvens og sannsynlighet fra analysen. Risikoverdi og «farge» overensstemmer med de tre risikonivåene i virksomhetens risikomatrise, som gjenspeiler akseptkriteriene (se eksempel i Tabell 9).

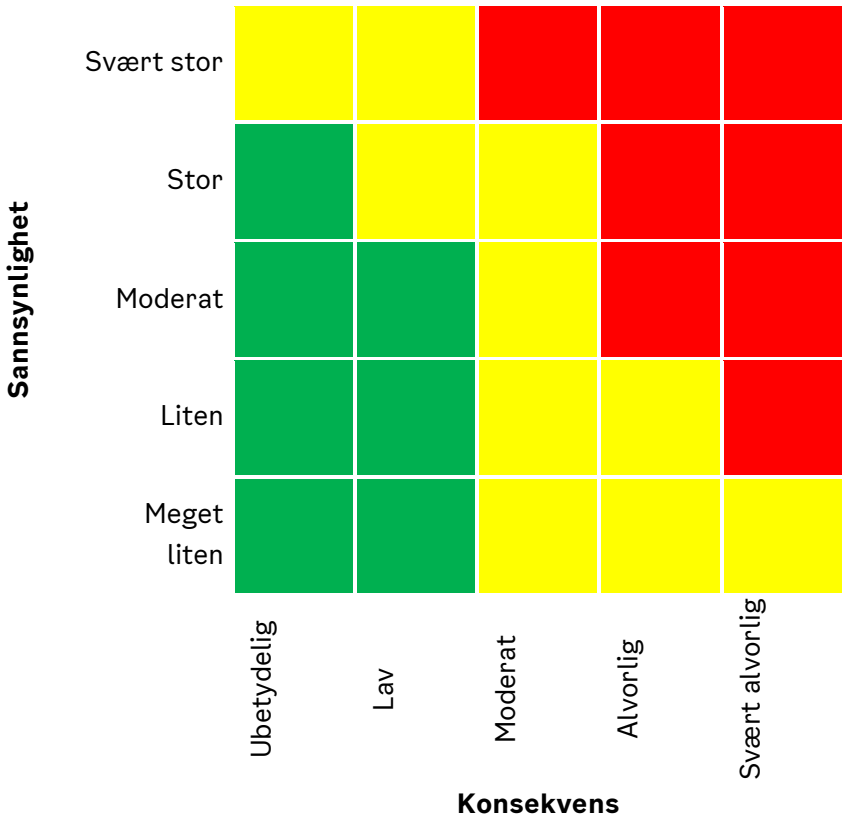
Uønsket hendelse	Begrunnelse av konsekvens	Konse-kvens	Begrunnelse av sann-synlighet	Sannsyn-lighet	Risiko
Brann i datasenter fører til tap av data og nedetid.	Redusert sårbarhet pga. redundant datasenter	Lav	Forventes å inntreffe sjeldnere enn én gang i året.	Meget liten	Lav
Ansatt klikker på en e-post som utløser løsepengevirus fra infisert e-post.	Sikkerhetskopier gjør at data ikke går tapt, men noe nedetid og merarbeid er forventet.	Moderat	Forventes å inntreffe omtrent månedlig.	Stor	Middels
Ansatt legger igjen papirdokumenter med helseopplysninger om tjenestemottaker som kan leses av rengjøringspersonell	Begrenset mengde personopplysninger. Rengjøringsperson ell har signert taushetserklæring og har rutiner for behandlinger av slike funn.	Moderat	Forventes å inntreffe omtrent månedlig.	Stor	Middels

Tabell 9 Eksempel på risikoanalyse

5.4 Risikomatrise

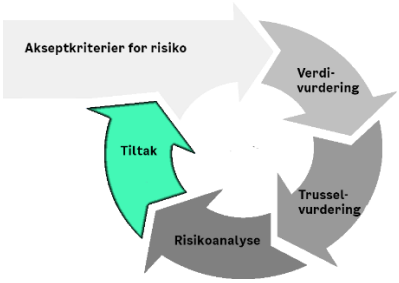
Risiko beskrives som konsekvens av og sannsynlighet for at en uønsket hendelse skal inntreffe. Hendelsene presenteres i en matrise, som illustrerer risikonivået. Å plassere hendelsene i en felles matrise, gjør det enklere å sammenligne risiko.

