Styrelsen for Samfundssikkerhed

Vejledning i risikostyring inden for informationssikkerhed

December 2025

Indhold

Forord

Formålet med denne vejledning er at give en bred introduktion til de grundlæggende begreber og aktiviteter i risikostyringsprocessen. ISO/IEC 27001 stiller krav til, at organisationer etablerer formaliseret it-risikostyring jf. kapitel 6 og 8, ligesom NIS 2 loven for NIS 2-omfattede organisationer stiller krav til organisationens og ledelsens ansvar for risikostyring. Vejledningen adresserer specifikt ISO/IEC 27001's krav om formaliseret risikostyring og tager udgangspunkt i, at organisationen også i sit øvrige informationssikkerhedsarbejde arbejder med implementering og efterlevelse af ISO/IEC 27001-standarden.

I vejledningen finder du blandt andet:

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

Vejledningen er henvendt til dig, der dagligt arbejder med informationssikkerhed og mere specifikt risikostyring i organisationen. Du kan enten være relativt ny inden for arbejdet med risikostyring og have brug for vejledningen som afsæt for og støtte i arbejdet. Du kan også have flere års erfaring og alligevel have brug for en bred indføring i – eller opfriskning af, – det teoretiske grundlag for arbejdet med risikostyring og -vurderinger. Er du ny i risikostyring, opfordres du også til at læse mere på sikkerdigital.dk/risikostyring.

Her kan du læse mere

Som nævnt stiller ISO/IEC 27001 krav til, at organisationer etablerer formaliseret it-risikostyring, men der stilles ikke krav til, hvilken metode der anvendes. Denne vejledning er baseret på fremgangsmåden fra standarden ISO/IEC 27005:2022.[1] I ISO/IEC 27005:2022 finder du mere detaljeret hjælp til denne metode og uddybende forklaringer på begreber og metode til it-risikostyring.

Derudover kan du på sikkerdigital.dk finde mere materiale om risikostyringsprocessen målrettet myndigheder. Blandt andet kan du finde et eksempel på et risikovurderingsværktøj, som du kan anvende eller tilpasse til din organisation. Desuden finder du inspiration til trusselskatalog, sårbarhedskatalog, konsekvens og sandsynlighedsskalaer, der før brug ligeledes skal tilpasses din egen organisation.

Ønsker du nærmere information om NIS 2-lovens krav til risikostyring, kan du læse i NIS 2-vejledningerne på Styrelsen for Samfundssikkerheds hjemmeside.

[1] ISO 27001, 27002 og 27005 kan rekvireres via Dansk Standard. For statslige myndigheder er de tre standarder frikøbt og kan anskaffes ved henvendelse på sikkerdigital@digst.dk.

1 Formålet med risikostyring

I alle organisationer er brugen af it-systemer, informationer og data forbundet med risici i større eller mindre omfang. Det er ikke altid muligt at fjerne risici, men det er muligt at reducere dem ved hjælp af en systematisk tilgang. Kort forklaret går risikostyring ud på at kende sin organisations risici for dermed at kunne prioritere og håndtere dem.

Risikostyring giver ledelsen overblik over organisationens risici og dermed mulighed for at træffe beslutninger om, hvilke informationssikkerhedsrisici organisationen skal reducere, hvor meget disse risici skal reduceres, og hvor mange ressourcer der skal anvendes på dette. Formålet med risikostyring er således at etablere et grundlag for, at organisationens ledelse kan anvende dens ressourcer, hvor de gør mest gavn. Da denne vejledning handler om risikostyring inden for informationssikkerhed, vil vi anvende begreberne informationssikkerhedsrisici og risici synonymt.

Vigtige begreber i risikostyringsprocessen

De mest centrale begreber indenfor risikostyring er:

- Trussel: En potentiel årsag til en hændelse, som, hvis den bliver aktuel, kan medføre en negativ konsekvens for organisationens informationssikkerhed, f.eks. hackerangreb, hvor ondsindede aktører vil stjæle en organisations data
- Sårbarhed: En svaghed, som kan medføre, at truslen kan materialiseres, f.eks. manglende sikkerhedsopdatering af et internt styresystem
- Risiko: En potentiel hændelse, som, hvis den indtræffer, vil have en negativ konsekvens for organisationens informationssikkerhed. En risiko indtræffer, når en trussel udnytter en sårbarhed, f.eks. en hacker (trussel), der skaber sig adgang til interne it-systemer, fordi it-systemerne ikke er opdaterede (sårbarhed).
- Konsekvens: Den konsekvens, som en risiko medfører, hvis den materialiseres, f.eks. hvordan omdømme eller økonomi kan blive påvirket, hvis organisationens data lækkes ifm. et hackerangreb
- Sandsynlighed: Med hvor stor sandsynlighed vil en given risiko materialiseres, f.eks. hvor sandsynlig et hackerangreb vurderes. Vurderingen kan baseres på trusselsniveauer, som Styrelsen for Samfundssikkerhed løbende opdaterer.

Andre relevante begreber inden for risikovurdering:

- Foranstaltning: Et eller flere tiltag organisationen foretager sig for at reducere en risiko, f.eks. automatiske sikkerhedsopdateringer
- Residualrisiko: Risikoen, når foranstaltningen er implementeret. Benævnes af nogle som netto- eller restrisiko
- Risikoaccept: Den risiko (kombination af sandsynlighed og konsekvens), som en ledelse vil acceptere, f.eks. kan en ledelse vælge at acceptere en lav risiko for læk af data ifm. et hackerangreb
- Risikoidentifikation: En proces, hvor organisationen forsøger at identificere relevante risici, som skal håndteres
- Risikovurdering: En proces, hvor organisationen forsøger at vurdere en potentiel risikos sandsynlighed og konsekvens
- Risikohåndtering: En proces, hvor organisationen forsøger at finde relevante foranstaltninger, typisk med det formål at reducere en risikos sandsynlighed og/eller konsekvens.

For en mere fyldestgørende gennemgang af begreber inden for informationssikkerhedsrisici henvises til ISO/IEC 27005:2022 afsnit 3 om termer og definitioner. Afsnittet i standarden indeholder de autoritative definitioner inden for området og bliver løbende vedligeholdt af International Organization for Standardization (ISO).
Risiko måles således ved at bedømme, hvor stor sandsynligheden er for, at en trussel vil kunne udnytte en sårbarhed, og hvor store konsekvenser det kan have.

