Skabelon for risikostyringspolitik

Følgende dokument er en skabelon til udarbejdelse af en risikostyringspolitik for virksomheder med en bestyrelse. Risikostyringspolitikken sætter rammerne for arbejdet med risikovurdering. Det er her I får defineret scoringer (input til risikologgen), uddelt roller (hvem gør hvad) og fastlagt arbejdsprocesserne (hvornår mødes vi og hvem skal informeres). Risikostyring bruges til at prioritere og planlægge implementering af IT-sikkerhedsforanstaltninger, så de passer til netop jeres organisation og situation. Dokumentet er én af flere skabelon-dokumenter, som indgår i det IT-sikkerhedsmateriale, som alle organisationer bør have.

Vi har i Lakeside lavet en række skabeloner, som du er velkommen til at bruge. Skabelonerne er tiltænkt SMV’er med produktion, men kan sagtens bruges af organisationer uden produktion (Operational Technology - OT). Skabelonerne er udarbejdet med udgangspunkt i små og mellemstore forsyningsselskaber.

* IT-sikkerhedspolitik
* IT-sikkerhedshåndbogen
* OT-leverandørpolitik, og leverandør tjeklister
* Nærværende risikostyringspolitik og Risikolog
* Hændelseshåndteringsproces og Hændelseslog
* Kriseberedskabspolitik, -planer og -skabeloner

Skabelonerne for de øvrige dokumenterne kan findes og downloades på [www.lakeside.dk/publikationer](http://www.lakeside.dk/publikationer)

**Sådan bruger du skabelonen**

* Tekster med gråt og i firkantede klammer er vejledningstekster, som slettes ved endt redigering.
* <Organisation> er en dokument-egenskab. Den kan rettes under Filer / Egenskaber / Brugerdefineret (nederste tekstboks) og derefter opdatere alle felter i hele dokumentet (vælg alt og højreklik).
* Alle tekster kan ændres efter behov og som tilpasning til din organisation. Alle tekster med gult bør du ændre eller som minimum forholde dig til.
* Kontaktinformation og organisation skal opdateres i sidehoved og sidefod. OBS! Organisation og logo på forsiden er også i en sidefod.

**Versionshistorik for skabelon:**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer |
| 1.0 | 13.12.2024 | MTH | Oprettet første version |
| 1.1 | 27.01.2025 | MTH | Opdateret ift. udkast til bekendtgørelse om modstandsdygtighed og beredskab i energisektoren. |
| 1.2 | 24.04.2025 | MTH | Opdateret scoring så den følger Energistyrelsens 5-trins konsekvensskala i Bilag B, samt tilføjet afsnit om leverandørrisici og projektrisikostyring. |

Dato | Version x.x

Risikostyringspolitik

TERmer

|  |  |
| --- | --- |
| Term | Forklaring |
| ROS-scenarier | Risiko- og sårbarhedsscenarier. Fx udgiver Energistyrelsen årligt et katalog over ROS-scenarier for energisektoren. |

Revisions- og Godkendelseshistorik

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer | Godkendt |
| [0.0] | [dd.mm.yy] | [INT] |  | [dato / navn] |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Kontaktpersoner

|  |  |
| --- | --- |
| Fornavn Efternavn (initialer)  Skriv din titel her, fx direktør  Tlf.: +45 xxxx xxxx  [xxx@domæne.dk](mailto:xxx@domæne.dk)  <Organisation> | Fornavn Efternavn (initialer)  Skriv din titel her, fx bestyrelsesformand  Tlf.: +45 xxxx xxxx  [xxx@domæne.dk](mailto:xxx@domæne.dk)  <Organisation> |

Indholdsfortegnelse

[1 Indledning 3](#_Toc196393625)

[1.1 Definition 3](#_Toc196393626)

[2 Principper for risikostyring 4](#_Toc196393627)

[2.1 Beskrivelse af risici 4](#_Toc196393628)

[2.2 Risikokategorier 4](#_Toc196393629)

[3 Organisering 5](#_Toc196393630)

[3.1 Ansvarsfordeling 6](#_Toc196393631)

[3.2 Kommunikation om risici 9](#_Toc196393632)

[4 Fastsættelse af rammer 9](#_Toc196393633)

[4.1 Risikotolerance og advarselslamper 9](#_Toc196393634)

[5 Proces for risikostyring 10](#_Toc196393635)

[5.1 Identificering 11](#_Toc196393636)

[5.2 Vurdering 11](#_Toc196393637)

[5.3 Planlægning 12](#_Toc196393638)

[5.4 Håndtering 12](#_Toc196393639)

[6 Risikolog & handlingsplan 13](#_Toc196393640)

[7 Projektrisici 14](#_Toc196393641)

[Bilag A - Generelle forhold 15](#_Toc196393642)

[Bilag B – Scoring 16](#_Toc196393643)

[Bilag C – Risikotolerance og advarselslamper 19](#_Toc196393644)

[Bilag D - Kommunikationsplan for risici 20](#_Toc196393645)

[Bilag E - Plan for risikostyring 1](#_Toc196393646)

# Indledning

Risikostyring i har til formål at understøtte selskabets overordnede prioritering af ressourcer og implementering af IT-sikkerhedstiltag til sikring af det rette sikkerhedsniveau ift. s risikoprofil.