Følgende kombinasjoner av nivå på konsekvens og sannsynlighet brukes for å beskrive risikonivå:



Figur 4 Risikomatrise

6 Tiltak og annen håndtering av risiko



6.1 Strategier for håndtering av risiko

Det finnes ulike strategier for å håndtere risikoen ved en hendelse. Prøv å tenke igjennom de ulike mulighetene, som er

1. redusere risiko, som typisk er tiltak for å redusere konsekvens av eller sannsynlighet for risikoen
2. overføre risiko, ved f. eks. å dele kostnaden med leverandør eller forsikringsselskap
3. akseptere risiko, ved å bringe det til ledelsen som godkjenner å fortsette til tross for risikoen
4. unngå risiko, som betyr at vi ikke finner tiltak og må unngå å gjøre «oppgaven» som forårsaker risikoen (ofte siste utvei)

Som oftest vil det være naturlig å håndtere risiko ved uønskede hendelser gjennom å innføre risikoreduserende tiltak.

6.2 Identifisering av tiltak

Forslag til tiltak kartlegges gjerne gjennom idemyldring i arbeidsmøter, men kan også foreslås basert på tidligere erfaringer hos møtedeltakerne eller på intervjuer av andre personer med relevant erfaring. Det kan benyttes standard sjekklister for sikkerhetstiltak basert på beste praksis, se også

.

Forslag til tiltak dokumenteres i regnearket. Det er gitt et par eksempler på tiltak i Tabell 1 nedenfor. Konsekvens og sannsynlighet før tiltak er utelatt fra eksemplet for å gi større skriftstørrelse og bedre lesbarhet.

Det skal settes inn tiltak mot uønskede hendelser i rødt felt i risikomatrisen. Hendelser i gult felt skal alltid vurderes for om det skal settes inn tiltak. Som et minimum må risikoen overvåkes eller følges opp. Det er ikke påkrevet å innføre tiltak for hendelser med Lav/grønn risiko.

Denne veilederen fokuserer på tiltak som reduserer risiko. Dette handler vanligvis om å redusere sårbarhet overfor truslene fordi det er vanskelig å påvirke trusler. Tiltak kan redusere sannsynligheten for og/eller konsekvensen av om hendelsen inntreffer.

Tiltakene som foreslås gjennomført vil påvirke restrisikoen. Denne er basert på konsekvens og sannsynlighet etter tiltak. Som tidligere benyttes skalaene fra risikomatrisen. Det anbefales å fylle ut konsekvens og sannsynlighet «etter tiltak» etter at alle tiltakene er lagt inn i regnearket. Informasjon om restrisiko kan være til hjelp ved prioritering av tiltak. Både tiltak med foreslått prioritet 1 og 2 tas med når restrisiko estimeres ved dette steget i prosessen.

Uønsket hendelse	Tiltak	Tiltaks-ansvarlig	Frist	Prior-itet	Konsekvens etter tiltak	Sannsynlig-het etter tiltak	Rest-risiko
Bruker utløser løsepenge-virus fra mottatt infisert e-post.	Innføre applikasjons-hvitelisting			1	Meget liten	Lav	Lav
	Redusere tid for gjen-oppretting			2			
Nøkkel-person er i koma og innlagt i 2 uker	Kritisk kompetanse er dublert hos minst 2 personer			1	Liten	Lav	Lav
	Viktig informasjon er dokumentert			2			

Tabell 1 Eksempel på tiltak for risikohåndtering

Ved avslutning av denne aktiviteten overleveres resultatene av risikovurderingen til henholdsvis leder som er ansvarlig for prosessen eller systemeier/-forvalter for systemet, for kostnadsestimering, prioritering og planlegging av tiltak.

