**Vejledning i risikovurdering af informationssikkerhed**

Version 1.0

xx. mmm 20nn

# Formål

Denne vejledning beskriver en overordnet metode til hvordan man vurderer virksomhedens kritiske informationsrisici, når man ikke har et komplet rammeværk for ledelsens styring af it-sikkerhed (ledelsessystem for informationssikkerhed også kaldet Information Security Management System eller ISMS). Det medfølgende regneark er bygget op om denne metode.

Vejledningen præsenterer en enkel model, der giver en introduktion til hvad risikovurdering er, hvordan det udføres og hvordan det kan bruges. Hovedformålet er, at små- og mellemstore virksomheder kan komme i gang med en enkel og praktisk brug af risikovurdering og opbygge erfaring med risikovurdering og risikostyring. Når virksomhedens behov for risikostyring vokser, kan der skiftes til mere avancerede modeller og metoder.

Metoden er rettet mod små og mellemstore virksomheder, som har en rimeligt enkel it-anvendelse i form af ca. 3-5 vigtige it-systemer, der er nødvendige for at virksomhedenkan fungere. Disse 3-5 it-systemer kan enten være administreret af virksomheden selv eller købt som en it-service fra en it-leverandør.

Har man i forvejen en risikovurderingsmetode, kan man fortsat bruge den. Større virksomheder og/eller virksomheder med en etableret it-/sikkerhedsafdeling, kan med fordel benytte Digitaliseringsstyrelsens metode og værktøj til risikovurdering[[1]](#footnote-1) eller se på DS/ISO/IEC 27005:2018.

**Om risikovurderinger**

God it-sikkerhed/informationssikkerhed handler grundlæggende om at sikre informationers tilgængelighed, fortrolighed og integritet på samme tid. *Tilgængelighed* vil sige, at informationer er til rådighed for dem, der skal bruge dem, når de skal bruge dem. *Fortrolighed* handler om, at uvedkommende ikke kan få adgang til informationer. *Integritet* handler om, at informationer er rigtige og troværdige og eksempelvis ikke er blevet ændret af uvedkommende.

Risikostyring er en central del af arbejdet med it- og informationssikkerhed, der gør det muligt for ledelsen at tage stilling til, og prioritere, de nødvendige investeringer og tiltag i forhold til virksomhedens risikovillighed. Udgangpunktet for dette er en risikovurdering.

En risiko betragtes i denne sammenhæng som en uønsket hændelse med uheldige konsekvenser for tilgængelighed, fortrolighed og/eller integriteten af informationssikkerheden.

Risikovurderingen har til formål at gøre risici sammenlignelige ved at risici eksempelvis udtrykkes som en talværdi. En høj risiko for virksomheden vises som en høj talværdi og tilsvarende udtrykkes en lav risiko som en lav talværdi.

Risikoen måles ved at bedømme, hvor stor sandsynlighed der er for, at en trussel kan udnytte en sårbarhed og hvilke, herunder hvor store, konsekvenser det kan have for virksomheden. Et eksempel er, at virksomheden mister en bærbar pc (trussel), der ikke er krypteret (sårbarhed), hvilket gør det muligt for uvedkommende at få adgang til firmamails og lignende på pc’en (konsekvens).

På baggrund af risikovurderingen skal virksomheden vurdere behovet for, og udpege, evt. yderligere sikringsforanstaltninger, der sikrer den nødvendige tilgængelighed, fortrolighed og integritet. I førnævnte eksempel kunne det være behovet for at kryptere bærbare pc’er. Den vurdering indgår i en risikohåndteringsplan.

Generelt arbejdes der med fire former for håndtering af risici:

* Risici accepteres
* Risici styres
* Risici deles (evt. gennem forsikring)
* Risici undgås

En måde at styre risici på, er at risici opdeles i kategorier, eksempelvis lav, middel og høj, der kan udtrykkes med hver sin farve, typisk grøn, gul og rød. Det er virksomhedens ledelse, der fastsætter kategorierne ud fra virksomhedens risikovillighed. Risikovillighed hos virksomhedens ledelse er udtryk for, hvad ledelsen er villig til at påtage sig af risiko.

