AALBORG UNIVERSITET
STUDENTERRAPPORT

31-05-2019

Risikovurdering af fagsystemer

Et design af en risikovurderingsmetode samt tilhørende værktøj med implementering og evaluering i en dansk kommune

Emma Juhl Nøhr
AALBORG UNIVERSITET | IT, LÆRING OG ORGANISATORISK OMSTILLING

Abstract

This Master Thesis is compiled in the spring of 2019 and seeks to develop a risk assessment method and risk assessment tool for use in the Danish commune of Hjørring. This particular subject is researched with inspiration from Design-Based Learning and through a phenomenological point of view. The idea is to develop a risk assessment method and risk assessment tool by using the four phases of Design-Based Learning and the method participant observation. The first phase is directed by a felt study done in the autumn of 2018, where the point was to research how the commune of Hjørring did risk assessments with qualitative methods such as interviews, participant observation and document analysis. The result was that the commune needed an organized process to lead the risk assessment work and a collaboration between the information security coordinator and the users of the it-systems. The phase then leads into a state of art analysis of other risk assessment methods to compare them and analyze how they live up to the ISO27001-standard and how the new assessment method can differ from these other methods. In the second phase the risk analysis tool and the risk analysis method are developed by using Microsoft Excel as a tool. In the third phase the design of the risk assessment method is tested in practice with the help of employees in the commune. To do this the researcher is using the method facilitation where the risk assessment method is tested in practice and the employees is educated on how to do a risk assessment. Furthermore, in phase four the test is evaluated with the qualitative methods interview and participant observation. The interview is performed with a Google Analysis formula, where the informants is asked two questions: what was functioning well in the workshop and what was not. The result showed that the employees would like to participate in the workshop again, but there are problems with the risk assessment method. The same result is showed in the participant observation examination. The problem with the risk assessment method is the vulnerability classification of the it-system. The classifications are not right for the commune as an organization and they are hard to use in practice. The conclusion is, that there needs to be done a second iteration process to identify new problems and correct the found problems in the risk assessment method. The risk assessment tool is not tested in practice in this Master Thesis and needs to be tested in the next iteration.

Indhold

1 Indledning

Dette speciale ønsker at undersøge, hvordan en risikovurderingsmetode samt tilhørende værktøj kan designes til brug af en kommune, og er derfor udformet som specialeform b. Specialet tager udgangspunkt i den internationale sikkerhedsstandard ISO27001. Med den fællesoffentlige digitaliseringsstrategi er de danske kommuner forpligtet til at efterleve principperne for ISO27001-standarden. Specialet er udarbejdet i samarbejde med Hjørring Kommune, hvor risikovurderingsmetoden og -værktøjet er specifikt designet til samt afprøvet og evalueret med deltagelse fra kommunens medarbejdere. I dette kapitel vil problemfeltet samt motivationen for specialet beskrives for at berette hvilke oplevelser, tanker og oplysninger, der har ledt til problemformuleringen. Derefter bliver målgruppen for specialet præsenteret samt en afgrænsning af problemet, hvor der til sidst vil være en begrebsafklaring samt læsevejledning.

1.1 Problemfelt

I maj 2018 blev EU's persondataforordning (GDPR) en realitet i Danmark, hvor danske offentlige institutioner, herunder kommunerne, skulle forhold sig til, hvordan de behandlede persondata både fysisk og digitalt. Med GDPR blev det samtidigt et krav, at kommunerne skulle have en risikobaseret tilgang til arbejdet med persondata. Udover GDPR er kommunerne igennem Den fællesoffentlige digitaliseringsstrategi 2016-2020 forpligtet til at efterleve principperne i ISO27001-standarden. I ISO27001-standarden beskrives det, hvordan kommunerne kan have en risikobaseret tilgang både til informationssikkerhed og herunder også behandlingen af persondata. Løsningen er en risikohåndteringsplan, som er begrundet i en risikovurdering (Digitaliseringsstyrelsen, u.d.). Samtidigt viser rapporten "Danskernes informationssikkerhed" udarbejdet af Danmarks Statistik i foråret 2018, at 28 procent af de offentlige ansatte sender fortrolige personoplysninger og 30 procent af de offentlige ansatte sender cpr-numre via ikke krypteret e-mail (Larsen, Sørensen, & Devantier, 2018). Altså tyder det på, at kommunerne ikke er i mål med risikohåndteringsplanen.

En del af problemet med risikohåndteringsplanen kan skyldes selve risikovurderingen for, hvordan laver kommunerne en risikovurdering? ISO27001-standarden og GDPR giver ikke nogen eksempler på, hvordan det skal gøres. Kommunernes Landsforening og Digitaliseringsstyrelsen har udarbejdet vejledninger omhandlende risikovurderinger, men tilbyder ikke en skabelon eller en standard, kommunerne kan bruge, hvor en eksplicit risikovurderingsmetode er beskrevet (Digitaliseringsstyrelsen, 2015b). Kommunerne kan derfor skelne til udenlandske firmaer, som tilbyder risikovurderingsværktøjer, men udvalget er stort og ofte er disse værktøjer væsentlige dyre, som kommunerne immervæk ikke har råd til grundende manglende ressourcer på informationssikkerhedsområdet (Calder & Watkins, 2007).

1.2 Motivation

I efteråret 2018 startede jeg i praktik som informationssikkerhedskoordinator i Hjørring Kommune. Efter få dage blev jeg sammen med kommunens egentlige informationssikkerhedskoordinator sendt på eksamineret

ledelseskursus i ISO27001-standarden sammen med informationssikkerhedskoordinatorer fra seks andre kommuner i landet. På dette kursus blev det klargjort, at alle kommunerne havde svært ved netop den samme proces i informationssikkerhedsarbejdet: risikovurderingsprocessen. Efterfølgende blev det besluttet, at jeg skulle arbejde med denne proces og se på, hvordan en risikovurderingsmetode og -værktøj kunne designes til brug i kommunen. Dette indledtes med en forundersøgelse til at se på, hvordan kommunen i forvejen arbejdede med risikovurdering af informationsaktiver. Her fandtes det, at risikovurdering ikke kun handler om at have en metode og et værktøj, der kan benyttes til at udføre opgaven, men medarbejderne i kommunen skal også undervises i brugen af metoden. Det er medarbejderne, der har de informationer og oplysninger samt det daglige arbejde med informationsaktiverne, som der er behov for i risikovurderingsprocessen (Nøhr, 2018).

1.3 Problemformulering

Med udgangspunkt i de forrige afsnit er der baggrund for følgende problemformulering:

> *Hvordan kan en risikostyringsmetode med tilhørende værktøj designes og implementeres i Hjørring Kommune således, at metoden og værktøjet kan understøtte kommunens arbejde med implementering af principperne fra ISO27001-standarden? Herunder udvikle færdigheder og kompetencer hos medarbejderne således, at de kan udføre en risikovurdering på kommunens fagsystemer?*

1.3.1 Undersøgelsesspørgsmål

Der er udarbejdet en række undersøgelsesspørgsmål med udgangspunkt i problemformuleringen, som jeg mener skal besvares for at komme med en fyldestgørende løsning på problemet:

1. Hvordan har Hjørring Kommune indtil videre arbejdet med risikovurdering?
2. Hvilke krav er der til risikovurdering i ISO27001-standarden?
3. Hvordan kan læring foregå på en arbejdsplads?

1.4 Målgruppe

Med dette speciale ønskes at skabe en risikovurderingsmetode samt værktøj, som kan benyttes af andre kommuner og eventuelt andre private eller offentlige organisationer.

1.5 Afgrænsning

I specialet ses der på, hvordan en risikovurderingsmetode og tilhørende værktøj kan designes med udgangspunkt i en risikovurdering af fagsystemer, i og med dette var bestemt på forhånd af kommunen. Derfor er der ikke set på om andre informationsaktiver, såsom arbejdsprocesser og servere, kan risikovurderes ud fra denne metode og gennem dette værktøj. Samtidigt er der i dette speciale kun fokus på første iteration af designprocessen. Dette er valgt, da der er mange aspekter i første iteration, som er vurderet at være vigtige at have med

for at få en fyldestgørende belysning og forståelse af designet. Derudover har der på grund af procesmæssige udfordringer i Hjørring Kommune ikke været muligt at færdiggøre en anden iteration.

1.6 Begrebsafklaring

Facilitator: Begrebet facilitator har i kapitel 5 *Fase 3- Afprøvning i praksis* to betydninger, nemlig som traditionel underviser og samtidigt som projektleder for en workshopsproces som beskrevet hos Cecilie Van Loon, Henrik Horn Andersen og Line Larsen (2016).

Informationssikkerhedsarbejdet: I specialet har informationssikkerhedsarbejdet betydning af alt det arbejde omhandlende informationssikkerhed herunder blandt andet it-beredskab, risikohåndtering og udarbejdelse af informationssikkerhedspolitikken.

Læringssyn: Læringssynet i specialet har betydning for valg i kapitel 3 *Fase 1 – Domænekendskab* og kapitel 6 *Fase 4 – Evaluering*. Dette læringssyn tager udgangspunkt i Knud Illeris' læringssyn (2003), som er inspireret af den konstruktivistiske læringsforståelse, der er udviklet af den schweiziske biolog, psykolog og erkendelsesteoretiker Jean Piaget. I dette læringssyn opstår læring i kognitive strukturerede skemaer, som kan deles op i kumulativ, assimilativ, akkommodativ og transformativ læring, og som går fra oprettelsen af nye skemaer, til tilføjelse til eksisterende skemaer over til ændring af eksisterende skemaer og i sidste ende destruktion af eksisterende skemaer (Illeris, 2003, s. 78-79).

1.7 Læsevejledning

Den overordnet metode i dette speciale er Design-Based Research, hvilket har en betydning for læseoplevelsen, da teorier og metoder først bliver præsenteret i de faser af undersøgelsen, hvor de bliver benyttet. Den overordnet metode samt videnskabsteoretiske retning bliver præsenteret i de indledende afsnit.

2 Videnskabsteori og metodologi

I dette kapitel bliver den videnskabsteoretiske retning for specialet, fænomenologi, præsenteret. Herefter bliver den overordnet metodologi Design-Based Research præsenteret med fokus på, hvordan ELYK-modellen er benyttet i forhold til specialets opbygning, og hvordan modellen er tilpasset specialet. Til sidst vil den overordnet metode deltagerobservation blive præsenteret, idet det er den metode, hvorved størstedelen af den indsamlede information er indsamlet.

2.1 Videnskabsteoretisk retning

I dette speciale er den videnskabsteoretiske retning, hvorpå viden formes på i specialet, fænomenologi som oprindeligt er en filosofisk skole grundlagt af Edmund Husserl i begyndelsen af 1900-tallet. Fænomenologi stammer fra det græske ord phainomenon, som betyder "det, som viser sig" og ordet logos, der betyder "lære". Fænomenologi betyder "*læren om det, der kommer til syne eller fremtræder for en bevidsthed"* (Jacobsen, Tanggaard, & Brinkmann, 2015, s. 217). Den centrale målsætning er at belyse fænomener, som de er i sig selv, og møde dem uden de idéer, stereotyper og indtryk som forskeren selv tillægger disse fænomener (Jacobsen, Tanggaard, & Brinkmann, 2015, s. 218).

