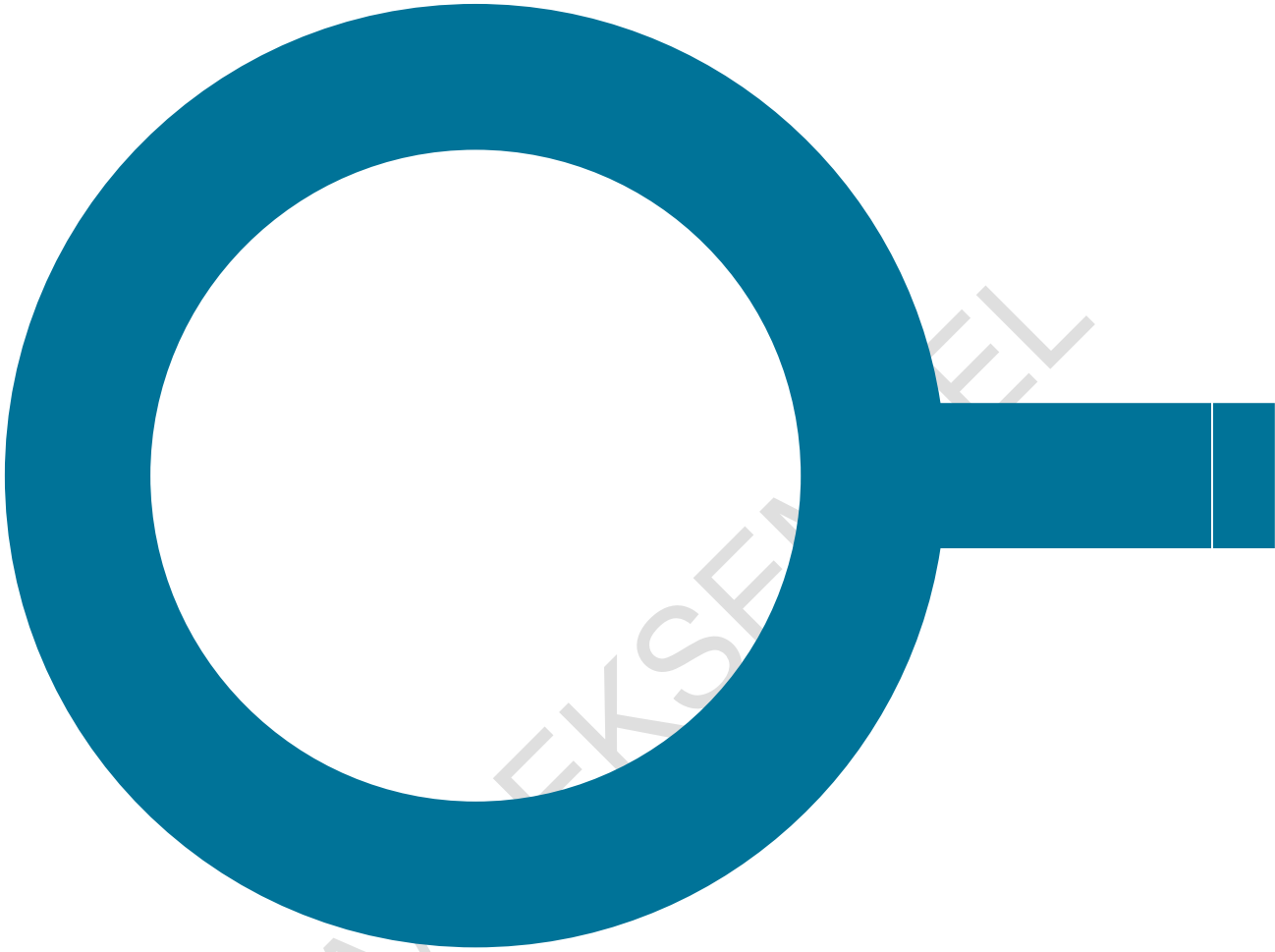


INFORMATIONSSIKKERHED – COMPLIANCE (GDPR & IT-SIKKERHED)

VEJLEDNING RISIKOVURDERING

Version 2.1

19. marts 2019

KOMBIT

Kommunernes it-fællesskab

Versions historik

Versions-nummer	Dato	Afsnit der er ændret
1.0	11.12.2017	Gældende version.
1.1	20.12.2018	Fjernet personoplysinger i afsnit 0 Stamdata.
2.0	01.03.2019	Gennemskrivning af vejledning. Gældende version.
2.1	19.03.2019	Ændringer i afsnit 2 Sandsynlighedsvurdering

Ansvarlig i KOMBIT

Indsatsområde	Indsatsansvarlig	Forretningejer (FE)
Indsatsområde nr. 3		

BEMÆRK!

Denne vejledning er udarbejdet med KOMBIT A/S for øje. Den kan derfor IKKE adopteres i sin nuværende form. Vejledningen er derfor ALENE tænkt som en inspiration til, hvordan GDPR-arbejdet kan brydes ned i mindre og mere forretningsnære størrelser.

KOMBIT A/S fraskriver sig derfor også ethvert ansvar, såfremt andre aktører anvender KOMBITs vejledninger/værktøjer i sin helhed eller brudstykker heraf i deres arbejde med EU's databeskyttelsesforordning.

A.INDLEDNING

Denne vejledning er én ud af en række vejledninger, som hører under indsatsområde 3 (compliance, styring og kontrol) i KOMBITs informationssikkerhedsstrategi.

Vejledningen handler om udarbejdelse af sikkerhedsmæssige it-risikovurderinger i KOMBIT – dels gennem vejledning[1] og dels gennem et fælles værktøj (Excel-ark).

KOMBITs fremgangsmåde til risikovurdering følger principperne fra ISO 27.001 og 27.005 og dermed også det samme grundlag som KL anvender i deres drejebog fra september 2017 om "Informationssikkerhedsaktiviteter – Kommunalt arbejde med øget informationssikkerhed". Drejebogen omhandler bl.a. en fremgangsmåde til risikovurdering i kommunerne og her vil KOMBITs risikovurdering for fælleskommunale it-løsninger kunne udgøre et input til kommunernes arbejde med risikovurdering af deres it-løsninger.

