AARHUS UNIVERSITET

Vejledning til udfyldelse af:

Risikovurderingsnotat

”Risikovurdering er et bærende element i styring af informationssikkerheden.

Det er risikovurderingen, der afdækker hvor høj grad af sikkerhed, der er nødvendig, så det kan sikres at designet af beskyttelsesforanstaltningerne (teknik, procedurer og kultur) passer til behovet.

Dermed kan man undgå at overbeskytte, men koncentrere ressourcerne på at beskytte de informationer, der har behov for det.”

Indholdsfortegnelse:

1. Indledning
2. System-/projektbeskrivelse
3. Overordnet vurdering, konklusion og anbefaling
4. Metode
5. Analyse
6. AU's risikobillede ved ibrugtagning samt vurdering og beregning af risici og afbødende tiltag
7. Samlet risikobillede
8. Underskrift og kvittering
9. Bilag og inspiration

Basale oplysninger:

Start med at udfylde skemaet med basale oplysninger om System- eller projektnavn, Dato, Deltagere, Dataklassifikation osv.

1. Indledning

Beskriv kort hvad formålet er med denne risikovurdering og hvilket system eller projekt det vedrører.

2. System-/ projektbeskrivelse

Beskriv kort hvad systemet/produktet skal bruges til på AU.

3. Overordnet vurdering, konklusion og indstilling

Udfyldes når risikovurderingen er udført og er et ledelsesresumé, som kort fortæller hvad risikovurderingen er endt op med i forhold til indstillinger, observationer og anbefalinger, som systemejer eller ledelse skal forholde sig til.

4. Metode

Risikovurderingen skal gennemføres for at sikre, at ledelsen er bekendt med de risici projektet eller brug af systemet kan medføre for AU.

Der skal overordnet vurderes brugen af personfølsomme og personhenførbare informationer og det gælder for nye såvel som eksisterende systemer.

Herefter foretages en bredere vurdering i forhold til økonomi, lovgivning og teknik, afhængig af hvilke informationer og data der ligger i eller bliver behandlet i systemet. Ikke alle 3 områder behøves nødvendigvis at blive vurderet eller gennemgået, hvis ikke der er belæg for det, men det skal man forholde sig til.

Resultatet er en sikkerhedsvurdering i forhold til 3 dimensioner (Fortrolighed, Integritet og Tilgængelighed). Dette kan direkte bruges til at kortlægge hvilke sikkerhedskrav, der skal efterleves.

Der dokumenteres herefter hvilke krav, der ikke efterleves, og gives forslag til hvilke tiltag, der kan gøres for at sikre bedre efterlevelse. Dette gøres af den ansvarlige systemejer, der vil anvende data på en ny måde eller i en ny løsning.

5. Analyse

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

- om der arbejdes med personfølsomme oplysninger,
- noget om accepteret nedetid,
- økonomiske, regulatoriske og tekniske overvejelser

- samt risikobillede, herunder beskrive begrundelse for vurdering og beregning af risiko samt beskrive afbødende tiltag.

Personfølsomme oplysninger:

Det er vigtigt at finde ud af, hvilke data og datatyper der arbejdes med i projektet eller systemet/delsystemer. Derfor er det vigtigt at få registreret, hvis der arbejdes med data og personoplysninger, som er følsomme:

Hvad er en personoplysning?

En personoplysning er enhver form for information om en identificeret eller identificerbar fysisk person.

Hvad er en behandling af personoplysninger?

En behandling af personoplysninger er enhver operation, som personoplysningerne gøres til genstand for - f.eks. indsamling, læsning, redigering, beregning, sammenstilling, videregivelse, opbevaring og sletning.

Vil der være behov for at en konsekvensanalyse skal gennemføres?

Se evt. link til Databeskyttelsesenhedens hjemmeside: Risikovurdering og konsekvensanalyse (au.dk)

En konsekvensanalyse skal gennemføres (lovpligtig iflg. GDPR) efter behov f.eks. ved etablering eller ved væsentlige ændringer af teknologier, som digitalt behandler personfølsomme oplysninger, eller som på anden måde har konsekvenser for data håndtering og privacy.

Det er ledelsens ansvar, at der bliver udarbejdet en konsekvensanalyse, hvis der er behov for det.