I fænomenologien er et af nøglebegreberne begrebet om livsverden, som er den konkrete verden, mennesket til daglig befinder sig i, og er konkret, da den er forankret kropsligt i tid og rum. Livsverden er en fælles verden, og er en social, kulturel og historisk kontekst, som danner en meningshorisont for det enkelte individ. Derfor spiller subjektet og den subjektive erfaring en rolle i et fænomenologisk perspektiv og er med til at konstituerer analysegenstanden. Helt metodisk handler fænomenologien om at forstå sociale fænomener ud fra aktørernes perspektiver og beskrive verden som den opleves af informanterne ud fra antagelsen om, at den vigtige virkelighed er den mennesket opfatter (Justesen & Mik-Meyer, 2010, s. 23).

2.2 Design-Based Research

Design-Based Research (DBR) også kaldet *design experiments, design research* og *educational design research* er initieret af blandt andre Ann Brown og Allan Collins. DBR er en bred forskningstilgang, som er designbaseret, hvilket betyder, at der generes ny viden gennem processer, som imedens udvikler, afprøver og forbedrer designs. DBR kan defineres som *"en systematisk men fleksibel metodologi med det formål at forbedre uddannelsespraksisser gennem iterativ analyse, design, udvikling og implementering, baseret på samarbejde mellem forskere og deltagere i virkelige omgivelser som ledere til kontekstsensitive designprincipper og -teorier"* (Shattuck & Anderson, 2013, s. 187, egen oversættelse). Det karakteristiske for DBR-projekter er, at designprocessen er en formgivningsproces, der er med til at udvikle, afprøve og forbedre designs til læringsmiljøer, som oftest udgøres af designtyperne: uddannelsesdesign, didaktiske design og læringsdesign. Designbegrebet kan defineres som *"en systematisk, planlagt og gennemtænkt kolonisering af tid og rum i et foretagendes tjeneste"* (Christensen, Gynther, & Petersen, 2012, s. 3). Udviklingen af nye designs til

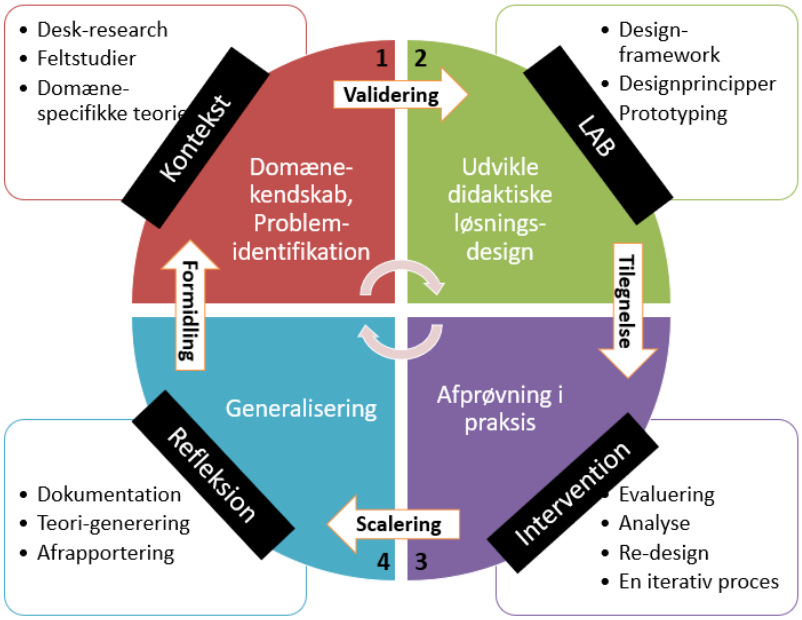
læringsmiljøer, kan på baggrund af denne definering derfor indeholde udvikling af både nye artefakter, men også nye måder at benytte eksisterende artefakter på (Christensen, Gynther, & Petersen, 2012, s. 3-4; Shattuck & Anderson, 2013, s. 187-189).

DBR består af en bred vifte af tilgange, men som har en række fundamentale antagelser til fælles. I DBR-tilgangen har konteksten en betydning for læring, hvilket betyder, at forskningen ikke kan foregå i et isoleret laboratorium. Derfor benyttes der etnografiske metoder i DBR til at fremskaffe domænespecifik viden og samtidig afklare specifikke problemer i en kontekst. Endvidere anvendes etnografiske metoder til at sammenføje og dokumentere anvendelse af et design i praksis. I et DBR-perspektiv er etnografi en forståelsesorienteret forskningstilgang, som ikke har en intention om at ændre eller forbedre praksis, men derimod udvikle og afprøve nye designs i praksis. En anden antagelse indenfor DBR er, at forståelse og forandring er to sider af samme sag, og derfor etableres der ikke et klassisk skel mellem forskning og udvikling, men i stedet er der et skel mellem forskningstilgange som ønsker at forstå et fænomen og forskningstilgange som forsøger at forstå og forbedre et fænomen (Christensen, Gynther, & Petersen, 2012, s. 4).

Til at guide et DBR-projekt er der en række karakteristiske forskningsprincipper. Det første princip er, at DBR er intervenerende i praksis med nye designs, som testes i en konkret praksissituation, og derfor bliver udvikling og afprøvning af prototyper et centralt fokus i DBR-projekter. Det næste princip er, at designprocessen er iterativ, hvilket betyder, at evaluering af et design sker med det formål at forbedre designet. Det tredje princip består i, at DBR er kollaborativ, hvilket betyder, at forskere og praksisdeltagere i samarbejde identificerer problemer og udvikler forslag til innovation af ny praksis. Det fjerde princip omhandler, at DBR er teoriorienteret, hvor DBR-designs er funderet i teoretiske positioner, men hvor afprøvning og test af designet også bidrager til teoriudvikling. Det sidste princip er, at DBR er anvendelsesorienteret og samtidigt er en pragmatisk forskningstilgang (Christensen, Gynther, & Petersen, 2012, s. 5-9).

2.2.1 ELYK-modellen

Ove Christensen, Karsten Gynther og Trine Brun Petersen (2012, s. 10) har i forbindelse med ELYK-projektet udviklet en innovationsmodel ud fra Thomas Reeves' DBR-fasemodel, som er en firefaset forskningsmodel indeholdende følgende faser: problemidentifikation, udvikling af løsningsforslag, iterative forløb og refleksion. ELYK-projektets innovationsmodel er struktureret i fire forskellige typer af forskningsopgaver, som har bestemte mål og specifikke metoder tilknyttet. Modellen er iterativ, men indikerer samtidigt en progression i et DBR-projekt og er illustreret i Figur 2.1 (Christensen, Gynther, & Petersen, 2012, s. 10-11).



Figur 2.1: ELYK innovationsmodel (Christensen, Gynther, & Petersen, 2012, s. 11)

I kontekstfasen starter et DBR-projekt med en kortlægning og analyse af identificerbare problemer i en læringskontekst. I LAB-fasen kombineres domænespecifikke viden med designframework og designprincipper og den første prototype udvikles med udgangspunkt i designmetodologier. I interventionsfasen bliver designet afprøvet i praksis, evalueret, analyseret samt der sker et redesign af designet. I den sidste fase, refleksionsfasen, laves en generalisering af designet, for at afgøre om designet er robust i forhold til forskellige kontekstyper (Christensen, Gynther, & Petersen, 2012, s. 11-14).

I dette speciale er DBR-tilgangen indarbejdet i forhold til arbejdsprocesserne i Hjørring Kommune, og derfor ændres faserne en anelse. Den første fase kaldes stadig kontekst, hvor der også sker en kortlægning samt analyse af problemer (se kapitel 3 *Fase 1 - Domænekendskab*). Den næste fase kaldes i dette projekt udvikling af design, men omhandler det samme som LAB-fasen i innovationsmodellen. Navneændringen er sket, da det for samarbejdspartnere i kommunen var misvisende med overskriften LAB (se kapitel 4 *Fase 2 – Udvikling af design*). Den tredje fase i projektet kaldes afprøvning i praksis. Det sker, da det i forhold til arbejdsprocessen giver mening at adskille afprøvning og evalueringen af designet ad (se kapitel 5 *Fase 3 – Afprøvning i praksis*). Derfor kaldes den sidste fase i dette projekt evaluering. Her vil designet blive evalueret samt analyseret og eventuelle forbedringsprincipper vil blive præsenteret til et fremtidigt redesign (se kapitel 6 *Fase 4 - Evaluering*). Selve generaliseringen sker i diskussionskapitlet (kapitel 7), da der i samarbejdet med kommunen ikke har været fokus på generalisering, og derfor placeres dette uden for de fire faser, der er blevet arbejdet med i samarbejde med kommunen.

2.2.2 Kritisk syn

En udfordring med hensyn til DBR er forskerrollen, som er tosidet, idet DBR-forskeren både er forsker og designer. En DBR-forsker er både interesseret i at udvikle en ny forståelse, men er også involveret i design af en ny praksis eller artefakt, som kan indgå i udviklingen af et nyt didaktisk design. En anden udfordring er problemet omkring generalisering. Det omhandler de nyudviklede didaktiske designs tilpasning til andre kontekster, og ikke kun gælder i den kontekst de er udviklet i. En løsning til denne udvikling kan enten være en meget detaljeret beskrivelse af den kontekst designet er udviklet i eller en opskalering til ny kontekster. Her er det graden om robusthed for designet, og de førnævnte detaljerede beskrivelser, som kan give andre interessenter muligheden for at vurdere designets plausible overførelse til den kontekst interessenterne repræsenterer (Christensen, Gynther, & Petersen, 2012, s. 15-16).

2.3 Deltagerobservation

Metoderne i dette speciale bliver præsenteret løbende gennem de fire faser, hvor de bliver benyttet. Deltagerobservation er dog benyttet gennem hele projektet, idet projektet er praksisnært og tager udgangspunkt i en praktik og efterfølgende ansættelse i Hjørring Kommune, hvor forskellige begivenheder i arbejdsdagen som møder, foredrag, samtaler med mere, samt de daglige oplevelser har været med til at give en bedre forståelse for de sociale fænomener, som har omringet projektet. Metoden, deltagerobservation, forbindes med antropologien som videnskabelig disciplin, hvor forskeren som observatøren deltager i et hverdagsliv, for eksempel på en arbejdsplads, hvor de personer, forskeren studerer er en del af (Justesen & Mik-Meyer, 2010, s. 100; Szulevicz, 2015, s. 81).

I deltaberobservation deltager forskeren under sine observation i de forskellige praksisser, som observation, og metoden kan høre under. Deltagerobservation er sammensat af to modsatrettede begreber: deltagelse, hvor forskeren er aktivt involveret i en praksis, og observation, hvor forskeren betragter en praksis uden at deltage i den. Deltagerobservation indebærer derfor, at forskeren skal udføre begge dele samtidigt (Szulevicz, 2015, s. 83).

2.3.1 Formål med deltagerobservation

Formålet med deltagerobservation er at beskrive og analysere det sociale situerede og partikulære knyttet til menneskelig praksis, men der er flere forskellige mål med metoden. Et mål kan være at åbne feltet op, da forskeren får adgang til den studerede praksis på andre måder end gennem andre kvalitative metoder, og gennem engageret deltagelse kan forskeren opnå en insider-viden om den observerede kultur. Forskeren kan også være interesseret i at opbygge en relation til de observerede deltagere. Et formål med deltagerobservation kan også være at blive i stand til at stille de rigtige spørgsmål, hvor forskeren får et indblik i de normativer og kulturelle koder, der præger fællesskaber, som kan give forskeren større mulighed for at stille de rigtige spørgsmål til deltagerne både gennem deltagerobservationen eller ved interviews. Forskerne kan også have som mål at få en intuitiv forståelse for datamaterialet og et mål kan være at beskrive en praksis. Et sidste formål med

deltagerobservation kan være at indfange og adressere forhold, som er utilgængelige ved hjælp af andre kvalitative metoder, hvor deltagerobservation kan være med til, at forskeren får øje på det ikke-italesatte, det hemmelige, det situerede med videre (Szulevicz, 2015, s. 86-87).