I anvendes risikostyring som en ramme for forvaltning af risici på tværs af alle dele af organisationen. Risikostyringen indeholder alle de aktiviteter, der kræves for at identificere og kontrollere eksponeringen for enhver form for risiko, som kan have en indvirkning på opnåelsen af organisationens forretningsmæssige mål og opretholdelse af det nødvendige IT-sikkerhedsniveau.

Risikostyringspolitikken skal til enhver tid understøtte s værdigrundlag og tilstræbe at implementerede IT-sikkerhedstiltag altid følger gældende standarder og love/regler, er effektiv og driftssikker samt er målrettet de konkrete opgaver, som selskabet udfører.

Hensigten med Risikostyringspolitikken er desuden at sætte rammerne for s arbejde med risikostyring.

## Definition

En risiko defineres som værende en mulig hændelse, der, hvis den opstår, vil have indvirkning på s it-sikkerhed. En hændelse kan være en trussel, som kan have en negativ indvirkning på organisationens it-sikkerhed og/eller drift stabilitet. En risiko angives som en kombination af sandsynligheden for at hændelsen indtræder og omfanget af dens indvirkning på/konsekvens for enten organisationen selv, personer hvorom persondata er registreret i s aktiver eller det samfund, som indgår i.

| Definition: Risiko |
| --- |
| En risiko defineres som en hændelse, der kan påvirke organisationens  it-sikkerhed og/eller drift til det værre. |

Bemærk, at der som udgangspunkt ikke anvendes positive risici (muligheder).

# Principper for risikostyring

Følgende afsnit præsenterer tre principper for risikostyring, herunder beskrivelse af risici, kategorisering af risici og brug af risikolog.

## Beskrivelse af risici

For at operationalisere beskrivelsen af risici opdeles de i tre komponenter:

Risikoårsagen er den bagvedliggende grund til, at risikoen eksisterer. Det kan for eksempel være forhold i organisationen eller vilkår i omverdenen, der betyder, at it-sikkerheden er sårbar.

Risikohændelsener den konkrete trussel, som organisationen står overfor. I praksis kan det være svært at skelne mellem årsag og hændelse, og i risikologgen er disse felter derfor slået sammen.

Risikokonsekvensenbeskriver hvad der sker, hvis hændelsen indtræffer. Risikokonsekvensen kan opgøres i tre nuancer:

* indflydelse på organisationens drift og processer – tid, økonomi og ressourcer
* omfang og konsekvens for organisationens registrerede - dvs. personer om hvem har registreret personhenførbare data
* indflydelse på det omkringliggende samfund som organisationen understøtter[[1]](#footnote-2).

## Risikokategorier

[Vejledning: brugen af risikokategorier kan give mening i nogle organisationer ift. opfølgning, overblik og ledelsesrapportering. Det er som sådan ikke obligatorisk, og afsnit 2.2 kan fjernes helt, hvis I ikke vurderer at det giver værdi i jeres arbejde med risici.]

Til identifikation og klassifikation af risici benytter sig af en inddeling af risici i fem risikokategorier, der er defineret i nedenstående tabel.

| Fem risikokategorier | |
| --- | --- |
| Medarbejder forhold | Potentielle hændelser der omhandler medarbejderes ageren tilsigtet eller utilsigtet. |
| Organisatoriske forhold | Potentielle hændelser der omhandler det organisatoriske setup, scope, organisationens modenhed og planlægning af mitigerende foranstaltninger. |
| Tekniske forhold | Potentielle hændelser der omhandler tekniske løsnings opfyldelse af kvalitetskrav og sikkerhed. |
| Drift forhold | Potentielle hændelser der omhandler driftens opfyldelses af kvalitetskrav og sikkerhed. |
| Leverandørforhold | Potentielle hændelser der omhandler leverandørens inddragelse og leverandørens opfyldelse af organisationens krav til it-sikkerhed og drift*.* |

# Organisering

Ansvaret for risikostyring følger selskabets organisatoriske opbygning. Den øverste risikoansvarlige er bestyrelsen. Bestyrelsen har det overordnede ansvar for risikostyring i organisationen med ansvar for at risici bliver håndteret og økonomi prioriteret. Direktøren har det overordnede ansvar for det daglige arbejde med risikostyringen og for at sikre, at risici bliver afdækket og at mitigerende handlinger bliver gennemført.