6.3 Prioritering og planlegging av tiltak

Det kan bli foreslått mange tiltak. Det er fornuftig å prioritere tiltakene ut fra hvor god effekt de har for å redusere risikoen. Videre er det viktig å sikre at en person (med en gitt rolle i en virksomhet) er ansvarlig for gjennomføring av tiltaket. For prosesser er prioritering leders ansvar. For systemer er prioritering systemeiers ansvar, men foreslås ofte av systemforvalter. Følgende kriterier benyttes for grov prioritering av tiltakene:

- Prioritet 1: Tiltaket skal gjennomføres snarest
- Prioritet 2: Tiltaket skal gjennomføres
- Prioritet 3: Tiltaket prioriteres ikke

Prioritet legges inn for de foreslåtte tiltakene i regnearket, ref. eksempel i Tabell 1. Dette vil være en foreløpig prioritering før kostnader er vurdert.

6.3.1 Ansvar for gjennomføring av tiltak

Ansvarlig for å gjennomføre et tiltak vil i mange tilfelle være en annen person enn leder med ansvar for prosessen eller systemeier fordi tiltaket er lokalisert i en annen avdeling eller virksomhet. Leder eller systemeier, eller systemforvalter på vegne av systemeier, må lage et forslag til hvilke roller/virksomheter som vil være ansvarlig for å gjennomføre de ulike tiltakene. Tiltak og ressurssituasjon må avklares med de som skal gjennomføre tiltakene. Ansvarlig rolle/virksomhet legges inn i regnearket.

6.3.2 Kostnadsestimering av tiltak

De høyest prioriterte tiltakene bør kostnadsestimeres for å komme frem til en endelig prioritering. Rolle/virksomhet som er ansvarlig for å gjennomføre et tiltak, bør gjennomføre kostnadsestimeringen av tiltaket.

6.3.3 Endelig prioritering av tiltak og godkjenning av restrisiko

Arbeid som bør utføres etter kostnadsestimering:

1. Leder eller systemeier bør be om bekreftelse fra de ulike tiltaksansvarlige på at de vil gjennomføre tiltakene og bli enige om en frist for hvert tiltak. Finansiering av nye tiltak må avklares.
2. Det skal nå være enighet om hvilke tiltak som skal gjennomføres, og finansiering skal være besluttet/godkjent av rette fora.
3. Sannsynlighet og konsekvens etter tiltak oppdateres for hendelsene i regnearket basert på godkjente tiltak, og restrisiko blir automatisk beregnet.
4. Dersom det nå finnes risikoer utenfor akseptabel risiko (grønt felt), skal restrisiko godkjennes av leder/systemeier på nivå i henhold til Tabell 2.

6.4 Planlegging og oppfølging

Gjennomføringsplan utarbeides av henholdsvis leder med ansvar for prosessen eller systemeier, eller forvalter på vegne av systemeier, og inkluderer ansvarlige og tidsfrister for tiltakene. Det kreves ikke en separat plan - oppgavene kan om ønskelig tas inn som en del av endringsprosjekt i virksomheten eller forvalters endringsplan for systemet.

Leder eller systemeier, eller forvalter på vegne av systemeier, må deretter følge opp at de ulike tiltakene blir gjennomført innenfor fristene man har blitt enige om. Det vil være en fordel om man avtaler at tiltaksansvarlig skal rapportere til leder/systemeier/systemforvalter når et tiltak i planen er gjennomført.

Status for gjennomføring av tiltak kan oppdateres i regnearket i kolonnen «Status» med verdiene

- Ikke planlagt
- Planlagt
- Pågående
- Fullført

7 Dokumentasjon og kommunikasjon av resultater

7.1 Utarbeidelse av rapport

Det anbefales å utarbeide en sluttrapport som dokumenterer resultatene av risikovurderingen av prosess/system. Hensikten er å gjøre resultatene lettere tilgjengelig for lesere som ikke har deltatt i aktivitetene og for ledere og tilsynsmyndigheter ved behov.

