**Risikovurderings notat for:**

**Projektnavn/system**

**Indholdsfortegnelse:**

[1. Basale oplysninger: 2](#_Toc131067671)

[2. Indledning 2](#_Toc131067672)

[3. System-/ projektbeskrivelse 3](#_Toc131067673)

[4. Overordnet vurdering, konklusion og anbefaling 3](#_Toc131067674)

[5. Analyse 3](#_Toc131067675)

[6. Økonomisk, regulatorisk og teknisk overvejelse 4](#_Toc131067676)

[7. AU’s risikobillede ved ibrugtagning samt vurdering og beregning af risici score og afbødende tiltag 6](#_Toc131067677)

[8. Samlet risikobillede: 12](#_Toc131067678)

[9. Underskrift og kvittering 12](#_Toc131067679)

## Basale oplysninger:

|  |  |
| --- | --- |
| System-/projekt navn: |  |
| Dato for risikovurdering: |  |
| Deltagere: |  |
| System- / dataklassifi-kation: | *A, B eller C* |
| Type:  fysisk / digitalt / blandet |  |
| Systemejer: | *Navn* |
| Drifts-/systemansvarlig: | *AU-IT/Egen drift/outsourcet/blandet* |
| Projektleder: | *Navn* |
| Brugere: | *Hvem er brugergruppen?* |
| Dataejer: | *Hvilken navngiven person med tilhørende funktion beslutter hvem der må tilgå data?* |
| Skriftlige procedurer: | *Er der brug for dette for at sikre og styre korrekt og lovlig brug af systemet og dets aktiver?* |

## Indledning

I forbindelse med og før idriftsættelse af et nyudviklet eller nyindkøbt system, skal der gennemføres en risikovurdering af projektets eller systemets informationssikkerhedsmæssige konsekvenser. Det er vigtigt, at have en risikobaseret tilgang i forbindelse med vurdering af systemer og projekter, både nye der skal idriftsættes, men også eksisterende systemer i drift.

Risikovurderingen skal gennemføres for at sikre at ledelsen er bekendt med de risici projektets gennemførelse og den efterfølgende brug af systemet medfører. Det er muligt at godkende løsningen med forbehold, det vil sige, at der kan være dele af systemet/løsningen, som ikke må tages i brug.

Hvis et system af en eller anden årsag er idriftsat uden risikovurdering, skal den gennemføres hurtigst muligt efter for at kunne justere og korrigere for evt. risici.

I dokumentet er anført med *rød kursivskrift* de steder, hvor der skal udfyldes med informationer, som skal ligge til grund for risikovurderingen.

Husk at holde fokus på, med en risikobaseret tilgang, at identificere de risici, som er størst og som kan skabe de største problemer for forretningen AU, hvis noget går galt og dermed har store konsekvenser forsknings- og uddannelsesmæssigt eller menneskeligt, det er disse risici, der skal vurderes mht. konsekvens og sandsynlighed.

## System-/ projektbeskrivelse

*Kort beskrivelse af hvad systemet/produktet bruges til på AU – hvad er formålet med brug af systemet/projektet.*

## Overordnet vurdering, konklusion og anbefaling

*Her skriver projektet den overordnede vurdering, konklusion og anbefaling kort så den relevante forretningsledelse kan se det først inden de gennemgår analysen og kvitterer skriftligt for accept af den foreliggende informations-risikovurdering.*

## Analyse

*Analysen er delt op i nogle områder, hvor der skal tages stilling til:*

* *Om der arbejdes med personoplysninger*
* *Accepteret nedetid*
* *Økonomiske overvejelser*
* *Regulatoriske overvejelser*
* *Tekniske overvejelser*

*Se detaljeret vejledning i underafsnittene.*

**Information om personoplysninger i systemet/projektet:**

1. Behandles der personoplysninger? (Ja/Nej)
2. Kan og vil vi undgå personoplysninger? (Ja/Nej)
3. Behandler hele systemet personoplysninger? (Ja/Nej)
4. Kan der afgrænses delsystemer som behandler personoplysninger? (Ja/Nej)
5. Er personoplysningerne anonymiseret/pseudonymiseret i en del af systemet? (Ja/Nej)

Hvis der indsamles og opbevares data samt personoplysninger, skal udfylder være opmærksom på evt. udarbejdelse af konsekvensanalyse for den registreredes rettigheder, når risikovurderingen er udarbejdet.