En traditionel risikovurdering gennemføres ud fra den dataansvarliges eller systemansvarliges synspunkt (typisk kommuner og KOMBIT[2]) og behandler risici for disse parter. I denne vejledning og værktøjet suppleres dette med en vurdering af risici fra registreredes/datasubjekternes (fx borger, medarbejder) synspunkt, således at der etableres fokus på registreredes (fx borgernes) privatliv ved behandling af personoplysninger i fælleskommunale it-løsninger og registreredes (fx medarbejderes) privatliv ved behandling af personoplysninger i KOMBITs egne it-løsninger. Dermed opnås en hybrid af en klassisk it-risikovurdering med det forretningsmæssige perspektiv og en risikovurdering set fra den registreredes perspektiv. Projekterne får dermed samlet de to vurderinger og undgår dermed at skulle gennemføre to separate men nært beslægtede vurderinger. Risikovurderingen af de registreredes risici er særligt relevant i forbindelse med at opnå GDPR-compliance, da vurderingen både skal bruges som en foranalyse til at fastslå om KOMBIT er pålagt at udarbejde en konsekvensanalyse (DPIA), og til at sikre, at der er implementeret tilstrækkelig sikkerhed i it-løsningen og processerne ved behandlingen af personoplysninger.

I tillæg til denne vejledning er der udarbejdet vejledninger om:

1. Dokumentation for datatyper og datastrømme
2. Dokumentation for registreredes rettigheder
3. Dokumentation for risikohåndtering

[1] Vejledningen er delvist baseret på på Digitaliseringsstyrelsens "Vejledning i it-risikostyring og vurdering" (2015).
[2] KOMBIT er normalt kun dataansvarlig for interne systemer.

B.FORMÅL MED RISIKOVURDERING

Risikovurderingen indgår som en ud af flere opgaver i det samlede GDPR compliance arbejde i KOMBIT, som alle projekter, specialer og supportfunktioner, der behandler personoplysninger, har ansvaret for at håndtere.

Formålet med risikovurderingen er at identificere, analysere og vurdere nuværende og fremtidige sikkerhedsrisici, der er knyttet til de kommunale systemer/it-løsninger, som er udviklet og forvaltes af KOMBIT og/eller som anvendes internt i KOMBIT (fx til HR eller økonomi).

Selve risikovurderingen består af en vurdering af, hvad sandsynligheden er, for at en given hændelse (der kan resultere i et sikkerhedsbrud) rammer en dataproces (se definition i vejledning om Dokumentation for datatyper og datastrømme), samt hvilke konsekvenser det vil kunne give for henholdsvis KOMBIT og den registrerede.

Risikovurderingen understøtter, at der til enhver tid er etableret de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, som kan beskytte data, som behandles i enten løsningerne eller i organisationen.

Risikovurderingen skal bruges i det videre arbejde med iværksættelse af organisatoriske og tekniske sikkerhedsmæssige tiltag til imødegåelse af de risici (risikohåndtering), der fremgår af risikovurderingen.

Konsekvenserne af at udelade risikovurdering kan være, at der ikke løbende stilles de nødvendige sikkerheds- og compliancekrav til løsningen under både udvikling og forvaltning, samt til de omkringliggende processer (kontroller). Dette kan føre til:

- Risiko for kompromittering af følsomme, fortrolige og/eller forretningskritiske oplysninger.
- Brud på persondataregulering
- Erstatningskrav
- Manglende kontrakthåndtag overfor leverandører, som drifter løsningen
- Tab af anseelse og troværdighed

C.PRAKTISK

Til brug for arbejdet med etableringen af dokumentation for risikovurdering er der udarbejdet et værktøj (skema i Excel), som skal benyttes hertil. Dokumentationen med skemaet SKAL navngives med unikke identer således, at der sikres den fornødne sammenhæng mellem skemaerne og det enkelte projekt. Den unikke ident som SKAL fremgå, er projektets nummer i Project Online. I tillæg vil det være muligt at indsætte en ident fra henholdsvis Qualiware og Pactius såfremt projektet har dette, men det er ikke obligatorisk.

For yderligere præcisering af navngivning af dokumenter henvises til dokumentet "Vejledning opdatering af compliance og udarbejdelse af årsplan"(findes i Share-IT under "Governance" – "Standarder og skabeloner (Metodematrixen)" – "Projektstyring"): https://share-it.kombit.dk/i/standarderogskabeloner/Metode Matrix/Vejledning - Opdatering af compliance og udarbejdelse af %C3%A5rsplan - Informationssikkerhed.docx

I værktøjet vil der fremgå en række spørgsmål, som skal besvares. Det er vigtigt at understrege, at det er obligatorisk, at alle felter besvares af hensyn til den efterfølgende dokumentation og proces. Det er således væsentligt, at man ved at kigge på besvarelserne kan se, at der er taget aktivt stilling til de fremsatte spørgsmål i projekterne. Det er muligt at anføre bemærkninger til svar i skemaet såfremt der er usikkerhed omkring svar eller der efterfølgende kan være behov, fx med projektjuristen eller KOMBITs DPO, eller hvor man allerede nu kan se, at der er forhold, som skal håndteres efterfølgende i de sikkerhedstiltag, der skal iværksættes i løsningen.

Det er et vigtigt hensyn, at dokumentationen foreligger i en form, som nemt kan tilgås i forbindelse med henvendelser fra dataansvarlige eller tilsynsmyndigheder, som har ret til at kontrollere KOMBITs overholdelse af GDPR og tilhørende persondataretlig og sikkerhedsmæssig lovgivning herom.

D.BEGREBER

Nedenfor gives en uddybende forklaring af begreber, der anvendes i denne vejledning (se endvidere øvrige vejledninger om informationssikkerhed):

Sikkerhedsbrud

Et sikkerhedsbrud opstår som følge af en eller flere uønskede eller uventede hændelser, der har en væsentlig sandsynlighed for at bringe it-løsningen/systemet i fare og true sikkerheden.

Hændelse – der påvirker en bestemt række af omstændigheder (dataprocesser)

En hændelse er den forekomst eller ændring af en bestemt række omstændigheder, der kan forårsage et sikkerhedsbrud. Derfor kaldes en hændelse ofte for et brud eller et uheld. Hændelser kan resultere i enten tab af fortrolighed, integritet og/eller tilgængelighed:

Tab af fortrolighed: Processens fortrolighed er truet pga. hændelsen; uautoriserede kan få viden om data i processen, som de ikke har ret til.

