Brukarrettleiing risikovurderingsverktøy

Om verktøyet

Verktøyet kan brukast som støtteverktøy/dokumentasjonsverktøy til metoden for risikovurdering som er skildra i rettleiingsmateriellet til Digitaliseringsdirektoratet. Metode for gjennomføring av sjølve risikovurderingane, samt organiseringa av arbeidet, er skildra i rettleiingsmateriellet. De må sjølv vurdere i kva grad det er føremålstenleg å bruke verktøyet i tilknyting til andre metodar.

Det er eit enkelt verktøy, laga i Microsoft Excel, som verksemder av ulik storleik og kompleksitet kan ta i bruk. Om de har behov for å endre på verktøyet, står de fritt til sjølv å tilpasse det. Vi gjer likevel merksame på at Digitaliseringsdirektoratet ikkje har høve til å hjelpe med tilpassingar eller brukarstøtte.

Om bruken av verktøyet

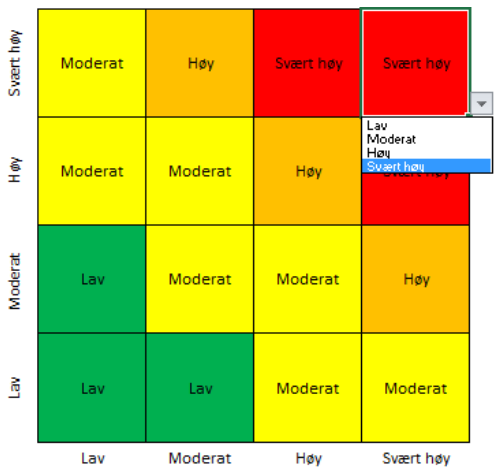
Vi har laga verktøyet for å forenkle gjennomføringa av risikovurderingar, mellom anna ved at de sjølv ikkje skal trenge å bruke tid og ressursar på å utvikle eigne verktøy.

Verktøyet må ein sjå i samanheng med resten av rettleiingsmateriellet frå Digitaliseringsdirektoratet, og døme på styrande dokument og føringar knytte til risiko. Mellom anna følgjande:

- Fire nivå på alvorsgraden til risikoane
- Fire nivå på sannsyn
- Fire nivå på konsekvens
- Verksemda skal kunne gje opp nivå/skildring av sannsyn og konsekvens
- Verksemda skal kunne gje opp skildringa av risikonivå
- Risko før og etter planlagde tiltak blir vist i riskomatrise
- Risiko blir uttrykt som kombinasjonen av sannsyn og konsekvens, ikkje produktet av sannsyn multiplisert med konsekvens.

Startbiletet

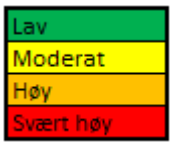
Startbiletet i verktøyet viser ei 4x4-matrise der y-aksen representerer sannsyn og x-aksen representerer konsekvens. De kan bruke startbiletet til å tilpasse matrisa, slik at ho på best mogleg måte gjev att føringane til verksemda for å fastsetje risikonivå. Dette gjerast ved å endre verdien og tilhøyrande fargeoppgjeving på kvar enkelt celle ved å velje frå nedtrekksmenyen slik figur 1 viser.



Figur 1

Vidare kan de endre nemninga på dei fire nivåa på risiko, konsekvens og sannsyn, for på denne måten å tilpasse

risikovurderinga til føringane for verksemda for å forstå, vurdere og handtere risiko. Dette gjerast ved å skrive inn det ein ønskjer i tabellane under matrisa slik figur 2 viser. Endring av nemningar vil samstundes føre med seg endring i sjølve matrisa og i risikovurderingsarket.

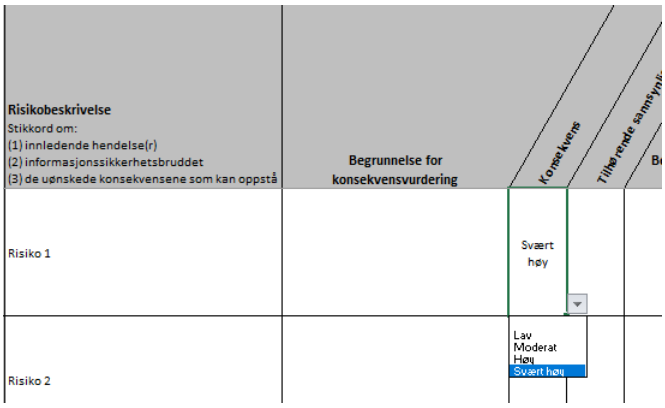


Figur 2

Når dei ulike nivåa og matrisa er slik ein ønskjer, må brukaren klikke på knappen «Til Risikovurdering».

Risikovurdering

Risikovurderinga tar utgangspunkt i at det blir gjennomført konsekvens- og sannsynsvurderingar av uønskte hendingar, som verksemda på førehand har diskutert seg fram til. Digitaliseringsdirektoratet tilrår at ein i analysen tar utgangspunkt i kva konsekvensen kan bli om ei gjeve hending skjer, og at det deretter gjerast ei vurdering av sannsynet for at hendinga skjer med den skildra konsekvensen. Verksemda må sjølv vurdere om det er føremålstenleg å vurdere sannsynet for ulike grader av konsekvensvurderingar av den same hendinga, eller om ein berre gjer sannsynsvurdering av det mest forventa utfallet. Ei meir detaljert skildring av framgangsmåte finn du i rettleiingsmateriellet.



