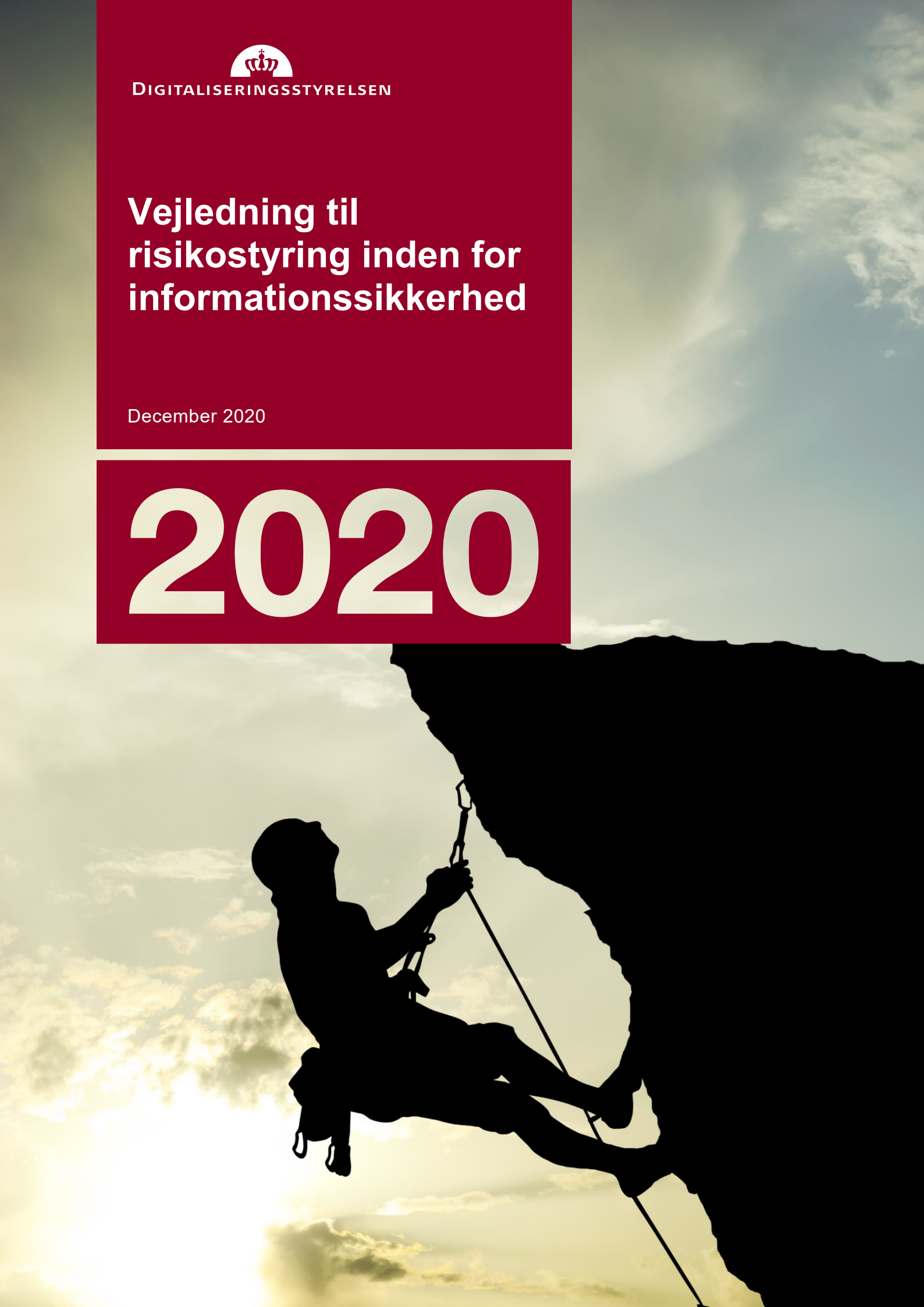
DIGITALISERINGSSTYRELSEN

Vejledning til risikostyring inden for informationssikkerhed

December 2020

2020



Indholdsfortegnelse

1. Formålet med risikostyring **4**

2. Overblik over risikostyringsprocessen **5**
Rammerne for risikostyringsprocessen 6
Hovedaktivitet 1: Etablering af kontekst 7
Hovedaktivitet 2: Risikovurdering 8
Hovedaktivitet 3: Risikohåndtering 8
Hovedaktivitet 4: Risikoaccept 9
Hovedaktivitet 5: Opfølgning på risici 9

3. Risikovurdering **10**
Risikoidentifikation 10
Risikoanalyse 13
Risikoevaluering 15

4. Risikohåndtering **17**
Udarbejdelse af risikohåndteringsplan 17
Ledelsesforankring af risikohåndteringsplan 18
Gennemførelse af risikohåndteringsplan 18
Inddragelse af leverandøren i risikohåndtering 18

5. Opfølgning og løbende forbedringer **20**
Risikostyring er en tilbagevendende proces 20

Formålet med denne vejledning er at give en bred introduktion til de grundlæggende begreber og aktiviteter i risikostyringsprocessen.

