DIGITALISERINGSSTYRELSEN

# Vejledning i it-risikostyring og -vurdering

Februar 2015

Vejledning i it-risikostyring og -vurdering

Udgivet februar 2015

Udgivet af Digitaliseringsstyrelsen

Publikationen er kun udgivet elektronisk

Henvendelse om publikationen
kan i øvrigt ske til:

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Tlf. 33 92 52 00

Publikationen kan hentes på
Digitaliseringsstyrelsens hjemmeside
www.digst.dk.

Foto Colourbox

Elektronisk publikation
ISBN 978-87-93073-09-8

# Indhold

# 1. Formålet med risikostyring

I alle organisationer er brugen af systemer, informationer og data i det hele taget forbundet med risici i større eller mindre omfang. Alle risici kan ikke fjernes helt, men det er muligt at styre dem ved hjælp af en systematisk tilgang til styringen.

Formålet med risikostyring er, at organisationens ledelse kan prioritere ressourcerne i forhold til, hvor de gør mest gavn. Risikovurderingen gør ledelsen bekendt med de aktuelle risici, så organisationen ikke udsætter sig for større risici, end hvad der er acceptabelt.

**Hvad er risiko?**

I ISO27000:2013 betegnes risiko som noget neutralt - *effect of uncertainty on objectives* – eller på dansk som effekten af usikkerhed på målsætninger. En risiko kan således både være en god eller negativ ting - alt efter hvad målsætningen er. Den almindelige forståelse af begrebet på dansk er dog, at risiko er negativt ladet, altså at noget uønsket sker.

Risikoen måles ved at bedømme, hvor stor sandsynlighed der er for, at en trussel vil kunne påvirke en sårbarhed og skabe en risiko, og hvor store konsekvenser det kan have. Konsekvenserne er de forretningsmæssige konsekvenser, dvs. hvilken betydning det vil have for organisationen og dens målsætninger. Sandsynligheden tager udgangspunkt i de trusler og sårbarheder, som findes.

De fleste organisationer benytter i forvejen risikostyring som et værktøj til at styre organisationen i den rigtige retning. For eksempel vil der typisk være en strategisk risikostyring, hvor de forretningsmæssige mål tilpasses.

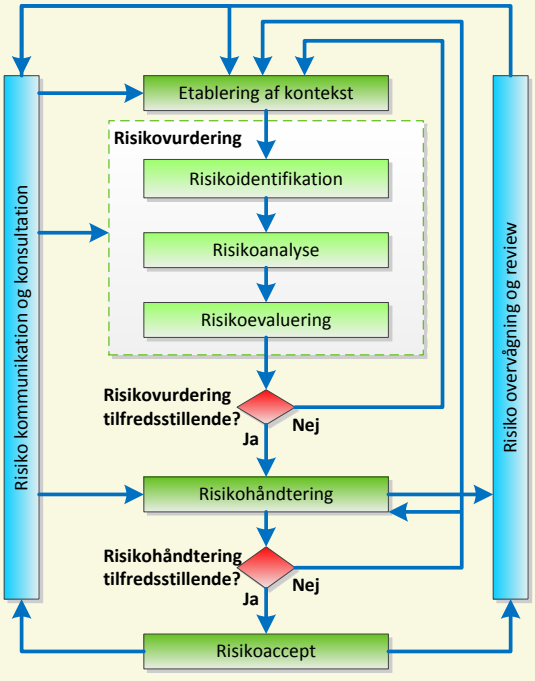
Risici i relation til brud på fortrolighed, integritet og tilgængelighed af data og systemer skal styres som en del af organisationens ledelsessystem for informationssikkerhed (ISMS). Dokumentationen og styringen af dette arbejde klarer nogen organisationer fint i Excel, mens andre har købt målrettede systemer. Det mest hensigtsmæssige vil i mange tilfælde være at integrere informationssikkerhedsstyringen med den øvrige risikostyring. En samlet risikostyringsproces og rapportering vil give et mere overskueligt og fyldestgørende risikobillede.

