Vejledning til risikovurdering af cybersikkerhed

DCIS TRANSPORT, Trafikstyrelsen

Version 1.0

*Indhold*

[1. Ændringshistorik 2](#_Toc156994926)

[2. Indledning 3](#_Toc156994927)

[3. Risikovurderingsmateriale 4](#_Toc156994928)

[2.1. Vejledning 4](#_Toc156994931)

[2.2. Trusselskatalog 4](#_Toc156994932)

[2.3. Risikoklassificeringsskema 4](#_Toc156994933)

[2.4. Analyseskema 5](#_Toc156994934)

[3. Sådan gennemføres en risikovurdering 5](#_Toc156994935)

[Projektbeskrivelse 5](#_Toc156994937)

[Risikoidentificering 6](#_Toc156994938)

[Risikoanalyse 7](#_Toc156994939)

[Risikoevaluering 7](#_Toc156994940)

[Risikohåndtering 7](#_Toc156994941)

[4. Bilag 8](#_Toc156994942)

[Centrale begreber 8](#_Toc156994943)

[Ordforklaringer 10](#_Toc156994944)

# Ændringshistorik

|  |  |  |
| --- | --- | --- |
| **Version** | **Ændring** | **Foretaget af** |
| 1.0 | Første udgave | DGRO |
|  |  |  |

# Indledning

I alle organisationer er brugen af digitale data og systemer forbundet med risici i større eller mindre omfang. Risici kan aldrig fjernes helt, men ved at organisationen danner sig et overblik over aktuelle risici kan ledelsen træffe beslutning om, hvordan organisationens ressourcer bedst skal prioriteres for at nedbringe risici til et acceptabelt niveau.

Dette er en vejledning i en metode til at risikovurdere cybersikkerhed i en organisation. Den er udgivet af Trafikstyrelsens decentrale cyber- og informationssikkerhedsenhed (DCIS-Transport) og er udarbejdet i samarbejde med transportbranchen og Center for Cybersikkerhed (CFCS). Værktøjet består af en række trusselsscenarier for digitale systemer og data, som anvendes i transportsektoren og kan understøtte transportvirksomheder i at udføre en grundlæggende risiko- og sårbarhedsvurdering.

Metoden kan anvendes uanset, om virksomheden i forvejen har en metode for risiko- og sårbarhedsvurderinger ift. cyber- og informationssikkerhed og blot søger input til analysen, eller hvis virksomheden skal have etableret en ny fast struktur for ROS-vurderinger på området. Den er desuden anvendelig for alle typer af organisationer, også de som ikke umiddelbart ses som en del af transportsektoren.

Som supplement til en effektiv risikovurdering af cybersikkerheden, kan det desuden anbefales at efterleve de tekniske minimumskrav for statslige myndigheder for 2024[[1]](#footnote-2).

Spørgsmål til brugen af metoden kan rettes til [cyber@trafikstyrelsen.dk](mailto:cyber@trafikstyrelsen.dk).

Vejledningsmaterialet består af:

1. Vejledning (dette dokument)
2. Trusselskatalog
3. Risikoklassificeringsskema
4. Analyseskema

# Risikovurderingsmateriale



## Vejledning

Vejledningen er virksomhedens hjælp til at anvende materialet til deres risikovurderingen. Det kan bruges uanset om virksomheden skal have etableret en ny fast struktur for risikovurderinger på området eller om virksomheden i forvejen har en veletableret metode for risiko- og sårbarhedsvurderinger ift. cyber- og informationssikkerhed. I sidstnævnte tilfælde kan materialet bruges input til analysen.

I vejledningen præsenteres det samlede materiale og hvordan en risikovurderingsproces ideelt set bør foregå. Vejledningen indeholder derudover en ordliste over centrale begreber og tekniske termer, som anvendes i materialet.

Vejledningen indeholder en ændringslog for det samlede materiale.

## Trusselskatalog

Trusselskataloget beskriver eksempler på trusler, som er relevante for virksomheden at forholde sig til. Virksomheder, som benytter sig af dette materiale, bør forholde sig til alle scenarierne – selvom der er trusler, som ikke er relevante, bør det noteres og begrundes i analyseskemaet. Det ligger virksomhederne frit for at tilføje yderligere trusler eller scenarier, som kunne være relevante at inddrage.