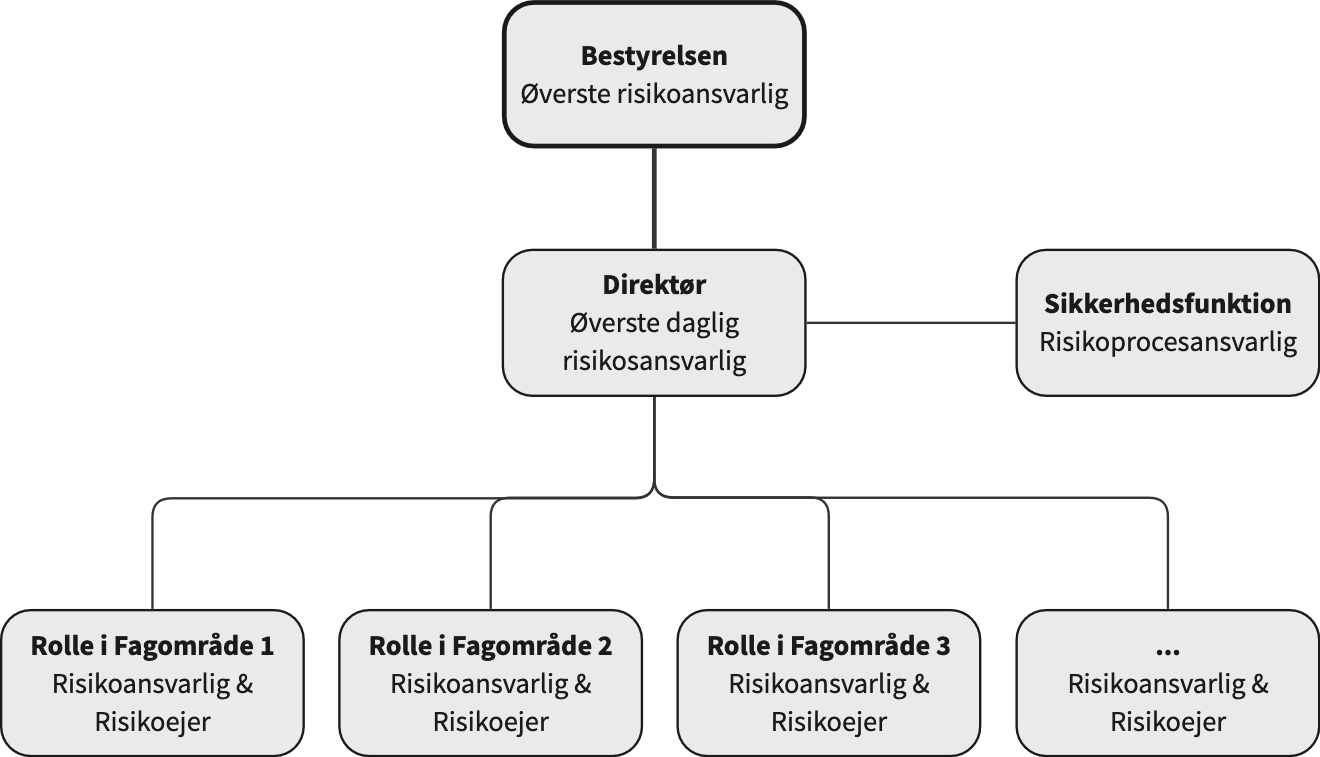
Risikoprocesansvarlig har ansvar for at holde risikologgen opdateret og løbende rapportere om risici samt holde øje med tidlige advarselsindikatorer for risici.

En udpeget Risikoansvarlig fra hver afdeling / team har ansvar for at bidrage til risikostyringen med risici fra eget fagområde. Det er vigtigt at der i risikoarbejdet er repræsentanter som dækker hele organisationen, så evt. risici afdækkes og vurderes baseret på faglig viden.

Alle risici delegeres til en Risikoejer*,* som har ansvaret for at følge op på risikoen og på de besluttede mitigerende tiltag.

Risikostyringsorganisationen følger IT-sikkerhedsorganisationen defineret i IT-sikkerhedspolitikken. Dvs. at IT-funktionen er Risikoprocesansvarlig, og at den IT-sikkerhedsansvarlige for et team også er udpeget som Risikoansvarlig for samme team.

Denne rolle- og ansvarsfordeling har til formål at sikre, at der er ledelsesinvolvering gennem hele processen, samt at de risikoansvarlige har de nødvendige kompetencer og faglige viden til at varetage deres opgaver i risikostyringsprocessen.



Figur 1: <Organisation>s risikostyringsorganisation.

[Vejledning: udskift ovenstående diagram med egen organisationsdiagram for risikostyring på rolleniveau – dvs. Driftschef, Administrationschef, Teamleder for kundeservice etc.]

s risikostyringsorganisation følger IT-sikkerhedsorganisationen og vedligeholdes i IT-sikkerhedspolitikkens Bilag A. Risikoorganisationen rapporterer direkte til bestyrelsen.