Når der arbejdes med styring af risici indenfor informationssikkerhed inddeles risici normalt i følgende kategorier (sommetider benævnt med forkortelsen FIT):

- Risiko for tab af **fortrolighed**, dvs. risikoen for at uautoriserede personer får kendskab til de pågældende informationer.
- Risiko for tab af **integritet**, dvs. risikoen for at informationerne bliver fejlbehæftede eller manipuleret, og
- Risiko for tab af **tilgængelighed**, dvs. risikoen for at man ikke kan få adgang til informationerne, når man skal bruge dem.

For at skabe et overblik over organisationers risici og sikre en systematisk tilgang til håndteringen af dem, vælger mange organisationer at anvende standardiserede arbejdsmetoder og begreber. Der findes mange metoder til styring af informationsrisici. Denne vejledning tager udgangspunkt i den internationale standard ISO/IEC 27005:2022, der også har status som både europæisk og dansk standard.

Der er intet specifikt metodekrav i ISO/IEC 27001 til, hvordan risikovurderingen gennemføres, andet end at den metode, man vælger, skal sikre, at resultaterne er konsistente, sammenlignelige og valide. Hvis man følger ISO/IEC 27005 er disse krav opfyldt. Dog skal der altid gennemføres en vurdering af risikoen for tab af fortrolighed, integritet og tilgængelighed. ISO/IEC 27001 stiller krav til, at risikovurderingsmetoden er dokumenteret.

Følges metoden i denne vejledning, og dokumenteres de valg, der foretages undervejs, er organisationens metode for risikovurdering dermed fastlagt.

Ud over en standardiseret arbejdsmetode vælger nogle organisationer at anvende specialiserede softwareløsninger til at understøtte arbejdsprocesserne vedrørende risikostyringen og opbevare informationer om risikovurderinger, risici og håndtering af risiciene. Alternativerne til sådanne softwareløsninger vil i mange tilfælde være regnearksprogrammer og tekstbehandling til at etablere strukturer og standardskabeloner til informationsindsamling og rapportering.

Net- og Informationssikkerhedsdirektivet (NIS2) og risikostyring

Med NIS2 direktivet styrker EU cybersikkerheden på tværs af unionen. Baggrunden for direktivet er bl.a. den stigende samfundsmæssige afhængighed af digitale systemer og netværk, i kombination med de stadigt flere og mere avancerede cybertrusler fra f.eks. hackere.

Med afsæt i ISO/IEC 27001 og GDPR har risikovurderinger hidtil skullet tage stilling til, hvilke risici for henholdsvis organisationen og individers rettigheder, der skal håndteres ved organisationens behandling af informationer. Med NIS2 understreges det, at fokus nu også skal have et bredere sigte på risici for hele samfundet. I en risikostyringssammenhæng betyder det, at myndigheder og private virksomheder, der er omfattet af NIS 2, også skal vurdere, hvorvidt en hændelse vil kunne påvirke eller skade andre.

I lighed med kravene i ISO/IEC 27001 lægger NIS2 vægt på, at ledelsen skal godkende og føre tilsyn med de sikkerhedsforanstaltninger, der skal håndtere risiciene. Ledelsens rolle og ansvar i forbindelse med risikostyring af cyberrelaterede risici er dog nu understreget yderligere i form af lovkrav i NIS2.

Dette kan f.eks. gøres ved, at den enkelte myndighed overvejer risici og konsekvenser for samfundet, hvis myndighedens kerneforretning rammes af en hændelse. F.eks. kan myndigheder i transportsektoren overveje risici forbundet med uautoriseret indgreb i trafikstyring i lufthavne eller manglende styring af trafiksignaler på jernbanenettet. For myndigheder i sundhedssektoren kunne eksempler være fejl i fordelingen af medicinrecepter til borgere eller manglende adgang til patientjournaler. Det er i denne forbindelse vigtigt at medtage potentielle konsekvenser og sandsynligheder i leverandørkæden for den pågældende service, når myndigheden afdækker det samfundsmæssige perspektiv ifm. risikovurderinger.

For nogle organisationer kan NIS2's krav til ledelsesinvolvering potentielt også betyde, at kriterierne for risikoaccept skal genbesøges. Se nærmere om fastsættelse af kriterier i denne vejlednings afsnit 3.3.

Der er udarbejdet en række vejledninger til NIS 2-loven, som beskriver kravene til risikostyring nærmere. Flg. kan fremhæves som relevant for arbejdet med risikostyring:

- NIS 2-vejledningen om implementering af cybersikkerhedsforanstaltninger beskriver lovens krav til politik for risikostyring og informationssystemsikkerhed i kapitel 1
- NIS 2-vejledningen om ledelsens rolle og ansvar beskriver de krav, der er til ledelsens styring af cybersikkerhedsrisici i kapitel 3.

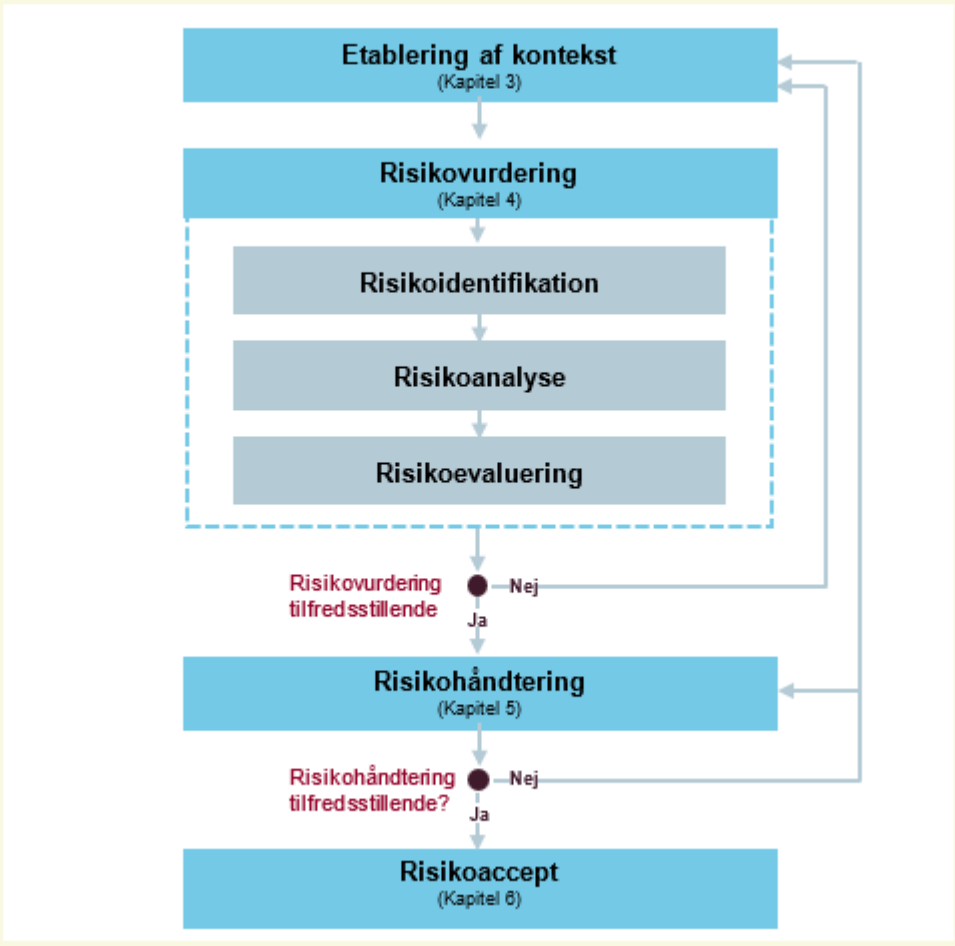
Vejledningerne findes på Styrelsen for Samfundssikkerheds hjemmeside.