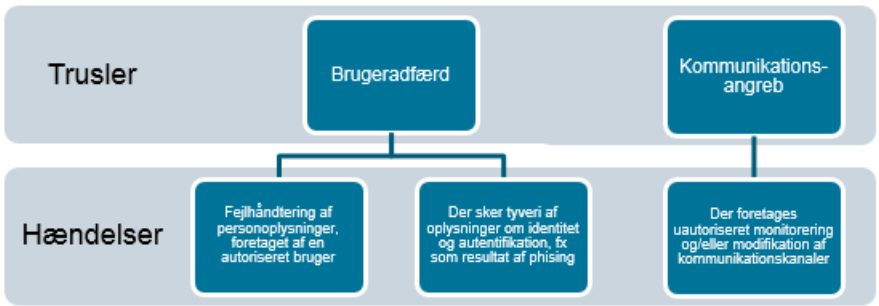
Tab af integritet: Processens integritet er kompromitteret pga. hændelsen og der kan ske uautoriserede ændringer af data, der betyder, at oplysningerne ikke er præcisere/korrekte og fuldstændige.

Tab af tilgængelighed: Tilgængeligheden til processen for autoriserede brugere er truet pga. hændelsen og oplysningerne kan ikke tilgås af de autoriserede brugere på de tidspunkter hvor der ønskes adgang til data.

Trussel – årsagen til hændelsen

Truslen er den potentielle årsag til den uønskede hændelse indtræffer. Én trussel har ofte mere end en hændelse tilknyttet.

Nedenfor er angivet et eksempel på hvordan en trussel kan have hhv. to og én hændelse tilknyttet.



System

Når der i hændelsesbeskrivelsen henvises til et system, menes det system/it-løsning, som er udgangspunktet for risikovurderingen. Vurdes eksempelvis AULA, er systemet der refereres til AULA som system/it-løsning.

Sandsynlighed – for at hændelsen indtræffer

Sandsynligheden er "chancen" for, at den uønskede hændelse indtræffer. Sandsynligheden tager udgangspunkt i sårbarhederne i it-løsningen/systemet og/eller de kontroller (sikkerhedsforanstaltninger) der er implementeret i it-løsningen/systemet, eller som tiltænkes at blive implementeret fx på baggrund af kravspecifikationen. Se endvidere anvendelse af skala til sandsynlighedsvurdering i afsnit E. Vejledning, 2. Sandsynlighedsvurdering.

Kontroller (sikkerhedsforanstaltninger)

En kontrol er en sikkerhedsforanstaltning, der sænker risikoen.

Sårbarhed

En sårbarhed er et systems/løsnings eller en sikkerhedsforstaltnings (kontrols) svaghed, som kan udnyttes af en eller flere trusler.

Konsekvens – af en uønsket hændelse

Konsekvensen er resultatet af en uønsket hændelse. Dette kan fx være de organisatoriske/forretningsmæssige konsekvenser for KOMBIT eller kommunen, samt de konsekvenser, der kan være for registrerede, såfremt der sker et sikkerhedsbrud. Når konsekvenserne skal identificeres, vurderes de på baggrund af de konsekvenser, som et tab af fortrolighed, integritet og tilgængelighed vil medføre for dataprocessen.

Risiko/Risici

Risikoen er et udtryk for en kombination af sandsynligheden for en uønsket hændelse og omfanget af konsekvenserne). "Risikoniveau" anvendes for at kunne sammenligne forskellige hændelser med højeste eller laveste risiko.

Risikoniveauet er givet ved den matematiske formel:

Risikoniveau = Sandsynlighedsniveau x Konsekvensniveau

E. VEJLEDNING TIL EXCEL-VÆRKTØJ

Selve gennemførelsen af risikovurderingen består af i alt 5 trin, som hver har sit faneblad i Excel-værktøjet:

0. Indtastning af **stamdata** for det projekt eller intern enhed og den dataproces, der vurderes

1. Opdatering af **trusselskatalog**

2. Vurdering af **sandsynlighed** for at de identificerede hændelser indtræffer

3a. Vurdering af de **konsekvenser** hændelsen kan resultere i hos **KOMBIT**

3b. Vurdering af de **konsekvenser** hændelsen kan resultere i for **registrerede**

Når disse trin er udført er risikovurderingen komplet og den samlede risiko kan aflæses i faneblade med oversigter over:

4a. **Resultat** med alle risici for **KOMBIT**

4b. **Resultat** med alle risici for **registrerede**

I det følgende fremgår det, hvordan de enkelte faner skal anvendes og udfyldes under den trinvise gennemførelse af risikovurderingen. Der skal udfyldes et Excel-dokument for hver dataproces, der er omfattet af løsningen og dermed indgår i riskovurderingen. Det valgfrit at slå flere dataprocesser sammen, hvis det vurderes, at sandsynlighed og konsekvenser vil være ens, fx pga. anvendelse af samme teknologi og datasæt. I så fald beskrives det under fanebladet ”0. Stamdata”, hvilke dataprocesser risikovurderingen omfatter.

0. Stamdata

Stamdata	Udfyld
Projektnavn / Speciale / Supportfunktion	
Dataproces	
Formål med dataproces	
Bemærkning	
Projektejer / Forretningsejer	
Projektleder / Leder af speciale el. supportfunktion	
Projektkoordinator	
Projekt Online reference	
Pactius reference	
Qualiware reference	

Den første fane skal indeholde en række stamoplysninger, som identificerer dataprocessen og projektet/enheden entydigt, og opmærksomheden henledes særligt på at sikre, at der angives en unik ident jf. det projektnummer som benyttes i Project Online og i tillæg endvidere anføres reference til Qualiware eller Pactius, hvis et sådant haves.

Derudover skal projektets/enhedens dataproces, der vurderes indskrives i kolonnen. Under bekrivelsen af "Formål med dataproces" og "Bemærkning" er det vigtigt, at det fremgår, hvad dataprocessen anvendes til eller i forbindelse med, og fx hvilke moduler eller dele af it-løsningen, der bliver anvendt i dataprocessen. Dette har betydning for den efterfølgende vurderingen af konsekvenser.

1. Opdatering af trusselskatalog

Formål: Sikring af at alle relevante, herunder særligt projektspecifikke, trusler er identificeret

Trusselskatalog (sidst opdateret d. 01.12.17)								
Nr.	Kategori	Type af trussel	Hændelse	*Beskrivelse af hændelse*	Indflydelse på:			Relevans
					F	I	T	
H1	Menneskeskabte	Autentificeringsangreb (tilsigtet)	Der sker en session hijacking	*Kompromittering af brugersession . Uautoriseret overtagelse af en allerede eksisterende, legitim session imellem to systemer, eller imellem system og brugere.*	x		x	a. Projekter
H2	Menneskeskabte	Autentificeringsangreb (tilsigtet)	Der opnåes uautoriseret adgang til legitime brugeroplysninger	*Uautoriseret adgang til en legitim brugers login-information, herunder brugernavn og kodeord. Kan opstå på flere måder: Læk af brugerinformation, usikker opbevaring af brugerinformation eller*	x			b. Internt

Under fanen ”1. Trusselskatalog” fremgår KOMBITs standardtrusselskatalog, som er tilpasset og prioriteret til KOMBITs behov.