Fokus for scenarierne i trusselskataloget er primært mobilitet – forstået som opretholdelse af samfundskritiske transportfunktioner – og på at sikre systemer, som er kritiske for passagernes sikkerhed både i relation til security-aspekter og safety-aspekter.

Trusselsscenarierne kan dog også have andre konsekvenser, fx økonomiske tab eller mindre driftsmæssige forstyrrelser, som er vigtige for virksomheden.

## Risikoklassificeringsskema

Virksomheden bør fastsætte niveauet for sin risikoaccept, dvs. risici, som virksomheden har identificeret, men som vurderes begrænsede nok til, at man ikke behøver mitigere (yderligere) for dem.

**Risiko** = *Konsekvensens alvorlighed x Sandsynlighed*

I TS’ risikoklassificeringsskema klassificeres ***Alvorligheden*** som 1) meget begrænset, 2) begrænset, 3) alvorlig, 4) meget alvorlig og 5) kritisk/katastrofal. ***Sandsynligheden*** klassificeres som 1) Meget lav, 2) lav, 3) moderat, 4) høj og 5) Meget høj.

Skemaet viser, hvordan virksomheden kan vælge at opgøre risikoaccept efter en farveskala, hvor grøn markerer accepteret risiko, og hvor gul og rød markerer risici, der ikke kan accepteres af virksomheden.

Skemaet viser et eksempel på, hvordan felterne kan farvebestemmes ud fra en række eksempler på konsekvenser ud fra de forskellige niveauer. Eksemplet er ikke udtryk for TS’ forventning til risikobilledet. Det er op til virksomheden selv at fastlægge accepteret og ikke-accepteret risiko

## Analyseskema

Analyseskemaet indeholder en forside samt selve analyseskemaet.

Forsiden indeholder udover baggrundsinformation omkring virksomheden, også en liste over de medarbejdere som har bidraget til risikovurdering.

Analyseskemaet dokumenterer og gennemgår risikovurderingens faser, som identificering, analyse, håndtering og efterfølgende evaluering af risici – ud fra forskellige trusselsscenarier, der kan true virksomhedens data- og informationssikkerhed. Den tilbageværende risiko i skemaet sammenlignes med virksomhedens definitioner for accepteret risiko (se mere under *Risikoklassificeringsskema*).

Analyseskemaet er virksomhedens eget dokument, og kan, når det er udfyldt, indeholde følsomme oplysninger.

# Sådan gennemføres en risikovurdering

En risikovurdering følger typisk følgende fem faser:

Projektbeskrivelse

Risikoidentificering

Risikoanalyse

Risikoevaluering

Risikohåndtering



### Projektbeskrivelse

Projektbeskrivelsen udgør rammen for risikovurderingen og den skal afgrænse hvad, der skal risikovurderes.

Projektbeskrivelsen indeholder en kortlægning af, hvilke funktioner i virksomheden, som er kritiske for at opretholde driften og hvilke digitale systemer og data, som understøtter disse funktioner.

Følgende spørgsmål bør besvares i kortlægningen:

Hvor opbevares og driftes virksomheden systemer og data? Hos virksomheden selv? Hos leverandører?

Hvilke data sammenstiller og gemmer virksomheden, og hvad bruges de til?

Hvilke systemer er virksomheden afhængige af i den daglige drift?

Det er vigtigt, at de fagligt relevante medarbejdere i organisationen inddrages i kortlægningen for at få et retvisende billede – både af de driftskritiske funktioner – men også af støttefunktioner, som fx logistik, beredskabsplaner, administrative systemer, mv., som indirekte bidrager til opretholdelsen af driften.

Medarbejdere i disse funktioner vil have et godt billede af, hvilke hændelser, som kan true disse dele af driften, og som derfor bør afspejles i den samlede risikovurderingen.