2 Overblik over risikostyringsprocessen

Styrelsen for Samfundssikkerhed anbefaler, at myndighederne følger metoden til styring af risici indenfor informationssikkerhed fra ISO/IEC 27005, som denne vejledning bygger på. Processen for vurdering og behandling af risici er i overensstemmelse med kravene til risikostyring i ISO/IEC 27001. Myndighederne kan med fordel anvende ISO/IEC 27005 som supplement til denne vejledning, når arbejdet med styring af informationssikkerhed skal tilrettelægges og gennemføres.

Risikostyringsprocessen, som er illustreret i figuren nedenfor, består af flere hovedaktiviteter. Figuren er en lidt forsimplet udgave af processen fra ISO/IEC 27005, men følger samme struktur. Hovedaktiviteterne er grundlæggende for den samlede proces og gennemgås i de efterfølgende kapitler.

Forenklet illustration af risikostyringsprocessen baseret på ISO/IEC 27005



Det er vigtigt at have rammerne på plads, før man starter med selve risikostyringsaktiviteterne. Risikostyring er en tværorganisatorisk proces, og der indgår mange mennesker med forskellige baggrunde, opgaver, ansvarsområder og forudsætninger for risikostyring.
Typisk vil det være et informationssikkerhedsudvalg med deltagelse fra topledelsen, som skal godkende og afgrænse rammerne for risikostyringen. Herunder at risikovurderingsprocessen igangsættes, og at der afsættes ressourcer til, at den kan gennemføres. Informationssikkerhedsfunktionen har det praktiske og koordinerende ansvar for risikostyringen, mens data- og it-systemejere har ansvaret for identifikation og håndtering af risici inden for deres eget område.

Kvaliteten af arbejdet med risikostyring, herunder risikovurderinger, afhænger af, at de rette medarbejdere i organisationen prioriterer deres tid og bidrager med deres indsigter for at skabe et retvisende samlet billede af organisationens risici.

Planlægning, koordination og kommunikation ligger derfor hele tiden som et bagtæppe i risikostyringsprocessen, både før og efter gennemførelse af hovedaktiviteterne. I næste kapitel kan du læse mere om den første officielle del af risikostyringsprocessen: etablering af konteksten.

3 Etablering af kontekst

Denne del af processen udgør rammen og retningen for arbejdet med risikostyringen, herunder en række valg, der danner grundlag for organisering af risikoarbejdet og metode til risikovurderingerne.

Visse elementer af konteksten er fælles for hele organisationen, f.eks. den pågældende sektor, som organisationen befinder sig i, og de reguleringsmæssige rammer. Vi taler her om organisationens kontekst.

Andre elementer af konteksten er mere snævre for selve risikostyringen, f.eks. hvem har hvilke roller i forbindelse med risikostyringen, hvilke kriterier og skalaer skal anvendes, og hvad kendetegner de risici, som ledelsen vil acceptere. Vi taler her om risikostyringens kontekst.

Både organisationens og risikostyringens kontekst skal fastlægges inden man kan gå i gang med selve risikostyringen. I regi af ISO/IEC 27001 relateres denne del til afsnit 4 og 6.2.1.

3.1 Risikostyringens 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. Kontekst bør allerede være fastlagt og beskrevet, når organisationen etablerer Ledelsessystemet for Informationssikkerhed (ISMS), som defineret i ISO/IEC 27001. Det kan dog være godt at genbesøge beskrivelsen af kontekst, når man fastlægger rammer for risikostyringen, så man sikrer, at den stadigvæk er gældende.

3.2 Risikostyringens organisering

I forbindelse med risikostyringsprocessen skal der fastlægges organisering, roller og opgaver. Boksen nedenfor beskriver de væsentligste roller og opgaver:

Roller og opgaver i risikostyring

- Ledelsen: Skal godkende organisationens samlede risikostyringsproces. Ledelsen vil også skulle godkende eventuelle resultater af risikovurderinger, der indebærer risici som er større end den fastlagte risikoaccept (se nedenfor).
- Informationssikkerhedsansvarlig: Den funktion/person som er udpeget af ledelsen til at sikre, at der etableres risikostyringsprocesser, og at disse udføres.
- Aktiv-/risikoejer: Den person/funktion som er ejer af et givet informationsaktiv, forretningsproces eller data, f.eks. et HR-system med tilhørende processer og data. Da personen er udpeget som ejer, vil denne person også almindeligvis have konkret indsigt i forskellige typer af konsekvenser af risici og sandsynlighederne for, at risiciene "materialiseres".

Ledelsens ansvar i forbindelse med risikostyring af informationssikkerhed er udtrykt i ISO/IEC 27001 og er nu også eksplicit udtrykt i NIS2-direktivet, hvor ledelsen bliver pålagt en mere aktiv rolle i risikostyringen af myndighedernes cybersikkerhed.

Ledelsen vil almindeligvis

etablere et informationssikkerhedsudvalg bestående af nøglepersoner fra disse grupper.

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.

Det er almindeligt forekommende, at ansvaret bliver varetaget af informationssikkerhedsudvalget, som så foretager periodisk rapportering til – og fra – den øverste ledelse. Oftest er det ligeledes informationssikkerhedsudvalget, der fastsætter og godkender organisationens metode til risikovurdering, som bl.a. bygger på de valgte kriterier for informationssikkerhed, der gennemgås i næste afsnit.

3.3 Kriterier for informationssikkerhed

Der skal fastlægges kriterier/skalaer for sikkerhedsrisici, før man kan gå i gang med risikovurderingerne. Denne del er grundlaget for risikostyringen, da det er her, man fastlægger den terminologi, som organisationen skal kunne genkende og anvende, når der drøftes risici.

Skalaer for konsekvens og sandsynlighed

Der skal fastlægges definitioner og skalaer for konsekvens og sandsynlighed.