# 2. Risikostyringsprocessen

I ISO27005 beskrives forslag til arbejdet med it-risikovurderinger. Standarden tager udgangspunkt i en generisk tilgang til risikostyring, som bygger på ISO31000. Denne tilgang kan anvendes, uanset hvilken type af risici der er tale om. Processen for risikovurdering, som beskrives i ISO27005, er i overensstemmelse med kravene til risikostyring i ISO27001 og er udgangspunktet for denne vejledning.

Risikostyringsprocessen, som illustreret i figuren nedenfor, består af seks hovedaktiviteter, hvoraf de tre omhandler risikovurderingen. De seks aktiviteter beskrives kort i det efterfølgende. For en mere detaljeret beskrivelse henvises til ISO27005.

**Illustration af risikostyringsprocessen**




**Kilde: ISO 27005**

# Etablering af kontekst

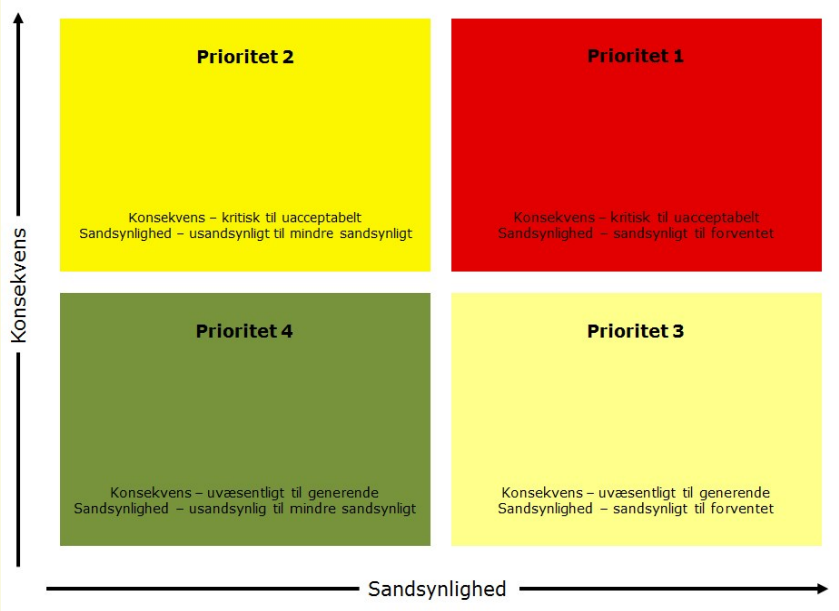
Med etablering af kontekst fastsættes rammerne for risikostyringen. Der foretages organisatorisk, fysisk og teknisk afgrænsning af risikostyringens omfang, der udpeges roller og ressourcer, defineres kriterier for risikotolerance og beskrives en metode for risikovurderingen.

# Risikovurdering

Risikovurderingen er omdrejningspunktet i risikostyringen. Her identificeres, analyseres og evalueres risici med udgangspunkt i den definerede kontekst. Resultatet af risikovurderingen er en liste over risici, som er prioriteret i forhold til de foruddefinerede kriterier. Risikovurderingen er yderligere beskrevet i sidste halvdel af denne vejledning.

Organisationens risici kan med fordel præsenteres grafisk i en illustration som i den nedenstående matrix, hvor risici placeres efter konsekvens og sandsynlighed.

**Risikobilledet i forhold til konsekvens og sandsynlighed**




Den mest almindelige fremgangsmåde er at tage udgangspunkt i aktiverne og vurdere dem ud fra den vurderede sandsynlighed og konsekvens. Alternativt kan risikobilledet fx udarbejdes ved at tage udgangspunkt i de forretningsprocesser, som aktiverne understøtter, eller som risiciene primært vil have indflydelse på.

# Risikohåndtering

Der er fire muligheder for at håndtere risici:

1. Acceptér (risikoen accepteres, og der foretages ikke yderligere).
2. Flyt (risikoen overføres til en tredjepart, fx ved hjælp af forsikring, outsourcing eller lignende).
3. Undgå (risikoen undgås ved at stoppe eller ændre den aktivitet, som er årsag til risikoen).
4. Kontroller (risikoen kontrolleres ved at indføre foranstaltninger, som fjerner eller reducerer sandsynligheden eller konsekvenserne).

