RETNINGSLINJER FOR RISIKOSTYRING

Systematiske risikovurderinger (også kalt risiko- og sårbarhetsvurderinger, ROS) utgjør en fundamental del av organisasjonens ledelsessystem for informasjonssikkerhet. Det skal foreligge en **plan for risikovurderinger** av alle prosesser[1] som behandler personopplysninger eller annen informasjon som er viktig for driften. I tillegg skal risikovurderinger foretas før alle betydelige endringer i slike prosesser.

De enkelte risikovurderingene resulterer i en liste over risikoelementer, hvor det for hvert element angis om dagens risikonivå er *akseptabelt*, *uheldig* eller *uakseptabelt* i henhold til kriteriene fastsatt i dette dokumentet. I de siste to tilfellene skal arbeidsgruppen som foretar vurderingen foreslå tiltak for å utbedre situasjonen. Disse forslagene behandles av de relevante beslutningstakerne, som innarbeider sine avgjørelser i en **risikohåndteringsplan** med prioriterte tiltak.

Samlingen av gjeldende risikovurderinger kalles **risikokatalogen**. Siden både denne og risikohåndteringsplanen inneholder detaljert informasjon om aktuelle svakheter ved organisasjonens informasjonssikkerhet må disse dokumentene behandles som sensitiv informasjon.

RISIKOVURDERING

Risikovurderinger utføres av arbeidsgrupper som inkluderer representanter for ulike interessenter og som til sammen besitter den nødvendige fagkunnskapen om hvordan prosessen faktisk utføres og om de støttesystemene som inngår i denne. I praksis inkluderer dette vanligvis avanserte brukere, IT-personell og prosess-, tjeneste eller systemansvarlige. Arbeidsmøtene kan gjennomføres med hjelp fra Sekretariat for informasjonssikkerhet i UH-sektoren eller fra eksterne, eller utføres helt internt.

[1] *Prosesser* inkluderer her rutiner, retningslinjer, systemer og tjenester i den form de faktisk benyttes i organisasjonen

Arbeidsgruppens oppgave er:

- å avdekke relevante risikoelementer
- å vurdere sannsynligheten for at de inntreffer og konsekvensen av at de eventuelt gjør det
- å foreslå mulige utbedringer av forhold som ikke kategoriseres som *akseptable*

RISIKOELEMENTER

Et risikoelement er definert som en potensiell sikkerhetshendelse med negative konsekvenser for organisasjonen. Innenfor informasjonssikkerhetsområdet kan slike hendelser gå ut over informasjonens konfidensialitet, integritet eller tilgjengelighet:

Konfidensialitet – Informasjonen er ikke tilgjengelig for uvedkommende
Integritet – Informasjonen er korrekt og fullstendig
Tilgjengelighet – Informasjonen kan ved behov brukes etter intensjonen

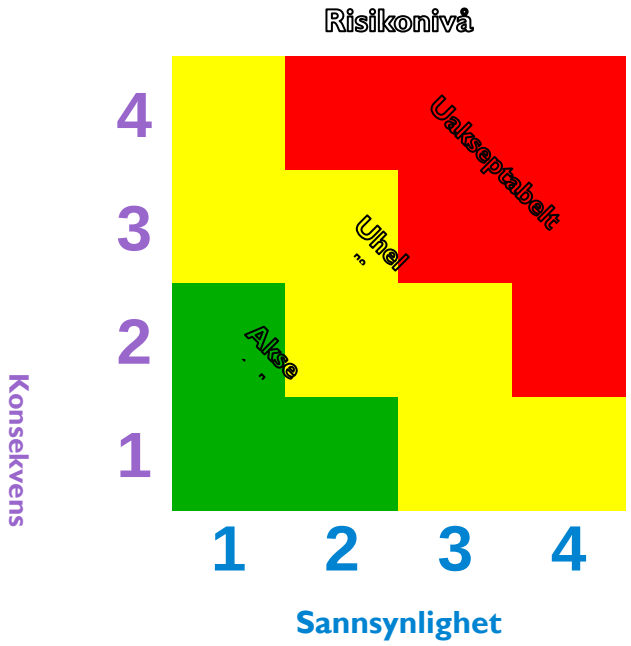
De viktigste kildene til risikoelementer som bør vurderes er:

- Tidligere risikovurderinger
- Tidligere sikkerhetshendelser
- Kunnskap om relevante sikkerhetstrusler
- Kjente sårbarheter som kan utnyttes
- Eksisterende sikringstiltak (som kan omgås)
- Generelle lister over mulige risikoelementer

Tre forhold må belyses for hvert risikoelement. Det første og viktigste er svakheter eller sårbarheter som forverrer situasjonen eller er grunnen til at risikoelementet i det hele tatt er til stede. Dernest kommer eksisterende tiltak som reduserer sannsynligheten for at en hendelse skal inntreffe, eller som begrenser skadeomfanget om det skulle skje. Til sist kommer eksisterende avdekkende eller kompenserende tiltak som ikke hindrer en hendelse i å skje, men som gjør det lettere å oppdage om det har skjedd, slik at tiltak raskt kan treffes, eller som gjør det lettere å gjenopprette normalsituasjonen eller hindre skaden i å fortsette å vokse.