For konsekvens anvender mange myndigheder og virksomheder en 4-trinsskala, gående fra "ubetydelig" til "katastrofal".

For sandsynlighed er en benyttet metode en 4-trinsskala gående fra "usandsynlig" til "meget sandsynlig".

For inspiration til skalaerne henvises til risikovurderingsværktøjet og de tilhørende bilag "3. Sandsynlighedsskema" og "4. Konsekvensskema", der kan anvendes.

Kriterier for risikoaccept

Der skal fastlægges kriterier for risikoaccept. Det vil sige, at ledelsen skal fastlægge, hvilke kombinationer af konsekvens og sandsynlighed der er acceptable for organisationen.

Med henvisning til skalaerne ovenfor vil de fleste ledelser ikke acceptere en risiko, som både er "forventet" og "graverende/ødelæggende". Derimod vil de fleste ledelser kunne acceptere risici, som både er "usandsynlige" og "ubetydelige".

Faktorer, der kan påvirke skaler og kriterier

Det skal fastsættes, hvilke væsentlige faktorer der – meget overordnet – vil kunne påvirke de kriterier og skalaer (sandsynlighed og/eller konsekvens), som er valgt til brug for risikovurderingerne. Det kan være forhold såsom geopolitiske forhold, klimaændringer, den teknologiske udvikling eller ændringer i regulering, der vil kunne ændre konsekvensskalaerne.

Organisationer kan selv vælge at opbygge sine egne kriterier. Det anbefales dog at benytte kriterierne i bilagene til denne vejledning, der oprindeligt er baseret på ISO/IEC 27005 og/eller har været anvendt i vejledninger og eksempler til myndigheder over en længere årrække.

I praksis er det vigtigt ikke at fortabe sig i, om kriterierne er endegyldigt rigtige. Hvis risikovurderingsprocessen er under udvikling, er det vigtigere at komme i gang, end at skalaer og kriterier er helt korrekte og entydige.

Opsummering: Når du har været igennem hovedaktiviteten "Etablering af kontekst", står du med følgende:

- Organisering af risikostyringsarbejdet
- Skalaer for konsekvens og sandsynlighed

- Et ledelsesgodkendt acceptabelt risikoniveau
- Ovenstående vil i dokumenteret form udgøre den metode for risikostyring, som ISO/IEC 27001 foreskriver

Case eksempel:

Case myndighed X har etableret et informationssikkerhedsudvalg. På opstartsmødet er man enige om, at brud på lovgivning vil medføre ledelsesmæssige konsekvenser, og at dette vil være helt uacceptabelt.

Man er også blevet enige om at indføre en sandsynlighedsskala, der baserer sig på casemyndighedens historik. Hvis f.eks. en hændelse har fundet sted i nærheden inden for det seneste år, vil man betragte den som sandsynlig.

Ledelsen har givet udtryk for, at man ikke vil acceptere sandsynlige hændelser, der kan resultere i uacceptable konsekvenser.

4 Risikovurdering

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

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

Helt overordnet er formålet med risikovurderinger at identificere og håndtere de risici, der er i forbindelse med organisationens brug af processer, it-systemer, informationer og data. Resultatet af risikovurderingen skal gerne være et overblik over organisationens risici og eventuelle anbefalinger til justeringer af risiciene – risikohåndtering (jf. kapitel 5).

Risikovurderingen bør altid foretages ud fra en fastlagt metode, som beskrevet i kapitel 3 om "Etablering af kontekst". Flere af aktiviteterne under risikovurderingen vil med fordel kunne udføres samtidigt. For eksempel vil mange risici både kunne identificeres og analyseres af de samme personer og på samme tid.

I praksis foretager nogle organisationer risikovurderinger gennem en række risikovurderingsworkshops med de relevante personer i organisationen, hvorefter den/de informationssikkerhedsansvarlige sammenfatter resultaterne. Dette er den anbefalede metode. I andre organisationer er praksis, at de informationssikkerhedsansvarlige igangsætter en proces, hvor aktivejer (f.eks. et it-systemkontor) selv gennemfører risikovurderingen og sammenfatter resultater. Det anbefales dog, at risikovurderingen gennemføres i et samarbejde mellem aktivejeren og den/de informationssikkerhedsansvarlige, idet en god risikovurdering normalt kræver forskellige kompetencer og erfaringsgrundlag.

De enkelte aktiviteter i risikovurderingen er uddybet nedenfor og relateres til afsnit 8.2 og 8.3 i ISO/IEC 27001. Til inspiration kan findes et risikovurderingsværktøj, der ligeledes indeholder hhv. trussels- og sårbarhedskatalog samt konsekvens- og sandsynlighedsskemaer, på sikkerdigital.dk.

4.1 Risikoidentifikation

Risikoidentifikation er processen med at identificere de risici og kilder til risici, som kan være relevante for organisationen. Formålet er at kortlægge og systematisere risiciene, så man kan kommunikere om dem og behandle dem struktureret. Det er således ikke nødvendigvis et mål at identificere flest eller færrest mulige risici.

Den aktivbaserede og den hændelsesbaserede metode til risikoidentifikation

Hidtil har den mest almindelige tilgang til identifikation af risici taget udgangspunkt i organisationens register over aktiver, f.eks. forretningsprocesser, it-systemer og informationer. Oftest vil organisationer tage udgangspunkt i de aktiver, som er klassificeret som de mest betydningsfulde.

Som et supplement findes den hændelsesbaserede metode, der i korthed går ud på at starte med at identificere den eller de hændelser, som holder ledelsen og aktiv-/risikoejerne "vågne om natten". Er man som myndighed i opstartsfasen med risikovurderinger, kan det være en fordel at starte med den hændelsesbaserede fremgangsmåde, da den kan være lettere at forstå og tage afsæt i for at komme i gang. Efterhånden som man opnår viden om, hvilke risikohændelser der måtte give bekymringer, og de konsekvenser disse kan medføre, bør man supplere denne viden med de aktiver, der indgår i de forskellige risikohændelser.

Nogle eksempler på den hændelsesbaserede metode kan være "vores mail bliver hacket" eller at "sagsbehandlingsoplysninger bliver offentliggjort", hvorved aktiver som mailsystemet eller journaliseringssystemet er relevante. Således bevæger man sig over i den aktivbaserede tilgang med en aktivliste, der er relevant for den givne hændelse – og den videre risikovurdering.

