|  |  |
| --- | --- |
| Bilag 1: Eksempel på risikovurderingsmetode – bør justeres til organisations kontekst før brug |  |

Metode for detaljerede risikovurderinger (Version 1.0)

Ejer af procedure/metode: [kontor/enhed]  
Dato for ikrafttrældelse: [dato]

Godkendt af: [Informationssikkerhedsudvalget]

Næste planlagte revision: [dato]

*Indledning*

I det følgende beskrives [organisationens] metode for detaljerede, systemnære risikovurderinger på informationssikkerhedsområdet samt for vurdering af risici for de registrerede. Modellen vedrører både risikovurderinger af it-nyanskaffelser og systemer, der er i drift.

De to typer består af de samme grundelementer, som er beskrevet i det følgende, men afviger alligevel fra hinanden i forhold til ansvar, sikkerhedskrav, mv. Processerne for hver type beskrives derfor særskilt i bilag 1 og 2 nedenfor.

*Baggrund*

Risikovurderingerne er et praktisk værktøj til at identificere hvilke forhold og sårbarheder ved et system, der kræver overvågning eller handling og derved et beslutningsgrundlag for styring og prioritering af informationssikkerhedsarbejdet ud fra et risikobaseret grundlag, jf. koncernfælles informationssikkerhedspolitik samt den internationale informationssikkerhedsstandard ISO 27001.

Jævnfør databeskyttelsesforordningens artikel 32 skal den dataansvarlige etablere passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der imødegår de risici, som behandlingen måtte medføre for de registrerede. Styrelsen skal som følge heraf foretage vurderinger af disse risici for at kunne fastlægge, hvilke foranstaltninger det er nødvendigt at etablere for at sikre de registreredes rettigheder.

Der er i standarden ikke et fast krav om valg af metode. Nærværende metode er derfor udarbejdet med inspiration fra:

 *Den internationale standard for risikostyring på informationssikkerhedsområdet ISO 27005*

 *Vejledning i udformning af risikostyringsarbejdet (offentlig tilgængelig på sikkerdigital.dk)*

 [*Vejledende tekst om risikovurdering, Datatilsynet og Rådet for Digital Sikkerhed, Juni 2019*](https://www.datatilsynet.dk/media/7900/vejledende-tekst-om-risikovurdering.pdf)

[ *Datatilsynet, Justitsministeriet, Digitaliseringsstyrelsen, Behandlingssikkerhed - Databeskyttelse gennem design og*](https://www.datatilsynet.dk/media/6879/artikel25og32-vejledning.pdf)[*standardindstillinger, Juni 2018*](https://www.datatilsynet.dk/media/6879/artikel25og32-vejledning.pdf)

*Roller og ansvar*

Ansvaret for gennemførsel af risikovurderingen er placeret hos det fagkontor, der har ansvaret for det aktiv, der risikovurderes (fx systemejeren). Det er således fagkontorets ansvar at inddrage [kontor/enhed] ved it- nyanskaffelser, og såfremt kontoret vurderer, at et system i drift bør risikovurderes, og det ikke indgår i den årlige plan for risikovurderinger, som [kontor/enhed] udarbejder. [Kontor/enhed] faciliterer risikovurderingen og leverer en risikovurderingsrapport, hvori de identificerede risici og anbefalinger til sikkerhedsforanstaltninger eller krav til leverandøren fremlægges. Fagkontoret spiller en central rolle i vurderingen, da det er repræsentanter herfra, der skal foretage vurderingerne og sørge for, at [kontor/enhed] har tilstrækkelig information om systemet til at anbefale sikkerhedsforanstaltninger. [Juridisk kontor/enhed] understøtter vurderingen af risici for de registrerede samt gennemgår tjekliste for de registreredes rettigheder.