## Ansvarsfordeling

|  |
| --- |
| Øverste risikoansvarlig |
| **Bestyrelsen** |
| Ansvar |
| [Vejledning: For virksomheder energisektoren på niveau 2 eller over er der krav om indsendelse af en ROS-konklusionsrapport til Energistyrelsen. Denne rapport skal være godkendt af bestyrelsen.]  Bestyrelsen er ansvarlig for at prioriterer risikoarbejdet og skal følge op på risici og mitigerende handlinger. Bestyrelsen godkender rammerne for risikostyring (nærværende politik) og skal forholde sig til den periodiske rapportering af risici og mitigeringstiltag.   * Godkender politikken og rammerne for risikostyring for organisationen: Organisationens risikovillighed, tolerancer og eskaleringsprocesser. * Review af risikorapportering – ROS-konklusionsrapport * Input til risikoarbejdet * Forholde sig til risikovurderingen i prioritering af økonomi |

|  |
| --- |
| Øverste ansvarlig for styring af risikoprocessen |
| Direktør |
| Ansvar |
| * Implementerer politikken og rammerne for risikostyring for organisationen i form af procedurer og allokering af ressourcer. * Er overordnet daglig ansvarlig for risikostyringen og at alle risici afdækkes. |

|  |
| --- |
| Risikoprocesansvarlig |
| Udpeget rolle som rapporterer direkte til direktøren.  I er rolle risikoprocesansvarlig. |
| Ansvar |
| Ansvarlig for identificering, vurdering og kontrol af risici. Derudover er Risikoprocesansvarlig blandt andet ansvarlig for at:   * eskalere ved afvigelser af toleranceniveauer for risici, se afsnit 4.1. * modtage information om uforudsete hændelser og meddele dem til ledelsen (tid og omkostninger) * aftale toleranceniveauer og relaterede advarselslamper og eskaleringsprocedurer med ledelsen, for eksempel baseret på:   + stigninger i risikoværdien   + den absolutte risikoværdi   + konkrete tidlige advarselsindikatorer * opdatere risikologgen; modtage og registrere nye risici eller ændringer til risici, som opsamles fra medarbejdere, ledelsen, leverandører og interessenter * årligt review af risikovurderingsprocessen |

|  |
| --- |
| Fagområdespecifik Risiko-ansvarlig & Risikoejer |
| Linjeledelse / udpeget rolle i team I er den udpegede IT-sikkerhedsansvarlige i et team også risikoansvarlig og risikoejer, da kobling af disse roller sikrer den rette kompetence og viden ind i risikostyringsprocessen. Som risikoejer kan man uddelegere mitigerende handlinger til egne medarbejdere og leverandører. |
| Ansvar |
| Risikoansvarlig:   * Identificering af risici i forhold til brugerne og forretningen i eget team. * Identificering, vurdering og kontrol af risici i forhold til leverandørers services, for leverandørrelationer som eget team forvalter.   Risikoejer:   * Opfølgning egne risici og mitigerende tiltag * Eskalering ved behov for yderligere ressourcer eller hjælp fra andre fagområder |

## Kommunikation om risici

Det er vigtigt at sikre, at de ansvarlige for styring af risici, og dem der påvirkes af risici, forstår det grundlag som beslutningerne træffes på, samt hvorfor bestemte tiltag er nødvendige.

Internt i organisationen skal risikooplysninger kommunikeres på en nyttig og meningsfuld måde på tværs af forskellige operationelle områder af organisationen.

Eksternt rettes kommunikationen mod kunder og interessenter, som kan være involveret i eller berørt af organisationens beslutninger og handlinger.

Bilag D indeholder s kommunikationsplan for risikostyring.

# Fastsættelse af rammer

Identifikation af s rammeforhold bruges som ramme for at identificere konkrete risici og fastlægge de standarder, som forskellige risici vurderes ud fra, på en sådan måde at disse kan sammenlignes.

Rammerne dannes af nogle generelle forhold, så som lovgivning og regulering, samt organisationens modenhed ift. IT-sikkerhed. Det primære mål er at identificere hvilke rammeforhold, der påvirker organisationens risikoprofil. De generelle rammer for er beskrevet i Bilag A, og s sandsynlighed- og konsekvenscore er defineret i Bilag B.

## Risikotolerance og advarselslamper

Et andet vigtigt element i rammesætningen er en vurdering og beskrivelse af organisationens risikotolerance, dvs. hvor grænsen går for, hvilke risici der er acceptable eller ikke-acceptable. Dette defineres i en såkaldt risikotolerancemodel. Risikotolerancemodellen benyttes til at prioritere implementering af tiltag.

Til at understøtte rollerne i risikostyring er der aftalt advarselslamper, som er en prædefineret og kvantificeret indikator på, at en risiko er nært forestående eller udvikler sig i en uhensigtsmæssig retning. Advarselslamper er en operationel måde at arbejde med tolerancer for risici, og muliggør en informeret og forberedt tilgang til at håndtere hændelsen eller at eskalere den til ledelsen.

s risikotolerancemodel og advarselslamper er defineret i Bilag C.