Forretningsprocesser og aktiver

ISO/IEC 27001 forventer, at organisationer har en fortegnelse over information og understøttende aktiver, også kaldet et aktivregister (anneks A, 5.9) . I praksis betyder det, at organisationer kan tage udgangspunkt i denne oversigt og påbegynde risikovurdering af prioriterede aktiver baseret på listen. Prioriteten baseres ofte på kritikaliteten af aktiverne, der ud fra skalaer vurderer de mulige konsekvenser ved en sikkerhedshændelse. Aktiver med højest eller høj kritikalitet, hvor tab eller kompromittering af aktivet vil påvirke organisationen og/eller samfundet signifikant, vil blive prioriteret i risikovurderingsøjemed. I mange tilfælde er aktiverne grupperet på en måde, hvor antallet begrænses, mens det stadig er muligt at knytte specifikke trusler til dem. F.eks. kan routere, switche, firewalls mv. være grupperet som netværksudstyr eller infrastruktur.

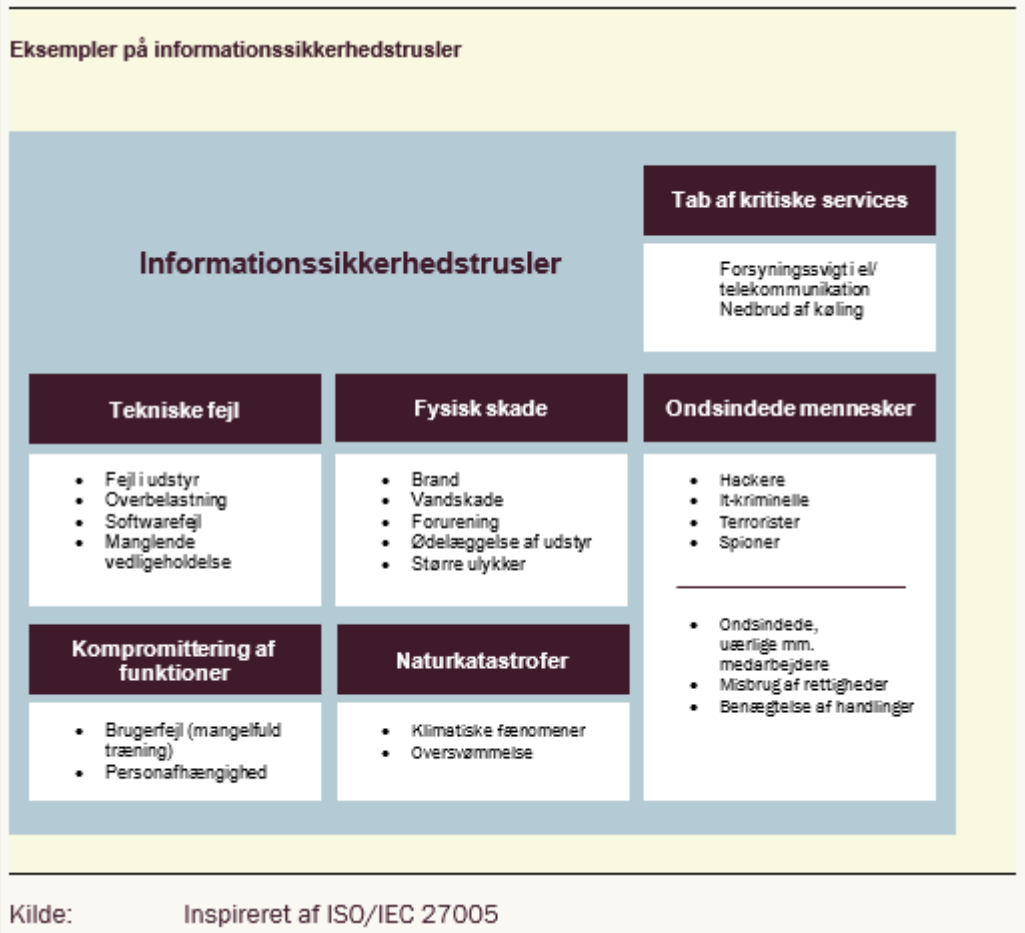
Endelig kan den hændelsesbaserede tilgang anvendes initialt, men vil som nævnt også ende i et eller flere aktiver.

Risikovurderingen bør ikke kun omfatte it-systemer, men alle de aktiver, som indgår i et informationssystem. Det inkluderer også fysiske aktiver som f.eks. 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.

Trusler

Næste skridt i risikoidentifikationen er at udpege de trusler, der er relevante for det enkelte aktiv eller den proces, der er fundet i foregående trin. Hvis der f.eks. er tale om et aktiv af typen "en server" vil relevante trusler f.eks. kunne være, at strømmen forsvinder, eller at serveren bliver stjålet. Et andet eksempel kan være en proces for udbetaling af offentlige midler, hvor relevante trusler kan være misbrug af rettigheder eller mangel på personale.

Identifikationen af relevante trusler er afgørende for, at man ikke overser risici, og bør ske på en systematisk måde og gerne med udgangspunkt i et trusselskatalog.



I ISO/IEC 27005 anneks A findes hjælp til arbejdet med at identificere relevante trusler. Disse trusler er opdelt i nogle hovedgrupper, som vist i figuren ovenfor. Det er vigtigt at bearbejde de trusselskilder/-kataloger, som man tager udgangspunkt i, til en række trusler, der er relevante for organisationen. F.eks. kan man argumentere for, at en trussel om jordskælv ikke er relevant i Danmark, men kan være relevant, hvis man er afhængig af aktiver i andre geografiske områder.

Se eksempel på trusselskatalog i risikovurderingsværktøjet på sikkerdigital.dk, som ved anvendelse skal tilpasses egen organisation.

Sårbarheder

En trussel kræver en sårbarhed for at kunne realiseres. I dette trin vurderer man aktiverne med henblik på at finde sårbarheder, som kan opstå i mange forskellige sammenhænge. Det kan f.eks. være en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en fejl i en teknisk opsætning, som gør, at it-systemet er åbent for angreb. En måde at afdække sårbarheder på er at gennemgå de implementerede foranstaltninger og vurdere deres effektivitet. Her kan der tages udgangspunkt i SoA-dokumentet (statement of applicability), som bør være udarbejdet og indeholder overblik over organisationens til- eller fravalg af foranstaltninger.

En anden måde at afdække sårbarheder på er at tage udgangspunkt i, hvordan relevante trusler kan påvirke aktivet. Såfremt f.eks. 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. Der kan hentes inspiration i f.eks. ISO/IEC 27005 for et sårbarheds- og trusselskatalog eller i risikovurderingsværkøjet, som findes på sikkerdigital.dk.