Figur 3

Nivået på konsekvens og sannsyn blir gjeve opp ved å velje frå nedtrekksmenyane. Innhaldet i menyane styrast av det brukaren har sett som nivå, jf. startbilete slik dette er omtalt ovanfor. Sjå figur 3 for illustrasjon.

Om konsekvensen av ei hending er vurdert som «Høg» (eller ei anna nemning tilsvarande nivå 3 på konsekvensskalaen) og sannsynet for dette er vurdert til «Svært høg» (eller ei anna nemning tilsvarande nivå 4 på sannsynsskalaen), vil risikoen uttrykkast automatisk som «Svært høg» med farge raud slik figur 4 viser. Likevel vil risikoen uttrykkast annleis om det gjerast fleire endringar i matrisa i startbiletet. Eit døme på dette kan vere cella der sannsyn = svært høg og konsekvens = høg, som frå før har verdi «Høg» og farge oransje. Om verdien til denne cella blir endra til «Svært høg», vil risikoen uttrykkast som «Svært høg» og med farge raud slik figur 5 viser.

Risikobeskrivelse Stikkord om: (1) innledende hendelse(r) (2) informasjonssikkerhetsbruddet (3) de uønskede konsekvensene som kan oppstå	Begrunnelse for konsekvensvurdering	Konsekvens	Tilhørende sannsynlighet	Begrunnelse for vurdering av tilhørende sannsynlighet	Risikonivå
Risiko 1		Høy	Svært høy		Høy

Figur 4

Risikobeskrivelse Stikkord om: (1) innledende hendelse(r) (2) informasjonssikkerhetsbruddet (3) de uønskede konsekvensene som kan oppstå	Begrunnelse for konsekvensvurdering	Konsekvens	Tilhørende sannsynlighet	Begrunnelse for vurdering av tilhørende sannsynlighet	Risikonivå
Risiko 1		Høy	Svært høy		Svært høy

Figur 5

Etter at risiko er analysert, må det gjerast ei evaluering av kvar enkelt risiko med tanke på om risikoen kan aksepterast slik han er, eller om han må handterast. I første omgang kan kolonnen «Vurdering av risikohandtering» brukast til å gje opp om ein risiko «Kan aksepterast» eller om han er «Ikkje akseptabel».

Vidare skal det gjerast framlegg om handtering av risikoane. Figur 6 viser korleis verktøyet kan vere ein støtte i dette, når ein vurderer den risikoreduserande effekten. Ved å gjere ei ny vurdering av konsekvens og sannsyn etter at eitt eller fleire tenkte tryggingsstiltak er implementerte, får ein eit bilete av kor stor risikoreduserande effekt tiltaket har. Risikoen ein då står igjen med er den gjenverande risikoen. Nivået på den gjenverande risikoen vil på same måte som før vere avhengig av korleis risikomatrisen i startbiletet er sett opp. Ver merksam på at også kostnader og uheldige sideeffektar må vurderast får ein vedtek endeleg handtering av risikoen.

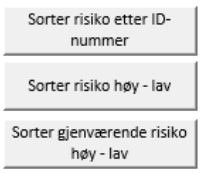
Risikobeskrivelse Stikkord om: (1) innledende hendelse(r) (2) informasjonssikkerhetsbruddet (3) de uønskede konsekvensene som kan oppstå	Begrunnelse for konsekvensvurdering	Konsekvens	Tilhørende sannsynlighet	Begrunnelse for vurdering av tilhørende sannsynlighet	Risikonivå	Vurdering av risikohåndtering	Konsekvens etter tiltak	Sannsynlighet etter tiltak	Gjenværende risiko
Risiko 1		Høy	Svært høy		Høy		Moderat	Moderat	Moderat

Figur 6

Frå ei verksemd til ei anna kan det variere stort kor mange uønskte hendingar det er aktuelt å analysere og evaluere. Det kan også vere stor variasjon internt mellom avdelingar og einingar. Det er i verktøyet sett av plass til at det skal vere mogleg å inkludere 100 risikoskildringar.

Sortering og oversikt over risikoar

Ofte vil det vere behov for å få ei oversikt over risikoane når vurderingane er ferdige. Dette er løyst på to måtar; sortert og plotta i risikomatrise.



Figur 7

I skjermbiletet «Risikovurdering» har brukaren høve til å sortere risikoane etter ID-nummer og etter risikonivå slik figur 7 viser. Sortering etter risikonivå kan gjerast på risikoane både før og etter planlagde tiltak.

Knappen «Til Risikomatrise» leiar til siste skjermbilete i verktøyet. Sjå figur 8. Her blir risikoane plotta inn i riktig celle på bakgrunn av vurderingane som er gjort i «Risikovurdering». Fargeattgjevinga til matrisa følgjer av korleis matrisa i startbiletet er sett opp, jf. punkt 1.

Figur 8