# Proces for risikostyring

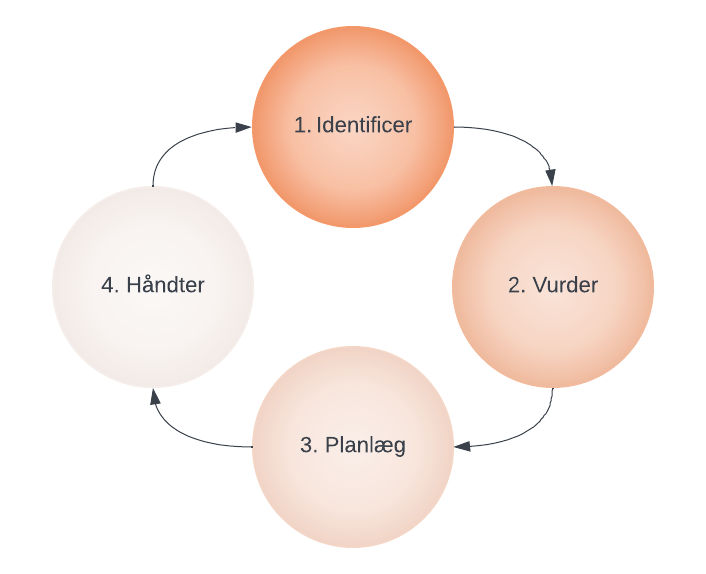
Dette afsnit beskriver processen for risikostyring. Derudover beskrives de organisatoriske perspektiver, hvori risikostyring indgår.

Organisationen arbejder med risici i fire procestrin, som angivet i Figur 2 herunder.

Risikostyringen foretages i risikoworkshops. Risikoworkshops er planlagte møder, med deltagelse af alle risikoansvarlige. Møderne afholdes med jævne mellemrum, se Bilag E, med deltagelse af repræsentanter fra alle afdelinger/teams i organisationen. Formålet er at få identificeret og vurderet alle sikkerhedsrisici, samt at få placeret ansvaret for mitigerende tiltag.

Risikoworkshops kan være ressourcekrævende, men det er vigtigt at alle afdelinger er involveret og bliver hørt.

Processen fortsætter igennem hele organisationens levetid, sådan at der løbende foretages identificering, vurdering, planlægning og håndtering af risici.



Figur 2: Risikostyringens fire trin

Processen indledes med identificering af risici. Her identificeres risikoelementer og deres indhold klarlægges.

Herefter vurderes sandsynlighed, konsekvens, tidspunkt for at risikoen kan indtræffe og potentielle tidlige advarselsindikatorer fastsættes.

Dernæst skal risikohåndteringen planlægges ved at angive mitigerende handlinger, som typisk vil minimere sandsynligheden eller konsekvensen af risikoen.

Endelig håndteresprojektets risici, og det sikres at der bliver fulgt op på denne håndtering.

Processen beskrives mere indgående i de følgende afsnit.

## Identificering

Første trin i processen for risikostyring er identificering af risici.

I denne proces identificeres de risici, som er for organisationens it-sikkerhed eller drift.

Risikoidentificeringen foregår som første del af en risikoworkshop. Risikoidentificeringen skal vigtigst af alt trække på den erfaring og viden, der allerede findes i organisationen, samt fra eksterne kilder såsom leverandører, it-sikkerhedstjenester, samarbejdspartnere, myndigheder etc. i form af varslinger eller ROS-scenarier.

Når risici er identificeret, beskrives de i Risikologgen, se afsnit 6. Her skrives både selve risikoen (risikohændelsen) samt en beskrivelse af mulige effekter og årsager til risikoen.

### Leverandør- og forsyningskæderisici

For alle direkte leverandører foretages en vurdering af risici, der er specifikke for den pågældende leverandør eller tjenesteudbyder, herunder risici forbundet med afhængigheder af underleverandører og internationale forhold.

For alle forsyningskritiske leverandører og tjenesteudbydere foretages dette via en årlig gennemgang af og opfølgning på overholdelse af indgåede aftaler.

## Vurdering

Når risici er identificeret, skal de vurderes. Vurderingen af risici er det andet trin i processen for risikostyring.

I vurderingsprocessen ses på sandsynligheden for, at en risiko indtræffer, samt hvad konsekvensen heraf er. Det er vigtigt at pointere, at der vil være tale om bedste gæt baseret på faglig ekspertise samt analyser og teknikker til vurdering. Formålet er ikke at give et endeligt svar på, om en risiko indtræffer, eller hvordan det helt præcist vil påvirke organisationen, de registrerede eller det omkringliggende samfund.

Organisationen har fastsat værdier for sandsynlighed og konsekvens så det stemmer med deres virkelighed. De fastsatte værdier betyder at risici kan prioriteres ud fra sammenlignelige kriterier, se Bilag C.

Den samlede risikoscore udregnes som sandsynligheden ganget med den højeste konsekvensscore.

## Planlægning

Når risici er identificeret og vurderet, planlægges hvordan risici håndteres. Planlægning af mitigerende tiltag er det tredje trin i processen for risikostyring.

Planlægningsprocessen har to formål. For det første skal den sikre, at der bliver iværksat mitigerende tiltag for risici, der kan påvirke organisationen væsentligt. For det andet skal planlægningsprocessen bruges til at planlægge nødprocedurer og beredskabsplaner for de største risici for , så organisationen ved hvad der skal ske, hvis risikoen indtræffer.

Planlægningsprocessen opdaterer handlingsplanen, se afsnit 6, for implementering af foranstaltninger. De økonomiske og ressourcemæssige konsekvenser af handlingsplanen afstemmes med ledelsen.

## Håndtering

Håndtering er det sidste procestrin i risikostyringen og skal sikre, at håndtering af risici bliver gennemført.