Beslutningen om, hvilke af anbefalingerne der skal følges og implementeres, ligger hos risikoejeren. Risikoejeren er typisk den person, som en risikohændelse vil have en direkte konsekvens for, og dermed har ansvaret for at risikoen håndteres. Risikoejeren bør deltage i risikovurderingsworkshopperne, og indstiller til ledelsen om en risiko bør accepteres eller nedbringes/reduceres. Ansvaret for udarbejdelse af risikohåndteringsplan ligger dermed også hos risikoejer. Risikoejer kan være kontorchefen, en systemansvarlig, projektejer, direktøren mv., afhængigt af risikoen. Der kan være flere risikoejere i et projekt, men ikke flere ejere af en enkelt risiko.

*Proces for risikovurdering*

Risikovurderingen indeholder de samme grundlæggende elementer, uanset om det vedrører en nyanskaffelse eller et system i drift. Risici beregnes, som vist i nedenstående figur, ved en sammenkobling af konsekvens og sandsynlighed (trusler/sårbarheder), som identificeres af fagkontoret og med bistand fra [kontor/enhed] og [juridisk kontor/enhed] på en række workshops.



Konsekvenser

Sandsynlighed

(trusler og sårbarheder)

Risiko

*Konsekvensvurdering*

Konsekvensvurderingen har til formål at afdække, hvilke konsekvenser et brud på hhv. fortroligheden, integriteten og tilgængeligheden (FIT) vil have i relation til en række forskellige konsekvenstyper, såsom økonomi, registrerede personer, organisationens evne til at nå strategiske mål mv. FIT er omdrejningspunktet for informationssikkerhedsarbejdet, og er derfor de centrale områder, informationssikkerheden italesættes ud fra.

Der gennemføres både en konsekvensvurdering fra [organisationens] perspektiv og fra de registreredes perspektiv.

Konsekvenserne afdækkes ved workshops med deltagelse af relevante personer, fx kontorchef, projektejer, projektleder, indkøbsansvarlig, systemansvarlig, osv. Workshoppene faciliteres af [kontor/enhed] og [juridisk kontor/enhed] og følger nærværende metode, hvor deltagerne besvarer spørgsmål vedrørende konsekvensdimensionerne i følgende dokumenter:

 *Konsekvensniveauer - Registrerede personer*

 *Konsekvensniveauer – Forretningsmæssige Trussels-, sårbarheds- og sandsynlighedsvurdering*

Trusselvurderingen skal afdække, hvilke relevante trusler der er rettet mod det pågældende system. [Kontor/enhed] faciliterer en trussels- og sårbarhedsworkshop, hvor relevante deltagere såsom kontorchef, projektejer, projektleder, indkøbsansvarlig, systemansvarlig, osv. vurderer de enkelte truslers relevans for systemet. Vurderingen tager udgangspunkt i [organisationens] interne trusselskatalog og deltagernes eventuelle input til relevante trusler. Truslerne kan bl.a. være cyberangreb, leverandørsvigt, tilsigtet læk, mv.

Trusselskataloget er et dynamisk dokument, som ændrer sig løbende, i takt med at nye trusler identificeres. Det er ikke et udtømmende dokument, men skal betragtes som inspiration og forslag til en udvælgelse af relevante trusler. Truslerne kan variere fra system til system.

Når de relevante trusler er identificeret, vurderes det dernæst om systemet eller forretningen er sårbart over for disse. Trusler udnytter sårbarheder, og bliver dermed først realiseret, såfremt omstændighederne tillader det. Eksempelvis kan en sårbarhed være, at der ikke findes nedskrevne processer vedrørende arbejdsgangene i systemet, at systemet ikke bliver vedligeholdt med sikkerhedsopdateringer, eller at der ikke er mulighed for at styre brugerrettigheder i systemet.

Sårbarhederne og truslerne kan dog ikke stå alene, da det er nødvendigt at vurdere, hvorvidt det er sandsynligt, at sårbarheden udnyttes og truslen dermed realiseres. Sandsynligheden for at en hændelse indtræffer kan være svær at vurdere, da det er en hypotetisk vurdering. I sin vurdering kan man dog medtage faktorer såsom konkret erfaring med hændelsen (om hændelsen er indtruffet før, eller at systemet ofte udsættes for en bestemt type angreb), det nationale trusselsbillede (udgives af Center for Cybersikkerhed), hvori der gives en indikator på, hvor høj truslen er for fx cyberangreb for offentlige myndigheder. Endelig kan man ud typen af data i systemet vurdere om det er sandsynligt, at der skulle indtræffe en hændelse. Har data værdi for fx fremmede magter, andre virksomheder eller hackere, er sandsynligheden for et angreb formentlig højere end ellers. Hvis der tillige er en sårbarhed tilstede, der gør det muligt at få succes med angrebet, er sandsynligheden for at hændelsen indtræffer dermed høj.