Derfor er det vigtig, at nedenstående spørgsmål bliver besvaret og beskrevet, således at det fremgår af risikovurderingsnotatet for nærmere analyse og udarbejdelse af konsekvensanalyse, hvis det bliver besluttet og fundet nødvendigt:

- Behandles der personoplysninger? (Ja/Nej)
- Kan og vil vi undgå personoplysninger? (Ja/Nej)
- Behandler hele systemet personoplysninger? (Ja/Nej)
- Kan der afgrænses delsystemer som behandler personoplysninger? (Ja/Nej)
- Er personoplysningerne anonymiseret i en del af systemet? (Ja/Nej)

- Beskriv overordnet, hvilke data der indsamles:
- Beskriv overordnet, hvorfor de indsamles (formål):
- Beskriv overordnet, hvem der kan få adgang til dem:
- Beskriv overordnet, hvorfor det giver værdi for virksomheden at indsamle personoplysninger:

6. AU's risikobillede ved ibrugtagning samt vurdering og beregning af risici og afbødende tiltag

Det skal herefter vurderes hvilke risici, der kan være forbundet med drift af system/produkt/ projekt.

Brainstorm over hvad der kan gå galt og hvis det går galt, hvad er så konsekvensen, hvis det sker og hvad er sandsynligheden for at det sker. (Konsekvens*Sandsynlighed = Risiko)

Skriv de fundne risikohændelser op inden for alle 3 kategorier Fortrolighed, Integritet og Tilgængelighed. Risikohændelserne for Fortrolighed benævnes med F1, F2 osv., Integritet med I1, I2 osv. samt Tilgængelighed T1, T2 osv.

For at bevare tilliden til Aarhus Universitet skal kritiske informationer beskyttes med foranstaltninger, der sikrer den nødvendige informationssikkerhed. Vi arbejder ud fra tre grundsten:

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

Eksempler på hvad der fx kan/skal overvejes mht. fortrolighed, integritet og tilgængelighed:

Fortrolighed:

- Overvej fx om der er medarbejdere der kan få adgang til data som de ikke skal kunne se.
- Hvilke adgangsrettigheder har forskellige roller og er de rigtig defineret eller sat op i systemet.
- Vurder nøje om der er risiko for datas placering, som iflg. GDPR skal være placeret indenfor EU og ikke i et usikkert tredjeland som fx USA, som kræver specielle juridiske afatler grundet Schrems 2.

Integritet:

- Overvej om der er risiko for at der kan ændres i data, som man kan tilgå, men som man ikke må eller
  har lov til.
- Kan der være risiko for at integrationer mellem systemer fejler i forbindelse med en ændring i et system (change) og derved placerer data forskelligt fra hvad de skulle.
- Overvej nøje om de data der behandles iog arbejdes med systemet har den rigtige klassifikation, dvs. er det personfølsomme data der faktisk arbejdes med, men medarbejdere og systemet behandler data som
  om at det er fortrolige – der er væsentlig forskel. (Klassifikation af data (au.dk))

Tilgængelighed:

- Hvad sker der, hvis de servere hvorpå data ligger ikke er tilgængelige og er der risiko for at det kan ske.
- Er der risiko for at nogle dele af et system ikke kan levere data til tiden til andre systemer, hvis noget går galt mht. server eller netværksproblemer.
- Hvis ikke et system kan betjenes af brugerne, er der så leverancer som forsinkes fx en lønkørsel.

Angiv svarene vurderet fra 1-4 og udregn Risiko for hver risikohændelse.

Begrundelse for vurdering og beregning af risiko.

Noter hvorfor risikohændelserne er placeret som de er i matrixen, dvs. hvad var jeres begrundelse for vurderingen fra 1-4 af konsekvens og sandsynlighed.

Afbødende tiltag.
Noter hvilke afbødende tiltag som allerede er identificeret eller tænkt på, for at afbøde de risici, der er fundet inden for Fortrolighed, Integritet og Tilgængelighed. Dvs. at man beskriver de tiltag, der kan udføres for at opnå efterlevelse (compliance).

I matrixen vises med farvekoden hvilke risici, der skal tages aktiv stilling til. Nødvendige kompenserende tiltag implementeres og rest-risiko skal accepteres af systemejer eller ledelsen (rektor, prorektor, universitetsdirektør, dekan, vicedirektør, fakultetsdirektør eller institutleder) afhængig af løsningens organisatoriske dækningsgrad.

Tiltagene kan både være fysiske, tekniske og organisatoriske.

7. Samlet risikobillede (matrix).

Herefter noteres risikohændelserne i matrixen med Fx, Ix og Tx numrene og som til slut angiver eller viser det samlede risikobillede.

8. Underskrift og kvittering

Når risikovurderingsnotatet er gennemgået med den systemejer eller ledelsesansvarlige skal det underskrives, således at der er dokumentation for, at risici er bekendtgjort og at det nu er op til ledelsen af vurdere hvilke tiltag der skal iværksættes og hvilke risici der accepteres som resterende og leve med – dvs. at ledelsens eller systemejers risikoappetit bliver synliggjort.