Det primære mål med håndteringsprocessen er at sikre, at de planlagte foranstaltninger bliver ført ud i livet. Ansvaret for at følge op på dette ligger både hos Risikoprocesansvarlig og hos de enkelte risikoejere:

* Risikoejeren følger op på de risici vedkommende er ansvarlig for og sikrer, at de bliver håndteret.
* Risikoprocesansvarlig sikrer, at risikologgen angiver det korrekte risikobillede for projektet, og at ledelsen er bekendt med dette.
* Risikoprocesansvarlig skal også sikre, at nødprocedurer og beredskabsplaner er opdateret og der forefindes effektive processer for iværksættelse af disse, hvis risici indtræffer.

### Mitigering

Når de mitigerende tiltag er blevet gennemført, revurderes risikoens sandsynlighed og konsekvens[[2]](#footnote-3), sådan at det bliver tydeligt, om der er behov for yderligere handlinger.

### Input til Beredskab

I visse tilfælde vil indtrufne risici få så store konsekvenser eller kræve så uhensigtsmæssigt mange ressourcer at håndtere, at der med fordel kan udarbejdes en nødprocedure for, hvad der konkret skal gøres, hvis risikoen indtræffer. Det drejer sig om de højest prioriterede risici, som:

* har en relativ høj sandsynlighed for at indtræffe,
* har alvorlige konsekvenser og
* ikke i tilstrækkelig grad kan forebygges for rimelige midler.

### Hændelseshåndtering

Risici, der indtræffer, er ikke længere risici, men hændelser. Det betyder, at risikoen, som nu er en hændelse, skal håndteres eksternt fra risikostyringen, i hændelseshåndteringsprocessen, nødprocedurer eller beredskab. Hændelser giver efterfølgende opdatering af risikologgen.

# Risikolog & handlingsplan

Til at understøtte risikostyringen er der udarbejdet et værktøj: Risikologgen. I forhold til organisationens anvendelse af risikologgen er det besluttet at:

* Loggen opdateres ved hver risikoworkshop, jf. risikostyringsplanen i Bilag E, så den vedvarende har værdi for s beslutninger
* Nye risici eller ændringer til risici opsamles fra medarbejdere, ledelsen, leverandører og andre interessenter jf. risikostyringsplanen i Bilag E, samt som en del af læringsprocessen efter indtrufne hændelser
* Afrapportere om risici til ledelsen jf. kommunikationsplanen i Bilag D, og som minimum ved overskridelse af tolerancer
* Indtrufne hændelser håndteres separat, som en del af hændelseshåndteringsprocessen eller beredskabsplanen.

Til at understøtte håndteringen af risici og mitigerende handlinger benyttes handlingsplanen. Handlingsplanen er s værktøj til opfølgning på de vedtagne mitigerende handlinger, se Bilag E.

I forhold til organisationens anvendelse af handlingsplanen er det besluttet at:

* Loggen opdateres ved hvert opfølgningsmøde, se Bilag E, så den kontinuerligt afspejler status for de vedtagne tiltag
* Hver handling skal tildeles en ansvarlig, som skal sikre fremdrift for tiltaget
* Ved handlinger der ikke kan overholde deadlines, mangler ressourcer eller på anden vis ikke kan overholde planen, eskaleres til ledelsen

# Projektrisici

arbejder med projektrisikostyring som minimum ved projekter som omhandler:

* Erhvervelse og udvikling af OT og OT-netværk, inkl. SRO-anlæg, adgangsstyring, logning, monitorering, backup etc.
* Outsourcing af udviklings-, drifts- og vedligeholdelsesopgaver, der kan påvirke leveringen af fjernvarme.

Risikostyringsprocessen for et projekt følger den samme fremgangsmåde som for organisationen, se afsnit 5 og 6, med projektgruppen som den udførende part. Det er dog vigtigt også i arbejdet med projektrisici at sikre en bred nok repræsentation i risikoarbejdet, så alle risici er afdækket.

Projektrisikovurderingen udarbejdes ved projektets opstart og foreligge skriftligt, inden projektet påbegyndes. Risikovurderingen skal opdateres, når projektets omfang, tidsplan og delleverancer ændres i en sådan grad, at det ændrer forudsætningerne for risikovurderingen.

Ved projekter af typen listet ovenfor, skal projektrisikovurderingen godkendes af bestyrelsen og sendes til Energistyrelsen til godkendelse senest én måned herefter.