2.3.2 Typer af observationer

Omfanget af forskerens deltagelse i en social praksis benyttes ofte til at skelne mellem forskellige typer af deltagerobservation, hvor forskeren kan bevæge sig fra at være primært observerende til at være fuldt deltagende i de aktiviteter, der observeres. I den forbindelse kan forskeren vælge at indtage forskellige roller; den totale deltager, deltageren som observatør, observatøren som deltager og den totale observatør. Deltageren som observatør er en forsker, der fortæller åbent om sit forskningsprojekt og formål med deltagelsen, og forskeren deltager ikke fuldt ud, men bevarer en distance til praksis. Observatøren som deltager er en forsker, der har kort tid til rådighed og har kun mulighed for at etablere overfladiske relationer til deltagerne, men igen skal forskeren være åben og ærlig omkring undersøgelsen. Forskeren der er observatør som deltager kan risikere at misforstå en række forhold, og metoden bør understøttes af andre metoder (Szulevicz, 2015, s. 83; Justesen & Mik-Meyer, 2010, s. 105).

I dette projekt er det deltageren som observatør, der er den primære rolle. Alle begivenheder bliver ikke gengivet i projektet, og derfor har alle deltagere ikke direkte i forbindelse med begivenheden fået besked om projektet. Ved gengivne begivenheder har deltagerne fået besked om projektet og deres roller heri. Det skal pointeres at ledere og medarbejdere på arbejdspladsen har fået besked om projektet og arbejdspladsens rolle i denne forbindelse ved et personalemøde.

2.3.3 Kritik

Der er undertiden blevet stillet spørgsmål ved nogle af præmisserne, som deltagerobservation foretages på baggrund af. For det første er deltagerobservation tidskrævende, som de færreste forskere har mulighed for at afsætte tid til. Det er ikke muligt at fastsætte, hvor lang tid forskeren skal bruge på deltagerobservation, men tiden kan forkortes ved, at forskeren er inde i de centrale teoretiske diskussioner på feltet, forskeren skal lade sig guide af gode forskningsspørgsmål og kan med fordel benytte en observationsguide til at give retning og fokus til observationerne. Et andet spørgsmål sættes ved metodens manglende legitimitet, som i forhold til deltagerobservation er tæt knyttet til spørgsmål omkring validitet, reliabilitet og generaliserbarhed. I forhold til validering, vil forskeren, der benytter deltagerobservation, udgøre et ekstra medierende led, som filtrerer observationerne, og derfor kan der sættes spørgsmålstegn ved, om den opnåede viden afspejler den observerede virkelighed (Szulevicz, 2015, s. 88-90)

3 Fase 1 – Domænekendskab

Dette kapitel repræsenterer starten af specialets iterationsproces. Den første fase kaldes domænekendskab og er en kortlægning samt analyse af identificerbare problemer i en læringskontekst (Christensen, Gynther, & Petersen, 2012, s. 11). Kapitlet starter med et feltstudie, der identificerer og analysere problemstillinger i forhold til Hjørring Kommunes nuværende risikovurderingsproces, og finder frem til en række forbedringspotentialer. Dernæst er der domænespecifikke teorier, der er med til at identificere, hvordan risikovurderingsdesignet kan leve op til principperne i ISO27001-standarden og samtidigt kortlægger, hvordan risikostyring kan foregå. Her analyseres også, hvordan voksne lærer i arbejdslivet, idet det er interessant i forhold til, at medarbejderne har behov for viden for at kunne udføre en risikovurdering. I afsnit 3.3 *Deskresearch* kortlægges nuværende internationale risikovurderingsmetoder og der gives samtidigt et bud på, hvordan risikovurderingsprocessen kan tilrettelægges og organiseres i Hjørring Kommune. Til sidst vil en række forbedringspotentialer opridses, som er genstand for designprocessen i kapitel 4 *Fase 2 – Udvikling af design*.

3.1 Feltstudie

I dette afsnit belyses underspørgsmål 1: *Hvordan har Hjørring Kommune indtil videre arbejdet med risikovurdering?* gennem et feltstudie.

Feltstudiet udgøres i dette speciale af en praktikrapport udarbejdet i september – december 2018 og bedømt i januar 2019. Praktikrapporten er et casestudie som er motiveret i en undersøgelse fra Danmarks Statistik omkring offentlige ansattes adfærd i forhold til informationssikkerhed og tager afsæt i Hjørring Kommunes håndtering af risikovurderingsprocessen, hvor problemformuleringen lyder således: ”*Hvordan arbejder Hjørring Kommune med risikovurdering som en del af principperne fra den internationale sikkerhedsledelsesstandard ISO27001?”* (Nøhr, 2018, s. 4).

Praktikrapporten undersøger problemet ved at analysere tre aktørers holdning til risikovurdering i Hjørring Kommune. Disse tre aktører er informationssikkerhedsudvalget, informationssikkerhedskoordinatoren og fagsystemsejerne. Til at belyse aktørernes holdning og sammenhængen mellem dem benyttes Engeströms ekspansiv læringsteori, herunder det kollektive aktivitetssystem og de interagerede aktivitetssystemer, som analyseværktøj. Aktørernes holdninger er indsamlet gennem metoderne dokumentanalyse, deltagerobservation og interview. I undersøgelsen bliver det klarlagt, at informationssikkerhedskoordinatoren og fagsystemsejerne har modsigende holdninger til risikovurdering, og gennem interagerende aktivitetssystemer er en række forbedringspotentialer formuleret (Nøhr, 2018, s. 17-24).

Disse forbedringspotentialer er:

- Der skal udvikles og designes en risikovurderingsmetode, som kan fungere som værktøj.
- Fagsystembrugerne skal identificeres.

- Der skal udarbejdes en struktureret og defineret risikovurderingsproces, som kan fungere som holdesnor i arbejdet.
- Fagsystemejerne og fagsystembrugerne skal opnå viden omkring risikovurderingsprocessen. Dette kan eksempelvis ske ved workshops og undervisning.
- Der skal etableres et samarbejde primært mellem informationssikkerhedskoordinatoren på den ene side og fagsystemejerne og fagsystembrugerne på den anden side. Dernæst kan man få informationssikkerhedsudvalget med i det samarbejde. (Nøhr, 2018, s. 24).

De resterende afsnit i dette kapitel vil have forbedringspotentialerne fra praktikrapporten som grundlag for undersøgelsesemnerne.

3.2 Domænespecifikke teorier

I det afsnit belyses underspørgsmål 2: *Hvilke krav er der til risikovurdering i ISO27001-standarden?* og underspørgsmål 3: *Hvordan kan læring foregå på en arbejdsplads?* For at belyse disse to spørgsmål starter afsnittet med en begrebsafklaring af informationssikkerhed og ISO27001-standarden på baggrund af Digitaliseringsstyrelsens vejledninger. Herefter ses på principperne fra ISO27001-standarden i særlig grad i forhold til risikostyring og herunder risikovurdering også på baggrund af Digitaliseringsstyrelsens vejledninger. Til sidst i afsnittet vil voksenlæringsteori blive belyst med udgangspunkt i Illeris' forskning.

3.2.1 Informationssikkerhed og ISO27001

Informationssikkerhed er en betegnelse for foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet og tilgængelighed. Ansvaret for styring af informationssikkerhed i en organisation ligger hos den øverste ledelse, hvilket indebærer ansvaret for at etablere, implementere, vedligeholde og løbende forbedre informationssikkerheden. Ledelsen har samtidigt ansvaret for at fastlægge et passende risiko- og sikkerhedsniveau og afgrænse opgaver samt prioritere ressourcer og sikkerhedsaktiviteter, hvilket stiller krav til, at ledelsen forholder sig til og godkender alle relevante forhold vedrørende informationssikkerhed. Den enkelte organisations indsats på sikkerhedsområdet vurderes med hensyntagen til sikkerhed, brugervenlighed og økonomi, og indsatsen skal være proportionel med truslerne på det konkrete område. Sikkerhedstiltagene bør være pragmatiske og ikke indføres på bekostning af brugeroplevelsen og effektiviteten, således at sikkerhed ikke arbejdes med for enhver pris, og samtidigt vil risici ikke kunne kontrolleres fuldstændigt. (Digitaliseringsstyrelsen, 2015a, s. 5)

I Danmark er den internationale sikkerhedsstandard ISO27001 valgt som standard til at etablere et ledelsessystem for informationssikkerhed, som tager udgangspunkt i en risikobaseret tilgang til styring af informationssikkerhed. ISO27001-standarden er en normativ standard, som indeholder krav til implementering og vedligeholdelse af en informationssikkerhedsledelse (ISMS) og tager udgangspunkt i den enkelte organisations risikoprofil som er baggrunden for en implementering af eksakte sikkerhedsforanstaltninger og kontrolprocedurer,

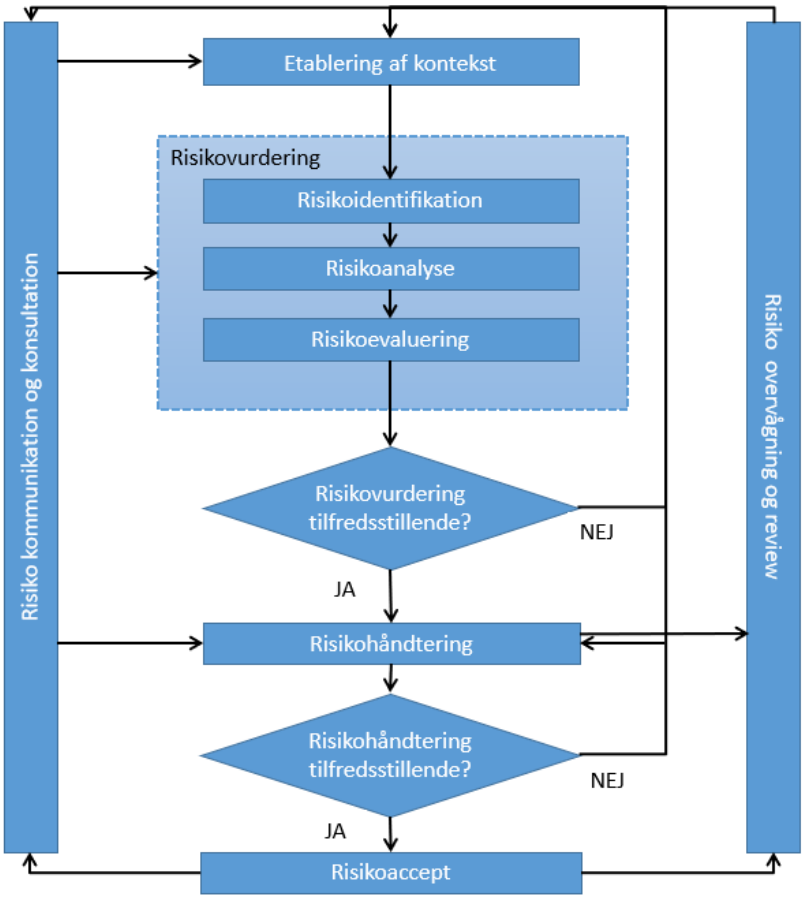
der er passende for den enkelte organisation. ISO27001-standarden stiller krav til at en række styringsaktiviteter er til stede for, at styringen af informationssikkerheden lykkes. Når der er et samspil mellem styringsaktiviteter i en organisation, er det et udtryk for at implementeringen af et fungerende ISMS er opnået. Organisationen skal forstå sine egne informationsaktivers forretningsmæssige betydning, som kan opnås igennem en overordnet vurdering af, hvordan informationsaktivernes risikobillede er påvirket af interne forretningsprocesser og it-systemer, omverdenen og interessenter (Digitaliseringsstyrelsen, u.d.; Digitaliseringsstyrelsen, 2015c, s. 2).