Er der tale om lav risikovillighed, vil der være mange talværdier, som ikke kan accepteres uden at der skal ske yderligere (dvs. røde værdier). Det gælder eksempelvis hvis man er meget afhængig af sine informationer. Er der tale om en mellem risikovillighed, vil talværdierne for grøn, gul og rød være mere jævnt fordelt. Såfremt risikovilligheden er høj, vil der være mange talværdier, som er acceptable for virksomheden (grønne værdier). Eksempelvis hvis man fint kan arbejde uden ens servere og man kun har meget få persondata,

Såfremt en høj/rød risiko ikke kan nedbringes, må risikoen undgås. Det kan eksempelvis betyde, at virksomheden måske skal ophøre med at udføre en opgave. Den øverste ledelse i virksomheden kan dog altid beslutte, at virksomheden godt kan leve med en rød risiko, hvis risikoen overvåges og forsøges styret så snart det bliver muligt. Se mere om den praktiske brug af dette i afsnit 2.1.

# Metode til risikostyring

Risikostyringsprocessen forløber som følger:

1. Den sikkerhedsansvarlige skal, i en dialog med evt. øverste ledelse, bestemme hvornår der skal foretages en risikovurdering, hvordan konsekvenserne skal vurderes, hvilke risici der kan accepteres og hvilke der skal håndteres (risikovillighed)   
     
   Typisk starter man med en årlig risikovurdering, og man vælger at udtrykke konsekvenser samt sandsynligheder på en numerisk skala gående fra 1 (lav) til 5 (høj). Risikoen er så produktet (sandsynlighed x konsekvens) af de to værdier, dvs. gående fra 1 (lavest) til 25 (højest). Se skalaerne nedenfor i punkt e) og f).
2. Den sikkerhedsansvarlige vurderer, gerne i dialog med ledere med kendskab til forretningen, hvilke forretningskritiske informationer, processer og it-systemer risikovurderingen skal udføres på. Man kan eksempelvis se på hvilke processer, der er kritiske for levering af en bestemt service eller fremstilling af bestemte produkter samt hvilke informationer og it-systemer disse processer er afhængige af.

Typiske emner er kundedata, økonomisystem og evt. kundevendte services samt medarbejderdata.

1. Når de kritiske systemer, data og processer er udpeget, skal der udpeges en risikoejer for hver af dem. Risikoejeren er den person, der kan indstille til ledelsen, at en konkret risiko accepteres eller nedbringes/håndteres.   
     
   Risikoejeren er typisk en økonomichef, driftsleder eller it-ansvarlig. Det kan også være direktøren.
2. Den sikkerhedsansvarlige identificerer, i en dialog med risikoejeren samt evt. andre it- og forretningskyndige, de trusler, som ved brug af eksisterende sårbarheder, kan give brud på tilgængelighed, fortrolighed og integritet af de valgte processer, data og it-systemer og dermed udgøre en risiko.

Typisk starter man med at se på hvad sådanne brud egentligt kunne være. Det kunne eksempelvis være risikoen for, at kundedatabasen afsløres til en konkurrent (en trussel), fordi en medarbejder ikke ved, hvordan mails behandles korrekt (sårbarheden).

Appendiks C og D i DS/ISO/IEC 27005:2018 indeholder lister over mulige trusler og sårbarheder, som man kan tage udgangspunkt i. Har man et højere ambitionsniveau kan man arbejde med en trusselsterminologi, som f.eks. OCTAVE-modellen[[2]](#footnote-2). OCTAVE-modellen gennemgår alle tænkelige trusler fordelt på tre hovedkategorier: Menneskelige trusler, systemmæsige trusler og trusler udenfor virksomhedens kontrol.

Menneskelige trusler kan komme fra interne medarbejdere eller fra personer udenfor virksomheden. Der kan være tale om bevidste/tilsigtede handlinger eller uheld. I denne hovedkategori finder vi eksempelvis korrupte medarbejdere, medarbejdere som glemmer en bærbar pc, hackere, og leverandører eller samarbejdspartnere, der laver en fejl.

Systemmæssige trusler findes f.eks., når der er en indbygget logisk fejl i et program, som da man opdagede ”Heartbleed” sårbarheden i 2014.

Trusler udenfor virksomhedens kontrol er f.eks. optøjer eller skybrud, der oversvømmer serverrummet.  
  
En anden kilde til identificering af relevante trusler er ”Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA)”, som i 2016 har publiceret en oversigt en oversigt over trusler*[[3]](#footnote-3)*.

1. Den sikkerhedsansvarlige fastlægger konsekvenserne ved disse risici, evt. i dialog med en fra ledelsen, og vurderer hvad dette vil betyde for virksomheden. Konsekvenserne angives i niveauer på følgende skala:

1 - Meget lille konsekvens – det har reelt ikke nogen betydning  
2 - Lille konsekvens – det kan håndteres som en del af driften  
3 - Nogen konsekvens – der skal nok søges om ekstra midler  
4 - Høj konsekvens – det har betydning for bundlinjen  
5 - Meget stor konsekvens – firmaet er truet

Et eksempel på en konsekvensvurdering er, at afsløring af informationer om vigtige kunders rabataftaler eller af sådanne informationer om et større antal kunder, kan påvirke omsætningen negativt (Høj konsekvens).