Som en del af risikohåndteringen udarbejdes en plan for, hvordan de identificerede risici skal håndteres. Når der udvælges kontroller til reducering af risici, skal det ske ud fra en cost/benefit-vurdering, så kontrollernes effekt på risikoen vurderes i forhold til omkostningerne.

I forlængelse af risikohåndteringsplanen bør organisationen opdatere SoA-dokumentet. SoA-dokumentet skal bl.a. indeholde en beskrivelse af de kontroller, som organisationen har valgt at implementere. SoA-dokumentet bør derfor altid opdateres, når der er gennemført en risikovurdering og taget beslutning om at ændre på kontrollerne.

I *Vejledningen til SoA-dokumentet* kan der findes mere information om, hvordan det udarbejdes og vedligeholdes.

# Kontroller

Formålet med implementering af kontroller er at reducere risikoen. I ISO27000:2013 er en kontrol defineret som en foranstaltning, som ændrer risikoen. Kontroller omfatter enhver proces, politik, plan, praksis eller andre handlinger, som ændrer risikoen.

Kontrollerne kan udføres manuelt eller automatisk.

# Risikoaccept

Risikoaccepten bør altid foretages af den øverste ledelse. Risikohåndteringsplanen kan i praksis benyttes som en anbefaling/indstilling fra informationssikkerhedsudvalget til ledelsen. Her anføres det, hvilke tiltag, som bør indføres, og hvilke risici, som bør accepteres med udgangspunkt i de fastsatte kriterier for risikotolerance.

Selvom risici kontrolleres ved at indføre yderligere kontroller, vil der i de fleste tilfælde altid være en restrisiko. Det er vigtigt, at der i risikohåndteringsplanen foretages en vurdering af de valgte kontrollers effekt på risikoen, og at den tilbageværende risiko vurderes og beskrives.

# Opfølgning på risici

Der bør løbende foretages opfølgning på risici. Dels bør det sikres, at de kontroller og tiltag, der indføres som en del af risikohåndteringen rent faktisk også bliver implementeret og fungerer efter hensigten. Dels bør der løbende følges op på de forudsætninger, som ligger til grund for risikovurderingen. Aktiver, trusler, sårbarheder og konsekvenser kan hurtigt ændres og medfører tilsvarende ændringer i risikobilledet. Organisationens risikostyring bør derfor sikre, at der på en struktureret måde foretages en løbende opfølgning på risici.

# Kommunikation om risici

Risikostyring er en tværorganisatorisk proces, og der indgår mange interessenter med forskellige opgaver og ansvarsområder. Kommunikation er derfor en central del af risikostyringen.

Typisk vil det være informationssikkerhedsudvalget og sikkerhedskoordinatoren, som har det praktiske ansvar for risikovurderingen, mens linjeledelsen har ansvaret for risici inden for eget område. For at sikre en fælles opfattelse og tilgang til risikovurderingen, bør kommunikationen planlægges, så der er en ensartet tilgang og fælles forståelse af processen.

# Risikostyring er en proces

Styring af risici er en løbende proces. Når der foretages en risikovurdering, er der tale om et øjebliksbillede af situationen på det tidspunkt, hvor vurderingen udarbejdes. Men både organisationen, informationsaktiverne, trusler, sårbarheder mv. ændres konstant.

**Hvem har ansvaret for risikovurderingen?**

Organisationens øverste ledelse har ansvar for at være orienteret om risikobilledet og træffe de nødvendige beslutninger for at nedbringe risici til et acceptabelt niveau. Dette ansvar omfatter også de operationelle risici, som opstår ved brug af informationssystemer.

Typisk vil ansvaret blive varetaget af informationssikkerhedsudvalget, som så foretager periodisk rapportering til den øverste ledelse.