Projekter/enheder skal ikke ændre i de allerede definerede trusler, men skal tilføje yderligere relevante trusler (se nedenfor).

Trusselskataloget består af:

- **Nr.:** Unikt ID for hændelsen
- **Kategori:** Kategorien af trusler hændelsen tilhører, fx menneskeskabte eller tekniske
- **Type af trussel:** Trusselstypen hændelsen tilhører, fx procesfejl, hacking mv.
- **Hændelse:** Kort beskrivelse af hændelsen
- **Beskrivelse af hændelse:** Uddybende beskrivelse af hændelsen
- **Indflydelse på hhv. F, I & T:** Såfremt hændelsen kan have betydning for hhv. tab af fortrolighed (F), integritet (I) og/eller tilgængelighed (T) er der sat et lille (lowercase)”x”.
    - *Eksempelvis vil hændelsen ”Fysiske angreb på faciliteter og dertilhørende infrastruktur” ikke umiddelbart true en dataproces’ fortrolighed og integritet, men kun tilgængelighed af data. Derfor skal konsekvensen kun vurderes ved ”Tab af tilgængelighed” og der er kun sat et ”x” under tilgængelighed (T).*
- **Relevans:** Herunder er det markeret, hvorvidt hændelsen er relevant for KOMBITs eksterne projekter eller kun for KOMBIT interne løsninger:
    - **a.** Projekter: Fokuseret på applikationsrettede sikkerhedshændelser relateret til fælleskommunale løsninger (KOMBIT projekter som fx AULA) og KOMBITs interne it-løsninger
    - **b.** Internt: Bredere fokus til risikovurdering af KOMBITs interne it-løsninger, der også omfatter sikkerhedshændelser relateret til brugere og organisationens it-infrastruktur (netværk, klienter). Såfremt det er en intern dataproces, der skal vurderes, fx i HR, skal disse hændelser også vurderes.

Tilføjelse af projektspecifikke trusler:

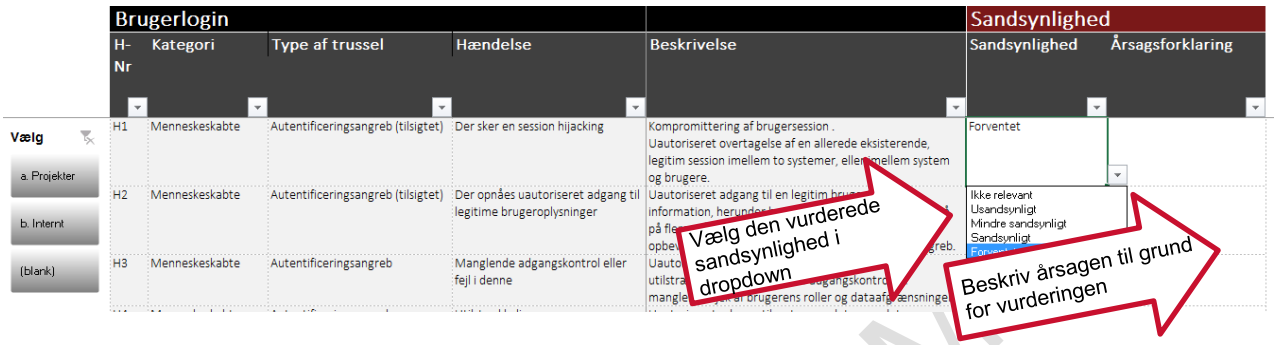
Såfremt der er identificeret nye trusler og hændelser, som er særligt relevante for den vurderede dataproces, skal disse tilføjes i trusselskataloget på fane 1. Det er vigtigt at alle kolonner udfyldes og at der under F, I, T skrives ”x” med lowercase (lille) og at der under relevans, vælges ”a. Projekter” eller ”b. Internt” fra dropdown boksen.

Herefter vil hændelserne automatisk blive overført til vurderings- og resultatarkene (2 - 4).

Hvis hændelsen også er relevant for projektets resterende dataprocesser er det vigtigt, at hændelsen tilføjes manuelt i alle de risikovurderings-Excel filer hvor de dataprocesser, som er knyttet til projektet, skal risikovurderes.

2. Sandsynlighedsvurdering

Formål: Vurdering af sandsynligheden for at en given hændelse rammer dataprocessen.

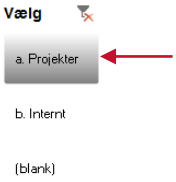


I fanebladet ”2. sandsynlighed” skal det vurderes hvor stor sandsynlighed, der er for at hver hændelse i trusselskataloget, rammer dataprocessen.

Ved vurdering af sandsynlighed for en hændelse skal den være relateret til den dataproces og it-løsning, der er udgangspunkt for risikovurderingen. Det betyder, at vurderingen omfatter selve dataprocessen og dens integrationer, det vil sige datastrømmen ind eller ud af løsningen, der risikovurderes. Den it-løsning som datastrømmen udveksler data til og fra indgår ikke i vurderingen af sandsynlig. Fx betyder det i forhold til Aula, at vurderingen ikke omfatter it-løsninger som Uni-Login eller læringsplatforme (udstillet via widgets), da disse skal risikovurderes som andre kommunale it-løsninger i henhold til kommunens praksis.

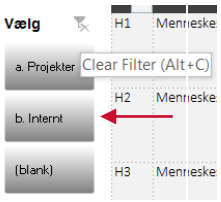
Primære deltagere til vurderingen af sandsynlighed og begrundelsen herfor, bør være personer i KOMBIT med teknisk kendskab til dataprocessen og it-løsningen.

Vælg hændelser til sandsynlighedsvurdering:



Hvis risikovurderingen foretages for en løsning der hører under et eksternt **KOMBIT-projekt** skal der klikkes på knappen ”a. Projekter”. Når dette er gjort, vil kun denne knap være markeret grå, og mange af hændelserne vil blive frasorteret.

*Intern løsning i risikogruppe ”**Lav**”:*



Hvis risikovurderingen foretages for en **intern løsning**, hvor det er vurderet, at løsningen er i risikogruppe ”Lav”, skal der klikkes på knappen ”b. Internt”. Når dette er gjort, vil kun denne knap være markeret grå, og mange af hændelserne vil blive frasorteret.