3.2.2 Risikostyring

Som en del af organisationens ledelsessystem for informationssikkerhed skal risici i relation til brud på fortrolighed, integritet og tilgængelighed af data og systemer styres. Alle organisationer står overfor risiko i en eller anden form på daglig basis og ifølge The National Institute of Standards and Technology i USA er risiko den samlede negative påvirkning på grund af udnyttelsen af en sårbarhed, i betragtning af både sandsynligheden og virkningen af forekomsten. I ISO27001-standarden defineres risiko også som kombinationen af sandsynligheden for et tilfælde og dets forekomst. Det er ikke muligt at fjerne alle risici, men potentielt kan de styres ved hjælp af en systematisk tilgang til styringen. Risikostyring er den proces, der gør det muligt for ledere at afbalancere de operationelle og økonomiske omkostninger ved beskyttelsesforanstaltninger og opnå gevinster i opgavekapacitet ved at beskytte it-systemer og data, der understøtter organisationens opgaver. Organisationer udvikler og implementerer risikostyringsstrategier for at reducere negative indvirkninger på organisationen og tilvejebringer et struktureret og konsekvent grundlag for beslutninger om risikoreducerende muligheder. Risikostyring har to faser: risikovurdering og risikohåndtering (Calder & Watkins, 2007; Digitaliseringsstyrelsen, 2015b, s. 2).

Risikostyringsprocessen

Risikostyringsprocessen består af seks hovedaktiviteter, hvoraf tre omhandler risikovurdering, som er illustreret i Figur 3.1. (Digitaliseringsstyrelsen, 2015b, s. 3).



Figur 3.1: Illustration af risikostyringsprocessen (Digitaliseringsstyrelsen, 2015b, s. 3)

Styring af risici er en løbende proces, da en risikovurdering foretages som et øjebliksbillede af situationen på det tidspunkt, hvor vurderingen udarbejdes, men både organisationen, informationsaktiverne, trusler, sårbarheder og lignende konstant ændres (Digitaliseringsstyrelsen, 2015b, s. 6).

Etablering af kontekst

Etableringen af kontekst fastsætter rammerne for risikostyringen, hvor der foretages organisatorisk, fysisk og teknisk afgrænsning af risikostyringens omfang, udpegning af roller og ressourcer, definering af kriterier for risikotolerance og beskrivelse af en risikovurderingsmetode (Digitaliseringsstyrelsen, 2015b, s. 4).

Risikovurdering

Risikovurdering er omdrejningspunktet i risikostyringen og benyttes til at kunne vurdere og håndtere risici og er processen med at identificere trusler og vurdere sandsynligheden for, at disse trusler udgør en organisationsmæssig sårbarhed samt den potentielle virkning af et sådan tilfælde. Den almindelige fremgangsmåde er at tage udgangspunkt i organisationens informationsaktiver og vurdere dem ud fra den vurderede sandsynlighed og konsekvens. Resultatet af risikovurderingen er en prioriteret liste over risici i forhold til foruddefinerede

kriterier. (Calder & Watkins, 2007; Digitaliseringsstyrelsen, 2015a, s. 9; Digitaliseringsstyrelsen, 2015b, s. 4).

Der kan med fordel tages udgangspunkt i organisationens forretningsprocesser, når risici skal identificeres. En gennemgang af processerne kan være med til at skabe et overblik over, hvilke informationsaktiver, der understøtter processerne og deres betydning, hvor det samtidigt er muligt at identificere sammenhænge og afhængigheder mellem informationsaktiverne. Informationsaktiverne bør identificeres på et passende niveau i forhold til organisationens størrelse og det ønskede detaljeringsniveau af risikovurderingen. Risikovurderingen bør ikke kun omfatte it-systemer, men alle informationsaktiver, der indgår i et informationssystem, hvilket inkluderer fysiske informationsaktiver. En forudsætning for at vurdere konsekvenserne for organisationen ved potentielle sikkerhedshændelser, er overblik og kendskab til processerne (Digitaliseringsstyrelsen, 2015b, s. 8-9).

Trusler og sårbarheder

For at man ikke overser risici, er identifikationen af relevante trusler afgørende, hvor en systematisk trusselsvurdering bør ske. Her kan tages udgangspunkt i et katalog over mulige trusler, hvor organisationen kan pejle sig ind på trusler, der er relevante for dens informationsaktiver. En trussel kræver en sårbarhed for at kunne resultere i en risiko og omvendt, hvor sårbarheder kan opstå i flere sammenhænge. En metode til at få afdækket sårbarhederne er ved at gennemgå implementerede kontroller og vurdere deres effektivitet (Digitaliseringsstyrelsen, 2015b, s. 9-10).

Risikohåndtering

Risikohåndtering er processen med at reagere på de identificerede risici. Eventuelle beslutninger og/eller aktioner i lyset af risikovurderingen er taget på baggrund af risikovurderingsprocessen og indgår i risikohåndteringsplanen, som sammen med risikovurderingsprocessen er den anden bestanddel af risikostyringen. Der er fire muligheder for at håndtere risici. Den første er, at acceptere risikoen og ikke foretage yderligere. Anden mulighed er, at overføre risikoen til en tredjepart for eksempel gennem forsikring, outsourcing eller lignende. Den tredje mulighed er at undgå risikoen ved at stoppe eller ændre den aktivitet, som er årsag til risikoen. Den sidste mulighed er at kontrollere risikoen ved at indføre foranstaltninger, som fjerner eller reducerer sandsynligheden eller konsekvenserne. Udvælgelsen af kontroller til reducering af risici, skal ske ud fra en cost/benefit-vurdering således, at kontrollernes effekt på risikoen vurderes i forhold til omkostningerne. I ISO27001-standarden er en kontrol defineret som en foranstaltning, som ændrer risikoen og omfatter enhver proces, politik, praksis eller andre handlinger. Efterfølgende udarbejdes en plan for, hvordan de identificerede risici skal håndteres (Calder & Watkins, 2007; Digitaliseringsstyrelsen, 2015a, s. 9; Digitaliseringsstyrelsen, 2015b, s. 5).

Opfølgning på risici

Der bør løbende foretages opfølgning på risici, hvor det bør sikres, at de indførte kontroller og tiltag bliver implementeret og fungerer efter hensigten. Derudover bør der løbende følges op på forudsætninger, som ligger

til grund for risikovurderingen, da informationsaktiver, trusler, sårbarheder og konsekvenser kan hurtigt ændres og medfører tilsvarende ændringer i risikobilledet. Organisationens risikostyring bør sikre, at der sker en struktureret løbende opfølgning på risici (Digitaliseringsstyrelsen, 2015b, s. 6).

Kommunikation om risici

Risikostyring er en tværorganisatorisk proces, hvor der indgår flere interessenter med forskellige opgaver og ansvarsområder, derfor er kommunikation en central del af risikostyringen. Informationssikkerhedsudvalget og informationssikkerhedskoordinatoren har det praktiske ansvar for risikovurderingen, hvor linjeledelsen har ansvaret for risici inden for eget område. Derfor skal en fælles opfattelse og tilgang til risikovurderingen sikres, og dermed skal kommunikationen planlægges, så der er en ensartet tilgang og fælles forståelse af processen (Digitaliseringsstyrelsen, 2015b, s. 6).

3.2.3 Voksenlæring

Ifølge Illeris omfatter læring samspillet mellem individet og omgivelserne, hvilket gør, at der må være afgørende aldersbetingede forskelle idet samspillet er af forskellige karakter i forskellige faser af livsforløbet, men der er også forskelle i den kognitive og den psykodynamiske dimension. Læringsmæssigt har det at være voksen betydningen af, at individet tager ansvar for sin egen læring, hvilket vil sige, at individet bevidst eller mindre bevidst er selektiv og tager stilling til hvad individet vil lære og ikke vil lære. Læring med voksne deltagere har et godt forløb, hvis de voksne selv tager et afgørende medansvar, hvilket forudsætter, at læringssituationens rammer skaber muligheden for det. Dette betyder, at læreren skal give plads til medansvaret og indholdsmæssigt skal forløbet være tilrettelagt, så der grundlæggende er mulighed for at de voksne deltagere lære noget som de selv føler er vigtigt og meningsfuldt. Generelt er voksnes læring karakteriseret ved at voksne lærer det de vil lære, det der er meningsfuld for dem at lære, voksne trækker i deres læring på de ressourcer de har og voksne tager det ansvar for deres læring de er interesserede i at tage (Illeris, 2003, s. 97-101).

En stor udfordring er, hvor læringssituationen skal placeres. Ifølge Illeris, er der tre centralt placerede parter, som har en interesse i, at væsentlige elementer af læring og uddannelse flyttes fra institutionerne til arbejdspladsen. Den første part er organisationen, der ved at flytte læringen til arbejdspladsen, vil kunne sikre sig, at medarbejderne lærer det de har brug for set fra ledernes perspektiv og dermed undgår at bruge tid på læring, der fra dette perspektiv er unødvendigt. Den anden part er deltagerne, som vil kunne undgå følelsen af at være på skolebænken igen, da læring i arbejdslivet ikke opleves som umyndiggørelse. Det gøres synligt for deltageren, hvad læringen skal bruges til og deltageren bliver ikke opfattet som en elev, men som en medarbejder, der bliver opkvalificeret. Den tredje part er staten, som kan have en interesse i, at en masse uddannelsesudgifter på denne måde kan overflyttes fra den offentlige til den privat økonomi. Foregår læringen i arbejdslivet og på organisationens præmisser, vil det som arbejdsgiverne opfatter som en hensigtsmæssig målrettethed kunne forvandles til en snæverhed i kvalificeringen, der forfølger kortsigtede organisationsnære mål. Dette kan resultere i en forsømmelse af en alsidig, bredt orienteret og teoretisk kvalificeret kompetenceudvikling, som er i

deltagernes, samfundets og organisationernes fælles langsigtede interesse. Der er samtidigt en risiko for, at kun få, og muligt også de i forvejen bedst kvalificerede grupper af medarbejdere, vil få del i kompetenceudviklingen, da organisationerne kan mene, at disse medarbejdere vil få det største og hurtigste afkast af uddannelsesinvesteringerne. Et andet problem kan være et pladsproblem, hvilket kan med det overstående kvalificeringsproblem sammenlagt udgøre et praktisk og økonomisk problem. Skal en afgørende større del af kompetenceudviklingen finde sted i arbejdslivets regi, er der behov for en dybdegående ændring i organisationernes holdninger til at gå ind i læringsarbejdet på en kvalificeret, imødekommende og ansvarlig måde samt bidrage med menneskelige, materielle og økonomiske ressourcer i et andet omfang end tidligere (Illeris, 2003, s. 122-123).

Læring i arbejdslivet

Det er et vigtigt udgangspunkt for læring i arbejdslivet, at det medfører i en eller anden grad en ekstra belastning af arbejdspladserne og medarbejderne, hvis denne læring skal kvalitativ og kvantitativ række ud over den almindelige og tilfældige læring. Her kan det give mening at fokusere på tilpasnings- og udviklingsorienteret læring (Illeris & Samarbejdspartnere, 2004, s. 202).