Sandsynligheden for, at et brud på informationssikkerheden indtræffer vurderes samlet for [organisationen] og de registrerede.

*Risikoscore og -villighed*

Niveauet for risikovillighed vedrørende informationssikkerhedsrisici i [organisationen] er godkendt i regi af [informationssikkerhedsudvalg], hvor bl.a. ledelsen er repræsenteret. I nedenstående farveskema angives det, hvilke risici der betragtes som værende meget lave/lave, og dermed automatisk ikke bør give anledning til yderligere behandling.

For hver sårbarhed er der vurderet en konsekvens ved et fortrolighedsbrud, integritetsbrud og tilgængelighedsbrud. Konsekvensvurderingerne for [organisationen] og de registrerede kan være forskellige. Der foretages en samlet sandsynlighedsvurdering. På baggrund af sandsynlighedsscoren og

konsekvensscores beregnes et risikotal. Alt efter resultatet placeres sårbarheden i en farvekategori, der angiver om den udgør en lav eller høj risiko for [organisationen] og de registrerede. I rapporteringen vil fokus ligge på, hvor risici ligger på nedenstående farveskala frem for talværdien.

*DPIA (Data Protection Impact Assessment)*

Ifølge EU’s databeskyttelsesforordning, skal der foretages DPIA (konsekvensanalyse for databeskyttelse) såfremt en række kriterier opfyldes vedrørende persondatamæssige risici vedrørende en ny behandlingsaktivitet/et nyt system. Det er omfattende at udarbejde en DPIA, og der stilles yderligere ikke krav i forordningen om, at det skal gøres for hvert system eller hver behandling. Derfor udarbejdes den kun i de tilfælde, hvor der vurderes at være en høj risiko for den registrerede forbundet med den specifikke behandling af personoplysninger.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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** | | |  |

*Rapportering og anbefalinger*

Rapporten udarbejdes af [kontor/enhed] og indeholder beskrivelse af systemet, hvilke komponenter det indeholder, hvilke der er medtaget i vurderingen, og en samlet analyse af, hvordan risici fordeler sig for [organisationen] og for de registrerede. I rapporten fremhæves de opmærksomhedspunkter, der har særlig betydning for sikkerheden, fx ved at være af kritisk karakter.

Der medtages ligeledes anbefalinger til foranstaltninger og tiltag samt anbefalinger til krav til leverandører, hvor det er muligt.

Der lægges vægt på, at anbefalingerne er relevante i forhold til systemet og resultaterne af risikovurderingen. I forbindelse med udvælgelse af anbefalingerne tages der primært udgangspunkt i ISO 27001, anneks A, interne politikker og retningslinjer samt publikationen *Sådan stiller du krav til leverandører om informationssikkerhed – Katalog*, 2017. Heri er der opstillet en række generiske krav ud fra hhv. ISO 27001 samt SANS CIS Critical Security Controls v. 6.1, der er af mere operationel karakter.

Rapporten høres og godkendes endeligt i det ansvarlige fagkontor. Beslutningen om, hvorvidt anbefalingerne i rapporten til- eller fravælges træffes desuden af risikoejer, evt. i fællesskab med de øvrige repræsentanter fra fagkontoret. Fagkontoret udarbejder risikohåndteringsplaner for de risici, der ønskes håndteret, og aktiviteterne indføres i styrelsens risikoregister. Begrundelsen for fravalg af anbefalingerne skal dokumenteres og vedlægges sagen.

*Rapportering til [informationssikkerhedsudvalg]*

I forbindelse med forelæggelse af den samlede årlige risikovurderingsrapport vælger og prioriterer [informationssikkerhedsudvalg], hvilke risici fra de enkelte risikovurderinger, de vurderer, skal rapporteres løbende til udvalget.