*Intern løsning i risikogruppe ”**Høj**”:*

Hvis risikovurderingen foretages for en **intern løsning**, hvor det er vurderet, at løsningen er i risikogruppe ”Høj”, skal der henholdsvis først klikkes på knappen ”a. Projekter” for udfyldelse af risikovurderingen og efterfølgende skal der klikkes på knappen ”b. Internt” for udfyldelse af den resterende del af risikovurderingen.

Når dette er gjort, kan vurderingen af sandsynligheder gå i gang.

Vurdering af sandsynlighed:

I kolonnen ”sandsynlighed” skal sandsynlighedsvurderingen angives. Der skal altid tages udgangspunkt i ”worst case scenarie”. Til brug for vurderingen skal nedenstående tabel anvendes til inspiration og indikation af niveauet 1-4. Såfremt hændelsen ikke vil kunne påvirke en proces vælges ”Ikke relevant”.

Niveau	*Indikation af sandsynlighedsniveau*
4 **Forventet**	Det forventes at hændelsen vil forekomme – Man har erfaring med hændelsen inden internt for de sidste 12 måneder. – Hænder jævnligt i offentlige og private virksomheder (hændelsestypen omtales ofte i pressen).
3 **Sandsynlig**	Det er sandsynligt at hændelsen vil forekomme – Man har erfaring med hændelsen internt, men ikke inden for de sidste 12 måneder. – Kendes fra andre offentlige og private virksomheder i Danmark (hændelsestypen omtales årligt i pressen).
2 **Mindre sandsynlig**	Hændelsen kan risikere at forekomme – Man har erfaring med hændelsen internt, for nogle år siden. – Kendes fra andre offentlige og private virksomheder i Danmark.
1 **Usandsynlig**	Hændelsen forventes ikke at komme. – Ingen erfaring med hændelsen internt. – Kendes kun fra få andre offentlige og private virksomheder, men ikke nødvendigvis i Danmark.
0 **Ikke relevant**	Der er ingen sandsynlighed for at hændelsen vil ramme processen, og hændelsen er dermed ikke relevant for den vurderede dataproces.

For interne enheder er der under ”b. Internt” i kolonnen ”Årsagsforklaring” indsat uddybende forklaringer samt retningslinjer for besvarelse, som skal understøtte, at enheden selv kan foretage vurdering af sandsynlighed samt angive den tilhørende årsagsforklaring. Den interne enhed vil dog have behov for hjælp til at færdiggøre enkelte vurderinger. Det fremgår af skemaet, hvilke hændelser dette gælder for.

Den interne enhed skal i forbindelse med udfyldelse af skemaet huske at tilpasse teksten i kolonnen ”Årsagsforklaring”, så feltet indeholder begrundelsen for den interne enheds valg af sandsynlighed for den konkrete hændelse.

For interne enheder vil vurderingen af sandsynlighed for en række hændelser være ens, da de baserer sig på anvendelsen af KOMBITs infrastruktur. Derfor ”b. Internt” for udfyldt med en vurdering af sandsynlighed for en række hændelser. De interne enheder skal huske at udfylde vurdering af sandsynlighed i de tomme felter.

Begrundelse for vurdering:

Udover ovenstående tabel, skal sandsynligheden vurderes ud fra en kombination af række forskellige parametre, som enten kan være med til at sænke eller hæve sandsynligheden. Disse parametre kan fx være:

- Aktører og deres motiver for at udøve trusler
- Truslens karakter
- Sårbarheder i processen
- Sikkerhedsforanstaltninger (kontroller), som er implementeret i dataprocessen
- Leverandører
- Andet

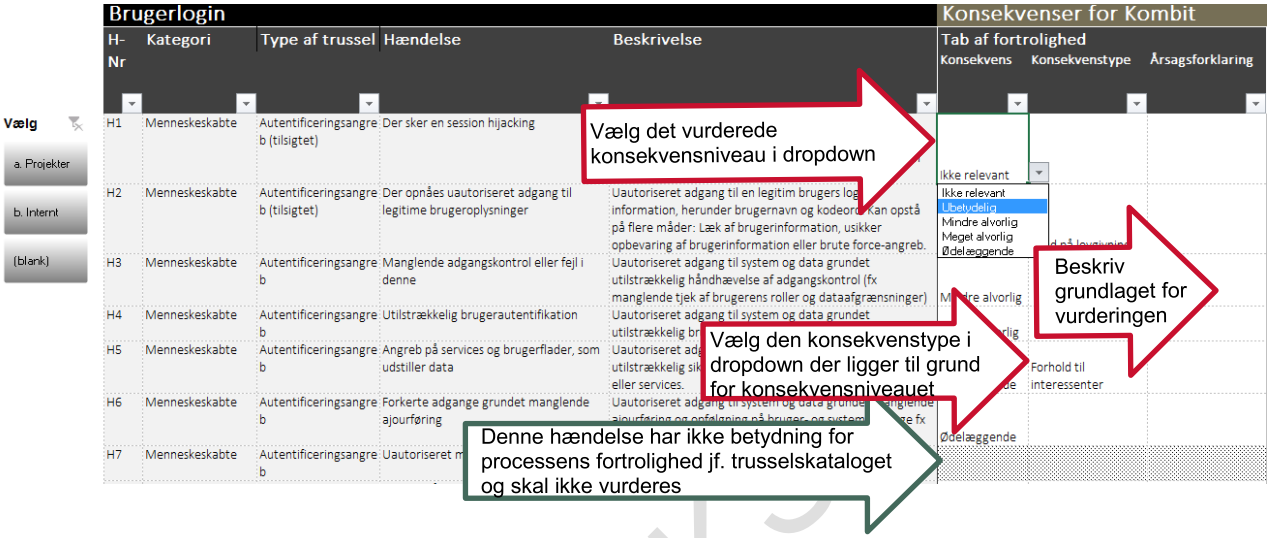
Sårbarheder kan for eksempel være en procedure eller arbejdsgang, som ikke fungerer efter hensigten eller en teknisk opsætning, som gør systemet eller dataprocessen åbent for angreb. En god måde at få afdækket sårbarhederne på er ved at gennemgå de implementerede eller planlagte sikkerhedstiltag/kontroller i it-løsningen og vurdere deres effektivitet.