OBS! Dokumentation og indsendelse af Risikovurderingsnotat

Når den samlede risikovurdering er færdig skal den indrapporteres til AU IT Informationssikkerhed.

Sendes til: Informationssikkerhed@au.dk

9. Bilag og inspiration:

Bilag 1: Trusselskatalog

Kriterie	1 Ubetydeligt (Uvæsentligt)	2 Mindre alvorlig (Generende)	3 Meget alvorlig (Kritisk)	4 Graverende /ødelæggende (Meget kritisk)
Menneskelige fejl:				
Ondsinde mennesker				
Hackere				
Spionage				
IT kriminelle				
Terrorister				
Kompromittering af funktioner				
Brugerfejl				
Manglende træning				
Personafhængighed				
Tab af kritiske services:				
Forsyningssvigt ved el og telekommunikation				
Nedbrud på køling				
Naturkatastrofer:				
Klimatisk fænomener				
Oversvømmelse				
Fysisk skade:				
Brand				
Vansskade				
Forurening				
Ødelæggelse af udstyr				
Større ulykke				
Tekniske fejl:				
Hardwarefejl - servere				
Netværksfejl				
Firewall fejl				
Overbelastning				
Softwarefejl				
Manglende vedligeholdelse				
Leverandør fejl - cloud				

Administrative tiltag

Forebyggende tiltag
Kan for eksempel være: sikkerhedspolitik, logning, compliance checks, medarbejder-awareness, systemdokumentation eller ændringsstyring.

Udbedrende tiltag
Kan for eksempel være: beredskabsstrategier, it-beredskabsplaner, disaster recovery-procedurer eller systemdokumentation.

Du skal vurdere de administrative tiltag ved at tage udgangspunkt i din virksomheds procesmodenhed og angive på en skala, hvilket modenhedsniveau sikkerhedsprocesserne befinder sig på ud fra nedenstående definition.

Modenhed af administrative tiltag

Optimerede	Der foretages løbende tilpasninger af definerede administrative tiltag mod truslen eller dens konsekvenser og deres implementering gennem rettidig opfølgning på metrikker og etablering af handlingsplaner.
Styrede	Der foretages målinger af definerede administrative tiltag mod truslen eller dens konsekvenser gennem løbende vurderinger af risiko, efterlevelse og sikkerhedsbevidsthed. Der anvendes desuden metrikker, der anskueliggør sikkerhedsniveauet
Beskrevne	Administrative tiltag mod truslen eller dens konsekvenser er baseret på en formel ansvarsdelegering og konsistent dokumenteret gennem formelle politikker, regler, planer og procedurer.
Uformelle	Administrative tiltag mod truslen eller dens konsekvenser er baseret på en uformel, men fastlagt ansvarsdelegering og en erfaringsbaseret, indarbejdet praksis.
Ad hoc	Administrative tiltag mod truslen eller dens konsekvenser er ikke systematiseret.

Tekniske og fysiske tiltag

Forebyggende tiltag
Kan for eksempel være: firewall, antivirus, alarmsystemer, RAID, redundans, adgangs kontrolsystemer eller server-clusters.

Udbedrende tiltag
Kan for eksempel være: standby-udstyr, serversnapshots, virtualisering, backup, brandslukning eller standby- driftscentre.

Der skal vurderes de forebyggende tekniske- eller fysiske foranstaltninger ved at tage udgangspunkt i den implementering, der er foretaget for at minimere forekomsten af trusselshændelserne og angive implementeringsgraden og effektiviteten af foranstaltningerne på en skala ud fra nedenstående definition.

Modenhed af tekniske og fysiske tiltag

Meget effektive	Der er foretaget systematiske tekniske / fysiske implementeringer i flere lag (i tilfælde af svigt af primære sikringsforanstaltninger) for at beskytte mod truslen eller dens konsekvenser, og tiltagene er baseret på anerkendt best practice og professionelt vurderet eller testet særdeles effektive.
Effektive	Der er foretaget systematiske tekniske / fysiske implementeringer for at beskytte mod truslen eller dens konsekvenser, og tiltagene er baseret på anerkendt best practice og professionelt vurderet eller testet effektive.
Implementerede	Der er foretaget systematiske tekniske / fysiske implementeringer for at beskytte mod truslen eller dens konsekvenser
Delvist implementerede	Der er foretaget sporadiske tekniske / fysiske implementeringer for at beskytte mod truslen eller dens konsekvenser.
Ikke eksisterende	Der er ikke foretaget tekniske / fysiske implementeringer for at beskytte mod truslen eller dens konsekvenser.