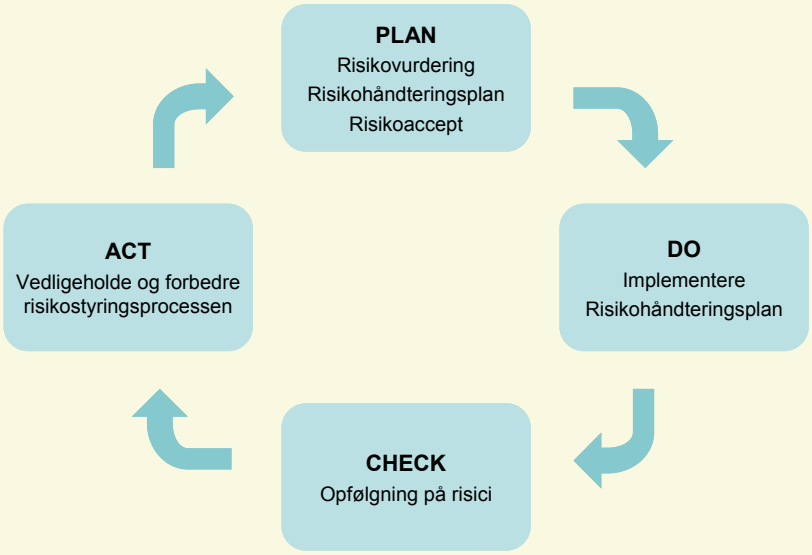
Følgende roller har ligeledes opgaver i relation til risikostyringen:

- Systemejer skal sikre styring af risici i relation til det enkelte it-system.
- Dataejer skal sikre styring af risici i relation til data.
- Ejere af fysiske aktiver skal sikre styring af risici relateret til disse.

Der skal derfor gennemføres periodiske risikovurderinger, dels for at følge op på risici og de tiltag, som implementeres, og dels for at følge op på selve risikostyringsprocessen og de overordnede rammer og principper, som ligger til grund herfor.

I figuren nedenfor er de forskellige aktiviteter i risikostyringsprocessen illustreret i plan-do-check-act-modellen.

**Risikovurdering sat ind i plan-do-check-act-modellen**



# 3. Risikovurdering

Risikovurderingen er fundamentet for risikostyringsprocessen. Det er her, at risici skal

- identificeres og beskrives (risikoidentifikation)
- analyseres og måles (risikoanalyse)
- evalueres i forhold til risikotolerancen (risikoevaluering).

## Risikovurdering kræver proces

Risikovurderingen bør altid foretages ud fra en fastlagt proces. De enkelte aktiviteter i risikovurderingen er uddybet nedenfor. Der er intet metodekrav i ISO27001 til, hvordan risikovurderingen gennemføres. Valg af metode kan bl.a. afhænge af organisationens størrelse og kompleksitet. Dog skal der altid gennemføres en vurdering af risikoen for tab af fortrolighed, integritet og tilgængelighed. Hvordan risikovurderingen i praksis udføres skal fremgå af en proces- og metodebeskrivelse, så risikovurderingen bliver systematisk og resultaterne sammenlignelige. Flere af aktiviteterne vil med fordel kunne udføres samtidigt. For eksempel vil mange risici både kunne identificeres og analyseres af de samme personer.

Identifikationen af risici bør være så omfattende som muligt. Det er bedre at inkludere for meget end at afgrænse sig fra potentielle risici. Desuden bør alle risici inkluderes, uanset om organisationen har indflydelse på dem eller ej.

### Processer

Når risici skal identificeres, kan der med fordel tages udgangspunkt i organisationens forretningsprocesser. Ved at gennemgå processerne opnås et overblik over, hvilke aktiver, der understøtter processerne og deres betydning herfor. Samtidig er det muligt at identificere sammenhæng og afhængigheder mellem aktiverne, som i sidste ende kan have stor betydning for risikoen. Et aktiv kan fx anvendes af flere forretningsprocesser til forskellige formål og med forskellige konsekvenser, hvis der sker en hændelse.

Overblik og kendskab til processerne er en forudsætning for at vurdere konsekvenserne for organisationen ved potentielle sikkerhedshændelser. Hvis hændelser har forskellige konsekvenser for forretningsprocesserne, skal der altid tages udgangspunkt i den mest alvorlige.