Hvis it-driften er outsourcet til en leverandør, kan det være en god idé at inddrage dem i forbindelse med sårbarhedsvurderingen, da de har viden om de tekniske løsninger og tekniske foranstaltninger, der er etableret, og dermed også måske nogle af de tekniske sårbarheder, der eksisterer. En god tilgang er at anvende uafhængige informationer såsom revisionsrapporter eller rapporter fra penetrationstest.

I praksis vil risikoidentifikationen udmunde i en liste over identificerede risici og relaterede trusler og sårbarheder.

4.2 Risikoanalyse

Formålet med risikoanalysen er at vurdere sårbarhedens risikoniveau ud fra sandsynlighed og konsekvens. Der tages udgangspunkt i de identificerede sårbarheder fra ovenstående aktivitet omhandlende risikoidentifikation.

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

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, f.eks. procenter eller kroner. 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 er 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 foranstaltninger, og hvor mange ressourcer man vil bruge på dem.

Identifikation af konsekvens og sandsynlighed

En del af risikoanalysen er en identifikation af konsekvenserne ved et aktivs tab af fortrolighed, integritet eller tilgængelighed.

Typer af konsekvenser

- **De forretningsmæssige konsekvenser**, dvs. hvilken betydning en realiseret hændelse vil have for organisationen og dens målsætninger. Det er vigtigt at tage udgangspunkt i hvilken betydning, det vil have for organisationen som helhed og ikke kun for et afgrænset område.
- **Konsekvenser for de registrerede**, dvs. hvilken betydning en realiseret hændelse vil have for de registreredes rettigheder. Denne del udspringer fra en GDPR-mæssig sammenhæng og vurderes i tilfælde af, at der behandles personoplysninger i aktivet.
- **Konsekvenser for samfundet**, dvs. hvilken betydning en realiseret hændelse vil have for samfundet som helhed. Denne del udspringer fra NIS2-direktivet.

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 foranstaltninger der etableres.

Et eksempel på vurdering af konsekvenser er anvist i nedenstående tabel, hvor konsekvenserne af et givet systems varierende nedetid er angivet. Det er dog vigtigt, at konsekvensen ikke blot vurderes ved et tilgængelighedsbrud, men også ved et fortroligheds- og integritetsbrud.

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.

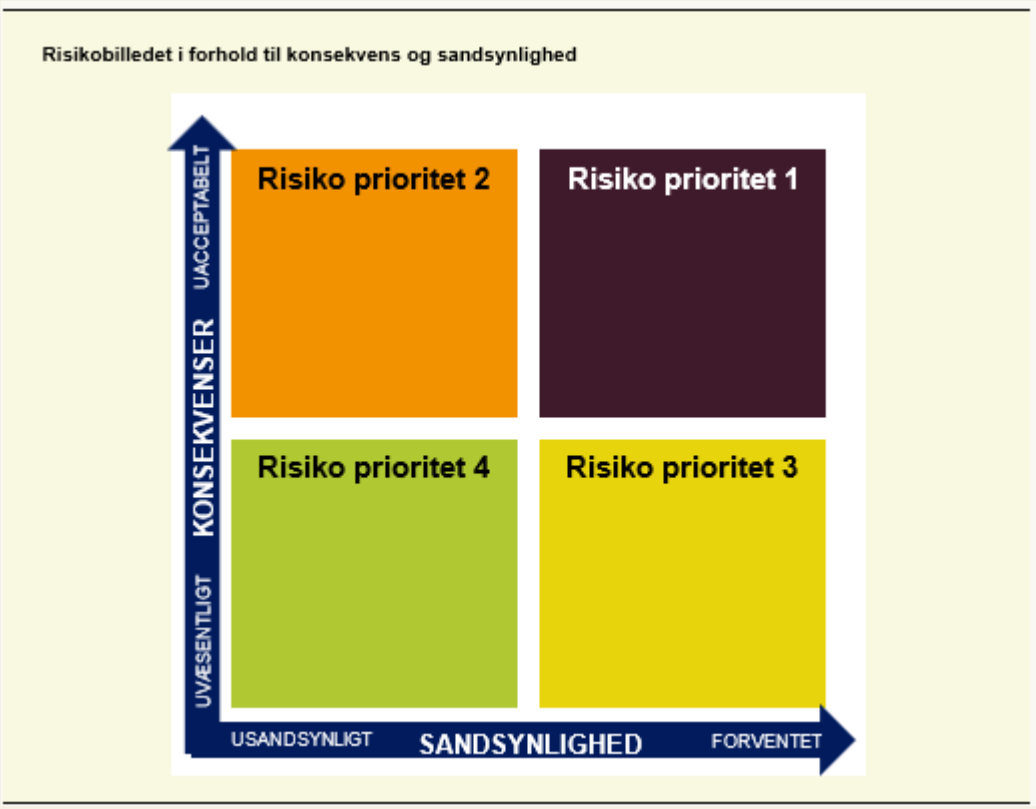
Det er vigtigt at understrege, at der både for så vidt angår sandsynlighed og konsekvens er tale om forventninger/vurderinger til fremtiden. Der er altså ikke tale om, at de kan eller skal være "korrekte" i en entydig matematisk forstand.

Sandsynlighedsbegrebet kan være vanskeligt at vurdere, da der i sagens natur er tale om forventninger til en fremtidig begivenhed. Mange organisationer anvender i stedet, som en tilnærmelse, erfaringer om historisk forekomst, som f.eks. "sker dagligt" eller "har ikke forekommet i organisationens historie".

Der findes flere hjælpeværktøjer, som kan bruges til at lette arbejdet med at registrere og beskrive risici, se eksempelvis risikovurderingsværktøjet på sikkerdigital.dk.

4.3 Risikoevaluering

Det sidste skridt i risikovurderingen er evalueringen af de fundne risici i forhold til de kriterier, som er fastlagt af ledelsen. Organisationen skal således vurdere, hvorvidt risiciene kan accepteres, eller om der er behov for at håndtere dem. Dette kan i praksis gøres på forskellige måder, f.eks. ved indplacering på en skala eller i et heatmap, som illustreret nedenfor. Et heatmap er et simpelt og effektivt værktøj til at formidle risici i organisationen med henblik på, at ledelsen kan prioritere organisationens indsats. Et eksempel på brug af et heatmap kan være, at ledelsen på forhånd har besluttet, at risici der befinder sig i området "Risiko prioritet 1" i figuren ikke kan accepteres, og altså skal håndteres for at nedbringe sandsynlighed, konsekvens eller begge dele. For inspiration til en risikohåndteringsplan henvises til risikovurderingsværktøjet på sikkerdigital.dk.