I vejledningen finder du blandt andet:

- Et overblik og kort gennemgang af risikostyringsprocessens fem hovedaktiviteter
- En model for, hvordan risikostyringsprocessen omsættes til det løbende sikkerhedsarbejde ud fra Plan-Do-Check-Act modellen
- En guide til metoden bag risikovurdering, herunder tabeller til beskrivelser af sandsynlighedsniveauer samt konsekvensskala og –typer
- Bilag der kan benyttes som inspiration til eget arbejde med risikovurdering

Vejledningen er henvendt til dig, der dagligt arbejder med informationssikkerhed i organisationen og står over for at skulle implementere en risikostyringsproces fra bunden – eller dig, der har brug for en bred indføring i det teoretiske grundlag for din organisations eksisterende risikostyringsproces. Den er også til dig, der søger konkrete skabeloner til brug for risikovurderingsarbejdet.

Her kan du læse mere
I *Vejledning til trusselsidentifikation* finder du uddybende forklaringer på begreber og metode til identifikation af trusler, som er en del af risikovurderingen. Derudover kan du på sikkerdigital.dk finde flere typer af materialer, der behandler risikostyringsprocessen hos myndigheder.

1. Formålet med risikostyring

I alle organisationer er brugen af systemer, informationer og data 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.

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 ISO 27001 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 positiv 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 sandsynligheden er for, at en trussel vil kunne påvirke en sårbarhed, og hvor store konsekvenser det kan have. Konsekvenserne er de forretningsmæssige konsekvenser, dvs. hvilken betydning det vil have for organisationen og dens målsætninger. Konsekvenser skal også vurderes for de registrerede, dvs. hvilken betydning truslen vil have for de registreredes rettigheder. Sandsynligheden tager udgangspunkt i de trusler og sårbarheder, som findes.

Risici i relation til informationssikkerheden dvs. 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. Overblik over risikostyringsprocessen

I ISO 27005 beskrives forslag til arbejdet med informationssikkerhedsrisikovurderinger. Standarden tager udgangspunkt i en generisk tilgang til risikostyring, som bygger på ISO 31000. Denne tilgang kan anvendes, uanset hvilken type af risici der er tale om. Processen for risikovurdering, som beskrives i ISO 27005, er i overensstemmelse med kravene til risikostyring i ISO 27001 og er udgangspunktet for denne vejledning.

Afgrænsning ift. ISO 27005

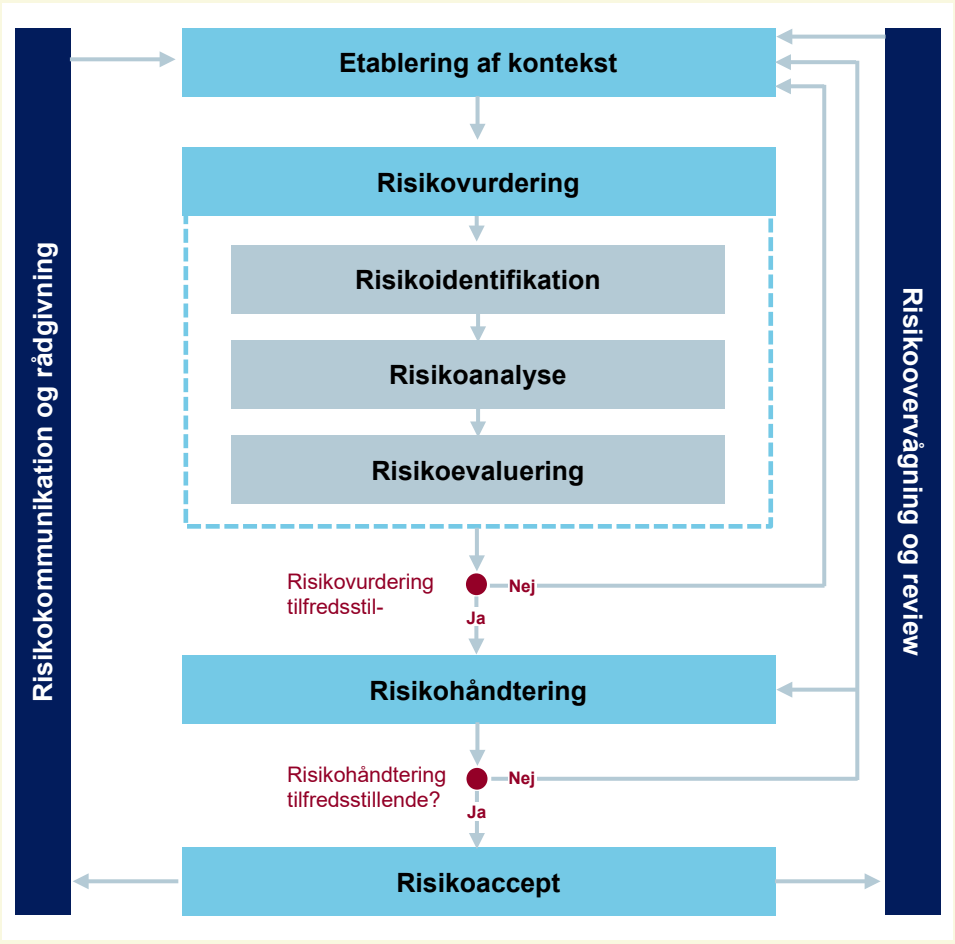
I den seneste udgave af ISO 27005 fra 2018 opereres med to typer af risikovurderinger: "*High-level information security risk assessment*" og "*Detailed information security risk assessment*". Det anbefales, at man starter med høj niveau-risikovurderingen for at få styr på prioriteringerne, fx ud fra en konsekvensvurdering: Hvad er konsekvensen, hvis en organisations sags- og dokumentstyringssystem eller forretningssystem er nede i længere tid (tilgængelighed), hvis data i systemet bliver ændret (integritet) eller hvis uvedkommende får adgang til følsomme oplysninger (fortrolighed)?