Se Databeskyttelsesenhedens hjemmeside: [Risikovurdering og konsekvensanalyse (au.dk)](https://medarbejdere.au.dk/informationssikkerhed/databeskyttelse/saerligt-om-forskning/risikovurdering-og-konsekvensanalyse/)

1. Beskriv overordnet, hvilke data der indsamles:

|  |
| --- |
| *Udfyldes* |

2. Beskriv overordnet, hvorfor de indsamles (formål):

|  |
| --- |
| *Udfyldes* |

3. Beskriv overordnet, hvem der kan få adgang til dem:

|  |
| --- |
| *Udfyldes* |

4. Beskriv overordnet, hvorfor det giver værdi for AU at indsamle personoplysninger:

|  |
| --- |
| *Udfyldes* |

**Hvilken type af data/personoplysninger arbejdes der med i systemet/projektet:**

Beskrives og vurderes kort ud fra AU dataklassifikations model med 4 kategorier, se evt.  [Klassifikation af data (au.dk)](https://medarbejdere.au.dk/informationssikkerhed/klassifikation-af-data)

|  |  |  |
| --- | --- | --- |
| Nr. | Kort data beskrivelse | Klassifikations kategorier: (Offentlig, Intern, Fortrolig, Følsom) |
| *x* | *Udfyldes* | *Udfyldes* |
|  |  |  |
|  |  |  |

**Hvor længe kan systemet/projektet accepteres at være nede uden tilgængelighed.**

Valgt vurdering udfyldes i skemaet herunder.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nede < 4 timer**  Manglende tilgængelighed vil være tidskritisk næsten med det samme. | **Nede 4-8 timer**  Manglende tilgængelighed må helst ikke vare mere end en enkelt arbejdsdag. | **Nede 2 dage**  Et par dages utilgængelighed er det maksimalt tilladelige. | **Nede < 1 uge**  Manglende tilgængelighed må vare mere end et par dage men helst ikke en hel arbejdsuge. | **Nede > 1 uge**  Manglende tilgængelighed må vare mere end en uge. |
| *X* | *X* | *X* | *X* | *X* |
| **Begrundelse/kommentar for valgt nedetids vurdering:**  *Udfyldes* | | | | |

Valget for accepteret nedetid har betydning for hvilket beredskab (teknisk og forretnings-mæssigt[[1]](#footnote-1)), der skal være for systemet/projektet samt hvilken risiko, man accepterer i forbindelse med nedetid.

## Økonomisk, regulatorisk og teknisk overvejelse

**Økonomisk**

* *Koster det AU noget at anskaffe, drive i licenser/bemanding/andet?*
* *Er der økonomiske gevinster?*

**Regulatorisk**

Det regulatoriske område deler sig i tre områder:

1. Lovgivningen
2. Det organisatoriske ansvar for brugen
3. Øvrige juridiske bindinger

Ad a Lovgivningen.

* *Hvilken lovgivning og regler gælder for de data og det system man ønsker at benytte? Her tænkes ofte på Persondataloven med tilhørende Sikkerhedsbekendtgørelse. Men øvrige regler og aftaler såsom EU lovgivning. Her skal også tænkes over at data, der bevæger sig over internettet, juridisk bevæger sig over landegrænser, hvis ikke datatransporten og lagringen er stramt styret.*

*For eksempel henvisning til Persondataloven og EU’s GDPR.*

Ad b Det organisatoriske ansvar for brugeren.

* *De data/informationer der behandles kan enten enkeltvis eller samlet skulle beskyttes og give anledning til at man skal beskrive vejledninger eller lægge tekniske begrænsninger ind og sikre at brugerne ved hvad der er korrekt brug og hvad der ikke er. Muligheden for vedhæftninger, fleksfelter og muligheden for at sende sager direkte fra systemerne bør overvejes for at prøve at gennemtænke om det kan give sikkerhedsbrister.*

*For eksempel: Primære brugere vil være … der skal …. Ikke-nødvendig brugeradgang til personoplysninger skal undgås. Der bør udarbejdes relevante instruktioner for administration og forvaltning af løsningen.*

*For eksempel: Øvrige brugere omfatter …, der skal …. For disse gælder tilsvarende, at ikke-nødvendig brugeradgang til personoplysninger skal undgås. Der bør udarbejdes relevante instruktioner for tilsyn og kontrol med brugeradgange og -rettigheder.*

Ad c Øvrige juridiske bindinger.