Opsummering: Når du har været igennem hovedaktiviteten "Risikovurdering", står du med følgende:

- En liste over risici tilhørende en eller flere givne aktiver med angivelse af tilhørende værdier for sandsynlighed og konsekvens.
- En samlet risikovurdering og forslag til prioritering. Listen vil almindeligvis skulle sorteres, så risici med højt niveau fremhæves (f.eks. risici, der er "uacceptable" og "forventede" eller har en "høj risikoscore", hvis man bruger numeriske værdier)
- Eventuelt kan udarbejdes et heat-map for at give et overskueligt overblik over risici i en organisation, som ovenfor illustreret. Hvad end man benytter en liste eller et heat-map, giver det ledelsen indsigt i, hvilke risici der skal fokuseres på.

Case eksempel

Med udgangspunkt i case myndighed X's aktivliste og prioritering af denne har myndigheden netop gennemført en risikovurdering af deres mailsystem.

Resultatet af risikoidentifikationen er bl.a., at en uautoriseret adgang til mails vil være en relevant trussel at forebygge, da der kan være tale om lovbrud. Også set i lyset af deres valgte risikoaccept.

I risikovurderingen finder informationssikkerhedsmedarbejderen ud af, at mail-serveren er placeret hos en mindre underleverandør i udkanten af byen, og at prisen har drevet denne beslutning. Placeringen betragtes som en væsentlig sårbarhed, der vil kunne gøre en trussel om tyveri af mail-serveren, og dermed eksponeringen af fortrolige mails, aktuel.

I risikoanalysefasen er det blevet vurderet, at indbrud er sandsynligt, da det er almindeligt forekommende i underleverandørens lokalområde. Underleverandøren har ingen tredjepartserklæring, der omhandler fysisk adgang til kundernes servere.

Det vurderes også, at konsekvensen af offentliggørelse af borgeres mails vil udgøre et kritisk brud på fortroligheden for de registrerede borgere. Konsekvensen for myndigheds X's forretning vil være graverende, da selv kort nedetid resulterer i store produktivitetstab, og at videnstabet i form af historiske mails vil medføre, at nogle af myndighedens lovbestemte tidsfrister ikke kan overholdes.

Udfaldet af risikovurderingen er derfor, at risikoen er "høj".

Ved evalueringen af risiko og mulige foranstaltninger finder udvalget ud af, at man bør håndtere risikoen ved at dele den med en mere professionel underleverandør, da man ikke selv har egnede lokaliteter til opbevaring af serveren eller kompetence til at vedligeholde den nødvendige sikkerhed.

5 Risikohåndtering

Efter at der er identificeret en række risici i ovenstående aktiviteter, med tilhørende sandsynligheder og konsekvenser, skal der arbejdes med at håndtere de pågældende risici.

Risikohåndtering består af tre trin:

- Udarbejdelse af en risikohåndteringsplan
- Ledelsesforankring af risikohåndteringsplan
- Gennemførelse af risikohåndteringsplan

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

Aktiviteten om risikohåndtering relaterer til afsnit 8.3 i ISO/IEC 27001.

5.1 Udarbejdelse af risikohåndteringsplan

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

Modificér betyder, at man etablerer foranstaltninger, der mindsker sandsynligheden for en hændelse eller mindsker konsekvensen, hvis en hændelse sker. En foranstaltning bevarer og/eller ændrer en risiko. En foranstaltning kan være forebyggende, opdagende, korrigerende eller en kombination af disse. Disse foranstaltninger kan være tekniske, f.eks. antivirusprogrammer eller af administrativ karakter som f.eks. uddannelse af medarbejdere i it-sikkerhed, herunder hvordan man undgår phishing, håndterer adgangskoder og beskytter følsomme data. Foranstaltninger, der mindsker sandsynligheden for sikkerhedshændelser benævnes *forebyggende foranstaltninger* og foranstaltninger, der mindsker konsekvenserne af sikkerhedshændelser benævnes *udbedrende foranstaltninger*. I mange tilfælde vil der være tale om en cost/benefit-analyse, hvor den mulige effekt vurderes i forhold til omkostningerne.

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, eller i praksis at der ikke er uendelige ressourcer til brug for foranstaltninger.

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 it-system, man holder op med at bruge.

Del betyder, at organisationen håndterer risikoen ved at dele den med andre. F.eks. 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 eller indstilling fra den

aktivansvarlige til organisationens ledelse. Her anføres det, hvilke tiltag som bør indføres, eventuelt hvornår, og hvilke risici der bør accepteres med udgangspunkt i de fastsatte kriterier for risikoaccept, som blev defineret under "Kriterier for informationssikkerhed". Rapportens konklusioner kan være, at de enkelte risici er tilstrækkeligt afdækket, bortset fra at visse højrisikoområder bør reduceres, f.eks. ved at styrke adgangskontrollen til direktionens mødereferater.

Planen udarbejdes efter sædvanlig standard for projektplaner. Det vil sige, at for hver aktivitet/tiltag beskrives:

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

Se også risikovurderingstemplaten og det tilhørende bilag om risikohåndtering for et eksempel på et skema til risikohåndtering.

5.2 Ledelsesforankring af risikohåndteringsplan

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

Det er ikke vigtigt, om organisationen kalder resultatet af risikovurderingen for en risikohåndteringsplan eller noget andet, blot ledelsen er enig i konklusionerne og tager stilling til de foranstaltninger, der imødekommer de risici, som ikke er tilstrækkeligt afdækket eller reduceret. I forlængelse af risikohåndteringsplanen bør organisationen vurdere, om den bør opdatere sit Statement of Applicability dokument (SoA-dokumentet). Ledelsen bør orienteres om og/eller godkende både risikohåndteringsplan samt opdateret SoA-dokument.

5.3 Gennemførelse af risikohåndteringsplan

Når ledelsen har godkendt risikohåndteringsplanen og accepteret restrisici, skal risikohåndteringsplanen gennemføres. Det er risikoejerens ansvar at sikre det. Er man eksempelvis blevet enige om at udarbejde en beredskabsplan for journaliseringssystemet, skal dette arbejde gennemføres.

Opsummering: Når du har været igennem hovedaktiviteten "Risikohåndtering", står du med følgende:

- Baseret på listen over de prioriterede risici (se forrige hovedafsnit), skal der udarbejdes en risikohåndteringsplan med anbefaling om, hvordan risiciene skal håndteres. Dette kan både indbefatte en plan om at håndtere, acceptere, dele eller undgå.
- Planen med risikohåndtering skal forelægges ledelsen.