Hvis en konsekvensvurdering foretages på alle systemer og forretningsprocesser, kan man derefter gå i dybden med en mere detaljeret vurdering af trusler, sårbarheder, risici og konsekvenser på de enkelte systemer og processer i en prioriteret rækkefølge.

Denne vejledning fokuserer udelukkende på høj niveau-risikovurderingen. Det anbefales, at man anskaffer sig ISO 27005 for at kunne gå i dybden med den detaljerede risikovurdering.

Risikostyringsprocessen, som illustreret i figuren nedenfor, består af flere hovedaktiviteter. Hovedaktiviteterne er grundlæggende for den samlede proces, og de beskrives kort i det efterfølgende. I de kommende kapitler uddybes enkelte af hovedaktiviteterne yderligere.

Figur 2.1
Illustration af risikostyringsprocessen



Kilde: Inspireret af ISO 27005

Rammerne for risikostyringsprocessen

Før hovedaktiviteterne gennemgås er det vigtigt at have rammerne på plads. Risikostyring er en tværorganisatorisk proces, og der indgår mange interessenter med forskellige opgaver og ansvarsområder. Planlægning, koordination og kommunikation ligger derfor hele tiden som et bagtæppe i risikostyringsprocessen – både før og efter gennemførelse af hovedaktiviteterne. Ledelsesforankring er afgørende for en vellykket risikostyringsproces.

Typisk vil det være informationssikkerhedsudvalget med deltagelse fra ledelsen, som skal godkende og afgrænse rammerne for risikostyringen. Herunder at risikovurde-

ringsprocessen igangsættes, og at der afsættes ressourcer til, at den kan gennemføres. Dette skyldes bl.a., at de forskellige roller, fx data- og systemejere, skal medvirke til at vurdere risici og konsekvenser ved tab af fortrolighed, integritet og tilgængelighed. Denne medvirken tager tid og kræver deres deltagelse. Informationssikkerhedsfunktionen har det praktiske og koordinerende ansvar for risikostyringen, mens data- og systemejere har ansvaret for identificering og håndtering af risici inden for eget område.

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 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.**
- **Procesejere skal sikre styringen af risici i relation til processer**

For at sikre en fælles opfattelse og tilgang til risikostyringen, bør kommunikation og løbende interessenthåndtering indgå i planlægningen, så der kan komme en ensartet tilgang og fælles forståelse af processen. Det er oplagt at bruge risikovurderingen aktivt til at skabe opmærksomhed om informationssikkerhed i hele organisationen ved fx at inddrage organisationens kommunikationsenhed i planlægningen af, hvornår og hvordan der skal kommunikeres om risikovurderingen. Ved at skabe opmærksomhed om fx organisationens risikobillede og -profil vil det samlede sikkerhedsarbejde og indsatserne blive synlige. Ikke kun for ledelsen, men også medarbejdere som i større eller mindre grad bliver påvirket af ledelsens prioritering af de nødvendige, fremtidige indsatser. Det kunne fx være indførsel af nye arbejdsgange eller skærpede retningslinjer til gamle systemer.

Hovedaktivitet 1: Etablering af kontekst

Hvis organisationen skal starte sin risikostyringsproces fra ny, eller hvis organisationen i sig selv er ny, skal man først og fremmest have styr på konteksten for organisationen, fx: Hvem er vi? Hvad er kerneforretningen og prioriteter? Hvilken samfundskontekst opererer vi i? Hvis organisationen ikke starter fra ny, men allerede har defineret sin kontekst i fx informationssikkerhedspolitikken, mål- og resultatplan eller ISMS'et, benytter organisationen selvfølgelig dette som udgangspunkt.

Derudover skal man i denne fase fastsætte den organisatoriske, fysiske og tekniske afgrænsning af risikovurderingerne. Der udpeges roller og ressourcer, defineres kri-

terier for risikotolerance og beskrives en metode for risikovurderingen. Dette godkendes af ledelsen – fx via informationssikkerhedsudvalget. Se også bilag 1 for et eksempel på risikostyringsmetode.

Hovedaktivitet 2: 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 (fx organisationens strategi eller systemets eller datas kritikalitet).

