Brukerveiledning risikovurderingsverktøy

Innledning

Verktøyet må sees i sammenheng med det øvrige veiledningsmateriellet fra Difi, især den delen som gjelder risikovurderinger. Metode for gjennomføring av selve risikovurderingene, samt organiseringen av arbeidet, er beskrevet i veiledningsmateriellet og blir ikke mye omtalt i denne brukerveiledningen.

Vi gjør oppmerksom på at verktøyet er ment å være en støtte i risikovurderingsarbeidet, og er laget slik at det skal være mulig for virksomheter av ulik størrelse og kompleksitet å ta det i bruk. Dersom virksomheter ønsker eller har behov for endringer står de fritt til selv å tilpasse verktøyet. Vi gjør imidlertid oppmerksom på at Difi ikke har anledning til å bistå den enkelte virksomhet dersom tilpasninger er nødvendig. Alle endringer skjer derfor på eget ansvar.

Excel-verktøyet er ment å fungere som støtteverktøy/dokumentasjonsverktøy til metoden for risikovurdering som er beskrevet i veiledningsmateriellet. Virksomheten må selv vurdere i hvilken grad det er hensiktsmessig å bruke verktøyet i tilknytning til andre metoder, eksempelvis Octave, NIST 800-30 eller liknende som ofte betinger ekstern bistand.

Verktøyets formål

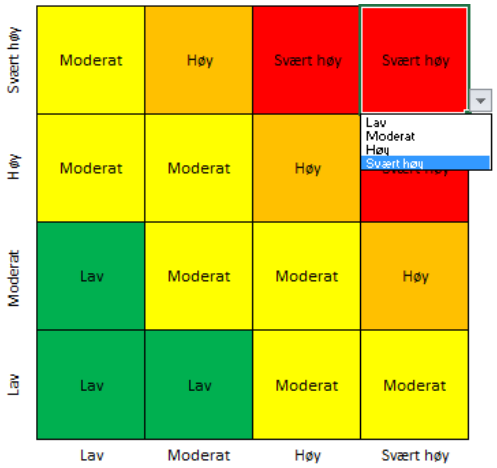
Excel-verktøyet er laget for å forenkle gjennomføringen av risikovurderinger, blant annet ved at virksomheten selv ikke skal trenge å bruke tid og ressurser på å utvikle egne verktøy.

Verktøyet er laget med utgangspunkt i Difis veiledning, blant annet følgende:

- Fire nivåer på risikoenes alvorlighetsgrad
- Fire nivåer på sannsynlighet
- Fire nivåer på konsekvens
- Virksomheten skal kunne angi gradering/beskrivelse av sannsynlighet og konsekvens
- Virksomheten skal kunne angi beskrivelsen av risikonivå
- Risiko før og etter planlagte tiltak skal vises i risikomatrise som gjenspeiler virksomhetens risikoappetitt
- Risiko uttrykkes som kombinasjonen av sannsynlighet og konsekvens, ikke produktet av sannsynlighet multiplisert med konsekvens.

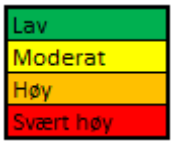
Startbildet

Startbildet i verktøyet viser en 4x4-matrise der y-aksen representerer sannsynlighet og x-aksen representerer konsekvens. Formålet med startbildet er å gi brukeren mulighet til tilpasse matrisen slik at den på best mulig måte gjengir virksomhetens risikoappetitt. Dette gjøres ved å endre verdien og tilhørende fargeangivelse på hver enkelt celle ved å velge fra nedtrekksmenyen slik figur 1 viser.



Figur 1

Videre kan brukeren endre betegnelsen på de fire nivåene på risiko, konsekvens og sannsynlighet, for på denne måten å tilpasse risikovurderingen til virksomhetens øvrige risikovurderinger. Dette gjøres ved å skrive inn det man ønsker i tabellene under matrisen slik figur 2 viser. Endring av betegnelser vil samtidig medføre endring i selve matrisen og i risikovurderingsarket.

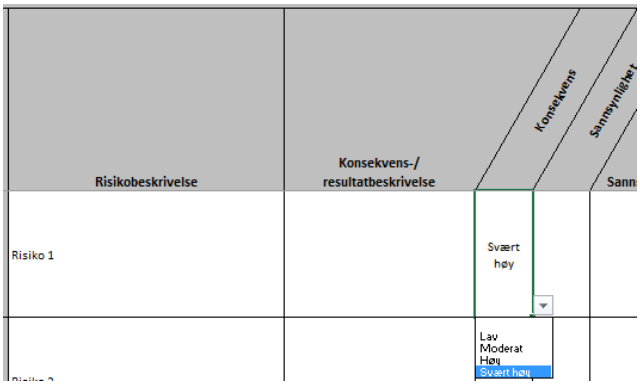


Figur 2

Når de forskjellige nivåene og matrisen er slik man ønsker, må brukeren klikke på knappen «Til Risikovurdering».