### Aktiver

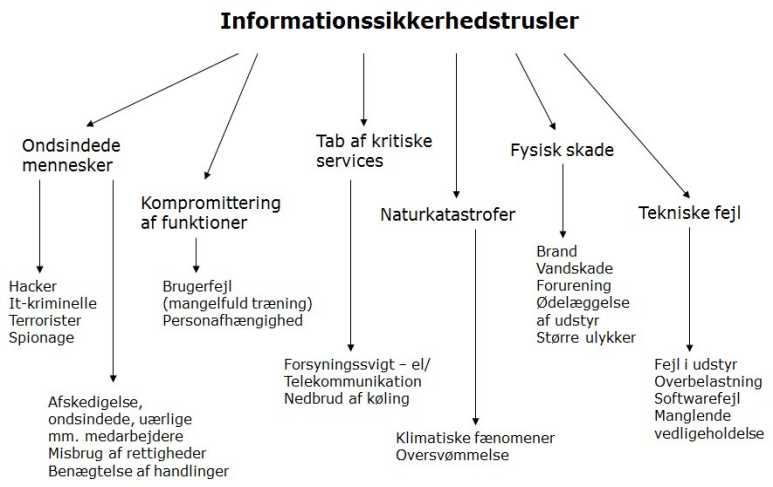
Risikoidentifikationen bør tage udgangspunkt i de aktiver, som er omfattet af organisationens informationssikkerhedsarbejde. Aktiverne bør identificeres på et passende niveau i forhold til organisationens størrelse og det ønskede detaljeringsniveau af risikovurderingen. I mange tilfælde kan aktiverne grupperes på en måde, hvor antallet begrænses, mens det stadig er muligt at knytte specifikke trusler til dem. For eksempel kan routere, switche, firewalls mv. grupperes som netværksudstyr eller infrastruktur.

Risikovurderingen bør ikke kun omfatte it-systemer men alle de aktiver, som indgår i et informationssystem. Det inkluderer også fysiske aktiver som fx papirarkiver, medarbejdere, immaterielle aktiver mv. Aktiverne kan med fordel grupperes efter deres type for at lette identifikationen, eftersom der ofte vil være en sammenhæng med de relevante trusler. I ISO27001 er der intet krav om, at risikovurderingen skal tage sit afsæt i aktiverne, men hvis organisationen har god erfaring med det, er det naturligvis en god idé at fortsætte. Ellers kan risikovurderingen gå på tværs af organisationen og tage sit afsæt i forretningsprocesserne.

## Trusler

Identifikationen af relevante trusler er afgørende for, at man ikke overser risici. Derfor bør trusselsvurderingen ske på en systematisk måde. Ved at tage udgangspunkt i et katalog over mulige trusler kan organisationen pejle sig ind på de trusler, der er relevante for de enkelte aktiver. Der findes meget omfattende trusselskataloger, som indeholder enhver tænkelig situation, men man kan også anvende mere generiske kataloger.

**ISO27005:2011 Risikoledelse**




Ifølge National strategi for cyber- og informationssikkerhed er det endvidere et krav, at cybertrusler indgår i myndighedernes risikovurderinger og risikoledelse fra 2015. I ISO27005 i anneks C beskrives et eksempel på mulige trusler. Disse trusler er opdelt i nogle hovedgrupper, som vist i figuren ovenfor. Der kan også ses på de trusselsvurderinger, som løbende udarbejdes af GovCERT[1] og øvrige myndigheder og organisationer på området.

[1] GovCERT er i dag en del af netsikkerhedstjenesten, der forebygger og imødegår avancerede cyberangreb rettet mod tilsluttede myndigheder og virksomheder. Netsikkerhedstjenesten medvirker til, at der i staten er overblik over avancerede cyberangreb rettet mod brugerkredsen. GovCERT er placeret hos Center for Cybersikkerhed.

## Sårbarheder

En trussel kræver en sårbarhed for at kunne resultere i en risiko og omvendt. Sårbarheder kan opstå i mange forskellige sammenhæng. Det kan for eksempel være en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør it-systemerne åbne for angreb. En god måde at få afdækket sårbarhederne på er ved at gennemgå de implementerede kontroller og vurdere deres effektivitet. Her kan igen tages udgangspunkt i SoA-dokumentet, hvis det er udarbejdet.