Risici der udvælges til rapportering til [informationssikkerhedsudvalg] registreres i risikoregistret. Risikoejeren (fx systemejeren) er ansvarlig for den løbende rapportering af risikohåndteringen til [informationssikkerhedsudvalg]. Ved it-nyanskaffelser og ikke- kritiske systemer i drift rapporteres risici kun til [informationssikkerhedsudvalg] i de tilfælde, hvor risikoejeren vurderer, at det er en nødvendighed for at være i stand til at håndtere disse.

**Bilag 1**

**Risikovurdering af it-nyanskaffelser**

I forbindelse med indkøb af et nyt system, er det enten projektejers eller kontorchefen for det pågældende fagkontors ansvar at inddrage [kontor/enhed] med henblik på at gennemføre en risikovurdering på informationssikkerhedsområdet. Dette bør ske så tidligt som muligt i processen, ideelt i planlægningsfasen inden valg af system eller leverandør, da det dermed bliver muligt at stille krav til sikkerhedsforanstaltninger, som leverandøren bør opfylde. Risici kan dermed nedbringes allerede inden systemet idriftsættes, og fravalg af systemer med risici, der ikke kan håndteres kan ske inden et indkøb er foretaget.

*Fremgangsmetode*

Risikovurdering af en it-løsning, som skal anskaffes, foretages efter følgende proces:

1. Beskrivelse af it-løsningen, som skal anskaffes, samt dets formål (fagkontor)
2. Konsekvensvurdering (fælles)
3. Trussels-, sårbarheds- og sandsynlighedsvurdering (fælles)
4. Anbefalinger til risikoreducerede sikkerhedsforanstaltninger og -krav ([kontor/enhed])
5. Rapportering ([kontor/enhed] i samarbejde med fagkontor og [juridisk kontor/enhed])
6. Implementering af sikkerhedskrav (fagkontor)

Følgende figur illustrerer forløbet:

Projekt etableres [Kontor] inddrages Risikovurderingsworkshops

afholdes

[Kontor] udarbejder risikovurderingsrapport med anbefalinger

Krav til systemet og leverandør udvælges af risikoejer

*Deltagere i risikovurderingen*

Risikovurderingen faciliteres af [kontor/enhed] på en række workshopper. [Juridisk kontor/enhed] understøtter vurderingen af risici for de registrerede. I risikovurderingen deltager kontorchefen for fagkontoret (eller en stedfortræder) og de medarbejdere, som er relevante i forhold til den konkrete anskaffelse. Det kan være systemforvalter, projektejer, indkøbsansvarlig, medarbejdere med viden om processerne, o. lign.

Indholdet på workshopperne vil typisk bestå af følgende:

* En redegørelse for systemet, hvilke processer det skal understøtte, hvilke data der lagres i systemet, hvor det skal hostes mv. Spørgerammen udfyldes af fagkontoret inden den første workshop.
* Efterfølgende foretages en vurdering af, hvilke konsekvenser brud på hhv. fortroligheden, integriteten og tilgængeligheden vil have inden for en række dimensioner, der vedrører [organisationen] som en forretning samt de registrerede.
* Deltagerne skal, med vejledning fra [kontor/enhed], identificere de trusler, der er relevante for den pågældende løsning. Til at understøtte dette trin, leverer [kontor/enhed] et katalog over trusler, som der kan tages afsæt i. Kataloget er dog ikke udtømmende, og deltagerne bør derfor overveje om der er øvrige relevante trusler, som bør medtages. Efterfølgende identificeres de sårbarheder, der kan være i forhold til systemet (eller den type af system), samt processerne. Sårbarhederne kobles sammen med de identificerede trusler, og der foretages en vurdering af, hvad sandsynligheden er for, at en trussel vil udnytte en sårbarhed.

*Rapportering*

[Kontor/enhed] samler resultaterne i en rapport, hvori anbefalinger til sikkerhedskrav eller -foranstaltninger indgår.