Vurderingen af sandsynligheden kræver derfor at hele dataprocessen og dens datastrømme tænkes igennem, for at sikre der tages højde for de væsentligste parametre og sandsynlighedsvurderingen bliver så præcis som mulig. Begrundelsen og parametre der ligger til grund for vurderingen, beskrives i fritekstskolonnen "Begrundelse for vurdering".

Eksempelvis kan man forestille sig, at det er "forventet", at en dataproces rammes af virus, men fordi der i processen er et stort fokus på sikkerhedsforanstaltninger mod virus er processen dermed er mindre sårbar overfor den slags hændelser. Derfor bør vurderingen måske sænkes til "sandsynlig" eller "mindre sandsynlig" alt efter hvor sårbar processen vurderes at være.

3. Konsekvensvurderinger

Formål: Vurdering af konsekvensen ved hændelsen for hhv. KOMBIT og den registrerede.



Overordnet opdeles konsekvensen i "konsekvensniveau" og "konsekvenstype", samt en "årsagsforklaring".

Konsekvensniveauet angiver *graden* af konsekvensen, konsekvenstypen angiver *hvilken* konsekvens der er tale om og årsagsforklaringen er en *uddybning* af begrundelsen for vurderingen.

Konsekvenserne varierer alt efter om det er dataprocessens fortrolighed, integritet eller tilgængelighed, der er truet (se forklaring heraf under D. Begreber, *Hændelse – der påvirker en bestemt række af omstændigheder (dataprocesser)*). Derfor skal der foretages en særskilt vurdering i de tre forskellige situationer.

Konsekvens ved tab af Fortroligheden opstår, når informationer i dataprocessen kompromitteres – eksempelvis gennem uautoriseret adgang til arkiver, hacking af systemer, utilsigtet læk af informationer osv.

Konsekvens ved tab af Integritet opstår, når informationer i dataprocessen bliver helt eller delvist fejlagtige – eksempelvis pga. fejl på lagermedie, eller fordi aktiviteter/processer producerer fejlagtige informationer og/eller forvansker allerede eksisterende informationer.

Konsekvens ved tab af Tilgængelighed opstår, når informationer i dataprocessen bliver helt eller delvist utilgængelige eller ophører med at fungere – eksempelvis pga. servernedbrud, brand, tyveri, hardware- eller softwarefejl, brugerfejl, medarbejdere ramt af sygdom mv. Tab af (eller manglende) tilgængelighed kan være permanent eller af midlertidig karakter. Derfor skal der foretages en vurdering af hvad konsekvensniveauet er ved tab af tilgængelighed i:

- 2 timer
- 1 dag
- 2 dage
- Op til 1 uge
- Over 1 uge

Skraverede felter 

Da det, som beskrevet under 1. Opdatering af trusselskatalog, ikke er alle hændelser, der vil kunne resultere i både et tab af fortrolighed (F), integritet (I) og tilgængelighed (T), skal der kun foretages en vurdering, hvis det i trusselskataloget er markeret, at hændelsen vil få betydning for hhv. tab af fortrolighed (F), integritet (I) og tilgængelighed (T). Såfremt hændelsen ingen betydning vil have, skraveres felterne og der skal derfor ikke foretages en vurdering af konsekvensen.

Grå felter 

Såfremt en hændelse er vurderet "ikke relevant", under 2. Sandsynlighedsvurdering, markeres feltet gråt, da konsekvensen i så fald ikke skal vurderes.

Udførelse af konsekvensvurdering:
Konsekvensvurderingen skal både udføres i henhold til de konsekvenser, en given hændelse kan have for *KOMBIT* og i henhold til de konsekvenser hændelsen kan have for den *registrerede*. Dette skal gøre i to separate faneblade, som hver indeholder tilpassede evalueringskriterier for typen af konsekvens:

"3a. Konsekvens for KOMBIT" og som angiver kriterierne der skal anvendes til vurderingen af konsekvenserne for *KOMBIT*

"3b. Konsekvens for registrerede" og som giver kriterierne der skal anvendes til vurderingen af konsekvenserne for de *registrerede*.

3a. Konsekvens for KOMBIT

I fanebladet "3a. Konsekvens for KOMBIT" skal de organisatoriske konsekvenser ved hændelserne vurderes.

Ved KOMBIT forstås KOMBIT som organisation. Der skal altså ikke foretages en vurdering af konsekvenserne for kommunerne.

Når konsekvensen for KOMBIT skal vurderes, skal nedenstående tabel anvendes til inspiration og indikation af hvilket niveau, samt hvilken type konsekvens der er tale om. Der skal altid tages udgangspunkt i "worst case scenarie" og derfor skal den konsekvenstype, der vil give den højeste konsekvens tastes ind.

Kriterie	1 Ubetydelig *(Uvæsentlig)*	2 Mindre alvorlig *(Generende)*	3 Meget alvorlig *(Kritisk)*	4 Graverende/ Ødelæggende *(Meget kritisk)*
Strategisk Medfører indskrænkninger i evnen til at handle i en periode	Ingen særlig påvirkning	Planlagte aktiviteter kan gennemføres med mindre justeringer	Medfører revurdering af vigtige aktiviteter på kort sigt	Bliver ude af stand til at gennemføre vigtige aktiviteter, som er planlagt i en periode fremover
Økonomisk Medfører meromkostninger eller tab	Ingen særlig påvirkning	Meromkostninger og tab i begrænset niveau, som kan kræve mindre budgetændringer	Store økonomiske tab med risiko for, at ledelsen bliver sat under skærpet tilsyn	Væsentlige økonomiske tab. Ledelsen bliver sat under skærpet tilsyn
Administrativ Medfører administrative belastninger	Håndteres uden særligt ressourcetræk i de administrative funktioner	Håndteres inden for rimeligt ekstra administrativt ressourcetræk	Der må trækkes væsentligt på eksisterende og nye administrative ressourcer	Administrative ressourcer må udvides urealistisk
Interessenter Påvirker forholdet til interessenter	Ingen særlig påvirkning	Forringet samarbejde med interessenter i enkeltsager	Generelt forringet samarbejde med interessenter	Væsentligt nedbrud i det generelle samarbejde med interessenter
Lovmæssige krav Medfører brud på lovgivning, fx GPDR, forvaltningslov og straffelov	Ingen særlig påvirkning	Manglende overholdelse af administrative procedurer og regler, som ikke er af kritisk karakter	Lovbrud, der er kritiske og kan stille administrationen i miskredit	Kritisk lovgivning, f.eks. straffeloven brydes. Den ansvarlige chef vil blive holdt ansvarlig
Politisk Medfører indskrænkninger i evnen til at handle i en periode	Ingen særlig påvirkning	Planlagte aktiviteter kan gennemføres med mindre justeringer	Medfører revurdering af vigtige aktiviteter på kort sigt	Den øverste ledelse må gå af. Bliver ude af stand til at gennemføre vigtige aktiviteter, som er planlagt i en periode fremover
Omdømme Påvirker omdømme i uønsket retning	Ingen særlig påvirkning	Forbigående opmærksomhed fra enkelte grupper	Offentligheden fatter generel negativ omdømme	Væsentlig skade på omdømme. Den ansvarlige chef må gå af

Eksempelvis får en autoriseret bruger adgang til nogle data, som vedkommende ikke skulle have haft adgang til. Det sker på baggrund af, at medarbejderens profil ikke er blevet kontrolleret i forhold dataafgrænsning og roller, fx hvis medarbejder har skiftet funktion i organisationen.