## Risikoanalyse

Den sidste del af risikoidentifikationen er en identifikation af de konsekvenser, som et tab af fortrolighed, integritet eller tilgængelighed for aktiverne vil medføre. Det er vigtigt at tage udgangspunkt i de forretningsmæssige konsekvenser, dvs. hvilken betydning det vil have for organisationen som helhed og ikke kun for et afgrænset område. Konsekvenserne kan opdeles i forskellige typer. Det kan være direkte økonomiske tab, ressourceforbrug, tid/forsinkelser, tab af omdømme, politiske konsekvenser mv.

Begreberne sandsynlighed, konsekvens og eksempler på maksimalt acceptabel nedetid er beskrevet i skemaerne på de næste sider. Disse termer anvendes til beskrivelse af sandsynlighed og konsekvens for risici samt klassifikation af systemer under vurderingen.

**Tabel med beskrivelse af sandsynlighed**

| Sandsynlighed | Eksempelbeskrivelse |
|---|---|
| **Usandsynligt** | Det anses for næsten udelukket, at hændelsen nogensinde kan forekomme<br>- Ingen erfaring med hændelsen<br>- Kendes kun fra få andre offentlige og private virksomheder, men ikke i Danmark |
| **Mindre sandsynligt** | Hændelsen forventes ikke at komme<br>- Ingen erfaring med hændelsen<br>- Kendes kun fra få andre offentlige og private virksomheder, men ikke i Danmark |
| **Sandsynligt** | Det er sandsynligt at hændelsen vil forekomme<br>- Man har erfaring med hændelsen, men ikke inden for de sidste 12 måneder<br>- Kendes fra andre offentlige og private virksomheder i Danmark (omtales årligt i pressen) |
| **Forventet** | Det ventes at hændelsen vil forekomme<br>- Man har erfaring med hændelsen inden for de sidste 12 måneder<br>- Hænder jævnligt i andre offentlige og private virksomheder (omtales ofte i pressen) |

**Tabel med konsekvensskala og konsekvenstyper**

| | Konsekvensskala | | | |
|---|---|---|---|---|
| **Konsekvenstype og konsekvensbeskrivelse** | Ubetydelig (uvæsentlig) | Mindre alvorlig (generende) | Meget alvorlig (kritisk) | Graverende/ ødelæggende (uacceptabelt) |
| **Strategisk** Medfører indskrænkninger i evnen til at handle i en periode | Ingen særlig påvirkning | Planlagte aktiviteter kan gennemføres med mindre justeringer | Medfører revurdering af vigtige aktiviteter på kort sigt | Bliver ude af stand til at gennemføre vigtige aktiviteter, som er planlagt i en periode fremover |
| **Økonomisk** Medfører meromkostninger eller tab | Ingen særlig påvirkning | Meromkostninger og tab i begrænset niveau, som kan kræve mindre budgetændringer | Store økonomiske tab med risiko for at blive sat under administration | Væsentlige økonomiske tab. Bliver sat under administration |
| **Administrativ/ procesmæssig** Medfører administrative belastninger | Håndteres uden særligt ressourcetræk i de administrative funktioner | Håndteres inden for rimeligt ekstra administrativt ressourcetræk | Der må trækkes væsentligt på eksisterende og nye administrative ressourcer | Administrative ressourcer må udvides urealistisk |
| **Omdømme** Påvirker omdømme i uønsket retning | Ingen særlig påvirkning | Forbigående opmærksomhed fra enkelte grupper | Offentligheden fatter generel negativ interesse, som kan medføre begrænset tab af kunder | Væsentlig skade på omdømme. Ministeren må gå af |
| **Politisk/strategisk** Medfører indskrænkninger i evnen til at handle i en periode | Ingen særlig påvirkning | Planlagte aktiviteter kan gennemføres med mindre justeringer | Medfører revurdering af vigtige aktiviteter på kort sigt | Ledelsen må gå af. Bliver ude af stand til at gennemføre vigtige aktiviteter, som er planlagt i en periode fremover |
| **Forhold til interessenter** Påvirker forholdet til interessenter | Ingen særlig påvirkning | Forringet samarbejde med interessenter i enkeltsager | Generelt forringet samarbejde med interessenter | Væsentligt nedbrud i det generelle samarbejde med interessenter |
| **Menneskelige** Medfører konsekvenser for det enkelte individ | Ingen særlig påvirkning | Den enkelte udsættes for gener, men ikke noget alvorligt | Alvorlig personskade | Menneskeliv står på spil |
| **Privacy** Medfører brud på privatlivets red (privacy) | Ingen særlig påvirkning | Der er formelle mangler i de oplysninger, der gives den enkelte, men ikke i graverende grad | Den enkelte fratages råderetten over egne data. Ikke-følsomme data videregives uretmæssigt | Den enkelte udsættes for uacceptable krænkelser af privatlivet. Der træffes bebyrdende afgørelser mod den enkelte på et forkert grundlag. Følsomme data videregives uretmæssigt |
| **Brud på lovgivningen** Medfører brud på lovgivning, f.eks. forvaltningslov og straffelov | Ingen særlig påvirkning | Manglende overholdelse af administrative procedurer og regler, som ikke er af kritisk karakter | Lovbrud, der er kritiske og kan stille ministeriet i miskredit | Kritisk lovgivning, f.eks. straffeloven brydes. Ministeren må gå af |