* *Ikke kun lovgivning kan påføre bindinger på datas/informationers brug og håndtering. Aftaler indgået med samarbejdspartnere såsom Databehandleraftaler og andre rettigheder kan også bestemme de regulatoriske* *rammer. Nogle gange pålægger disse aftaler krav som er strammere end lovgivningen foreskriver.*

**Teknisk**

* *Her beskrives løsningens tekniske sikkerhedsmæssige elementer overordnet mht. til sikring af adgange til informationerne, sikkerhed omkring opbevaring, sikkerhed ved transport af data, kendte begrænsninger o.a.*

1. Opbevaring af data (lokation, teknologi, kryptering):
2. Backup af data (lokation, frekvens, opbevaring):
3. Kommunikation af data (netværk, teknologi, kryptering):

## AU’s risikobillede ved ibrugtagning samt vurdering og beregning af risici score og afbødende tiltag

I tabellen nederst i dette afsnit listes de risici der identificeres og begrundelser for vurdering samt beregning af risiko score og beskrive hvilke afbødende tiltag der planlægges eller allerede eksisterer. Her fokuseres alene på de risici som AU pådrager ved at benytte informationer og behandle dem i forbindelse med at tage systemet i brug. Det er de risici, som er størst, der vurderes mht. konsekvens og sandsynlighed.

Risiciene skal navngives ud fra om de er vurderet ud fra:

* + Fortrolighed (F). Kun personer med et legitimt behov må have adgang til informationer.
  + Integritet (I). Informationer skal være konsistente og i en form, som man kan stole på.
  + Tilgængelighed (T): Informationer skal være tilgængelige for de rette personer, når der er behov for det.

Der skal kunne tegnes et risikobillede som forretningen i form af Styregruppen/systemejer kan tage stilling til. Risici fra Risikotabellen indsættes i matrix under punkt 8 med angivelse af Fx, Ix eller Tx nummer.

Konsekvens (K) og sandsynlighed (S) vægtes fra 1- 4 for F, I, T - hvor 4 er det mest kritiske. Der skal vurderes og vægtes hvad sandsynligheden er for at en risiko indtræffer og hvad er konsekvensen hvis det sker.

Systemejer fastlægger konsekvenserne ved disse risici, evt. i dialog med en fra ledelsen, og vurderer hvad dette vil betyde for virksomheden. Konsekvenserne angives i niveauer på følgende skala:

1 – Ubetydelig - uvæsentligt  
2 – Mindre alvorlig - generende  
3 – Meget alvorlig - kritisk  
4 – Graverende og ødelæggende – uacceptabelt

Et eksempel på en konsekvensvurdering er, at afsløring af informationer om vigtige forskningsresultater eller af sådanne informationer om et større antal forskningsprojekter, kan påvirke omsætning/omdømme negativt (Høj konsekvens).

Systemejer vurderer, i en dialog med evt. andre it- og forretningskyndige, sandsynligheden for, at den pågældende risiko erfaringsmæssigt optræder som en faktisk sikkerhedshændelse. Sandsynlighederne fastlægges også i niveauer på følgende skala:

1 – Usandsynligt   
2 – Mindre sandsynligt  
3 – Sandsynligt

4 – Forventet

Når man vurderer sandsynlighederne, skal man tage højde for de administrative og tekniske sikkerhedstiltag, der allerede er implementeret, og som kan medvirke til at reducere de erfaringsbaserede sandsynligheder. Uddanner man f.eks. medarbejderne i korrekt brug af systemer og værktøjer, samt i generel sikkerhed, kan dette reducere sandsynligheden for at information om forskningsprojekter afsløres. Det samme gælder, hvis man har begrænset adgangen til medarbejdere med et forretningsmæssigt behov.

**OBS!**Det er vigtigt, at man beskriver og noterer de relevante risici og begrundelsen for både konsekvensen og sandsynligheden i felterne ”Hvorfor vurderes konsekvens/sandsynlighed til dette?” i risikovurderingsarket. Dels så risikovurderingen kan foreligges for ledelsen og dels så man senere kan følge op på, om der er ændringer i risikobilledet (trusler, sårbarheder, konsekvenser og/eller nye emner, der skal vurderes).