Tilpasningsorienteret læring indebærer, at individet eller gruppen lærer noget med udgangspunkt i givne opgaver, mål og forudsætninger uden at rette spørgsmål til eller forsøge at ændre opgaven. Tilpasningsorienteret læring tilsigter, at der kan udføres arbejdsopgaver, som vedrører en del eller en komponent i en større sammenhæng samt kan løse problemer af en type som kendes i forvejen. Udviklingsorienteret læring indebærer, at individet lærer at formulere problemer og ikke kun at løse givne problemer. Den tilpasningsorienteret læring er dominerende, hvis arbejdet følger produktionens logik, hvor hovedvægten lægges på effektiv handling på et rutine- eller regelbaseret handlingsniveau, problemløsning gennem tilpasning af givne regler eller instruktioner, ensartethed og sædvanlige tænkemåder, stabilitet samt sikkerhed, læring der tilsigter bemestring af procedurer og rutiner (Illeris & Samarbejdspartnere, 2004, s. 203-204).

Udviklingsorienteret læring tilsigter, at der kan udføres arbejdsopgaver, som vedrører en helhed eller et system, formulere problemer og analysere hvordan de opstår, hvordan de behandles eller løses, at der kan foregå en kritisk bedømmelse af måleværdier og disse kan behandles hensigtsmæssigt samt der kan tages ansvar for større områder eller processer. Den udviklingsorienterede læring er dominerende, hvis arbejdet følger udviklingens logik, hvor hovedvægten lægges på tankevirksomhed og refleksion, alternativ tænkning, eksperimenter og risikotagning, tolerance i forhold til forskellighed og usikkerhed samt fejlhandlinger (Illeris & Samarbejdspartnere, 2004, s. 203-204).

Hovedpointen er en hensigtsmæssig og tidssvarende læring i arbejdslivet må omfatte både tilpasningsorienterede og udviklingsorienterede forløb, hvorimod hvis der er kun er tale om tilpasningsorienteret læring, bliver arbejdet rutinemæssigt, og hvis der kun er tale om udviklingsorienterede forløb, kan det blive for krævende og uden stabilitet og forankring. Denne balance skal etableres mellem to forskellige logikker: den tendentielt

kortsigtede produktionslog, der har fokus på effektivitet samt minimering af tidsforbruget, og den tendentielt langsigtede udviklingslogik med fokus på fortsat konkurrencedygtighed og dermed stadig videreudvikling af både produkter, processer og medarbejdernes kompetencer, hvilket umiddelbart indebærer et krav om et ikke-produktionsrettet tidsforbrug. Den optimale balance skal etableres på basis af et konflikterende forhold, der tilspidses omkring tidsforbruget, men i høj grad samtidigt vedrører forbruget og orienteringen af menneskelige og andre ressourcer, hvor der i praksis-situationer vil være en tendens til at produktionens logik vil presse sig igennem. Derfor skal der fastholdes en vilje og opmærksomhed, som kan sikre, at den udviklingsorienterede og mere langsigtede logik ikke skubbes i baggrunden (Illeris & Samarbejdspartnere, 2004, s. 205).

3.3 Deskresearch

Dette afsnit er delt op i to dele. Den første del er en kortlægning af andre risikovurderingsmetoder og -værktøjer med udgangspunkt i Alan Calder og Steve Watkins forskning i organisationers implementering af ISO27001-standardens principper. Den anden del tager fat på forbedringspotentialepunktet fra feltstudiet: *Der skal udarbejdes en struktureret og defineret risikovurderingsproces, som kan fungere som holdesnor i arbejdet.* Det gøres med udgangspunkt i vejledningerne fra Digitaliseringsstyrelsen samt metoden deltagerobservation er benyttet til at indsamle empiri og information, der analyseres i forhold til en Plan-Do-Check-Act-model, der forklares i afsnit 3.3.2 *Organisering af informationssikkerhedsarbejdet*.

3.3.1 Risikovurderingsmetoder

Risikovurdering kan oftest deles op kvantitative og kvalitative vurderinger. Den største fordel ved kvalitative risikovurderinger er, at risiciene prioriteres og samtidigt identificeres områder til øjeblikkelig forbedring af håndtering af sårbarhederne. Ulempen ved den kvalitative vurdering er, at den ikke giver specifikke kvantificerbare målinger af størrelsen af virkningerne således, at for eksempelvis en cost-benefit-analyse af eventuelle anbefalede kontroller kan benyttes. Den største fordel ved en kvantitativ risikovurdering er, at den giver en måling af størrelsen af virkninger, der kan anvendes i en cost-benefit-analyse af anbefalede kontroller. Til gengæld er konsekvenser, hvor det er vanskeligt at kvantificere meningsfuldt såsom tab af omdømme, tab af troværdighed, tab af offentlighedens tillid med mere. Den måde til at udgå dette er at anvende kvalitative foranstaltninger så som ”høj” eller ”meget høj” uden at kunne kvantificere betydningen af udtrykket. Den yderligere ulempe ved kvantitative vurderinger er, at afhængigheden af de numeriske områder, der kan benyttes til at beskrive virkningerne, kan være uklare i forhold til betydningen af vurderingen, hvilket kan resultere i, at resultatet skal fortolkes på en kvalitativ måde (Calder & Watkins, 2007).

Kvantitativ risikovurdering

Den kvantitative risikovurderings fremgangsmåde består af to vurderingselementer: et for sandsynligheden for en hændelse, og det andet elementer er det sandsynlige tab, hvis en hændelse skulle opstå. Vurderingen opstår ved at multiplicere det potentielle tab med sandsynligheden, hvilket kaldes den ”årlige tabsforventning” eller den ”anslåede årlige omkostning”. Jo højere antal gange et tilfælde eller risiko er sket, des mere seriøs er det

for organisationen. Det er herefter muligt at rangordne risici ud fra den årlige tabsforventning og derefter træffe beslutninger baseret på dette (Calder & Watkins, 2007).

Problemet med den type risikovurdering er, at der kan gå lang tid med at producere et element, og derefter revidere tallene i lyset af sammenligning med andre aktiver, trusler og sårbarheder, at der ikke gøres nogen fremskridt mod den faktiske implementering af ISMS. I nogle tilfælde kan denne tilgang fremme eller reflektere selvtilfredshed kontra den reelle betydning af særlige risici. Den potentielle tabs monetære værdi vurderes ofte subjektivt, altså den bruger kvalitative data, og når de to komponenter multipliceres sammen, er resultatet ligeså subjektivt. En metode til risikovurdering, som giver resultater, der i høj grad er afhængige af subjektive, individuelle beslutninger, som næppe ligner en anden persons beslutninger, er ikke en, der vil give resultater, som er reproducerbare og sammenlignelige, og det vil mislykkes at implementere kravene i ISO27001-standarden. Desuden skal kontrol og modforanstaltninger ofte tackle en række potentielle hændelser, og begivenhederne selv er ofte indbyrdes forbundne. En detaljeret placering på baggrund af den årlige tabsforventning kan gøre det vanskeligt at identificere disse sammenhænge og kan føre til dårlige beslutninger om kontroller, og denne fremgangsmåde anbefales derfor ikke. Ikke desto mindre anerkendes det, at en række organisationer med succes har valgt en kvantitativ risikovurderingsmetode (Calder & Watkins, 2007).

Kvalitativ risikovurdering – ISO27001 fremgangsmåde

En kvalitativ risikovurdering tager udgangspunkt i ISO17799-standarden, som giver vejledning om, at risikovurderingsmetoden skal gøre det muligt for organisationen at estimere omfanget af sikkerhedsrisici og bruge disse oplysninger til at træffe beslutninger om forholdsmæssige sikkerhedskontrol. Estimering og forholdsmæssigt er to principper, der danner basis for en kvalitativ risikovurderingsmetode, der ikke kræver en nøjagtigt beregnet årlig tabsforventning. En kvalitativ metode rangerer identificerede risici i forhold til hinanden ved hjælp af en kvalitativ eller hierarkisk skala som f.eks. går fra *meget seriøs* til *ikke et problem*. Vurdering af alvorlighed og sårbarhed samt sandsynlighed og indflydelse er også baseret på lignende kvalitative hierarkier (Calder & Watkins, 2007).

En af nøglebegreberne i forhold til kvalitativ risikovurdering er, at aktiver skal værdiansættes for at tage hensyn til de identificerede retslige og erhvervsmæssige samt konsekvenserne omkring tab af fortrolighed, integritet og tilgængelighed. En måde at udtrykke aktivværdier på er at bruge forretningsmæssige virkninger som uønskede hændelser, der kan være offentliggørelse, ændring, manglende tilgængelighed og/eller ødelæggelse, vil have på informationsaktiver og de forretningsmæssige interessenter, der vil være direkte eller indirekte beskadiget. Endelig identificeres de effektværdier, der udtrykker de potentielle forretningseffekter, hvis fortroligheden, integriteten eller tilgængeligheden eller enhver anden vigtig egenskab af aktiver er beskadige. Det foreslås, at en standardværdi for et informationsaktivs værdiansættelse skal defineres for informationsaktiver for at hjælpe informationsaktivejere med en korrekt vurdering af informationsaktiver (Calder & Watkins, 2007).

En kvalitativ metode er den mest udbredte tilgang til risikovurdering, og den opfylder kravene i ISO27001-standarden. Risikoniveauet er baseret på båndværdier eller niveauer for sandsynlighed og påvirkning, således at nøjagtige beregninger ikke er nødvendige. For at sikre, at resultaterne er sammenlignelige og reproducerbare, skal båndene defineres således, at et mellemstød i en persons vurdering kan påvises som sammenlignelig med en mellemfælg i en andens. Resultatet af risikoen vil også være kvalitativt. En af de vigtigste og praktiske fordele ved en kvalitativ risikovurderingsmetode er, at den erkender, at der uundgåeligt er et subjektivt aspekt ved enhver risikovurdering, og det opsætter en ramme for, hvordan sådanne vurderinger kan give sammenlignelige og reproducerbare resultater. Der er også mulighed for at gennemføre den indledende risikovurdering inden for en rimelig tidsperiode, og acceptere, at det ved vurderingen og kontrollen af risikoen er at fortrække at være omtrent korrekt, snarere end netop forkert (Calder & Watkins, 2007).

Andre risikovurderingsmetoder

CRAMM

Det britiske statslige agentur Central Computer and Telecommunications Agency har udviklet metoden Risk Analysis and Management Method (CRAMM) som stammer fra 1985. CRAMM følger tre trin, der indebærer en informationsaktivs identifikation og værdiansættelse, trussel- og sårbarhedsvurdering samt valg af modforanstaltning og henstilling. Denne metode anvender en kvalitativ risikovurdering på et enkelt informationsaktivniveau, og vurderer informationsaktiver primært i forhold til den effekt, der vil opstå på baggrund af brud på fortrolighed, integritet og tilgængelighed. CRAMM-metoden er i overensstemmelse med kravene i ISO27001-standarden, men metoden gennemføres primært ved brug af CRAMM-værktøjer (Calder & Watkins, 2007).