1. Den sikkerhedsansvarlige vurderer, i en dialog med evt. andre it- og forretningskyndige, sandsynligheden for, at den pågældende risiko erfaringsmæssigt optræder som en faktisk sikkerhedshændelse. Sandsynlighederne fastlægges også i niveauer på følgende skala:

1 - Sjælden eller usandsynlig  
2 - Vil næppe forekomme  
3 - Er mulig  
4 - Må forventes at kunne ske  
5 - Vil blive udnyttet

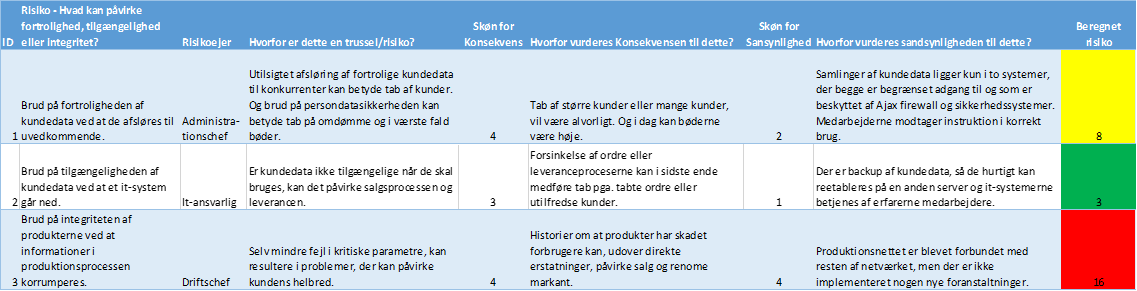
Når man vurderer sandsynlighederne, skal man tage højde for de administrative og tekniske sikkerhedstiltag, der allerede er implementeret, og som kan medvirke til at reducere de erfaringsbaserede sandsynligheder. Uddanner man f.eks. medarbejderne i korrekt brug af systemer og værktøjer, samt i generel sikkerhed, kan dette reducere sandsynligheden for at information om kunders rabataftaler afsløres. Det samme gælder, hvis man har begrænset adgangen til medarbejdere med et forretningsmæssigt behov.

**OBS!**Det er vigtigt, at man beskriver og noterer de relevante risici og begrundelsen for både konsekvensen og sandsynligheden i felterne ”Hvorfor vurderes konsekvens/sandsynlighed til dette?” i risikovurderingsarket. Dels så risikovurderingen kan foreligges for ledelsen og dels så man senere kan følge op på, om der er ændringer i risikobilledet (trusler, sårbarheder, konsekvenser og/eller nye emner, der skal vurderes).

## 2.1 Resultatet

Den beregnede risiko man har fundet frem til ovenfor, med de nuværende sikkerhedstiltag, kaldes også restrisikoen.

Restrisikoen farves/grupperes ud fra virksomhedens risikovillighed, så man kan se hvilke risici ledelsen umiddelbart kan leve med og hvornår man skal gøre noget for håndtere dem, f.eks.ved at gennemføre nye tiltag. Se eksempelvis:



I det medfølgende ark udtrykkes risikovilligheden i en farveskala, baseret på katagorierne lav, mellem og høj. Dvs. at den beregnede risiko fra 1-25 opdeles i intervaller, som vist i modellens kolonne Q:

* Grøn farve er en lav risiko, på 5 eller derunder, hvor risici umiddelbart kan accepteres af ledelsen.
* Gul farve er en mellem risiko, fra 6 til og med 9. Her vurderer ledelsen fra gang til gang, om man kan acceptere risikoen eller om man vil gøre noget for at nedbringe den, eksempelvis ved at indføre ekstra foranstaltninger.
* Rød farve er en høj risiko, på 10 eller derover. Her bør der gøres noget for at håndtere risikoen.

Denne opdeling afspejler en passende lav risikovillighed, hvor man kan leve med meget store konsekvenser (5), bare sandsynligheden er lav (1). Stiger sandsynligheden til 2, bliver risikoen 10 og kan derfor ikke accepteres (markeret med rød). Det glæder også, hvis man eksempelvis har en risiko med en mulig (3) sandsynlighed for en høj konsekvens (4). Så bliver risikoen 12 og kan heller ikke accepteres.