I *Vejledning til Trusselsidentifikation* er der yderligere hjælp til, hvordan relevante trusler for informationssikkerheden kan identificeres i risikovurderingens første fase. Se også bilag 2 og 3 for inspiration til hhv. trussels- og sårbarhedskatalog samt bilag 4-6 for eksempler på hhv. spørgerammer tbf. risikovurderinger, konsekvens- samt sandsynlighedsskemaer.

Formelt bør risikovurdering initieres af informationssikkerhedsudvalget i organisationen eller den øverste ledelse.

Den mest almindelige fremgangsmåde er at tage udgangspunkt i de primære aktiver som forretningsprocesser og informationer og vurdere sårbarhedernes risikoniveau ud fra den vurderede sandsynlighed og konsekvens.

I kapitel 3 om risikovurdering uddybes sandsynligheds- og konsekvensvurderinger samt delprocesserne identifikation, analyse og evaluering.

Hovedaktivitet 3: Risikohåndtering

Der er fire muligheder for at håndtere risici:

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

Som en del af risikohåndteringen udarbejdes en risikohåndteringsplan, som ud fra ovennævnte muligheder beskriver, hvordan de identificerede risici skal håndteres.

Se også bilag 7 for eksempel på skema til risikoregistrering og –håndtering samt bilag 8 for eksempel på en skabelon til en risikovurderingsrapport.

Formålet med implementering af kontroller er at reducere risikoen. I ISO 27000:2020 er en kontrol defineret som en foranstaltning, som ændrer risikoen. Kontroller kan omfatte enhver proces, politik, plan, praksis eller andre handlinger, som ændrer risikoen. Kontrollerne kan udføres manuelt eller automatisk.

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 vurdere, om den bør opdatere sit Statement of Applicability (SoA) dokument. Ledelsen bør orienteres og/eller godkende både risikohåndteringsplan samt SoA-dokument.

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

I kapitel 4 nedenfor uddybes de aktiviteter, risikohåndteringen består af, yderligere.

Hovedaktivitet 4: Risikoaccept

For kritiske aktiver og processer bør risikoaccepten altid foretages af den øverste ledelse. Risikohåndteringsplanen kan i praksis benyttes som en anbefaling/indstilling fra aktiv- eller procesejeren til ledelsen. Her anføres de 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.

Hovedaktivitet 5: 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, dvs. at organisationens risikostyring følger en planlagt og tilbagevendende proces, gennemfører dokumenterede vurderinger ud fra den samme metode med henblik på at opnå sammenlignelige resultater.

Kapitel 5 nedenfor uddyber yderligere, hvordan organisationen struktureret kan følge op på risici.

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).

Risikovurderingen bør altid foretages ud fra en fastlagt metode. De enkelte aktiviteter i risikovurderingen er uddybet nedenfor. Der er intet metodekrav i ISO 27001 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.

Risikoidentifikation

Identifikationen af risici bør tage udgangspunkt i forretningens kerneområder, dvs. de mest kritiske forretningsprocesser og aktiver. Derfra kan omfanget udbygges til at omfatte flere processer og aktiver, så man ikke overser potentielle risici. Se også bilag 4 for eksempel på spørgeramme til brug for risikovurdering.

Forretningsprocesser og aktiver

Når risici skal identificeres, kan der med fordel tages udgangspunkt i organisationens forretningsprocesser. 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.

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 (eksempelvis et it-system) kan fx anvendes af flere forretningsprocesser til forskellige formål og med forskellige konsekvenser, hvis der sker en hændelse.

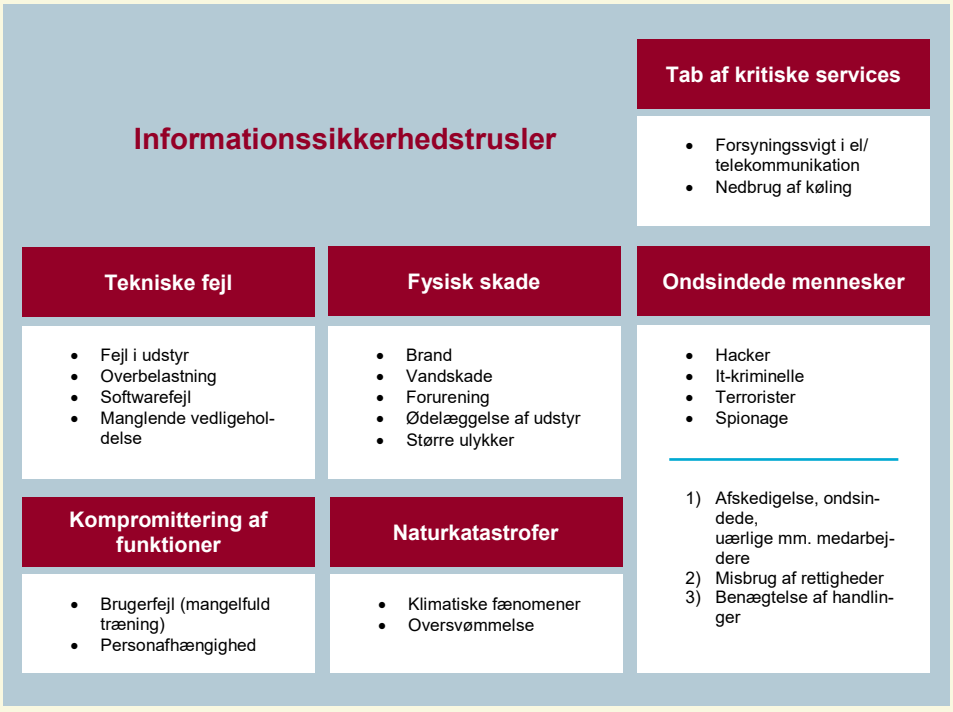
Aktiverne bør identificeres på et passende niveau i forhold til organisationens størrelse og det ønskede detaljeringsniveau af risikovurderingen. I mange tilfælde kan aktiverne grupperes på en måde, hvor antallet begrænses, mens det stadig er muligt at knytte specifikke trusler til dem. For eksempel 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 ISO 27001 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.