*Dette vil formodentligt have **ubetydelige** konsekvenser for det strategiske, økonomiske (i sammenhængen med økonomisk tab) og det administrative. Det kan være **mindre alvorlig** i*

*forhold til interessenter, da en enkeltstående interessent ikke ønsker af dele oplysninger fremadrettet. Men at medarbejderen har fået adgang til nogle data som måske har en følsom karakter, kan blive betegnet som en **meget alvorlig** sag for den lovmæssige konsekvens og ligeledes for den politiske konsekvens. Det lovmæssige, fordi det er et kritisk lovbrud og det vil kunne udstille organisationens procedurer. Omkring de politiske konsekvenser, vil det kunne skabe et dårligt omdømme for organisationen, hvis dette bliver offentliggjort i dagspressen.*

*Derfor vil man skulle vurdere denne hændelse som en niveau **3 – meget alvorlig**, da det altid er den højeste (worst case) som man skal kunne håndtere. Da der i dette eksempel er to konsekvenstyper som begge er **meget alvorlig**, bør man udpege den lovmæssige som vigtigste og i kommentarboksen notere at omdømme ligeledes er **meget alvorlig.***

3b. Konsekvens for registrerede

I fanebladet ”3b. Konsekvens for registrerede” skal konsekvenserne ved hændelserne vurderes ud fra den betydning hændelsen kan have for den registreredes privatliv og rettigheder.

Når konsekvensen for registrerede skal vurderes, skal nedenstående tabeller anvendes til inspiration og indikation af hvilket niveau, samt hvilken type konsekvens der er tale om. Det er vigtigt at understrege, at tabellen kun er vejledende og derfor ikke en facitliste, da der altid skal tages udgangspunkt i den pågældende behandling i processen. Der skal altid tages udgangspunkt i ”worst case scenarie” og derfor skal den konsekvenstype der vil give den højeste konsekvens tastes ind.

	1 Ubetydelig *(Uvæsentlig)*	2 Mindre alvorlig *(Generende)*	3 Meget alvorlig *(Kritisk)*	4 Graverende/ Ødelæggende *(Meget kritisk)*
Hændelses-påvirkning	Personoplysningerne der udsættes for en hændelse er i forvejen offentlige tilgængelige.	Almindelige personoplysninger der normalt deles uden særlige forbehold, kan tilgås eller ændres af uautoriserede.	Almindelige, men fortrolige, personoplysninger offentliggøres eller følsomme personoplysninger kan tilgås eller ændres af uautoriserede.	Følsomme personoplysninger kan tilgås eller ændres af uautoriserede eller offentliggøres for offentligheden. Følsomme personoplysninger kan ikke tilgås på ønskede tidspunkter.
Eksempler på person-oplysninger (kategorier anvendt i datatyper og datastrømme)	Alle i forvejen offentliggjorte oplysninger, fx på google, dgs.dk eller krak.dk	Kontaktinformation, herunder: Navn Adresse Alder Køn E-mail Familierelation Medarbejder-nr.	Strafbare forhold Kundeoplysninger Digitale fodspor Uddannelse & CV Medarbejderoplysninger Familieoplysninger Økonomiske oplysninger CPR-nummer Øvrige ID-numre (udover CPR-nummer) Personlige oplysninger	Biometriske oplysninger (FPO) Genetiske oplysninger (FPO)* Helbredsoplysninger (FPO)* Filosofiske overbevisninger (FPO)* Politiske overbevisninger (FPO)* Race/etnicitet (FPO)* Religiøse overbevisninger (FPO)* Seksualliv (FPO)* Seksuel orientering (FPO)* Fagforeningsmedlemskab (FPO)*

Da der behandles forskellige kategorier af personoplysninger i de forskellige dataprocesser, og konsekvenserne ofte vil hænge sammen med hvilke personoplysninger, det er der udsættes for et sikkerhedsbrud, skal nedenstående tabel anvendes som en indikation af niveauet for konsekvensen.

Eksempelvis, at en medarbejder glemmer sin computer i toget på vej hjem fra arbejde. På computeren har medarbejderen gemt nogle arbejdsdokumenter. Nogle af disse dokumenter bliver lækket på internettet. Dokumenterne indeholder oplysninger om enkelte borgere herunder deres navne, deres religion, økonomiske situation og seksuelle orientering.

*Af tabellen ses, at navn ligger under **mindre alvorlig**, økonomiske situation under **meget alvorlig** og religion og seksuelle orientering under **graverende/ødelæggende**.*

*Udgangspunktet for hvilket konsekvensniveau denne hændelse vil ligge på, vil derfor være **graverende/ødelæggende**, da dette er den højeste (worst case). Det er dog ikke den*

endegyldige vurdering, da der også skal tages højde for konsekvenstypen, hvilket gøres i næste tabel (fortsættes efter nedenstående tabel).