Rapporten bør som minimum beskrive følgende:

- kort introduksjon til prosessen/systemet
- deltakere i risikovurderingen
- omfang av risikovurderingen
- kort beskrivelse av fremgangsmåte
- viktigste risikoer
- viktigste tiltak med ansvarlige og tidsfrister
- akseptert restrisiko etter gjennomføring av besluttede tiltak

Det er utarbeidet en mal for slike rapporter som vil bli lagt ut på kommunens felles intranett.

7.2 Beskyttelse og kommunikasjon av risikovurderingen

Rapporten vil normalt inneholde informasjon om sårbarheter og skal beskyttes mot uautorisert innsyn. Tilgang til rapporten og til underliggende informasjon fra risikovurdering, skal kun gis iht. tjenstlig behov. Rapporten bør lagres/arkiveres sammen med underliggende regneark og med korresponderende versjonsnumre.

Rapporten skal inngå i grunnlaget for ledelsens gjennomgang og virksomhetsleders egenerklæring.

7.3 Godkjenning av risikovurderingsrapporten

Det er viktig at virksomhetsleder/systemeier er kjent med og har forstått innholdet i rapporten. Virksomhetsleder/systemeier har ansvar for å godkjenne denne.

8 Vedlegg

Vedlegg 1– Kriterier for konsekvens (Eksempel fra HEI-sektor)

Konsekvenskategorier og -nivåer					
	Liv og helse	**Økonomi**	**Tillit**	**Etterlevelse av lov, forskrift og avtaler**	**Måloppnåelse**
Svært alvorlig	Dødsfall eller flere personer rammes av alvorlig varig funksjons-nedsettelse eller skade.	Tap/skade på over 5 millioner kroner for virksomheten.	Langvarige og svært negative oppslag i riksdekkende media. Vesentlig tap av tillit hos innbyggere og samfunnet.	Kan medføre eller bidra til alvorlig brudd på lov, forskrift eller annet regelverk.	Manglende oppnåelse av kritiske mål for virksomheten.
Alvorlig	Alvorlig personskade eller varig funksjons-nedsettelse.	Tap/skade mellom 1 og 5 millioner kroner for virksomheten.	Negative oppslag i riksdekkende media over flere dager. Tap av tillit hos innbyggere og samfunnet.	Kan medføre eller bidra til brudd på lov, forskrift eller annet regelverk.	Manglende oppnåelse av mindre kritiske mål for virksomheten.
Moderat	Mindre alvorlig personskade.	Tap/skade mellom 250.000 og 1 mill. kroner for virksomheten.	Mindre eller kortvarige oppslag i media.	Kan medføre eller bidra til mindre alvorlige brudd på lov, forskrift eller annet regelverk. Kan medføre brudd på intern instruks eller reglement.	Moderat innvirkning på oppnåelse av virksomhetens mål.
Lav	Småskader	Tap/skade mellom 50.000 og 250.000 kroner for virksomheten.	Henvendelse fra media uten negative oppslag.	Kan medføre brudd på intern instruks eller reglement, uten at dette medfører brudd på lov, forskrift eller annet regelverk.	Liten innvirkning på oppnåelse av virksomhetens mål.
Ubetydelig	Ingen skade	Tap/skade på mindre enn 50.000 kroner for virksomheten.	Ubetydelig påvirkning fra media.	Påvirker ikke etterlevelse.	Ubetydelig innvirkning på oppnåelse av virksomhetens mål.