Det er afgørende, at projektet har opbakning fra den øverste ledelse – både mht. inddragelse af funktioner rundt omkring i organisationen og for at fastsætte organisationens risikoaccept. Det er topledelsens ansvar at fastsætte, hvilken risiko som organisationen kan leve med. Dette kan fx gøres vha. *risikoklassificeringsskemaet*.

Såfremt organisationen har outsourcet en eller flere virksomhedsfunktioner, herunder drift af digitale systemer, bør den eksterne leverandør også inddrages i analysearbejdet. Det kan gælde for administrativ IT såvel som for driftskritisk IT, men det kan også omfatte andre dele af organisationens drift såsom fysisk sikring for anlæg, kundekommunikation, mv.

*Eksempler på fagligt relevante kompetencer: CISO, it-chef, topledelse, beredskabsansvarlig, IT-ansvarlig, leverandører, underleverandører og centrale eksterne parter.*

### Risikoidentificering

Risikoidentificeringen beskriver de potentielle *trusler*, der kan ramme organisationen, de *sårbarheder*, der kan udnyttes under de enkelte farer samt *konsekvenserne* for organisationen, hvis truslen ikke kan afværges. Jo større eller mere kompleks, organisationens drift er, desto grundigere skal risikoidentificeringen være.

Ligesom ved projektbeskrivelsen, er det afgørende, at man inddrager relevante faglige kompetencer fra kolleger i og udenfor organisationen. *Trusselskataloget*, som er tilknyttet Cyber-ROS materialet, kan bruges som input til at identificere farer samt mulige sårbarheder og konsekvenser.

Det er vigtigt at understrege, at risikoidentificeringen altid er op til den enkelte organisation. Alle scenarier i trusselskataloget vil ikke nødvendigvis være relevante for alle aktører i sektoren. Der kan også være andre relevante scenarier for en organisation eller andre kombinationer af trusler, sårbarheder og konsekvenser, end, der beskrives i kataloget. Disse kan man med fordel selv tilføje i *Trusselskataloget* og indsende som en del af konklusionsskemaet til TS.

### Risikoanalyse

Risikoanalysen handler om at afdække eksisterende barriere (forebyggende og konsekvensreducerende), som organisationen har iværksat samt vurdere, hvor effektive disse er.

I Trusselskatalog præsenteres en række overvejelser, som virksomhederne kan vurdere for at afdække eksisterende barriere.

De samme overvejelser kan bruges som inspiration for at identificere yderligere tiltag i risikohåndteringsfasen, hvis risikoen i første omgang vurderes at være for høj.

### Risikoevaluering

I risikoevalueringen vurderes konsekvensernes alvorlighed samt sandsynligheden for at de indtræffer, med eksisterende foranstaltninger taget i betragtning.

Herefter vurderes de enkelte trusler for alvorlighed og sandsynlighed. Hvis risikoen vurderes at ligge inden for området for *acceptabel risiko* (grønt område) er der ikke behov for at gå videre med yderligere risikoreducerende barriere.