OCTAVE

Kriteriet Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) er udviklet af Carnegie Mellon University, og er et sæt kriterier, der kan udvikles til mange metoder, som både kan være kvantitative og kvalitative metoder. OCTAVE-kriterierne består af et sæt principper, attributter og udfald, og omfatter selvreguleringsprincippet, ved hjælp af et tværfagligt team, og udfaldet vedrører tre faser af vurderingen. For at anvende OCTAVE arbejder et lille team, kendt som analyseteamet, fra hele organisationen sammen for at overveje organisationens sikkerhedsbehov og samtidig afbalancere operationel risiko, sikkerhedspraksis og teknologi. OCTAVE har alle aspekter af risiko i beslutningsprocessen, hvilket vil sige, at det omfatter informationsaktiver, trusler, sårbarheder og organisatorisk indvirkning i processen. OCTAVE bruger en trefaset tilgang, der gør det muligt for analyseteamet, at udarbejde et omfattende billede af organisationens informationssikkerhedsbehov. I den første fase bestemmer analyseteamet, hvilke informationsrelaterede aktiver der er vigtige for organisationen og identificerer de kontroller, der for øjeblikket er på plads for at beskytte disse informationsaktiver. Derefter identificerer teamet trusler mod hver af disse informationsaktiver, hvilket skaber en trusselsprofil for det pågældende informationsaktiv. ISO27001-standarden kræver derimod inddragelse af

individuelle informationsaktivejere og forventer, at alle informationsaktiver vil blive inkluderet. I fase to undersøger analyseteamet netværksadgangsstier, identificerer klasser af informationsteknologikomponenter relateret til ethvert kritisk informationsaktiv og bestemmer derefter, i hvilket omfang hver klasse af komponent er modstandsdygtig over for netværksangreb. ISO27001-standarden søger i sammenligning alle potentielle sårbarheder, herunder fysiske, der skal identificeres. I den sidste fase identificerer analyseteamet risici for de identificerede kritiske informationsaktiver og beslutter, hvad de skal gøre ved dem, og skaber planer for at imødegå risiciene for informationsaktiverne, baseret på fase 1 og 2-analysen (Calder & Watkins, 2007).

IRAM, SARA og SPRINT

Informationssikkerhedsforummet (The Information Security Forum, ISF) er en privat organisation med omtrent 260 medlemmer over hele verden, men som kun er for disse medlemmer. Forummet har udviklet et sæt metoder og værktøjer, som kun er tilgængelige for medlemmerne, og disse omfatter værktøjer til gennemførelse af informationssikkerhedsvurderinger. Disse værktøjer er til designet til at blive anvendt komplementært. Det første værktøj er til selve analysemetoden og kaldes ”Information Risk Analysis Methodologies” (IRAM). ”Simple to Apply Risk Analysis” (SARA) er et værktøj, der er primært rettet mod risiko i forretningskritiske systemer. Værktøjet ”Simplified Process for Risk Identification” (SPRINT) er primært rettet mod vigtige, men ikke kritiske it-systemer. ISF-værktøjssættet understøtter alle de grundlæggende risikostyringsfaser og har mange komponenter, som kan være nyttige i en ISO27001-risikovurdering. Fokus er imidlertid på forretningssystemer, ikke på individuelle informationsaktiver, og derfor skal ISF-værktøjerne tilpasses ISO27001-standardens informationsaktivbaseret risikovurdering. Værktøjerne er ikke offentlig tilgængelige, og derfor er der ikke stor sandsynlighed for, at de fleste organisationer vil benytte dem (Calder & Watkins, 2007).

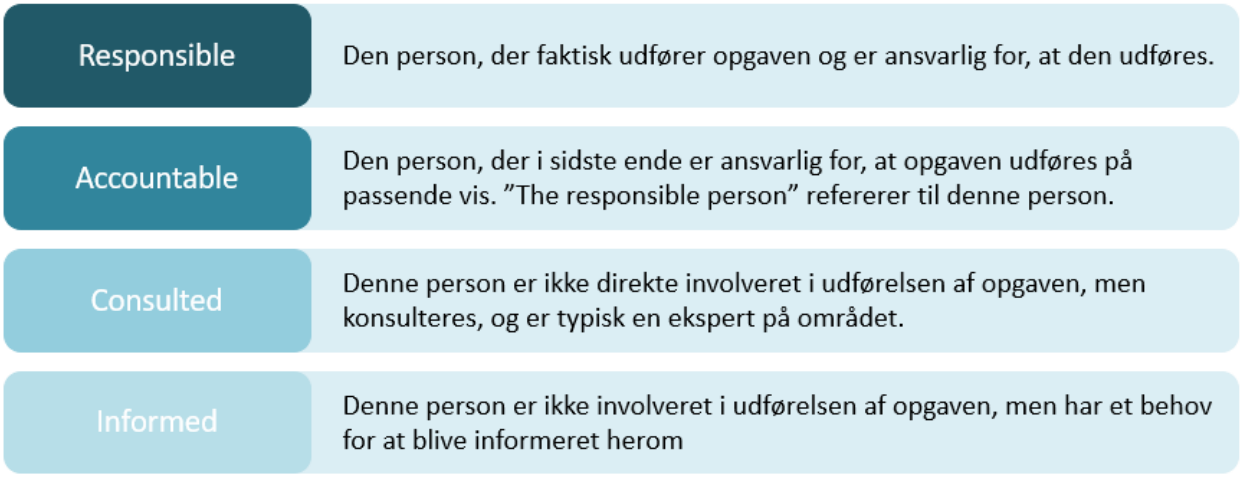
3.3.2 Organisering af informationssikkerhedsarbejdet

I forhold til informationssikkerhedsarbejdet, er det vigtigt, at det planlægges, således at roller og ansvar for gennemførelse af de planlagte og ikke-planlagte aktiviteter er fordelt, for at sikre, at de rette instrumenter til styring er til stede (Digitaliseringsstyrelsen, 2016, s. 3).

Organisering

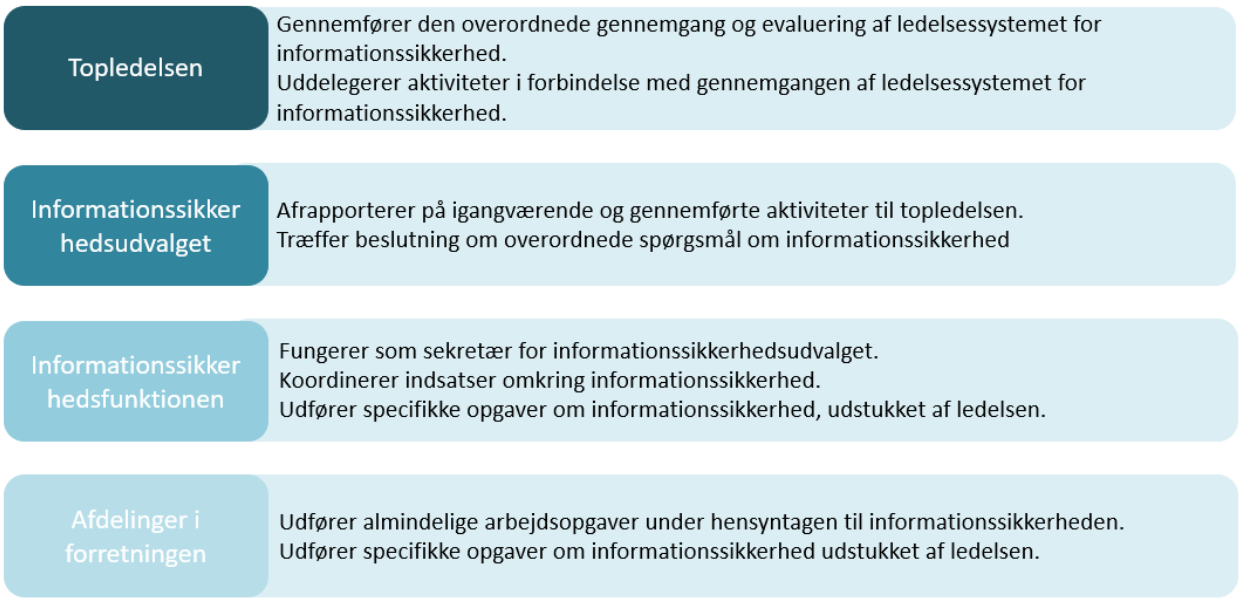
I det daglige er det informationssikkerhedsudvalget, som varetager den ledelsesmæssige opgave i forhold til at drive og vedligeholde informationssikkerhedsarbejdet. Dette udvalg bør arbejde ud fra et dokumenteret og godkendt kommissorium og sammensætningen af udvalget skal overvejes nøje, således at organisationen er godt repræsenteret, samtidig skal de nødvendige kompetencer til at løse informationssikkerhedsopgaver være til stede. Imedens kan organisationen overveje, om en af direktørerne skal indgå i udvalget for at skabe en ledelsesforankring på højt niveau i organisationen. Organisationens informationssikkerhedsfunktionen behandler input til og output fra informationssikkerhedsudvalget, og har til opgave at drive planlagte aktiviteter og fungerer også som sekretær i informationssikkerhedsudvalget. For at skabe en forståelse omkring, hvem

der har hvilke roller og ansvar i en organisering af informationssikkerheden, skal det defineres, hvem der gør hvad, som kan illustreres ved hjælp af RACI-modellen som i Figur 3.2 (Digitaliseringsstyrelsen, 2016, s. 5).



Figur 3.2: RACI-modellen (Digitaliseringsstyrelsen, 2016, s. 5)

Organisationens ledelsesmæssige lag behandler og afklarer overordnede spørgsmål om informationssikkerheden, hvor de underliggende lag håndterer konkrete aktiviteter på baggrund af ledelsens beslutninger, således er det ikke informationssikkerhedsfunktionen, som alene udfører det praktiske arbejde. Informationssikkerhedsarbejdet er en tværgående disciplin, der involverer alle funktioner, der har kontakt med organisationens informationer, som er illustreret af en udbygning af RACI-modellen i Figur 3.3. (Digitaliseringsstyrelsen, 2016, s. 6)



Figur 3.3: Organisatorisk RACI-model (Digitaliseringsstyrelsen, 2016, s. 6)

Medarbejderne i organisationen skal derudover uddannes og vejledes i regler generelt for informationssikkerhed i organisationen og hvilke regler, der gælder for deres specifikke arbejdsområder. Medarbejderne skal være vidende om, hvordan de observerer og håndterer brud på informationssikkerheden og om nye relevante regler og tiltag (Digitaliseringsstyrelsen, 2016, s. 7).

Aktiviteter i et ledelsessystem for informationssikkerhed

I planlægningen af informationssikkerhedsarbejdet er de centrale elementer i ledelsessystem for informationssikkerhed, at ledelsen bliver i stand til at styre håndteringen af forskellige typer af afvigelser, korrigerende handlinger, opfølgning og løbende forbedringer. En forudsætning herfor er en organisering af informationssikkerhedsarbejdet, hvor der tages højde for den kontekst, organisationen befinder sig i og en styring af både tilbagevendende og enkeltstående aktiviteter. Alle funktioner, der arbejder med informationer, i organisationen inddrages i et ledelsessystem for informationssikkerhed. Disse funktioner bidrager med input vedrørende afvigelser til informationssikkerhedsudvalgets arbejde, løser opgaver og hjælper med opgaver. Derfor kan funktioner i organisationen have forskellige roller i forhold til RACI-modellen, alt afhængig af situationen, hvorimod informationssikkerhedsudvalget og topledelsens roller er mere konstante (Digitaliseringsstyrelsen, 2016, s. 8).