Vedlegg 2 – Kriterier for sannsynlighet (Eksempel fra HEI-sektor)

Sannsynlighetskategorier og -nivåer					
	Hvor ofte skjer det?		**Hvor lett skjer det?**		
	Forventning	**Estimert sannsynlighet**	**Sårbarhet**	**Kapasitet og evne**	**Intensjon**
Svært stor	Forventes å inntreffe tilnærmet ukentlig.	Hendelsen vil oppstå under de fleste omstendigheter (inntreffer med over 70 % sannsynlighet)	Sikkerhetstiltak er ikke etablert eller fungerer ikke etter hensikten	Sikkerhetstiltak kan omgås eller brytes av egne medarbeidere og eksterne: • Med små til normale ressurser • Uten kjennskap til tiltakene	Egne medarbeidere og eksterne opptrer med ubetenksomhet, eller hendelsen skjer ved uhell
Stor	Forventes å inntreffe tilnærmet månedlig.	Hendelsen kan oppstå under flere omstendigheter (inntreffer med 30 – 70 % sannsynlighet)	Sikkerhetstiltak er i noen grad etablert eller det er usikkert om de fungerer etter hensikten	Egne medarbeidere • små til normale ressurser • uten kjennskap til tiltakene Eksterne • små til normale ressurser • kjennskap til tiltakene	Egne medarbeidere opptrer med ubetenksomhet, eller hendelsen skjer ved uhell Eksterne bryter sikkerhetstiltakene bevisst.
Moderat	Forventes å inntreffe minst kvartalsvis.	Hendelsen kan oppstå under noen omstendigheter (inntreffer med 10 – 30 % sannsynlighet)	Sikkerhetstiltak er delvis etablert, og fungerer delvis etter hensikten	Egne medarbeidere • små til normale ressurser • noe kjennskap til tiltakene • uten kompetanse Eksterne • normal til gode ressurser • god kjennskap til tiltakene	Egne medarbeidere bryter sikkerhetstiltakene bevisst. Eksterne planlegger og bryter sikkerhetstiltakene.
Liten	Forventes å inntreffe årlig.	Hendelsen kan oppstå under sjeldne omstendigheter (inntreffer med 5 – 10 % sannsynlighet)	Sikkerhetstiltak er etablert etter sikkerhetsbehovet og fungerer etter hensikten	Egne medarbeidere • små til normale ressurser • kjennskap til tiltakene • en viss kompetanse Eksterne • gode ressurser og spisskompetanse • fullstendig kjennskap til tiltakene	Egne medarbeidere bryter sikkerhetstiltakene bevisst. Eksterne planlegger over lengre tid og bryter sikkerhetstiltakene.
Meget liten	Forventes å finne sted sjeldnere enn en gang pr år.	Hendelsen vil kun oppstå under helt spesielle omstendigheter (inntreffer med under 5 % sannsynlighet)	Sikkerhetstiltak er etablert etter sikkerhetsbehovet og det kontrolleres at de fungerer etter hensikten	Tiltakene kan kun brytes av egne medarbeidere • med gode ressurser, • god/fullstendig kjennskap til tiltakene. Eksternt personell kan kun omgå eller bryte tiltakene med hjelp fra interne.	Egne medarbeidere planlegger og bryter sikkerhetstiltakene.

Vedlegg 3 – Trusselvurdering

Følgende tabeller viser innebygde beregninger for trusselvurdering i regneark for risikovurdering. Følgende indikatorer benyttes for henholdsvis aktører og fenomener (se Tabell 6 Indikatorer for trusselaktører og **Feil! Fant ikke referansekilden.** for beskrivelse av disse):

Indikator	Aktør	Fenomen
A	**Tilstedeværelse**	**Potensial**
B	**Kapasitet**	**Forutsetninger**
C	**Intensjon**	**Utbredelse**
D	**Historikk**	**Historikk**
E	**Målvalg**	**Omstendigheter**

Tabell 2 Indikatorer for aktører og fenomener

Kriterier for trusselaktører	Trusselnivå
Kriteriene A, B, C og E er tilstede.	**Svært høyt**
Kriteriene A, B og C eller A, D og E (i tillegg til at enten B eller C er tilstede.	**Høyt**
Kriteriene A, D og E eller A og B (i tillegg til enten D eller E) eller A og C (i tillegg til enten D eller E) er tilstede	**Middels**
Kun kriteriene A og B er tilstede eller A og en av C, D eller E er tilstede	**Lavt**
Kriteriene A eller B er tilstede	**Ubetydelig**