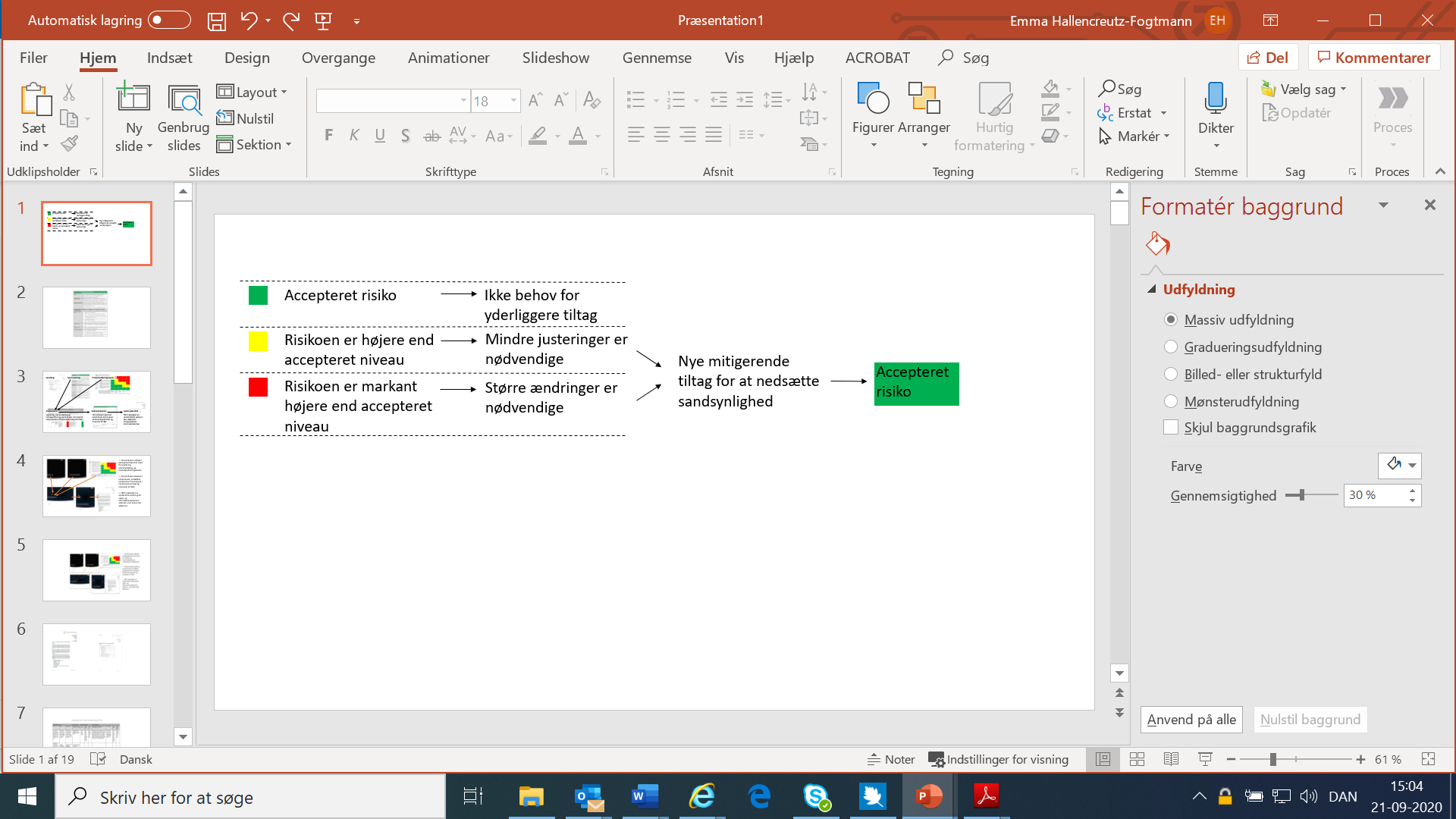
Det er topledelsens ansvar at fastsætte, hvilken risiko som organisationen kan leve med og sikre forankring af ejerskab over risici i organisationen. Dette kan fx gøres vha. *risikoklassificeringsskemaet*, hvor ledelsen kan definere intervallerne for de grønne/gule/røde felter. Det medfølgende risikoklassificeringsskema tjener som eksempel på, hvordan felterne kan farvebestemmes.

### Risikohåndtering

Hvis risikoniveauet ud fra eksisterende foranstaltninger ikke ligger inden for intervaller for acceptabel risiko, er der behov for at identificere yderligere forebyggende- og/ eller skadebegrænsende tiltag, der kan nedsætte sandsynligheden eller alvorlighed.

De nye tiltag indsættes i analyseskemaet under risikohåndtering. Her angives også, hvilken eller hvilke funktioner i organisationen, som er ansvarlig for at gennemføre indsatserne.

Til sidst evalueres den nye sandsynlighed for, at de beskrevne konsekvenser realiseres som ganges med konsekvensens alvorlighed fra den første risikoevaluering. Det resulterer således i den tilbageværende risiko for den beskrevne konsekvens. Den bør så ligge inden for virksomhedens fastsatte område for accepteret risiko (grønt område).