Figur 3.1
Informationssikkerhedstrusler



Kilde: Inspireret af ISO 27005

I ISO 27005 anneks C beskrives et eksempel på mulige trusler. Disse trusler er opdelt i nogle hovedgrupper, som vist i figuren ovenfor.

I *Vejledning til trusselsidentifikation* findes hjælp til arbejdet med at identificere relevante trusler. Se yderligere bilag 2 for eksempel på trusselskatalog.

Sårbarheder
En trussel kræver en sårbarhed for at kunne realiseres. Sårbarheder kan opstå i mange forskellige sammenhænge. Det kan for eksempel være en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør at it-systemet er åbent for angreb.

En måde at afdække sårbarheder på er ved at gennemgå de implementerede kontroller og vurdere deres effektivitet. Her kan igen tages udgangspunkt i SoA-dokumentet, hvis det er udarbejdet.

En anden måde er at tage udgangspunkt i, hvordan relevante trusler kan påvirke aktivet. Såfremt fx truslen om misbrug af systemadgange kan realiseres, hvis adgangsstyringen ikke er på plads, udgør den manglende adgangsstyring en sårbarhed.

Der kan i forbindelse med sårbarhedsvurderingen tages udgangspunkt i et sårbarhedskatalog. Se fx ISO 27005 for et sårbarheds- og trusselskatalog samt bilag 3 til denne vejledning for et eksempel på et sårbarhedskatalog.

Hvis it-driften er outsourcet til en ekstern leverandør vil det være en god ide at inddrage dem i forbindelse med sårbarhedsvurderingen, da de har viden om de tekniske løsninger og tekniske kontroller der er etableret og dermed også hvilke tekniske sårbarheder der er.

Risikoanalyse

Formålet med risikoanalysen er at vurdere sårbarhedens risikoniveau ud fra sandsynlighed og konsekvens.

Nedenfor ses en risikomatrice, der er en måde at illustrere risikoanalysen på.

Tabel 3.1
Risikomatrice

Konsekvens					
Graverende/Ødelæggende (uacceptabelt)	Under middel Score: 4	Middel Score: 8	Over middel Score: 12	Høj Score: 16	
Meget alvorlig (kritisk)	Lav Score: 3	Under middel Score: 6	Middel Score: 9	Over middel Score: 12	
Mindre alvorlig (generende)	Lav Score: 2	Under middel Score: 4	Under middel Score: 6	Middel Score: 8	
Ubetydelig (uvæsentlig)	Lav Score: 1	Lav Score: 2	Lav Score: 3	Under middel Score: 4	
	Usandsynligt	**Mindre sandsynligt**	**Sandsynligt**	**Forventet**	**Sandsynlighed**
	Lav - under middel: Bør ikke give anledning til yderligere behandling				
	Middel: bør give anledning til løbende overvågning				
	Over middel: Bør give anledning til håndtering				
	Høj: Bør håndteres med det samme				

Risikoanalysen kan udarbejdes 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. Denne metode 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.

Identifikation af konsekvens og sandsynlighed
En del af risikoanalysen er en identifikation af konsekvenserne ved et aktivs tab af fortrolighed, integritet eller tilgængelighed. 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. Derudover skal konsekvenserne for de registrerede vurderes i tilfælde af, at der behandles personoplysninger i aktivet.

Konsekvenserne kan opdeles i forskellige typer. Det kan være direkte økonomiske tab, ressourceforbrug, tid/forsinkelser, tab af omdømme, politiske konsekvenser mv. Man bør forholde sig til hvilke konsekvenstyper, der er vigtige for organisationen. Er miljømæssige konsekvenser vigtigere end økonomiske eller menneskelige? I sidste ende kan det have betydning for hvilke risikomitigerende tiltag, der etableres. Se også bilag 5 og 6 for eksempler på konsekvens- og sandsynlighedsskemaer.

I tabellen ses et eksempel på en beskrivelse af maksimalt acceptabel nedetid. Dog er det vigtigt, at konsekvensen ikke blot vurderes ved et tilgængelighedsbrud men også ved et fortroligheds- og integritetsbrud.