Tabell 3 Kriterier for trusselnivå for aktører

Kriterier for trusselfenomener	Trusselnivå
Kriteriene A, B, C og E eller A, B, D og E er tilstede.	**Svært høyt**
Kriteriene A, B, C og D er tilstede.	**Høyt**
Kriteriene A, B og C eller A, B og E er tilstede.	**Middels**
Kriteriene A og B er tilstede.	**Lavt**
Kriteriene A eller B kan være tilstede	**Ubetydelig**

Tabell 4 Kriterier for trusselnivå for fenomener

Vedlegg 4 - Sjekkliste for gjennomføring av risikovurdering

Før møtene

- Avklare med aktuell leder eller systemeier/systemforvalter:
  - Omfang av risikovurderingen
  - Mål, tidsperspektiv, kriterier for sannsynlighet og konsekvens
  - Deltakere; ingen fasitsvar, men mellom 5 og 10 anbefales. Typisk
    - Leder med ansvar for prosessen, eller systemeier og systemforvalter(e)
    - Ansatte eller andre som utfører prosessen eller bruker systemet
    - Driftspersonell, f.eks. hos UKE
    - Informasjonssikkerhetskoordinator
    - Sikkerhetsansvarlig hos driftsleverandør
    - Relevante linjeledere
    - Eventuelt egen/egne fasilitator(er)
  - Rammer og tidspunkt for workshoper (dato og klokkeslett som passer for deltakerne)
- Sette opp agenda for møtene:
  - Verdi- og trusselvurderingsmøte med leder, eller systemeier og -forvalter
  - Risikovurderingsworkshop 1 og 2
  - Risikohåndteringsworkshop
- Innkalle til workshoper, og eventuelt avtale intervju med enkeltpersoner for å kartlegge risikoer
  - Husk å informere i epost personer som blir innkalt om hvorfor de blir innkalt til risikovurdering og evt. hvem som har oppgitt dem
  - Sende med eventuell underlagsinformasjon, som for eksempel agenda, dokumentasjon, rapporter knyttet til den aktuelle prosessen / det aktuelle systemet, evalueringer etc.

I verdivurderings- og trusselvurderingsmøtet

- Presentere metodikk for risikovurdering
- Identifisere informasjonsverdier. Vurdere taps-/skadepotensial for verdiene med hensyn til brudd på konfidensialitet, integritet og tilgjengelighet
- Identifisere trusler. Vurdere alvorlighetsgrad for de ulike truslene

I risikoanalyse-workshop 1 og 2

- Presentere metodikk for risikoanalyse for «nye» deltakere. Tydeliggjøre fasilitators rolle: Ordstyrer og prosessveileder
- Identifisere uønskede hendelser.
  - Diskusjon rundt hver enkelt risiko.:
    - Hvorfor er det en risiko?
    - Hva kan skje dersom risikoen inntreffer?
    - Hva gjøres i dag for å håndtere risikoen?
  - Sikre at deltakerne er omforent om hendelseslisten
- Analysere konsekvens av og sannsynlighet for de enkelte hendelser

- Dokumentere risikonivå for de uønskede hendelsene i regneark for risikovurdering

I risikohåndteringsworkshop (tiltak)

- Identifisere aktuelle tiltak for å redusere risiko for identifiserte ulike hendelser
- Legge inn verdier for konsekvens og sannsynlighet etter tiltak i regnearket
- Prioritere tiltak i kategoriene Prioritet 1 (Høy) – 3 (Lav)
- Legg inn forslag til ansvarlig rolle/virksomhet for de ulike tiltakene