# Bilag

## Centrale begreber

Følgende begreber (samt synonymer herfor) bruges:

|  |  |
| --- | --- |
| **Trussel**  Kaldes også: *Fare, risk-event/ Top-event/hændelse* | En trussel er en uønskelig tilstand, aktivitet eller begivenhed der ved tab af kontrol kan lede til en konsekvens, hvis ikke den afværges.  Trusler identificeres uden hensyn tagen til eksisterende foranstaltninger. Dvs. trusler, som ses som usandsynlige fordi man har mitigeret for konsekvenserne er stadig trusler, og bør tages med i ROS-vurderingen. |
| **Årsag** | En sårbarhed kan alene eller i kombination med andre sårbarheder resultere i en trussel, hvis ikke den afværges. |
| **Konsekvens** | Konsekvens er resultatet af en trussel, hvor kontrol ikke genvindes. Det vil sige, at konsekvensen opstår, når en trussel ikke afværges.  Konsekvens kan være brud på enten tilgængelighed, fortrolighed eller integritet – eller en kombination af de tre (se definitioner på ordene i ordforklaringen). |
| **Alvorlighed** | En konsekvens kan have forskellige alvorlighedsgrader. Det kan være tale om et omfattende angreb, der medfører tab af menneskeliv eller omfattende materiel skade eller en begrænset hændelse, med minimal betydning for passagerer, personale og transportydelse.  I risikoklassificeringsskemaet defineres konsekvensens alvorlighed på en skala fra 1-5 (Meget begrænset til Kritisk/ Katastrofal) |
| **Sandsynlighed**  Kaldes også: *Frekvens* | Sandsynligheden defineres typisk ud fra hvor ofte, konsekvensen er opstået, dvs. med hvilken frekvens. Sandsynligheden kan være svær at vurdere. Man kan derfor med fordel studere hændelser i andre organisationer eller beskrivelser af sandsynlighed i eksterne trusselsvurderinger for at få flere bud på niveauet.  I risikoklassificeringsskemaet defineres sandsynligheden på en skala fra 1-5 (Usandsynlig til Meget sandsynlig) |
| **Risiko** | Risikoniveauet er konsekvensens alvorlighed gange dens sandsynlighed, dvs.  ***Alvorlighed*** x ***Sandsynlighed*** = ***Risikoniveau***  I risikoklassificeringsskemaets bruges 5-gradige skalaer for at klassificere alvorlighed og sandsynlighed. Risikoniveauet klassificeres enten som grøn, gul eller rød:  Det gøres opmærksom på, at forskellige kombinationer af alvorlighed og sandsynlighed kan resultere i samme tal for risikoniveau, som kan ligge både inden for og udenfor det grønne interval.  Fx:  *Alvorlighed 2* x *Sandsynlighed 3* = *Risiko 6* (grønt område i risikoklassificeringsskemaet)  og  *Alvorlighed 3* x *Sandsynlighed 2* = *Risiko 6* (gult område i risikoklassificeringsskemaet)  Risikoniveauet kan derfor ikke kun udtrykkes som et tal men skal læses som hele funktionen alvorlighed x sandsynlighed og sammenlignes med de fastlagte områder i skemaet.    Den ***acceptable* *risiko*** fastlægges af organisationens ledelse. Den ligger indenfor et interval, som markeres med grøn farve i risikoklassificeringsskemaet.  Organisationen skal indsætte foranstaltninger, der nedbringer risikoen indenfor intervallet for acceptabel risiko. Det risikoniveau, som organisationen ender med kaldes den ***tilbageværende* *risiko***. |
| **Foranstaltninger**  Kaldes også: Tiltag, r*isikoreducerende tiltag/ Kontroller/ Sikkerhedsforanstaltninger/ Barrierer* | Foranstaltninger kan både indsættes for at nedsætte sandsynligheden for, at en konsekvens opstår (forebyggende), og efter, at den er opstået for at nedsætte konsekvensernes alvorlighed og genvinde kontrol (afhjælpende).  I analyseskemaet skal virksomheden under ***risikoanalysen*** angive eksisterende foranstaltninger. Disse bidrager til den indledende risikovurdering. Såfremt risikoen ligger over det interval for risikoaccept, som virksomheden har fastsat, skal virksomheden identificere og implementere yderligere foranstaltninger. Disse bidrager til en ny vurdering af den tilbageværende risiko.  ***Trusselskataloget*** præsenterer en række overvejelser, som virksomhederne kan gøre sig ift. foranstaltninger. Disse kan både bidrage til at kortlægge eksisterende foranstaltninger og til at identificere yderligere tiltag.  Tiltagene kan omhandle digitale barrierer og tekniske installationer, men de kan også bestå af påvirkning på menneskelig adfærd, beredskabsprocedurer mv. – eller en kombination heraf. |