# Bilag A - Generelle forhold

[Vejledning: Generelle forhold identificerer de rammeforhold der helt overordnet påvirker organisationens risikoprofil. Disse giver input til risikovurderingsprocessen, idet de fastsætter den baggrund, som de enkelte risici vurderes ud fra.]

|  |  |
| --- | --- |
| Hvor vigtig er organisationen for samfundet? | [Vejledning: NIS2 vigtig eller væsentlig virksomhed? Niveau placering ift. Bekendtgørelse om modstandsdygtighed og beredskab i energisektoren?] |
| Hvilke politiske bindinger er der på organisationen? | [Vejledning: Hvilken lovgivning sætter rammerne for organisationens it-sikkerhed og beredskab? Fx Bekendtgørelse om modstandsdygtighed og beredskab i energisektoren og GDPR.] |
| Hvilket modenhedsniveau har organisationen i forhold til it-sikkerhed? | [Vejledning: Er it-sikkerhed og it-sikkerhedsprocesser: ikke implementeret/planlagt/ad hoc/delvist implementeret/fuldt implementeret? Fx ift. overholdelse af SektorCERTs 25 anbefalinger.] |
| Har organisationen tilstrækkelige ressourcer til at foretage de fornødne mitigerende tiltag? | [Vejledning: Er opgaverne placeret hos medarbejdere/samarbejdspartnere med de rette kompetencer og mulighed for at prioritere opgaverne? Fx bestyrelsen og ledelsen er involveret og prioriterer opgaver og mitigerende tiltag, og sikrer kompetence via uddannelse af nøgle medarbejdere, samt brug af eksterne specialister.] |

# Bilag B – Scoring

[Vejledning: I dette bilag skal I fastsætte jeres egne scoringsværdier. Der er indsat eksempler med gul overstregning, men de er blot eksempler og bør fastsættes ud fra jeres forretning. Der er her valgt 3 konsekvenskategorier: Økonomi, produktion og konsekvens for de registrerede. Det er ikke sikkert at disse konsekvenskategorier passer til jeres virksomhed. I såfald tilpasser I til jeres behov.]

|  |
| --- |
| Sandsynlighed |
| Sandsynligheden for, at de identificerede trusler hænder. Vurderes på en  5-punktsskala. |
| 1: Meget Lav = 100 år hændelse  2: Lav = 10 års hændelse  3: Medium = årlig hændelse  4: Høj = månedlig hændelse  5: Meget høj = ugentlig hændelse |

Konsekvenserne af forskellige trusler i forhold til forskellige konsekvenskategorier, som kan være konsekvenser for organisationen selv, de registrerede og samfundet. Nedenfor er defineret de konsekvenskategorier, som benyttes i .

|  |
| --- |
| Økonomisk konsekvens |
| Vurderes for hhv. tid, økonomi og ressourcer, ift. de forbundne omkostninger for . Vurderes på en 5-punktsskala. |
| 1: Meget begrænsede = 1-1000 kr  2: Begrænsede = 1000-10.000 kr  3: Alvorlige = 10.000-100.000 kr  4: Meget alvorlige = 100.000-500.000 kr  5: Kritiske / katastrofale = 500.000+ kr |

|  |
| --- |
| Konsekvens for produktionen |
| Vurderes for antallet af berørte personer (samfundsmæssig konsekvens).  Vurderes på en 5-punktsskala. |
| 1: Meget begrænsede = 1-10 berørte husstande  2: Begrænsede = 11-100 berørte husstande  3: Alvorlige = 101-1000 berørte husstande  4: Meget alvorlige = 1000-2000 berørte husstande  5: Kritiske / katastrofale = 2000+ berørte husstande |

|  |
| --- |
| Konsekvens for de registrerede |
| Vurderes for antallet af berørte personer sammenholdt med klassifikationen af de berørte personhenførbaredata jf. formlen      hvor antallet af personer og følsomheden af dataene vurderes på en 5-punktskala (se nedenfor), og resultatet heraf divideres med 4 for at normalisere resultatet ift. de andre konsekvenskategorier. |
| Antal[[3]](#footnote-4):  1: Meget begrænsede = 1-10 berørte personer  2: Begrænsede = 11-100 berørte personer  3: Alvorlige = 101-1000 berørte personer  4: Meget alvorlige = 1000-10.000 berørte personer  5: Kritiske / katastrofale = 10.000+ berørte personer |
| Klassifikation[[4]](#footnote-5):  1: Meget begrænsede = offentlige persondata  2: Begrænsede = ikke-følsomme persondata  3: Alvorlige = anden kategori (cpr-nr og information om strafbareforhold)  5: Kritiske / katastrofale = følsomme persondata |

# Bilag C – Risikotolerance og advarselslamper

[Vejledning: her definerer I de forskellige risikoniveauer for den beregnede risiko. Herefter vurderer I hvor jeres tolerance niveau ligger. Der er indsat forslag med gult.]

Risikotolerancemodellen benyttes til at prioritere implementering af tiltag.

|  |  |
| --- | --- |
| Risikoværdi | Beskrivelse |
| 0 < x <= 6 | Accepteres – ingen handlinger foretages |
| 6 < x <= 16 | Handlinger overvejes, men er ikke planlagt som første prioritet |
| 16 < x <= 25 | Der skal planlægges og implementeres yderligere sikkerhedstiltag til adressering af risici i det omfang det er muligt. |

Følgende advarselslamper er aftalt:

[Vejledning: Eksempler indsat. Tilpas dem ift. jeres organisation]

* Risikoværdien er over 16
* Risikoværdien er stigende
* Tidspunktet for en risiko kan indtræffe nærmer sig

Ved aktivering af en advarselslampe eskaleres risikoen til øverste risikoansvarlig.