Organisering af risikovurderingsarbejdet i Hjørring Kommune

I Hjørring kommune udgør byrådet topledelsen, som udvælger databeskyttelsesrådgiver og godkender informationssikkerhedspolitikken. Dernæst er der informationssikkerhedsudvalget, som består af repræsentanter fra forvaltningsområder, som primært er kontorchefer, informationssikkerhedskoordinatoren, IT-driftschefen samt en formand for udvalget. Informationssikkerhedsudvalget uddelegerer opgaver i forbindelse med risikovurderingen til informationssikkerhedsfunktionen og godkender den overordnet risikovurdering, samt bestemmer hvorledes risici skal håndteres, det vil sige, om risikoen skal accepteres, flyttes, undgås eller kontrolleres, samt hvilke kontroller, som skal implementeres. Informationssikkerhedsfunktionen består i skrivende stund af informationssikkerhedskoordinatoren samt to medarbejdere (hvoraf den ene er forfatteren af dette speciale). Alle medarbejdere i informationssikkerhedsfunktionen arbejder deltids med informationssikkerhed, hvilket vil sige, at medarbejderne også arbejder med andre ikke informationssikkerhedsrelateret arbejdsopgaver. Informationssikkerhedsfunktionen organiserer risikovurdering, udvikler risikostyringsværktøj, underviser fagsystemejere og -brugere i risikovurdering, og behandler den indsendte risikovurdering, samt giver forslag til håndtering af risici til informationssikkerhedsudvalget. Fagsystemejere er kontorchefer på forvaltningsniveau, og er derfor også medlem af informationssikkerhedsudvalget. Fagsystemejerne har det overordnet ansvar for, at der foretages en risikovurdering på de fagsystemer de ejere, og samtidigt udpeger de fagsystembrugerne, som benytte fagsystemerne i sådan en grad, at de vurderes til at kunne foretage en solid risikovurdering af de specifikke fagsystemer. Fagsystembrugerne sidder i forskellige afdelinger i kommunen og arbejder med vidt forskellige arbejdsopgaver og har forskellige uddannelsesniveau samt kompetencer. Fagsystembrugerne skal

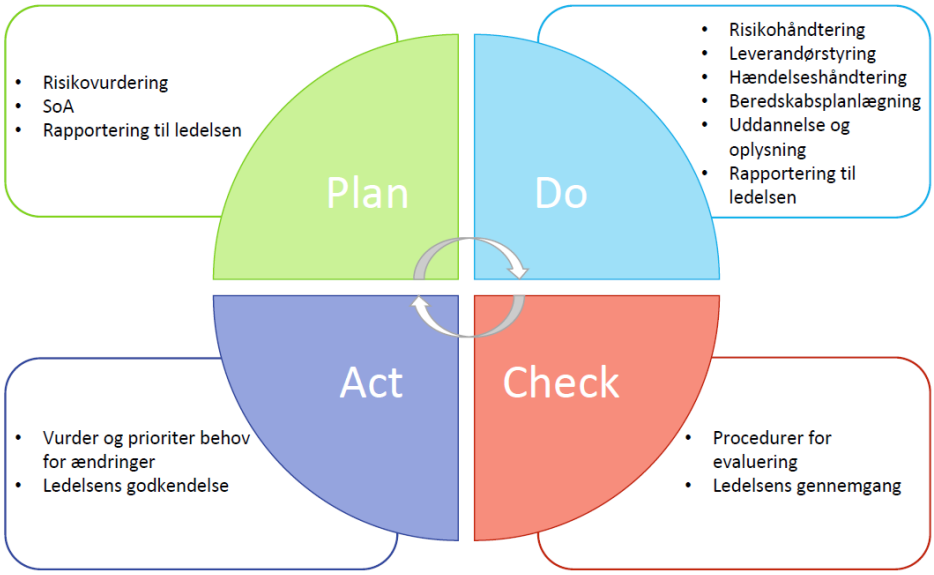
foretage risikovurdering af deres specifikke fagsystem, med vejledning og hjælp fra informationssikkerheds-funktionen. Rollerne i Hjørring Kommunes organisering af risikovurderingsarbejdet i forhold til den førom-talte RACI-model er illustreret i Tabel 3.1.

	Responsible	Accountable	Consulted	Informed
Byrådet				X
Informationssikkerhedsudvalget		X		
Informationssikkerhedsfunktionen	X		X	
Fagsystemejere	X	X		X
Fagsystembruger	X			X

Tabel 3.1: Roller i Hjørring Kommunes organisering af risikovurdering i relation til RACI-modellen. Inspireret af Digitaliseringsstyrelsen, 2016, s. 8.

Planlægning af risikovurdering i Hjørring Kommune

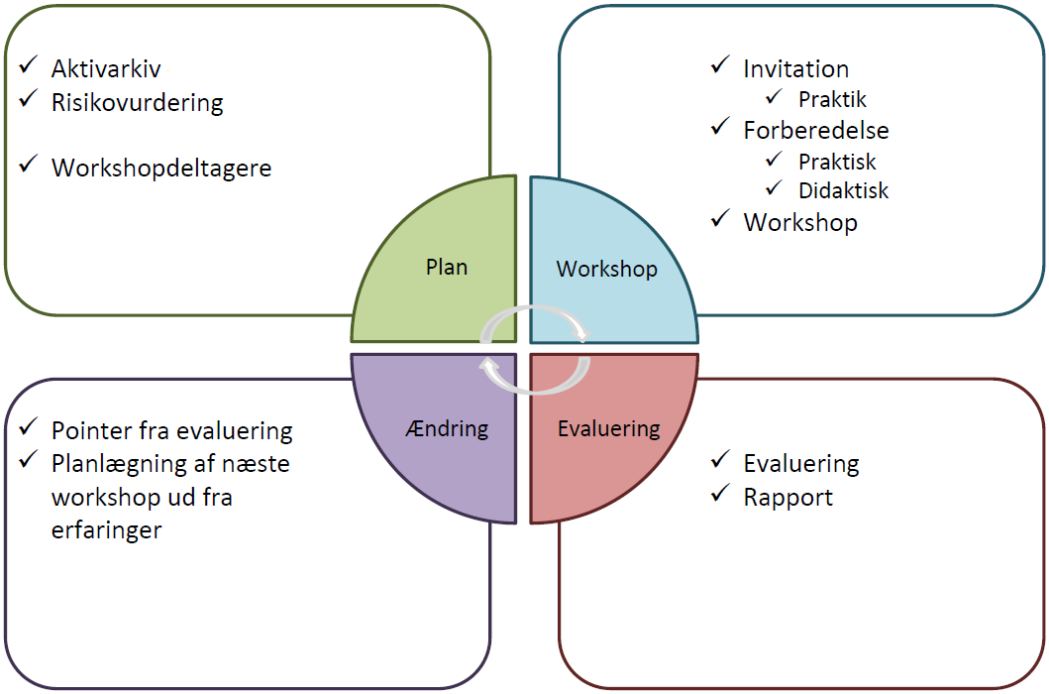
Risikovurdering er en iterativ proces, idet selve risikovurderingen skal ske én gang årligt, idet risici vil forandre sig over tid. Derfor er der i planlægning af risikovurdering behov for en model, der illustrerer denne proces. Den model, der er valgt i Hjørring Kommune er Plan-Do-Check-Act, som er en procesmodel, som illustrerer fire faser i forbindelse med informationssikkerhedsarbejdet. Den første fase er planlægningsfasen, hvor en række arbejdsopgaver skal udføres, herunder risikovurdering, således at vigtige og prioriteret arbejdsopgaver kan planlægges i det videre forløb. Den anden fase er udførelsesfasen, hvor prioriteret risikohåndteringskon-troller implementeres i organisationen, her vil man bl.a. benytte sig af awareness, som indeholder undervisning i og oplysning om kontrollerne. Den næste fase er evalueringsfasen, hvor de implementeret kontrollers effekt evalueres, og samtidig skal der foregå en intern audit, som skal evaluere på informationsledelsessystemets håndtering af risikostyringen. I den sidste fase skabes forandring på baggrund af evalueringen, hvor der vil være fokus på selve ledelsessystemets arbejde med informationssikkerhed (Digitaliseringsstyrelsen, 2015b). Plan-Do-Check-Act-modellen for Hjørring Kommunes informationssikkerhedsarbejdet er illustreret i Figur 3.4.



Figur 3.4: Plan-Do-Check-Act-model for informationssikkerhedsarbejdet i Hjørring Kommune

Som det fremgår af Figur 3.4 skal ledelsen rapporteres til, gennemgå og godkende de forskellige faser. Her vil det primært være informationssikkerhedsudvalget, som påtager denne opgave, hvorimod det er informationssikkerhedsfunktionens opgave at organisere og planlægge aktiviteterne, primært i fase et og to. Denne proces vil omtrent vare et år, da risikovurdering er en årlig begivenhed (Digitaliseringsstyrelsen, 2015b).

Risikovurdering er, som det fremgår i Figur 3.4, essentiel i forhold i informationssikkerhedsarbejdet, idet det er en del af planlægningsfasen, og de øvrige informationssikkerhedsaktiviteter vil tage udgangspunkt i risikovurderingen. Derfor er der også skabt en Plan-Do-Check-Act-model for risikovurdering i den første iteration, hvilket vil sige den iteration, hvor metoden og tankerne bag vil blive efterprøvet samt risikostyringsværktøjets første prototype bliver skabt. Plan-Do-Check-Act-modellen for risikovurdering er illustreret i Figur 3.5.



Figur 3.5: Plan-Do-Check-Act-model for risikovurdering iteration 1

Det fremgår af Figur 3.5, at modellen har ændret sig fra modellen i Figur 3.4. Dette gøres for at specificere de forskellige faser i forbindelses med risikovurderingen. Den første fase er planlægningsfasen, hvor der skabes et informationsaktivarkiv og et risikovurderingsark i risikostyringsværktøjet, for at prioritere, hvilke fagsystemer, der skal være en del af den første risikovurderingsiteration (hvilket kan læses mere om i kapitel 4 *Fase 2 – Udvikling af design*). Fagsystemerne er valgt på forhånd af informationssikkerhedsudvalget. Når fagsystemerne er prioriteret, kan workshopsdeltagerne identificeres. Workshopsdeltagerne består af fagsystemejere og fagsystembrugerne. Fagsystemejerne identificeres ved hjælp af Hjørring Kommunes KITOS-arkiv, som er en oversigt over fagsystemerne i kommunen. Derefter udvælger fagsystemejerne fagsystembrugerne, baseret på en vurdering af fagsystembrugerens kendskab til fagsystemet, f.eks. kan fagsystembrugerne være en superbruger, eller en medarbejder, der bruger fagsystemet til flere arbejdsopgaver. I workshopfasen udsendes en invitation til fagsystemejerne og -brugerne, og herefter planlægges en workshop, hvor til sidst workshoppen afholdes (der kan læses mere om workshoppen i kapitel 5 *Fase 3 – Afprøvning i praksis*). I evalueringsfasen evalueres workshoppen både internt i informationssikkerhedsfunktionen, men også med inddragelse af workshopsdeltagerne (læs mere herom i kapitel 6 *Fase 4 - Evaluering*) og der udarbejdes en rapport til intern brug i næste iteration. I den sidste fase, identificeres forbedringer til næste iteration, hvilket kan læses mere om i kapitel 6 *Fase 4 - Evaluering*.

3.4 Forbedringspotentiale

Med udgangspunkt i dette kapitel, er der en række forbedringspotentialer der skal tages med i overvejelsen i design- og afprøvningsfasen:

1. Der skal udvikles en risikovurderingsmetode, der kan benyttes af både informationssikkerhedsfunktionen og fagsystembrugerne.
2. Til at understøtte risikovurderingsmetoden skal der udvikles et risikovurderingsværktøj til brug af informationssikkerhedsfunktionen.
3. Der skal overvejes, hvordan fagsystembrugernes risikovurderinger indgår i risikovurderingsværktøjet.
4. I forbindelse med risikovurderingen skal fagsystembrugerne, og i en hvis grad fagsystemejerne, undervises i risikovurdering ud fra Illeris' teori om voksenlæring og principperne om tilpasningsorienteret og udviklingsorienteret læringstilgange.
5. I forbindelse med undervisningen skal risikovurderingsmetoden afprøves og evalueres for at metoden kan videreudvikles.