Risikovurdering

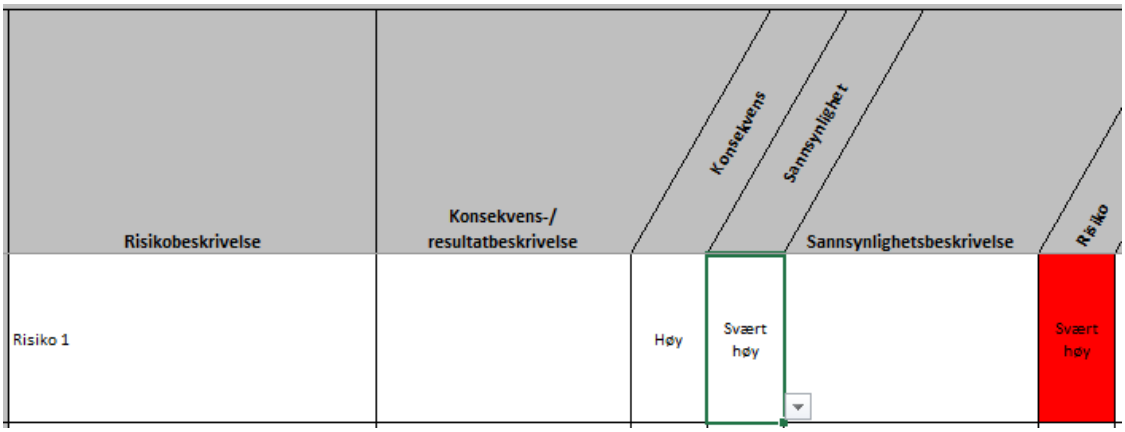
Risikovurderingen tar utgangspunkt i at det gjennomføres konsekvens- og sannsynlighetsvurderinger av spesifikke scenarioer, eller hendelser, som virksomheten på forhånd har diskutert seg frem til. Difi anbefaler at man i analysen tar utgangspunkt i hva resultatet kan bli dersom en gitt hendelse inntreffer, og at det deretter gjøres en vurdering av sannsynligheten for at hendelsen inntreffer med det beskrevne resultatet. Virksomheten må selv vurdere om det er hensiktsmessig å vurdere sannsynlighet for ulike grader av konsekvensvurderinger av den samme hendelsen, eller om man kun gjør sannsynlighetsvurdering av det verst tenkelige utfallet. En mer detaljert beskrivelse av fremgangsmåte er gjengitt i veiledningsmateriellet.



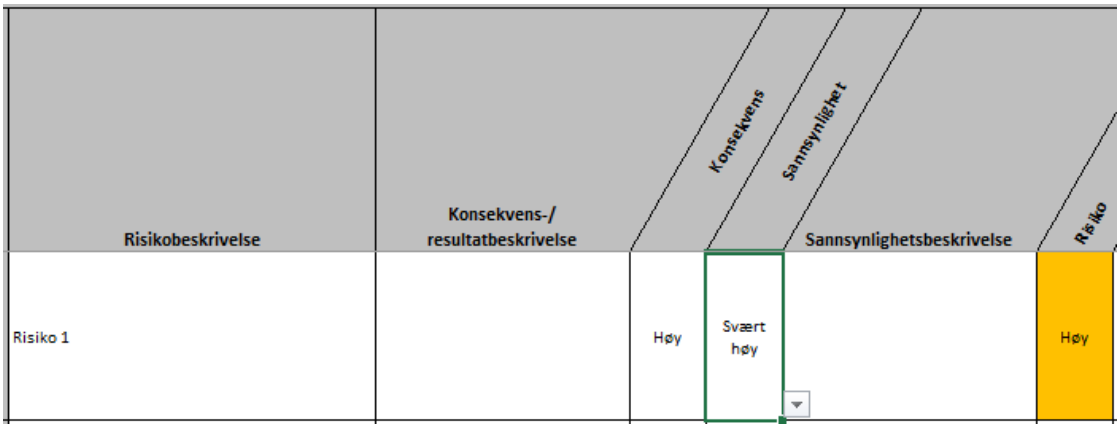
Figur 3

Gradering av konsekvens og sannsynlighet gjøres ved å velge fra nedtrekksmenyene. Innholdet i menyene styres av det brukeren har satt som nivåer, jmf. startbilde slik dette er omtalt ovenfor. Se figur 3 for illustrasjon.