**Tabel med sandsynlighedsskala og beskrivelser:[[2]](#footnote-2)**

|  |  |  |
| --- | --- | --- |
| **Værdi** | **Sandsynlighed** | **Eksempel beskrivelse** |
| 1 | **Usandsynligt** | Det anses for næsten udelukket, at hændelsen nogensinde kan forekomme   * Ingen erfaring med hændelsen * Kendes kun fra få andre offentlige og private virksomheder, men ikke i Danmark |
| 2 | **Mindre sandsynligt** | Hændelsen forventes ikke at forekomme   * Ingen erfaring med hændelsen * Kendes kun fra få andre offentlige og private virksomheder, men ikke i Danmark |
| 3 | **Sandsynligt** | Det er sandsynligt at hændelsen vil forekomme   * Man har erfaring med hændelsen, men ikke inden for de sidste 12 måneder * Kendes fra andre offentlige og private virksomheder i Danmark (omtales årligt i pressen) |
| 4 | **Forventet** | Det ventes at hændelsen vil forekomme   * Man har erfaring med hændelsen inden for de sidste 12 måneder * Hænder jævnligt i andre offentlige og private virksomheder (omtales ofte i pressen) |

**Tabel med konsekvensskala og eksempler på konsekvenstyper:[[3]](#footnote-3)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Værdi** | **1** | **2** | **3** | **4** |
| **Konsekvens-type og konsekvens-beskrivelse** | **Ubetydelig (uvæsentlig)** | **Mindre alvorlig (generende)** | **Meget alvorlig (kritisk)** | **Graverende/ ødelæggende (uacceptabelt)** |
| **Strategisk:**  Medfører indskrænkninger i evnen til at handle i en periode | Ingen særlig påvirkning | Planlagte aktiviteter kan gennem- føres med mindre justeringer | Medfører revurde-ring af vigtige aktiviteter på kort sigt | Bliver ude af stand til at gennemføre vigtige aktiviteter, som er planlagt i en periode fremover |
| **Økonomisk:**  Medfører meromkostnin- ger eller tab | Ingen særlig påvirkning | Meromkostninger og tab i begrænset niveau, som kan kræve mindre budget-ændringer | Store økonomiske tab med risiko for at blive sat under admini-stration | Væsentlige økonomiske tab. Bliver sat un- der admini-stration |
| **Administrativ/procesmæssig:**  Medfører administrative belastninger | Håndteres uden særligt ressourcetræk i de admini- strative funktioner | Håndteres inden for rimeligt ekstra administra-tivt res- sourcetræk | Der må trækkes væsent-ligt på eksiste-rende og nye  admini-strative ressour-cer | Administrative ressourcer må udvides urealistisk |
| **Omdømme:**  Påvirker omdømme i u-ønsket retning | Ingen særlig påvirkning | Forbigåen-de op- mærksom-hed fra enkelte grupper | Offentlig-heden fatter generel negativ interesse, som kan medføre begrænset tab af forskere og stude-rende | Væsentlig skade på omdømme. Ansvarlig leder må gå af |
| **Politisk/stra-tegisk:**  Medfører indskrænknin-ger i evnen til at handle i en periode | Ingen særlig påvirkning | Planlagte aktiviteter kan gennem- føres med mindre justeringer | Medfører revurde-ring af vigtige aktiviteter på kort sigt | Ledelsen må gå af. Bliver ude af stand til at gennemføre vigtige aktiviteter, som er planlagt i en periode fremover |
| **Forhold til interessenter:** Påvirker forholdet til interessenter | Ingen særlig påvirkning | Forringet samarbejde med inte- ressenter i enkeltsager | Generelt forringet sam- arbejde med interes- senter | Væsentligt nedbrud i det generelle samar- bejde med interessenter |
| **Menneskelige:**  Medfører konsekvenser for det enkelte individ | Ingen særlig påvirkning | Den enkelte udsættes for gener, men ikke noget alvorligt | Alvorlig person-skade fysisk eller mentalt | Menneskeliv, førlighed eller helbred står på  spil |
| **Privacy.**  Medfører brud på privatlivets fred | Ingen særlig påvirkning | Der er formelle mangler i de op- lysninger, der gives den enkelte, men ikke i graverende grad | Den enkelte fratages råderet-ten over egne data. Ikke-følsomme data videregi-ves uret- mæssigt | Den enkelte udsættes for uacceptable krænkelser af privatlivet.  Der træffes bebyrdende afgørelser mod den enkelte på et forkert grundlag. Følsomme data videregives uret- mæssigt |
| **Brud på lovgivningen** Medfører brud på lovgivning, f.eks. forvaltningslov og straffelov | Ingen særlig påvirkning | Manglende over- holdelse af admini-strative procedurer og regler, som ikke er af kritisk karakter | Lovbrud, der er kritiske og kan stille AU i miskredit | Kritisk lovgivning, f.eks. straffeloven bry- des. Ansvarlig leder må gå af |

**Obs!** Risikotabellen herunder skal udfyldes med afbødende tiltag. Konsekvens og sandsynlighed er under forudsætning af, at de afbødende tiltag iværksættes.