Tabel 3.2
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.

Et værktøj kan hjælpe arbejdet med at vurdere og håndtere risici. Se bilag 4 for eksempel på værktøj til at vurdere risici samt bilag 7 for et eksempel på skema til registrering af risici.

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, tilgængeligheden og integriteten. Klassifikation kan foretages

med udgangspunkt i sikkerhedscirkulærets[1] fastlagte principper samt ud fra organisationens interne principper for klassifikation. For den interne klassifikation anvendes ofte 3-5 forskellige niveauer, fx offentligt, internt, fortroligt mv.

Klassifikationen kan foretages ud fra en vurdering af kritikaliteten. Kritikaliteten angiver i hvilken, og i hvor høj grad, det påtænkte system vil kunne medføre uønskede konsekvenser for den understøttede del af forretningens opretholdelse, fx ved ukomplette data, systemfejl, datakorrumpering og nedbrud. Ved høj kritikalitet kan forretningen ikke varetages. Ved mellem kritikalitet kan forretningen varetages, men med store negative konsekvenser for myndigheden. Ved lav kritikalitet vil det påvirke omdømme og være til gene for myndigheden. Nedenfor ses et eksempel på vurdering af kritikalitet ud fra tilgængelighed.

Kategorisering af systemkritikalitet ift. tilgængelighedsbrud

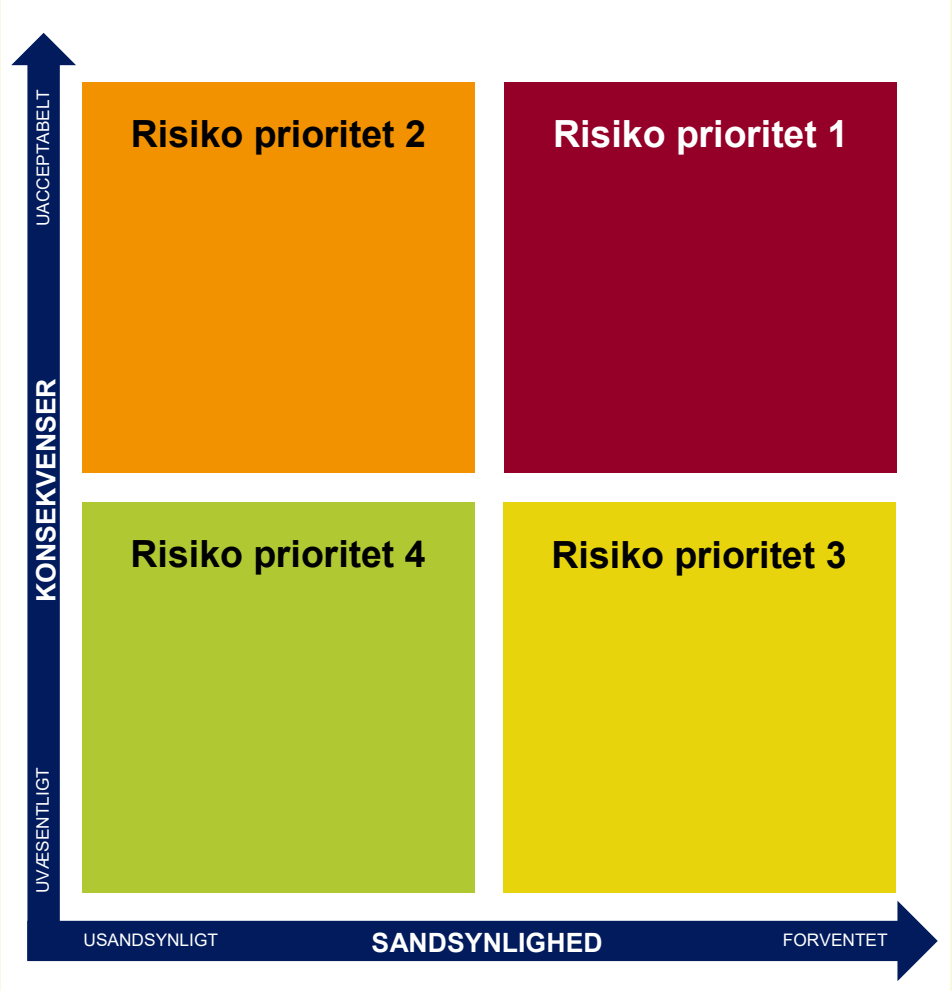
- **A. Korte systemafbrud (timer) vil medføre katastrofale følgevirkninger for forretningen som følge af væsentlige og uoprettelige svigt i målopfyldelse eller brud på love eller aftaler.**
- **B. Langvarige afbrud (dage) vil medføre katastrofale følgevirkninger for forretningen som følge af væsentlige 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.**

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 nedenfor. Et risikobillede er et simpelt og effektivt værktøj til at formidle risici i organisationen. Se også bilag 8 for eksempel på skabelon til risikovurderingsrapport.