Dersom konsekvensen av en hendelse er vurdert som «Høy» (eller en annen betegnelse tilsvarende nivå 3 på konsekvensskalaen) og sannsynligheten for dette er vurdert til «Svært høy» (eller en annen betegnelse tilsvarende nivå 4 på sannsynlighetsskalaen), vil risikoen uttrykkes automatisk som «Svært høy» med farge rød slik figur 4 viser. Imidlertid vil risikoen kunne uttrykkes annerledes dersom det gjøres endringer i matrisen i startbildet. Et eksempel på dette kan være cellen i skjæringspunktet sannsynlighet = svært høy og konsekvens = høy som fra før har verdi «Svært høy» og farge rød. Hvis verdien til denne cellen endres til «Høy», vil risikoen uttrykkes som «Høy» og med farge oransje slik figur 5 viser.

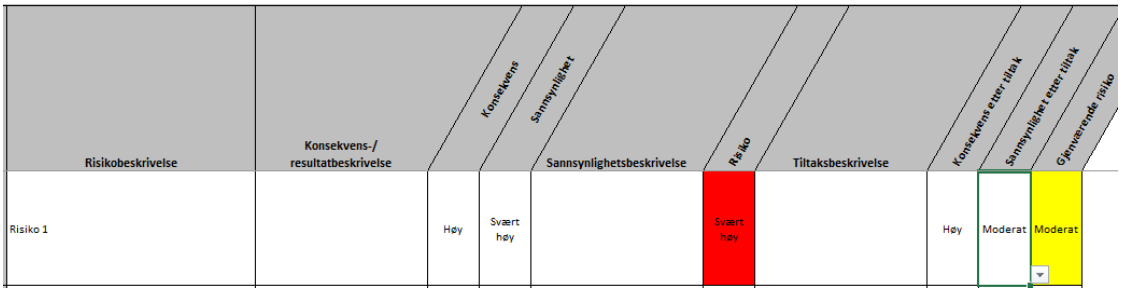


Figur 4



Figur 5

Etter at risiko er analysert, må det foretas en evaluering av hver enkelt risiko med tanke på hva slags sikkerhetstiltak som egner seg for å redusere risiko til et akseptabelt nivå. Figur 6 viser hvordan dette er tenkt i verktøyet, og det foregår i stor grad på samme måte som for analysen ved at det gjøres en ny vurdering av konsekvens og sannsynlighet etter at ett eller flere tenkte sikkerhetstiltak er implementert. Risikoen man da står igjen med er den gjenværende risikoen. Nivået på den gjenværende risikoen vil på samme måte som før være avhengig av hvordan risikomatrisen i startbildet er satt opp.



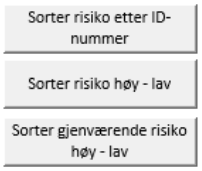
Figur 6

Fra en virksomhet til en annen kan det variere stort hvor mange hendelser/scenarioer det er aktuelt å analysere og evaluere. Det kan også være stor variasjon internt mellom avdelinger og enheter. Det er i verktøyet avsatt plass til at det skal være mulig å inkludere 100 hendelser/scenarioer.

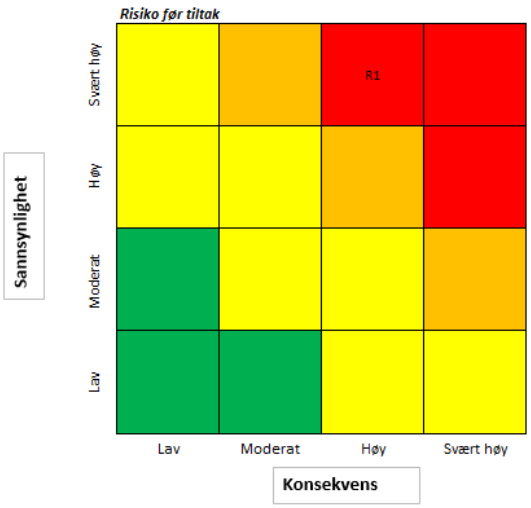
Sortering og oversikt over risikoer

Ofte vil det være behov for å få en oversikt over risikoene når vurderingene er ferdig. Dette er løst på to måter; sortert og plottet i risikomatrise.

I skjermbildet «Risikovurdering» har brukeren anledning til å sortere risikoene etter ID-nummer og etter risikonivå slik figur 7 viser. Sortering etter risikonivå kan gjøres på risikoene både før og etter planlagte tiltak.



Figur 7



Knappen «Til Risikomatrise» leder til siste skjermbilde i verktøyet. Se figur 8. Her blir risikoene plottet inn i riktig celle på bakgrunn av vurderingene som er gjort i «Risikovurdering». Matrisens fargegjengivelse følger av hvordan matrisen i startbildet er satt opp, jf. punkt 1.

Figur 8