## Ordforklaringer

|  |  |
| --- | --- |
| CFCS | Center for Cybersikkerhed |
| DDoS | Distributed Denial of Service (vedvarende angreb mod virksomhedens it-infrastruktur via internettet) |
| End-of-life/end-of-support | Et produkt, der er leveret til kunder, som er blevet utidssvarende og vil blive udfaset af leverandørerne |
| Fysisk sikring | Dækker over sikring såsom alarmer, adgangsstyring, indhegning, mærkning |
| Fortrolighed | Det skal sikres, at informationen ikke gøres tilgængelig eller afsløres for uautoriserede personer, brugere eller processer. |
| Industrikontrolsystemer (ICS) | Betegnelse for systemer, der styrer, overvåger og kontrollerer. Dette kan f.eks. være SCADA eller andre Industrial Control Systems (ICS) |
| Informationssikkerhed | En bred betegnelse for de samlede foranstaltninger til at sikre informationer iht. ”fortrolighed”, ”integritet” og ”tilgængelighed” |
| Integritet | Det skal sikres, at informationsaktiverne (data og informationssystemer) er nøjagtige og fuldstændige. |
| Kill-switch | Kill-switch teknologi giver mulighed for at lukke ned for f.eks. en internetforbindelse eller afbryde applikationer øjeblikkeligt |
| Legacy-system | Legacy it-systemer er ældre it-systemer baseret på gammel it-arkitektur og/eller teknologi |
| Logning | Registrering af aktiviteter i virksomhedens IT-systemer. Kan være et vigtigt redskab til at sikre beviser i et efterforskningsøjemed ifm. et cyberangreb. |
| Nedetid | Udtrykket nedetid (eller downtime) bruges til at henvise til den tidsperiode, hvor et system ikke er tilgængeligt. |
| Omdømme | Virksomhedens ry og rygte, påvirkning af dette. |
| Operational technology (OT) | Operational Technology, dækker over de fysiske systemer, der overvåges eller styres af SCADA eller ICS. |
| Patching | Proces mhp. opdatere og reparere software, f.eks. for at eliminere en sårbarhed |
| Privacy | Persondatabeskyttelse, herunder i forhold til gældende lovgivning. |
| Remote sites | Anlæg eller systemer, som styres med fjernstyring |
| Recovery Point Objective (RPO) | Udtryk for, hvor ofte virksomhedens ønsker at tage backup |
| Recovery Time Objective (RTO) | Udtryk for, hvor hurtigt virksomheden ønsker at være oppe igen efter et nedbrud. |
| Remote Access Tool (RAT) | RAT, eller remote access tool, er software som giver en bruger fjernadgang til enheder/systemer/netværk/computer |
| SCADA | Supervisory Control and Data Acquisition. Bruges til overvågning og kaldes også SRO, HMI og ICS-anlæg. |
| Sikkerhed | Passagersikkerhed og/eller medarbejdersikkerhed |
| Spear-phishing | Et målrettet angreb rettet mod enkeltpersoner f.eks. ved, at en ondsindet aktør fremsender tillokkende mails mhp. at indhente forretningsoplysninger eller bruger-id. |
| Switch | Et stykke hardware, som kan bruges til at sende datapakker ud |
| Tilgængelighed | Det skal sikres, at informationsaktiverne (data og informationssystemer) er tilgængelige og anvendelige ved anmodning fra en autoriseret bruger eller person. |

1. <https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav/tekniske-minimumskrav-2024> [↑](#footnote-ref-2)