# Bilag D - Kommunikationsplan for risici

[Vejledningstekst: Ved fastlæggelsen af kommunikationsaktiviteter indenfor risikostyring kan organisationen afklare følgende spørgsmål:

* Hvilken type oplysninger skal kommunikeres? (Hvilken type oplysninger har interesserenter og påvirkede parter brug for, og hvilken type ønsker de?)
* Hvad er målgruppen for de forskellige typer af oplysninger? (internt personale, ledelse, eksterne interessenter, herunder offentligheden etc.)?
* Hvilken kommunikationskanal bør anvendes til at kommunikere oplysninger til den tiltænkte målgruppe?]

| Målgruppe | Kommunikationskanal | Type oplysninger |
| --- | --- | --- |
| Ledelsen | [Fastsatte møder.] | [Vejledning: I nogle organisationer deltager ledelsen i risikoworkshoppen. I andre fastlægges der særskilte møder, evt. med længere kadence end ovenstående. Den Risikostyringsprocesansvarlige skal fokusere sin kommunikationsindsats på de største risici, så ledelsen hele tiden er på linje med organisationens risici og kan agere derudfra. Dette muliggør også, at ledelsen får truffet beslutninger om håndtering af de største risici, hvis de overskrider de givne tolerancer] |
| Internt personale (medarbejdere) | [Mail] | [Vejledning: Information om ændringer der har direkte effekt på deres arbejdsopgaver og -rutiner.] |
| Bestyrelsen | [Rapport] | [Vejledning: Årlig rapport med status på risici arbejdet og planlagte handlinger] |
| Leverandører | [Mail] | [Vejledning: Information om ændringer der har direkte effekt på deres arbejdsopgaver og -rutiner.] |
| Kunder | [Mail] | [Vejledning: Information om ændringer der har direkte effekt på deres leverancer.] |
| Myndigheder | [virk.dk] | [Vejledning: Omfanget af afrapportering til myndighederne fastsættes ift. NIS2 implementeringen i de enkelte sektorer] |
| [Andre] |  |  |

# Bilag E - Plan for risikostyring

Dette bilag indeholder planen for risikostyring for it-sikkerhed og drift, som den er udmøntet i . Rollen der står understreget, er ansvarlig for gennemførelsen af aktiviteten.

[Vejledning: tilpas tabellen efter jeres behov. Forslag er indsat med gul tekst, men de er blot forslag. Sæt en realistisk kadence som både giver tid til at opgaverne udføres, og samtidig sikrer fremdrift.]

|  |  |  |  |
| --- | --- | --- | --- |
| Aktivitet | Kadence | Deltagere | Indhold |
| Risikoworkshop | Hvert kvartal fx d. 1. onsdag hver 3. md. Ca. 5 timer | * Risikoprocesansvarlig * Risikoejere * Ledelses-repræsentant | Risikoprocesansvarlig indkalder til workshops, og sikrer at risikolog og handlingslog ajourføres.  Risikolog: identificering / vurdering  Handlingsplan: planlægning |
| Opfølgning på handlingsplan | Månedligt fx d. 1. onsdag i md. Ca. 1 times varighed | * Risikoprocesansvarlig * Risikoejere | Risikoprocesansvarlig indkalder til statusmøder, og ajourfører handlingslog.  Handlingsplan: håndtering |
| Rapportering | Årligt fx 4 uger inden planlagt generalforsamling. | * Ledelsesrepræsentant * Bestyrelsen | Ledelsesrepræsentanten rapporterer til bestyrelsen.  Ledelsesrapportering af igangværende risici, implementerede tiltag og udvikling i trusselsbillede etc.  Opdateret risikorapport og opsummeret præsentation med mulighed for spørgsmål |
| Review og godkendelse af risikovurderings-politikken | Årligt fx ultimo Q3 | * Risikoprocesansvarlig * Ledelsesrepræsentant * Bestyrelsen | Risikoprocesansvarlig foretager den årlige ajourføring af nærværende dokument, i koordination med ledelsesrepræsentanten. Ledelsesrepræsentanten sikrer at bestyrelsen er opdateret ift. evt. ændringer.  Revisions-historikken i starten af dokumentet opdateres i denne forbindelse. Den nye version godkendes af bestyrelsen. |

1. Hvis organisationen er en vigtig eller væsentlig virksomhed under NIS2 eller er en leverandør, der understøtter forsyningskædesikkerheden for en vigtig eller væsentlig virksomhed. Fx niveauplacering jf. Bekendtgørelse om modstandsdygtighed og beredskab i energisektoren. [↑](#footnote-ref-2)
2. Under step 3 i risikovurderingsprocessen [↑](#footnote-ref-3)
3. Baseret på pointskalaen i Datatilsynets vejledning om tilsyn: https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet\_Vejledning%20om%20tilsyn%20med%20databehandlere\_oktober-2021.pdf [↑](#footnote-ref-4)
4. Baseret på Datatilsynets vejledning om klassifikation af persondata: <https://www.datatilsynet.dk/regler-og-vejledning/grundlaeggende-begreber/hvad-er-personoplysninger> [↑](#footnote-ref-5)