[1] Sikkerhedscirkulæret er et regelsæt, som angiver en række bestemmelser for håndtering, opbevaring og behandling af klassificeret information. Formålet er at beskytte klassificeret information tilstrækkeligt og ensartet i Danmark, NATO og EU. Danske myndigheder er internationalt forpligtet til at overholde disse regelsæt.

Figur 3.2
Risikobilledet i forhold til konsekvens og sandsynlighed



4. Risikohåndtering

Risikohåndtering består af tre hovedaktiviteter:

- Udarbejdelse af en risikohåndteringsplan
- Ledelsesforankring af risikohåndteringsplan
- Gennemførsel af risikohåndteringsplan

Anvendes en ekstern leverandør til outsourcet drift af systemer og behandling af data, er det vigtigt, at leverandøren er inddraget i risikohåndteringen.

Udarbejdelse af risikohåndteringsplan

Første trin i risikohåndteringen er etableringen af en risikohåndteringsplan. Planen etableres ud fra de ovenfor nævnte muligheder for at håndtere risici:

Modificér betyder, at man etablerer kontroller, der mindsker sandsynligheden for en hændelse eller mindsker konsekvensen, når en hændelse sker. Disse tiltag kan være af såvel teknisk som administrativ karakter. Tiltag, der mindsker sandsynligheden for sikkerhedshændelse benævnes *forebyggende tiltag* og tiltag, der mindsker konsekvenserne af sikkerhedshændelser benævnes *udbedrende tiltag*.

Acceptér betyder, at organisationen vælger at leve med en risiko. Denne måde at håndtere risici på, er en naturlig følge af, at 100% sikkerhed ikke findes.

Undgå. Denne mulighed indebærer typisk, at organisationen ophører med en aktivitet, som giver anledning til en given risiko. Det kan f.eks. være et usikkert system, man holder op med at bruge.

Del betyder, at organisationen håndterer risikoen ved at dele den med andre. For eksempel gennem forsikring eller gennem leverandørkontrakter, hvor der betales et forsikringsselskab eller en leverandør for at have en del af risikoen. Det skal bemærkes, at det overordnede ansvar for enhver risiko altid vil ligge hos organisationen.

Beslutningerne om, hvordan de identificerede risici håndteres, dokumenteres i en risikohåndteringsplan (handlingsplan). Risikohåndteringsplanen kan i praksis benyttes som en anbefaling/indstilling fra den aktivansvarlige til organisationens ledelse. Her anføres det, hvilke tiltag som bør indføres og evt. hvornår, og hvilke risici som bør accepteres med udgangspunkt i de fastsatte kriterier for risikotolerance.

Planen udarbejdes efter sædvanlig standard for projektplaner. Dvs. at for hver aktivitet/tiltag beskrives:

- Formål
- Ansvarlig (risikoejer)
- Ressourceindsats
- Risikohåndteringstiltag (mitigerende handlinger)
- Øvrige omkostninger
- Tidsplan

Se også bilag 7 for et eksempel på et skema til registrering og håndtering af risici.

Ledelsesforankring af risikohåndteringsplan

Når risikohåndteringsplanen er udarbejdet, skal den forelægges for virksomhedens ledelse. Ledelsen skal godkende de tiltag, der iværksættes, herunder den ressourceindsats og øvrige omkostninger, der er nødvendige for at gennemføre tiltagene. Ledelsen skal endvidere godkende accept af de risici, der ikke iværksættes tiltag for.

Gennemførelse af risikohåndteringsplan

Når ledelsen har godkendt risikohåndteringsplanen og accepteret risici, hvor der ikke iværksættes tiltag samt restrisici, skal risikohåndteringsplanen gennemføres. Dette er risikoejerens ansvar at sikre.

Når risikohåndteringsplanen er blevet gennemført, skal det vurderes, om SoA-dokumentet skal opdateres. SoA-dokumentet indeholder bl.a. en beskrivelse af de sikringsforanstaltninger, som organisationen har valgt at implementere. SoA-dokumentet skal som udgangspunkt opdateres, når der er gennemført en risikovurdering, og sikringsforanstaltninger er blevet ændret. Se også *Guide til SoA-dokumentet.*

Inddragelse af leverandøren i risikohåndtering

Den gennemførte 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 fx over for leverandøren. Resultatet af risikovurderingen kan vise, om der er uoverensstemmelse mellem myndighedernes sikkerhedsbehov og leverandørens sikkerhedsniveau.

Anvendes en ekstern leverandør til outsourcet drift af systemer og behandling af data, er det vigtigt, at leverandøren orienteres om resultatet af risikovurderingen, så systemer og data beskyttes i overensstemmelse med den accepterede restrisiko. Organisationen bør forud for dette vurdere, i hvilken grad risikovurderingen deles med eksterne, herunder leverandøren. En risikovurdering behandles typisk som et forretningsfortroligt dokument.

Leverandører og brug af cloudservices

Organisationer skal være opmærksomme på, at ved brug af cloudservices kan mulighederne for dialog med leverandøren være stærkt begrænsede. Derfor kan håndteringen af risici knyttet til disse services håndteres på anden vis – typisk gennem kompenserende foranstaltninger, med mindre der kan tilkøbes yderligere tjenester hos leverandøren. Se også *Vejledning i anvendelse af cloudservices* på digst.dk.