- I langt de fleste tilfælde vil informationssikkerhedsudvalget stå med et beslutningsreferat, hvoraf det fremgår, at der iværksættes x foranstaltninger til håndtering af y risici. Ledelsesbeslutningen/mødereferatet er samtidig mandat til risikoejerne om at gå i gang med at etablere foranstaltningerne.
- Skulle ledelsens beslutning være, at den ikke ønsker at håndtere visse af de risici, den er blevet forelagt, hvilket almindeligvis vil være resultatet af en forretningsmæssig afvejning af risikoaccept og ressourceforbrug, vil der således i mødereferatet foreligge en dokumenteret ledelsesmæssig beslutning om at acceptere risikoen på dens nuværende niveau.

Case eksempel

Som del af risikohåndteringen foreslår informationssikkerhedsmedarbejderen en foranstaltning, der går ud på at flytte mailserveren til Statens Its sikrede serverrum og i samme anledning overdrage opgaven med sikkerhedsovervågning og patching af serveren til Statens It.

Statens It er desuden certificeret efter ISO/IEC 27001 og underlagt tilsyn, så kunder kan få indblik i, hvordan kundernes it-sikkerhed forvaltes.

Informationssikkerhedsudvalget vurderer, at restrisikoen for lovbrud pga. tab af fortrolighed i forbindelse med mails er "lav", da man med forslaget vil kunne reducere sandsynligheden til "usandsynligt".

Informationssikkerhedsmedarbejderen har indhentet tilbud på omkostningerne til flytning og hosting af serveren hos Statens It.

6 Risikoaccept

For kritiske aktiver og processer bør risikoaccepten altid foretages af den øverste ledelse. Risikoappetit kan være en smule uhåndgribeligt, men går grundlæggende ud på at fastlægge den mængde it-sikkerhedsrisiko, en organisation er villig til at acceptere i relation til dens informationssystemer og data for at udføre sine opgaver. En organisation med høj risikoappetit kan acceptere, at nogle af deres data ikke er perfekt beskyttet mod datalækager, hvis det betyder, at de kan implementere hurtigere forretningsløsninger eller spare penge på sikkerhed.

Risikohåndteringsplanen eller -rapporten kan i praksis benyttes som en anbefaling/indstilling fra aktiv- eller procesejeren til ledelsen. Her anføres de foranstaltninger, som bør indføres, og hvilke risici som bør accepteres med udgangspunkt i de fastsatte kriterier for risikoaccept (jf. kapitel 2).

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

I denne forbindelse vil der typisk kunne opstå en drøftelse om ressourcer og kommercielle forhold, dvs. om hvorvidt de foreslåede foranstaltninger er "pengene værd", om der findes andre lige så gode foranstaltninger med videre. Man kan også forestille sig, at en risiko kan være så ressourcekrævende at reducere, at ledelsen vælger at acceptere den. Det er altid en konkret afvejning, som ledelsen skal foretage.

ISO/IEC 27001 afsnit 6.1.2.a) omhandler risikoacceptkriterier og afsnit 6.1.3.f) omhandler accept af restrisiko.

Opsummering: Når du har været igennem hovedaktiviteten "Risikoaccept", står du med følgende:

- Accepten af restrisikoen er en del af risikohåndteringen i forrige hovedaktivitet. Aktiviteten er dog her behandlet særskilt for at fremhæve betydningen af, at ledelsen, hvad angår de kritiske aktiver og processer, enten skal acceptere risikohåndteringsplanen eller skal vælge ikke at håndtere den risiko, som risikoplanen lægger op til. Nogle organisationer behandler alle risici under et som beskrevet i forrige afsnit under risikohåndteringsplanen, hvorimod andre organisationer isolerer behandlingen af de mest kritiske aktiver og processer til behandling på det øverste ledelsesniveau. Det er i praksis et spørgsmål om, hvilket beslutningsmandat/bemyndigelse de enkelte ledelseslag har fået tildelt.

Case eksempel

Ledelsen fastsatte i afsnit 3.3. "kriterier for informationssikkerhed", at man ikke ville acceptere en risiko der var sandsynlig og ville kunne medføre personalemæssige konsekvenser for ledelsen. Ved risikohåndteringsdrøftelserne har det endvidere vist sig, at omkostningerne ved at flytte serveren til Statens It kunne rummes i organisationens budget.

På informationssikkerhedsudvalgsmødet konstaterer ledelsen derfor, at risikoen vil blive nedbragt til et risikoniveau under acceptkriteriet og accepterer på den baggrund tiltaget, hvilket dokumenteres i referatet fra mødet.

Flytningen skal nu effektueres.

7 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 bør sikres, at de foranstaltninger, der indføres som en del af risikohåndteringen rent faktisk også bliver implementeret og fungerer efter hensigten.

Har handlingerne til håndtering af risici f.eks. haft til formål at nedbringe antallet af hændelser, skal der følges op på, om dette er tilfældet.

For det første er det relevant at evaluere, om f.eks. selve risikohåndteringsplanen er gennemført til tiden, og om der kan drages andre læringspunkter fra planen, f.eks. om 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 et relevant målepunkt. Man kan også sætte mål om, at risikoen for fortrolighedsbrud skal nedbringes, f.eks. 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. Her kan organisationen med fordel anvende ISO/IEC 27004 Informationsteknologi – Informationssikkerhedsledelse – Monitorering, måling, analyse og evaluering.

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.

7.1 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, it-systemer, informationsaktiverne, processer, nye trusler, sårbarheder, sikkerhedshændelser med videre kan give anledning til, at der foretages en fornyet vurdering. Det kan f.eks. være, at man har opdaget en ny sårbarhed, der kan påvirke sikkerheden i organisationens cloud-løsning. Der skal derfor gennemføres periodiske risikovurderinger, dels for at følge op på risici og de foranstaltninger, som implementeres, dels for at følge op på selve risikostyringsprocessen og de overordnede rammer og principper, som ligger til grund herfor.

Vi anbefaler, at der etableres et "årshjul", hvor alle tilbagevendende aktiviteter indarbejdes. I dette årshjul kan man indarbejde planer for revision eller revurdering af de enkelte risikovurderinger, f.eks. at risikovurderinger med høj risiko skal revurderes årligt i oktober måned, risikovurderinger med lav risiko revurderes hvert andet år i august måned etc. Det vil være nyttigt at afstemme terminer og tidspunkter i årshjulet med møder i organisationens ledelse.

Plan-do-check-act-modellen er en ofte anvendt model for at sikre sig, at risikostyring bliver en tilbagevendende proces.

Proces for risikostyring

De forskellige aktiviteter i risikostyringsprocessen kan f.eks. kategoriseres som nedenfor i forhold til Plan-do-check-act tanken.

Plan: Planlægning af gennemførelse 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 (f.eks. en hændelse), som bør risikovurderes.

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

Check: Risikohåndteringsplan udarbejdes og risici prioriteres. Plan godkendes af ledelsen, og foranstaltninger indføres.

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