**Tabel med beskrivelse af acceptabel nedetid**

| Acceptabel nedetid | Beskrivelse |
|---|---|
| **Under 4 timer** | Manglende tilgængelighed vil være tidskritisk næsten med det samme. |
| **4 – 8 timer** | Manglende tilgængelighed må helst ikke vare mere end en enkelt arbejdsdag. |
| **2 dage** | Et par dages utilgængelighed er det maksimalt tilladelige. |
| **Under en uge** | Manglende tilgængelighed må vare mere end et par dage men helst ikke en hel arbejdsuge. |
| **Mere end en uge** | Manglende tilgængelighed må vare mere end en uge. |

Der findes flere hjælpeværktøjer, som kan bruges til at lette arbejdet med at registrere og beskrive risici.

Nedenfor er vist et eksempel på et ark til opsamling af risici og dokumentation af vurderingen af konsekvens og sandsynlighed.

## Eksempel på Excel-ark til registrering af risici

**Eksempel på Excel-ark til registrering af risici**

| Aktiv navn | Aktiv kategori | Trusler | Sårbarheder | Sandsynlighed | Konsekvens | Konsekvenstype | Vægtning | Forklaring | Risiko |
|---|---|---|---|---|---|---|---|---|---|
| System A | It-systemer | Scenarie 1: Tekniske fejl - Softwarefejl | Software: Utilstrækkelig test | Sandsynligt (3) | Generende (2) | Administrativ | 1 | ..... | Middel |
| Krydsfelt | It-infrastruktur | Scenarie 5: fysisk skade - ødelæggelse | Hardware: Udsat placering | Sandsynligt (3) | Kritisk (3) | Administrativ | 1,5 | ..... | Høj |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

I forlængelse af vurderingen af konsekvenserne kan man med fordel samtidig opdatere informationsaktivets klassifikation og kritikalitet. Disse oplysninger anvendes i flere sammenhænge til at bestemme, hvilke kontroller, beredskabsniveau mv., som aktivet skal have.

Klassifikationen er en vurdering af, hvor følsomme informationerne er, og hvilke krav der er til fortroligheden. Der anvendes ofte 3-5 forskellige niveauer, fx offentligt, internt, fortroligt mv.

Kritikaliteten bruges oftest som betegnelse for, hvor vigtig tilgængeligheden (og eventuelt integriteten) er for aktivet. Det er vigtigt, at systemerne kategoriseres korrekt i forhold til behovet for tilgængelighed.

**Kategorisering af systemkritikalitet**

A. Korte systemafbrud (timer) vil medføre katastrofale følgevirkninger for forretningen som følge af væsentlige og uoprettelige svigt i målopfyldelse eller brud på love eller aftaler.
B. Langvarige afbrud (dage) vil medføre katastrofale følgevirkninger for forretningen som følge af væsentlige og uoprettelige svigt i målopfyldelse eller brud på love og aftaler.
C. Afbrud vil medføre væsentlig ulempe, men vil ikke i væsentlig grad hindre målopfyldelse eller føre til brud på love eller aftaler.
D. Afbrud medfører mindre ulemper og begrænsede tab eller omkostninger.