**Risikotabel:**

I nedenstående tabel er indsat eksempler på risici (markeret med rødt) indenfor alle 3 områder Fortrolighed, Integritet og Tilgængelighed. Her skal selvfølgelig indsættes risici, som I finder relevante i relation til det system eller projekt risikovurderingen vedrører. Men måske er nogle af eksemplerne relevante.

| **Fortrolighed** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr**  Fx | **Risiko** | **Beskrivelse:** | **Afbødende tiltag:**  **(hvad tænkes iværksat af sikkerheds foranstaltninger)** | **Hvorfor vurderes konsekvens/sandsynlighed til de angivne værdier?** | **Konse-kvens**  **K** | **Sandsyn-lighed**  **S** | **Risiko**  **(K\*S)** |
| F1 | *IT indbrud (hackere mm)* | *Udfyldes* | *Udfyldes* | *Udfyldes* | *K* | *S* | *K\*S* |
| F2 | *Manglende træning* |  |  |  |  |  |  |
| F3 | *Anvendelsesfejl* |  |  |  |  |  |  |
| F4 | *Systemfejl* |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

| **Integritet** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr**  Ix | **Risiko** | **Beskrivelse:** | **Afbødende tiltag:**  **(hvad tænkes iværksat af sikkerheds foranstaltninger)** | **Hvorfor vurderes konsekvens/sandsynlighed til de angivne værdier?** | **Konse-kvens**  **K** | **Sandsyn-lighed**  **S** | **Risiko**  **(K\*S)** |
| I1 | *Fejl i integration til* | *Udfyldes* | *Udfyldes* | *Udfyldes* | *K* | *S* | *K\*S* |
| I2 | *Fejl i integration til* |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

| **Tilgængelighed** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr**  Tx | **Risiko** | **Beskrivelse:** | **Afbødende tiltag:**  **(hvad tænkes iværksat af sikkerheds foranstaltninger)** | **Hvorfor vurderes konsekvens/sandsynlighed til de angivne værdier?** | **Konse-**  **Kvens**  **K** | **Sandsyn-**  **Lighed**  **S** | **Risiko**  **(K\*S)** |
| T1 | *Nedetid på grund af systemfejl* | *Udfyldes* | *Udfyldes* | *Udfyldes* | *K* | *S* | *K\*S* |
| T2 | *Nedetid på grund af brand, vandskade mm* |  |  |  |  |  |  |
| T3 | *Nedetid på grund af hw-fejl* |  |  |  |  |  |  |
| T4 | *Manglende opgradering af* |  |  |  |  |  |  |
| T4 | *Anvendelsesfejl* |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

## Samlet risikobillede:

I nedenstående matrix indsættes risici, fra Risikotabellen i punkt 7, med angivelse af de identificerede risici udtrykt ved Fx, Ix eller Tx nummer.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Konsekvens | Kritisk  4 |  |  |  |  |
| Alvorligt  3 |  |  |  |  |
| Nogen betydning  2 |  |  |  |  |
| Uden betydning  1 |  |  |  |  |
|  | Usandsynligt  1 | Lidt sandsynligt  2 | Meget sandsynligt  3 | Vil komme  4 |
| S a n d s y n l i g h e d | | | |

**Rød:** Skal der tages stilling til og reageres på straks.

**Gul:** Skal vurderes og overvejes.

**Grøn:** Umiddelbart ingen behov for reaktion.

## Underskrift og kvittering

Resultatet af dette risikovurderingsnotat med anførte risici er accepteret samt taget til efterretning og vil blive vurderet for igangsætning af evt. tiltag for at minimere risici

ved drift af systemet/projektet.

Den: xx / xx / xxxx

Underskrift: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Systemejer eller ledelsesansvarlige for systemet/projektet.

1. <https://medarbejdere.au.dk/informationssikkerhed/forretningsberedskab> [↑](#footnote-ref-1)
2. Indhold inspireret fra Digitaliseringsstyrelsen: Vejledning i it-risikostyring og - vurdering [↑](#footnote-ref-2)
3. Indhold inspireret fra Digitaliseringsstyrelsen: Vejledning i it-risikostyring og -vurdering [↑](#footnote-ref-3)