Hvis man ønsker en anden fordeling af værdierne i forhold til farverne (risikovilligheden), kan man ændre dette ved at angive andre tal i kolonne Q for de enkelte farver. Har man eksempelvis en høj risikovillighed, kunne gul farve sættes fra 8 til 14 og rød kunne være 15 eller derover. Grøn er så 7 eller derunder.

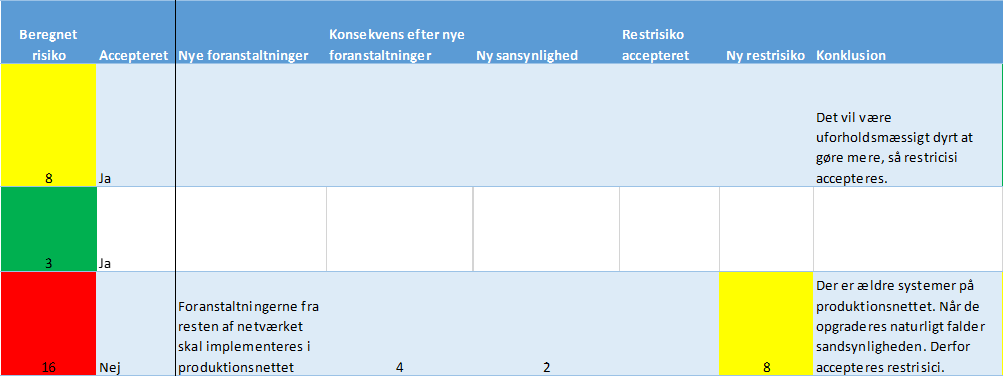
Overvejelser om hvilke risici, der skal gøres noget ved og hvad som skal gøres, dokumenteres i en risikohåndteringsplan.

## 2.2 Risikohåndteringsplan

Med udgangspunkt i risikovurderingen vurderes det, om sikkerheden er på et acceptabelt niveau, eller om man skal iværksætte flere sikkerhedstiltag, for at reducere sandsynligheden for den enkelte trussel mod det enkelte aktiv. Dette vil afhænge af om det er økonomisk rentabelt. Man kan også overveje at ophøre med de risikobetonede aktiviteter, hvis det er muligt. Endelig kan man overveje, om man kan dele den resterende risiko med leverandører eller forsikre sig ud af det.

I ovenstående eksempel, vil det klart være nødvendigt at gøre noget ved risiko nr. 3. F.eks. at man som minimum implementerer den samme sikkerhed i produktionsnettet, som i resten af netværket.  
Man kan overveje, om der er noget, man kan gøre ekstra, for at nedbringe sandsynligheden for risiko nr.1. Risiko nr. 2 kan man godt acceptere.

Risikohåndteringsplanen kan enten beskrives i et særskilt dokument eller indbygges som ekstra kolonner i det regneark man bruger til risikovurderingen. I det medfølgende regneark kan de sidste kolonner (J-O) bruges. Her kan man angive om restrisici kan accepteres eller om der skal gøres noget ved dem. I tilfælde af at der skal gøres noget, noteres de nye foranstaltninger og hvilken ny sandsynlighed, og dermed ny restrisici, det vil give. Se eksempelvis:



## Vedligeholdelse

Risikovurderingen og -håndteringsplanen er ikke statiske dokumenter, som efter ledelsens godkendelse, bare kan ”sættes hen på en hylde”.

Ud over at risikohåndteringsplanen skal implementeres, herunder opdateringer af f.eks. beredskabsplanen, skal man følge op på, om der er ændringer i risikobilledet (trusler, sårbarheder, konsekvenser og/eller nye emner, der skal vurderes). Er der det, skal processen gentages for de pågældende ændringer.

Ideelt sker det løbende, f.eks. ved større ændringer i virksomhedens it eller processer, og når der opdages nye trusler. Man bør sikre sig, at det sker regelmæssigt, f.eks. mindst en gang om året, med en hyppighed baseret på hvor dynamisk virksomhedens verden er.

Er der identificeret røde risici, bør man følge op og rapportere på disse oftere. Hvis der omvendt er risici som gentagende gange er grønne, kan man måske gøre det lidt sjældnere for dem, f.eks. hvert andet år.

Der bør også være en proces, som orienterer ledelsen om større ændringer i risikobilledet og vurderingerne. Som minimum bør den sikkerhedsansvarlige bringe det op på næste ledelsesmøde.

1. <https://digst.dk/sikkerhed/hjaelp-til-sikkerhedsarbejdet/vejledninger-til-sikkerhedsarbejdet/risikovurdering/> [↑](#footnote-ref-1)
2. <http://www.cert.org/resilience/products-services/octave/>. [↑](#footnote-ref-2)
3. <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/at_download/file> [↑](#footnote-ref-3)