Orienteringen til leverandøren kan 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.

Generelt bør kontrakten mellem kunde og leverandør indeholde bestemmelser om risiko- og sårbarhedsvurderinger, så leverandøren fx forpligtes til at komme relevante trusler i møde som følge af en risikovurdering.

Standardklausuler til informationssikkerhed

Digitaliseringsstyrelsen har udarbejdet en række standardkontrakter (K01, K02, K03, K04), som det anbefales, at de statslige institutioner anvender inden for de respektive kontrakters anvendelsesområde. Standardkontrakterne kan også anvendes til it-projekter i kommuner og regioner samt på det private marked. Det er tilladt enhver vederlagsfrit at kopiere og anvende standardkontrakternes tekster helt eller delvist i forbindelse med udarbejdelse af kontrakter for aftaler om udvikling af it-projekter.

I tilknytning til kontrakterne er der udarbejdet en række standardklausuler til sikkerhedsmæssige krav. Formålet med klausulerne er at støtte myndighederne i forbindelse med indgåelse af it-kontrakter og dermed forenkle arbejdet med at stille hensigtsmæssige krav i it-kontrakter.

Kravene relaterer sig dels til den helt basale håndtering af de omfattede data, dels til efterlevelse af love for deling af og adgange til disse data på tværs af de involverede myndigheder. Desuden relaterer de sig i høj grad også til muligheden for at opretholde privatlivsfred og indblik i den faktiske anvendelse af de personlige data.

Standardkontrakterne og inspiration til informationssikkerhedskrav findes på digst.dk.

5. Opfølgning og løbende forbedringer

Efter gennemførelse af risikohåndteringsplanen og opdatering af SoA-dokumentet skal der følges op på, om planen har haft den ønskede effekt. Det fremgår således af ISO 27001, at "den resultatrelaterede effektivitet af disse handlinger skal evalueres".

Har handlingerne til håndtering af risici fx haft til formål at nedbringe antallet af hændelser, skal der følges op på, om dette er tilfældet. Generelt skal organisationen fastsætte målsætninger for alle relevante emner inden for informationssikkerhed, som skal være i overensstemmelse med informationssikkerhedspolitikken. De skal om muligt være målbare – her er antallet af hændelser et oplagt målepunkt, men det kræver, at organisationen har klarhed over, hvad en hændelse er.

For det første er det relevant at evaluere om fx selve risikohåndteringsplanen er gennemført til tiden, og om der kan udlægges andre læringspunkter for planen, fx anvendelse af ledelsesdokumentationen, om ressourcerne har været anvendt tilfredsstillende, og om der har været andre projektrelaterede læringspunkter.

For det andet skal de iværksatte initiativer i planen gerne have den ønskede effekt. Her kan antallet af hændelser som nævnt være en relevant målpunkt. Man kan også sætte mål om, at risikoen for fortrolighedsbrud skal nedbringes, fx ved måling på anvendelse af sikker print på organisationens printere eller udlevering af gæstekort til konsulenter, gæster mv. Andre eksempler på målepunkter kan være viden hos medarbejdere om, hvordan hændelser indberettes, kendskab til retningslinjer for informationssikkerhed mv.

For det tredje indgår det i selve præmissen for risikovurderinger, at der gennemføres en evaluering af risikovurderingsprocessen. Der bør derfor sættes tid af til gennemførelse af evalueringen med henblik på opfølgning og forbedring af risikovurderingen.

Risikostyring er en tilbagevendende proces

Når der foretages en risikovurdering, er der tale om et øjebliksbillede af situationen på det tidspunkt, hvor vurderingen udarbejdes. Men ændringer i både organisationen, systemer, informationsaktiverne, processer, eller nye trusler, sårbarheder, sikkerhedshændelser mv. kan give anledning til at der foretages en fornyet vurdering. 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.

Plan-do-check-act-modellen er en typisk måde at sikre sig, at risikostyring bliver en tilbagevendende proces.

Figur 5.1
Proces over risikostyring

De forskellige aktiviteter i risikostyringsprocessen kunne fx kategoriseres som neden for ift. Plan-do-check-act tanken.

Plan: Planlægning af gennemførsel af risikovurdering(er). Dette kan være afledt af 1) risikovurdering som en periodisk tilbagevendende opgave, 2) en evaluering peger på behov for risikovurdering, eller fordi 3) organisationen er blevet opmærksom på en problematik (fx en hændelse), som bør risikovurderes.

Do: Gennemførsel af risikovurdering(er), herunder analyse og vurdering af risici, samt afrapportering af risici.

Check: Risikohåndteringsplan udarbejdes og risici prioriteres. Plan godkendes af ledelsen og risikomitigerende tiltag indføres.

Act: Risikohåndteringsaktiviteter gennemføres, og der følges op på håndteringen af risici frem mod planlægningen af næste risikovurdering

Vejledning til risikostyring inden for informationssikkerhed
Udgivet december 2020
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
www.sikkerdigital.dk.

Foto Colourbox

ISBN 978-87-93073-31-9