Formålet med risikoanalysen er at måle størrelsen af de identificerede risici i form af sandsynligheden og konsekvensen. Overordnet set kan dette gøres på to forskellige måder, kvantitativt eller kvalitativt.

Med en kvantitativ fremgangsmåde anvendes numeriske værdier som for eksempel procenter eller kroner og øre. Det kan være meget omfattende at udføre en kvantitativ analyse, og det vil ofte være svært at sætte tal på de indirekte konsekvenser såsom tab af omdømme. En måde at gribe det an på kan være ved at spørge, hvor meget man er villig til at betale for at undgå en bestemt hændelse.

De kvalitative metoder definerer skalaer med et vist antal trin. Herefter rangordner og indplacerer man hændelser inden for disse trin. En sådan metode er relativ hurtig at anvende, om end det vil være svært at placere en konkret indeksering på en skala. Brug af kvalitative vurderinger til at indplacere hændelser er i sagens natur ikke præcise. Erfaringen viser imidlertid, at denne metode ofte giver et kvalificeret bidrag til at afdække de nødvendige indsatsområder.

I praksis kan organisationen med fordel benytte en kombination af kvalitative og kvantitative metoder i risikovurderingsprocessen. Eksempelvis kan der indledes med en kvalitativ vurdering af konsekvenser. Denne kan efterfølgende underbygges kvantitativt for at beslutte, om der i konkrete tilfælde skal indføres skærpede kontroller.

## Risikoevaluering

Det sidste skridt i risikovurderingen er evalueringen af de fundne risici i forhold til de kriterier, som er fastlagt af ledelsen. Der foretages en prioritering af risici, fx ved indplacering i en skala eller risikobillede, som illustreret på side 4. Et risikobillede er et simpelt og effektivt værktøj til at formidle risici i organisationen.

## Kontroller

De eksisterende kontroller bør gennemgås og vurderes i forhold til deres effektivitet. Dette er nødvendigt for at kunne identificere eventuelle sårbarheder, der skal håndteres. Gennem-

gangen af kontrollerne er også en forudsætning, hvis man ønsker at dokumentere effekten heraf, ved at vurdere risikoen både før og efter en kontrol er implementeret.

Hvis der er udarbejdet et SoA-dokument, som beskriver de indførte kontroller, kan der med fordel tages udgangspunkt heri.

## Ledelsesforankring

Risikovurderingen er den aktivitet, som ved involvering af ledelsen kan skabe grundlaget for ledelsesforankring.

Ved at initiere en debat og vurdering af organisationens risikobillede og -profil vil det samlede sikkerhedsarbejde og indsatserne blive synlige for ledelsen. Samtidig kan det knyttes til en prioritering af de nødvendige, fremtidige indsatser.

## Leverandørstyring

Den gennemførte it-risikovurdering vil give et samlet risikobillede, og der vil være taget stilling til eventuelle handlinger med henblik på at mindske risici gennem implementering af yderligere kontroller. Anvendes ekstern leverandør til drift af systemer og data, er det vigtigt, at leverandøren informeres om resultatet af risikovurderingen, så systemer og data beskyttes i overensstemmelse med den accepterede restrisiko.

Informationen til leverandøren kan derfor indeholde følgende:

- Samlet oversigt over risikobilledet for systemer, der er driftet hos leverandøren.
- Krav til tilgængelighed for de enkelte systemer, herunder til oppetider og maksimal acceptabel nedetid.
- Krav til fortrolighed – vurdering af korrekt beskyttelse af data både i forhold til fortrolighed generelt og i forhold til karakteren af personoplysninger som fx adgangsstyring og kryptering.
- Krav i forbindelse med tab af data.
- Krav til særlige kontroller som fx fysisk sikkerhed, adgangsstyring, driftsprocedurer, udvikling og vedligeholdelse, logning, rapportering, backup og restore.

Leverancer fra eksterne leverandører skal sikres gennem kundeaftaler. Ved særlige sikkerhedskrav, herunder håndtering af personoplysninger, skal der indgås en databehandleraftale.