Risikonivå

Gitt disse forutsetningene vurderes *sannsynligheten* for at risikoelementet materialiserer seg i form av en sikkerhetshendelse og *konsekvensen* for organisasjonen om dette skjer, begge på en skala fra 1 til 4 som nærmere beskrevet nedenfor. *Risikonivået*, som er det man er ute etter å finne, utgjøres av kombinasjonen av disse to verdiene i henhold til følgende tabell:



Sannsynlighetsskalaen

Ved vurdering av sannsynlighet tar man i de aller fleste tilfeller forventet frekvens som utgangspunkt. Bare i de relativt sjeldne tilfellene hvor man ikke har erfaringsgrunnlag for å estimere frekvens benytter man i stedet andre indikatorer som hvor lett det vil være for noen å utløse risikoen, og hvilken motivasjon de behøver.

	1 lav	2 moderat	3 høy	4 Svært høy
Frekvens	Sjeldnere enn hvert 5. år	Sjeldnere enn årlig	Oftere enn årlig	Flere ganger per halvår
Letthet	Relevante og fungerede sikkerhetstiltak finnes. Kan omgås av ansatte med privilegert tilgang og god kjennskap til tiltakene. Eksterne kan ikke omgå tiltakene uten intern hjelp.	Relevante og fungerede sikkerhetstiltak finnes. Kan omgås av ansatte med normal tilgang og kjennskap til tiltakene. Eksterne behøver kompetanse og god kjennskap til tiltakene	Sikkerhetstiltak er ikke effektive og målrettede. Kan omgås av ansatte uten spesielle ressurser eller kunnskap, eller av eksterne med normal kjennskap til tiltakene.	Sikkerhetstiltak er ikke til stede eller er mangelfulle. Kan omgås av ansatte eller eksterne uten spesielle ressurser eller kjennskap til tiltakene.
Motivering	Ansatte med privilegert tilgang og spesiell kunnskap må opptre med forsett. Eksterne må ha spisskompetanse og samarbeide med ansatte.	Ansatte med kjennskap til sikkerhetstiltakene må opptre med forsett. Eksterne må ha høy kompetanse og angripe sikkerhetstiltakene planmessig.	Ansatte kan utløse sikkerhetshendelser ved uaktsomhet (uten forsett). Eksterne må ha noe kompetanse og opptre med forsett.	Både ansatte og eksterne uten spesiell kunnskap eller kompetanse kan utløse sikkerhetshendelser ved uaktsomhet (uten forsett).

KONSEKVENSSKALAEN

Konsekvens er vanskeligere enn sannsynlighet å sammenligne på tvers av ulike typer hendelser. Innenfor informasjonssikkerhet er skadevirkningen på organisasjonen i siste instans oftest økonomisk eller knyttet til omdømmet.

	1 liten	2 moderat	3 alvorlig	4 svært alvorlig
Økonomisk	Tap opp til _____	Tap opp til _____	Tap opp til _____	Tap over _____
Omdømme	Anses å ha utvist dårlig dømmekraft	Anses som uaktsom; lokalt omfang	Anses som uansvarlig; regionalt omfang	Anses som hensynsløs; nasjonalt omfang

I praksis kan det ofte være omstendelig å trekke konsekvensen av en hendelse helt opp til dette nivået. For de vanligste formene for sikkerhetsbrudd er det derfor utarbeidet egne skalaer:

	1	2	3	4
Konfidensialitet	Mangelfull logging av tilgang til person-opplysninger	Eksponering av enkeltindividers personopplysninger	Eksponering av sensitive eller større mengder personopplysninger	Eksponering av større mengder sensitive personopplysninger
Integritet	Uklart når eller hvordan ikke-kritisk informasjon sist ble oppdatert	Inkomplett eller utdatert ikke-kritisk informasjon	Viktig informasjon mangler eller er feil	Kritisk informasjon mangler eller er feil
Tilgjengelighet	Opp til 1 arbeidsdag (eksamen/registrering: opp til 1 time)	Opp til 5 arbeidsdager (eksamen/registrering: opp til 3 timer)	Opp til 3 uker (eksamen/registrering: opp til 1 dag)	Over 3 uker (eksamen/registrering: over 1 dag)

Under konfidensialitet er det her bare spesifisert personopplysninger. Disse har hatt særskilt fokus blant annet fordi det på dette området finnes omfattende lovregulering som man må ta hensyn til. Annen informasjon av verdi for organisasjonen vurderes imidlertid også analogt med dette.