**Bilag 2**

**Risikovurdering af systemer i drift**

I forbindelse med den årlige planlægning af systemnære risikovurderinger, udarbejder [kontor/enhed] en plan for de idriftsatte systemer, der skal risikovurderes. Beslutningen træffes ud fra forskellige kriterier, fx om systemet er forretnings- eller samfundskritisk, resultater fra seneste risikovurdering, dato for seneste risikovurdering, eller om fagkontoret har bestilt en risikovurdering af systemet. Som udgangspunkt er det dermed [kontor/enhed], der har ansvaret for at udvælge og planlægge risikovurderinger, mens det pågældende fagkontor er forpligtet til at stille repræsentanter og information til rådighed til workshopperne.

*Fremgangsmetode*

Risikovurdering af en it-løsning, som er i drift, foretages efter følgende proces:

1. Resultat fra tidligere risikovurdering fremlægges, såfremt en sådan findes. Resultatet drøftes, og det besluttes, hvilke trusler der skal vurderes igen, tilføjes eller udgå.
2. Beskrivelse af it-systemet samt dets formål om nødvendigt (fagkontor)
3. Konsekvensvurderinger (fælles)
4. Trussels-, sårbarheds- og sandsynlighedsvurdering (fælles)
5. Anbefalinger til risikoreducerende sikkerhedsforanstaltninger og -krav ([kontor/enhed])
6. Rapportering ([kontor/enhed] i samarbejde med fagkontor og [juridisk kontor/enhed])
7. Udarbejdelse af risikohåndteringsplan (fagkontor)
8. Implementering af sikkerhedsforanstaltninger (fagkontor) Følgende figur illustrerer forløbet:

[Kontor] udvælger system (evt. på baggrund af bestilling fra fagkontor)

Fagkontor notificeres

Risikovurderingsworkshops afholdes

[Kontor] udarbejder

risiko rt med

vurderingsrappo

anbefalinger

Sikkerhedsforanstaltninger udvælges af risikoejer

*Deltagere i risikovurderingen*

Risikovurderingen faciliteres af [kontor/enhed] og der afholdes en række workshopper. [Juridisk kontor/enhed] understøtter vurderingen af risici for de registrerede. I risikovurderingen deltager kontorchefen for fagkontoret (eller en stedfortræder) og de medarbejdere, som er relevante i forhold til den konkrete anskaffelse. Det kan være systemforvalter, indkøbsansvarlig, medarbejdere med viden om processerne, o. lign.

Indholdet på workshopperne vil typisk bestå af følgende:

* + Såfremt der tidligere er foretaget en risikovurdering, drøftes denne og det besluttes, hvilke elementer, der fortsat er gældende. Er der ikke udarbejdet en risikovurdering, eller er denne ikke fyldestgørende, gives der af fagkontoret en indføring i, hvad formålet er med systemet, hvilke processer det skal understøtte, hvilke data der lagres i systemet, hvor det skal hostes mv. Spørgerammen forsøges udfyldt af fagkontoret inden workshoppen.
  + Efterfølgende foretages en vurdering af, hvilke konsekvenser brud på hhv. fortroligheden, integriteten og tilgængeligheden vil have inden for en række

dimensioner, der vedrører [organisationen] som en forretningen samt de registrerede.

* + Deltagerne skal, med vejledning fra [kontor/enhed], identificere de trusler, der er relevante for den pågældende løsning. Afhængigt af, om øvelsen er lavet tidligere, kan man overveje at genbruge vurderinger og blot tilføje eller rette til. Til at understøtte dette trin, leverer [kontor/enhed] et katalog over trusler, som der kan tages afsæt i. Kataloget er dog ikke udtømmende, og deltagerne bør derfor overveje om der er øvrige relevante trusler, som bør medtages.
  + Efterfølgende identificeres de sårbarheder, der kan være i forhold til systemet (eller den

type af system), samt processerne. Sårbarhederne kobles sammen med de identificerede trusler, og der foretages en vurdering af, hvad sandsynligheden er for, at en trussel vil udnytte en sårbarhed.

*Rapportering*

[Kontor/enhed] samler resultaterne i en rapport, hvori anbefalinger til sikkerhedskrav eller -foranstaltninger indgår.