Vedlegg 5 – Definisjoner og forkortelser

Ord/begrep	Forklaring
Informasjonssikkerhet	Fysiske, systemtekniske og organisatoriske tiltak for å sikre tilfredsstillende konfidensialitet, integritet, tilgjengelighet og kvalitet for personopplysninger og annen informasjon. Annen informasjon kan være informasjon som er unntatt offentlighet etter offentleglova eller informasjon som er taushetsbelagt i lov (IKT-reglement).
Akseptkriterier	Ledelsens beskrivelse av hvor stor risiko de er villig til å akseptere før det må settes inn tiltak.
Integritet	Å sikre at informasjonen er korrekt og pålitelig.
Konfidensialitet	Å hindre at uvedkommende får tilgang til informasjon, herunder personopplysninger og virksomhetskritisk informasjon, som krever beskyttelse.
Konsekvens	Konsekvensen av en uønsket hendelse beskriver hvor alvorlig hendelsen vil være for verdier
Konsekvensnivå	Konsekvensnivåene beskriver mulig tap eller skade og angir øvre grense for hvor alvorlige en hendelse kan bli.
Personopplysninger	Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjons-nummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, øko-nomiske, kulturelle eller sosiale identitet. (GDPR)
Restrisiko	Gjenværende risiko etter gjennomføring av tiltak.
Risiko	Forhold eller hendelser som kan inntreffe og påvirke oppnåelse av målsettinger negativt. Risiko vurderes i forhold til sannsynligheten for at den inntreffer, og den forventede konsekvensen den vil medføre for virksomhetens måloppnåelse dersom den inntreffer.

Risikoanalyse	Identifisere uønskede hendelser og vurdere konsekvenser og sannsynlighet for de ulike hendelsene.
Risikostyring	Risikostyring er en prosess integrert i mål- og resultatstyringen som: er utformet for å kunne identifisere, vurdere, håndtere og følge opp risiko med identifiserte tiltak slik at risikoen er innenfor akseptert nivå; gjennomføres av virksomhetens ledelse og øvrige ansatte; og anvendes i fastsettelse av strategi og planer og på tvers av virksomheten for å gi rimelig grad av sikkerhet for virksomhetens oppnåelse av sine målområder.
Risikovurdering	En samlet prosess som består av trinnene verdivurdering, trusselvurdering, risikoanalyse og risikohåndtering (tiltak). Risikoanalysen utføres ved kartlegging av uønskede hendelser og årsaker til og konsekvenser av disse, NS 5814:2008 (Norsk standard).
Sannsynlighet	Et mål på hvor ofte og hvor lett en hendelse kan forventes å inntreffe i fremtiden.
Sannsynlighetsnivå	Beskriver hvor hyppig hendelsen antas å forekomme.
Særlige kategorier personopplysninger	Personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering. (GDPR)
Sårbarhet	En sårbarhet er noe som gjør at informasjonsverdien er mer utsatt for en hendelse, eller at konsekvensen blir større enn nødvendig.
Tilgjengelighet	Å sørge for at informasjon, herunder personopplysninger og virksomhetskritisk informasjon, er tilgjengelig for autoriserte personer når disse trenger informasjonen. (UKE veileder)
Tiltak	Handling for å redusere risikoer som er høyere enn det som er akseptabelt.
Trusselaktør	En trusselaktør er et individ eller en gruppe individer med en mulig intensjon som gjennom bevisste handlinger ønsker å ramme virksomhetens funksjon og verdier.
Trusselfenomen	Trusselfenomener oppstår naturlig eller som resultat av tilfeldigheter, og kan potensielt skade virksomhetens funksjon og verdier.
Trusselnivå	Beskriver i hvor stor grad en trussel utgjør en fare eller ikke.
Trusselvurdering	Vurdering av trusselaktører og –fenomener som kan forårsake uønskede hendelser.
Verdi	Informasjon, system, informasjonsbehandlingsutstyr og annet som krever beskyttelsestiltak av hensyn til integritet, konfidensialitet og tilgjengelighet (Instruks for informasjonssikkerhet).

Forkortelse	Forklaring
IKT	Informasjons- og kommunikasjonsteknologi
ISO	International Standards Organisation
POL	Personopplysningsloven
UKE	Utviklings- og kompetanseetaten
Verdivurdering	En vurdering av hvor viktig informasjonen er for virksomheten i forhold til konfidensialitet, tilgjengelighet og integritet. Brukes for å kunne prioritere systemer og er et viktig ledd i risikovurderingen.