SPESIELLE TILFELLER

Noen risikoelementer er av en slik natur at de kan inntreffe i større og mindre alvorlighetsgrad, og slik at sannsynligheten for tilfellene med størst konsekvens er lavere enn for tilfellene med mindre konsekvens. Det blir da systematisk feil å kombinere den høyeste sannsynligheten og den største konsekvensen. I stedet vurderer man individuelt det mest sannsynlige tilfellet og det mest alvorlige tilfellet. Den kombinasjonen som gir lavest risikonivå kan droppes; hvis nivået blir det samme droppes den situasjonen som oppfattes som den minste trusselen.

Dersom arbeidsgruppen er komfortabel med bruken av skalaene og oppfatter resultatene som rimelige i forhold til egen oppfatning av situasjonen, så kan det i grensetilfeller være legitimt å sette verdien på én av aksene delvis basert på hvilket risikonivå dette vil resultere i.

RISIKOHÅNDTERING

For risikoelementer hvor risikonivået er *uakseptabelt* eller *uheldig* skal arbeidsgruppen foreslå tiltak for å håndtere risikoen. I enkelte tilfeller vil noen av de tilstedeværende være bemyndiget til å umiddelbart bestemme at slike tiltak skal gjennomføres, men generelt er forslagene innspill til beslutningstakere som skal vurdere hvorvidt de skal innlemmes i risikobehandlingsplanen, og hvordan de skal prioriteres.

Tiltak faller i fire eller fem kategorier, alt etter hvordan man grupperer dem. I økende relevans:

1 Man kan **dele risikoen** med andre eller overføre den helt (for eksempel ved forsikring)
2 Man kan **unngå risikoen** ved å trekke seg ut av aktiviteten som medfører den
3 Man kan velge å bevisst **akseptere risikoen** til tross for risikonivået – dette skjer helst hvis situasjonen er tidsbegrenset, eller hvis ethvert effektivt tiltak vil være uakseptabelt kostbart og man ikke kan trekke seg ut av aktiviteten
4a Man kan **redusere risikoen** ved å gjennomføre tiltak som begrenser **konsekvensen** hvis hendelsen inntreffer
4b Man kan **redusere risikoen** ved å gjennomføre tiltak som senker **sannsynligheten** for at hendelsen vil inntreffe

RISIKOKATALOGEN

Tilgang til eksisterende risikovurderinger er svært verdifullt ved alt senere sikkerhetsarbeid, men fordi de avslører sårbarheter i prosesser og systemer er tilgang for uvedkommende potensielt svært skadelig. Alle risikovurderinger bør derfor samles på ett sted, med et egnet tilgangsregime som tar hensyn til begge disse forholdene. De til enhver tid gjeldende sikkerhetsvurderingene kalles samlet for risikokatalogen.

BIDRAG TIL ÅRSHJUL FOR LEDELSESSYSTEMET

Informasjonssikkerhetsansvarlig CSO skal gjennom året løpende:

- Sørge for at risikovurderinger gjennomføres i henhold til plan for risikovurderinger
- Følge opp at risikohåndteringsplanen oppdateres ved funn i risikovurderinger
- Følge opp at risikohåndteringsplanen blir satt ut i livet av de aktuelle aktørene

Til ledelsens gjennomgang skal informasjonssikkerhetsansvarlig:

- Innhente informasjon fra alle risikoeiere (prosess-, tjeneste eller systemeiere) om hvorvidt sist foretatte risikovurderinger er dekkende for dagens situasjon, eller om en ny vurdering må foretas
- Presentere status for gjennomføring av risikovurderinger
- Presentere status for gjennomføring av risikohåndteringsplanen
- Foreslå oppdatert plan for risikovurderinger

For å tilfredsstille kravene til et ledelsessystem for informasjonssikkerhet må ledelsen årlig:

- Vurdere om retningslinjene i dette dokumentet behøver justeringer
- Følge opp eventuelle problemer med gjennomføring av risikohåndteringsplanen, enten med styringssignaler eller ved ressursfordeling
- Vedta en oppdatert plan for risikovurderinger

Revisjoner:

Versjon	Dato		Beskrivelse/ kommentar	Utført av
0.01	Sep - 2018		Etablering av dokument	Gunnar
0.02	Nov - 2019		Justeringer	Gunnar
1.0	Des - 2019		Vedtatt	Marit
1.0.1	Mai - 2022		Endret oppsett og skriftstørrelse	Gunnar