Efter at have fået en indikation af konsekvensniveauet ud fra ovenstående tabel, skal typen af konsekvensen vurderes og det egentlige konsekvensniveau fastlægges. Til vurderingen heraf skal der tages udgangspunkt i følgende tabel, som også kun skal anvendes til inspiration:

Kriterie	1 Ubetydelig *(Uvæsentlig)*	2 Mindre alvorlig *(Generende)*	3 Meget alvorlig *(Kritisk)*	4 Graverende/ Ødelæggende *(Meget kritisk)*
Privatlivs-rettigheder Medfører sociale tab og/eller skade på omdømme	Ingen særlig påvirkning	Registreredes eksponeres internt for uautoriserede	Registreredes eksponeres på en måde som skader de sociale relationer, såvel internt blandt kollegaer/elever og eksternt uden for organisationen. Registrerede fratages potentielt retten til at være anonym	Væsentlig skade på registreredes ry/omdømme, der kan føre til store sociale tab. Registrerede fratages muligheden for at være anonym, da fortroligheden af data mistes.
Friheds-rettigheder Medfører materielle (fx økonomiske) tab, indskrænket kontrol eller GDPR-rettigheder	Ingen særlig påvirkning	Registrerede oplever ingen særlige materielle tab. Registreredes valgfrihed og kontrol over sine personoplysninger forringes. Registrerede kan ikke gøre brug af sine rettigheder i en kortere periode	Registrerede oplever mindre materielle tab. Registreredes valgfrihed og kontrol over sine personoplysninger fratages. Registrerede mister helt muligheden for at gøre brug af sine rettigheder	Væsentlige materielle tab, der påvirker registreredes livssituation væsentligt
Menneskelige Medfører mangel på fysisk sikkerhed eller påvirker registreredes helbred fysisk eller psykisk	Ingen særlig påvirkning	Registrerede udsættes for fysiske og/eller psykiske helbredsmæssige gener i mindre grad – intet alvorligt	Registrerede fysiske og/eller psykiske helbred eller fysiske sikkerhed påvirkes	Registreredes udsættes for fundamental helbredsmæssig fare. Registreredes fysiske sikkerhed er i fare. Menneskeliv kan stå på spil
Børn Beskyttelsen af børns privacy forringes	Ingen særlig påvirkning	Børn eksponeres internt for uautoriserede. Forældres kontrol over barnets oplysninger forringes.	Børn eksponeres på en måde som ikke tjener den registrerede, og kan blive ekskluderet fra sociale netværk. Forældres kontrol over	Børn lider væsentlig skade på omdømme, der kan føre til sociale tab. Børns helbred er i fundamental fare

		Børns udsættes for helbredsmæssige gener – intet alvorligt	barnets personoplysninger fratages. Børns helbred påvirkes	

*Eksempel fortsat: Efter at have vurderet at niveauet ligger omkring **graverende/ødelæggende** pga. af oplysningerne om religion og seksuelle orientering, skal konsekvenstypen og det endelige niveau fastlægges.*

*Grundet oplysningerne og deres sensitivitet, vil det kunne have store konsekvenser for den registreredes omdømme, og kunne skade den registreredes respekt og agtelse i samfundet. Derfor vil man vurdere privatlivsrettigheder til en **graverende/ødelæggende** konsekvens for den registrerede. Da det er ikke umiddelbart er oplysninger som vil kunne betyde fx økonomiske tab for den registrerede, vil man vurdere frihedsrettigheder til at være **ubetydelig**. Det er heller ikke oplysninger som umiddelbart vil betyde noget for den registreredes fysiske helbred, men det kan have en mindre psykisk betydning, hvorfor man på det menneskelige kriterie, vil vurdere konsekvensen til **mindre alvorlig**.*

*Vurderingen for denne hændelse vil derfor ligge på **graverende/ødelæggende**, da det altid er den højeste (worst case) som man skal vurdere ud fra.*

4a. og 4b. Risici for KOMBIT og registrerede

Resultatet af risikovurderingen bliver præsenteret i en samlet oversigt for hhv. KOMBIT og registrerede, hvoraf alle risici i forhold til tab af fortrolighed, integritet og tilgængelighed fremgår.

Det er muligt at sortere på KOMBIT-projekt og intern løsning ved at klikke på knapperne ”a. Projekter” og ”b. Internt”. Når dette er gjort vil mange af hændelserne vil blive frasorteret.

I oversigten er risici er markeret med farve i forhold til risikoens størrelse med en opdeling i tre niveauer som illustreret nedenfor, hvor rød er en høj risikoprofil (tal angiver samlet risikoscore).

Konsekvens				
Forventet	4	8	12	16
Meget sandsynligt	3	6	9	12
Sandsynligt	2	4	6	8
Mindre sandsynligt	1	2	3	4
	Ubetydelig (Uvæsentlig)	Mindre alvorlig (Generende)	Meget alvorlig (Kritisk)	Graverende/ Ødelæggende (Meget kritisk)

Sandsynlighed

Såfremt en hændelse ikke er markeret i trusselskataloget, som havende betydning for henholdsvis tab af fortrolighed, integritet eller tilgængelighed skraveres feltet, på samme måde under konsekvensvurderingen.

Såfremt det under sandsynlighed og/eller konsekvens er vurderes at hændelsen *ikke er relevant* for dataprocessen, markeres feltet gråt.

Såfremt der mangler at blive vurderes sandsynlighed og/eller konsekvens vil feltet være hvidt.

Eksempel på uddrag af samlet oversigt med alle risici:

Brugerlogin				Samlet risici for kombit										
H-Nr	Kategori	Type af trussel	Hændelse	Tab af fortrolighed		Tab af integritet		Tab af tilgængelighed						
				Risiko	Konsekvenstype	Risiko	Konsekvenstype	Risiko					Konsekvenstype	
								2 timer	1 dag	2 dage	op til 1 uge	over 1 uge		
H1	Menneskeskabte	Autentificeringsangreb (tilsigtet)	Der sker en session hijacking		-	0	-						-	
H2	Menneskeskabte	Autentificeringsangreb (tilsigtet)	Der opnåes uautoriseret adgang til legitime brugeroplysninger	1	Brud på lovgivningen	0	-	0	0	0	0	0	-	
H3	Menneskeskabte	Autentificeringsangreb	Manglende adgangskontrol eller fejl i denne	4	-	6	Brud på lovgivningen	0	0	0	0	0	-	
H4	Menneskeskabte	Autentificeringsangreb	Utilstrækkelig brugerautentifikation	9	-	12	Økonomisk	0	0	0	0	0	-	
H5	Menneskeskabte	Autentificeringsangreb	Angreb på services og brugerflader, som udstiller data		Forhold til interessenter		Forhold til interessenter							
H6	Menneskeskabte	Autentificeringsangreb	Forkerte adgange grundet manglende ajourføring	4	-	2	Strategisk	0	0	0	0	0	-	
H7	Menneskeskabte	Autentificeringsangreb	Uautoriseret manipulation af logs	0	-	6	-	0	0	0	0	0	-	
H8	Menneskeskabte	Autentificerringsangreb	Angreb på personoplysninger under lagring	0	-	0	-	0	0	0	0	0	-	
H9	Menneskeskabte	Brugeradfærd (utilsigtet)	Der sker en brugerfejl (tilfældig/uheld/uagtsomhed)	4	-	0	-	0	0	0	0	0	-	