Disse forbedringspotentialer er grundlag for design- og implementeringsvalg i kapitel 4 *Fase 2 – Udvikling af design*, kapitel 5 *Fase 3 – Afprøvning i praksis* og kapitel 6 *Fase 4 - Evaluering*.

4 Fase 2 – Udvikling af design

I dette kapitel kombineres de domænespecifikke teorier med designframework og designprincipper (Christensen, Gynther, & Petersen, 2012, s. 12). Kapitlet er opdelt i to dele. Den ene halvdel omhandler designet af risikovurderingsmetoden og -værktøjet og den anden halvdel omhandler, hvordan designet skal spille sammen med fagsystemsbrugernes risikovurderinger, idet det er vedtaget i informationssikkerhedsfunktionen, at fagsystembrugerne ikke skal have adgang til risikovurderingsværktøjet, og derfor skal der udvikles en idé og et design til, hvordan deres risikovurderinger kan sammenkobles med risikovurderingsværktøjet. Til dette kapitel hører også en Excel-mappe med risikovurderingsværktøjet som er vedhæftet den digitale besvarelse.

4.1 Design

Dette afsnit tager udgangspunkt i forbedringspotentialepunkterne 1: *Der skal udvikles en risikovurderingsmetode, der kan benyttes af både informationssikkerhedsfunktionen og fagsystembrugerne* og 2: *Til at understøtte risikovurderingsmetoden skal der udvikles et risikovurderingsværktøj til brug af informationssikkerhedsfunktionen.* Afsnittet starter med en begrundelse for valg af software, idet valget både medfører designpotentialer, men også indeholder hæmsko i forhold til designet. Dernæst bliver begreber i forhold til sårbarhedsvurdering af fagsystemerne præsenteret, da det ifølge Calder og Watkins samt Digitaliseringsstyrelsen er vigtigt, at have en samlet begrebsforståelse for at kunne udføre sammenlignelige risikovurderinger. Herefter bliver opbygningen af risikovurderingsværktøjsdesignet præsenteret med baggrund i viden fra afsnit 3.2.2 *Risikostyring*. Til sidst bliver risikovurderingsmetoden præsenteret med teoretisk baggrund i afsnit 3.2.2 *Risikostyring* og afsnit 3.3.1 *Risikovurderingsmetoder*.

4.1.1 Valg af software

Til risikostyringsværktøjet har informationssikkerhedsfunktionen valgt Microsoft Excel, som er et regneark udviklet af Microsoft. Valget er faldet på Excel på baggrund af flere faktorer. Den første er, at Excel er et program Hjørring Kommune i forvejen har adgang og licens til, hvilket vil sige, at der ikke er en merudgift i forhold til programmet. Derudover er det et program som medarbejderne i informationssikkerhedsfunktionen er vant til at arbejde med. Dernæst kan programmet i kraft med, at det er et regneark lave automatiske beregninger, så længe der er opsat bestemte formler, hvilket er med til at gøre den administrative proces enklere. Samtidigt er risikoniveauet ikke defineret af de prædefinerede formler, og dermed udregninger idet, at celler, hvor formlen står kan ryddes, og der derfor er mulighed for, at indsætte et andet risikoniveau ind, hvis f.eks. informationssikkerhedsudvalget ikke er enige i det beregnede risikovurderingsniveau. En stor faktor i valget af Excel er brugervenligheden. For det første er Excel nemt at tilpasse således, at risikostyringsværktøjet passer til Hjørring Kommunes behov i forbindelse med risikovurdering og samtidigt kan leve op til dokumenteringskravene i ISO27001-standarden. Samtidigt er der mulighed for at designe værktøjet med grupperinger og rullelister, så et overblik over de forskellige aktiver og trusler nemt kan etableres, og essentielle begreber og

klassifikationer kan vælges i rullelisterne, så den ansvarlige for at opdatere risikostyringsværktøjet ikke behøver at finde begreberne andre steder. Den sidste faktor er, at Digitaliseringsstyrelsen anbefaler organisationer at benytte Excel som risikostyringsværktøj (Digitaliseringsstyrelsen, 2015b).

4.1.2 Begreber

Digitaliseringsstyrelsen (2015b) pointere behovet for fastsatte begreber i forbindelse med risikovurdering. Grunden til dette er, at der er mange medarbejdere (fagsystembrugere), der skal udføre risikovurderinger på fagsystemer, og der er derfor behov for fastsatte begreber til at vurdere risiciene for fagsystemerne, for at opnå en række risikovurderinger, der er sammenlignelige, og undgå risikovurderinger, der tager afsæt i en subjektiv vurdering af fagsystemerne. Hjørring Kommunens risikovurderingsmetode (læs mere herom i afsnit 4.1.4 *Risikovurderingsmetode*), er der to faktorer fagsystembrugerne skal vurdere, i forbindelse med risikovurdering, som er fagsystemets *sårbarhed* og hvilke *trusler*, der kan fører til en hændelse, hvor risikoen er produktet af *sårbarhed* og *trusler*. Det er ikke nødvendigt at fastsatte en række begreber i forhold til truslerne idet, at der er udviklet et *trusselskatalog* (læs mere herom i afsnit 4.1.3 *Opbygning af design*), der er med til at forklare de forskellige trusler, og hvorfor de trusler opstår. I forhold til fagsystemet *sårbarhed* er der imod behov for en række veldefineret begreber, idet *sårbarheden* vurderes ud fra en række kriterier.

Sårbarhed er en fortegnelse for, hvor sårbart fagsystemet er i forhold til, at trusler mod fagsystemet kan føre til en sikkerhedshændelse. Dette vurderes ud fra fire kriterier: *fortrolighed, forretningskritikalitet, finansielle værdi* og *persondata*. Baggrunden for valg af disse fire kriterier, er at de alle kan beskrive forskellige aspekter af fagsystemet i forhold til dets sårbarhed. De fire kriterier er udvalgt af informationssikkerhedsudvalget og beskrevet ved hjælp af Neuparts sikkerhedsstyringsværktøj SecureAware, som er Hjørring Kommunes tidligere risikostyringsværktøj.

Fortrolighed benyttes til at vurdere om hvorvidt den data, der forefindes i fagsystemet kan deles med samarbejdspartnere, borgere eller pressen, og om en offentliggørelse af disse data har en konsekvens på det omdømmemæssige, retslige og økonomiske plan. Klassifikationen af fortrolighed inddeles i *yderst hemmeligt, hemmeligt, fortroligt, begrænset*, og *offentlig*, og er forklaret i Tabel 4.1.

Yderst hemmeligt	Et brud på fortroligheden kan have exceptionel alvorlig skadelige omdømmemæssige, retslige eller økonomiske konsekvenser for kommunen.
Hemmeligt	Et brud på fortroligheden kan have alvorlige skadelige omdømmemæssige, retslige eller økonomiske konsekvenser for kommunen.
Fortroligt	Et brud på fortroligheden kan have skadelige omdømmemæssige, retslige eller økonomiske konsekvenser for kommunen.
Begrænset	Et brud på fortroligheden kan have uønskede omdømmemæssige, retslige eller økonomiske konsekvenser for kommunen.
Offentligt	Et brud på fortroligheden kan have ingen omdømmemæssige, retslige eller økonomiske konsekvenser for kommunen.

Tabel 4.1: Fortrolighedsklassifikation

Forretningskritikalitet er et udtryk for, hvor vigtigt fagsystemet er for kommunens arbejdsprocesser. Ved en vurdering af et fagsystems forretningskritikalitet vurderes det, hvor lang tid fagsystemet kan undværes ved et eventuelt nedbrud inden det påvirker kommunens processer. Forretningskritikalitet klassificeres som *forretningskritisk*, *vigtigt* og *ikke kritisk*, og er forklaret i Tabel 4.2.

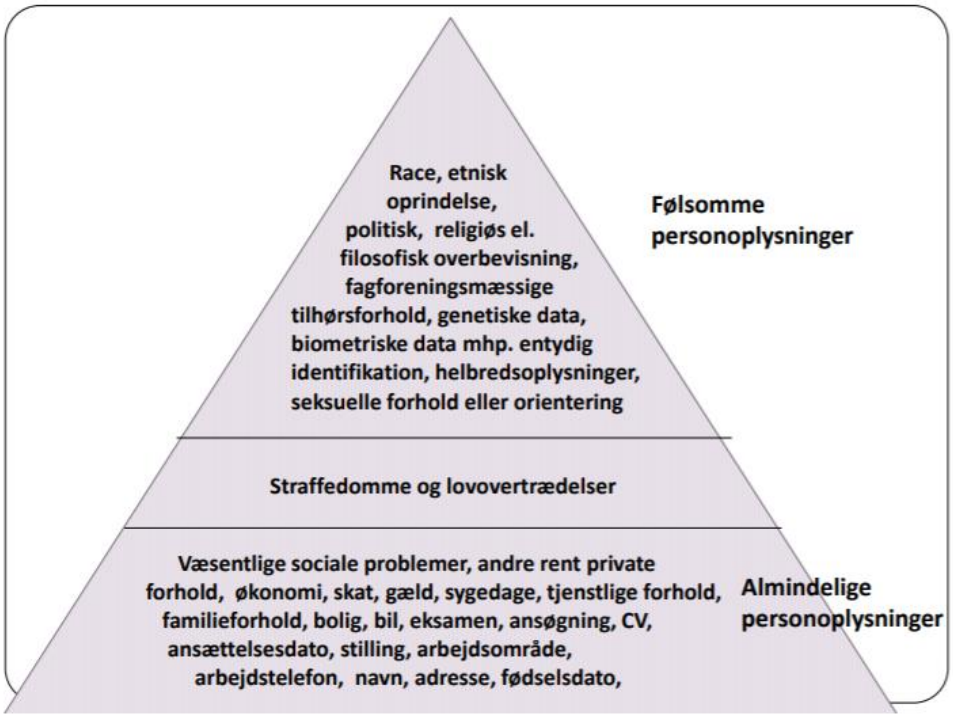
Forretningskritisk	Det pågældende fagsystem kan kun undværes i et kort tidsrum, timer til få dage, før kommunens processer påvirkes i uacceptabel grad.
Vigtigt	Det pågældende fagsystem kan kun undværes i et moderat tidsrum, fra nogle få dage til en uge, før kommunens processer påvirke i uacceptabel grad.
Ikke kritisk	Det pågældende fagsystem kan undværes i et længerevarende tidsrum, flere uger, før kommunens processer påvirkes i en uacceptabel grad.

Tabel 4.2: Forretningskritikalitetsklassifikation

Den finansielle værdi er et udtryk for, hvad det vil koste kommunen, hvis fagsystemet bryder ned, herunder genoprettelse af fagsystemet, arbejdstab, medarbejderomkostninger. Den finansielle værdi inddeles i *mindre end 5.000 DKK*, *5.000 – 10.000 DKK*, *10.000 – 50.000 DKK*, *50.000 DKK – 100.000 DKK* og *mere end 100.00 DKK*.

Kriteriet om persondata er valgt, da det giver en sammenkobling mellem risikovurdering og persondataforordningen, hvor fagsystemsbrugerne skal vurdere om fagsystemet indeholder *ingen personoplysninger*,

almindelige personoplysninger og *følsomme personoplysninger*. Betydningen af klassifikationerne er illustreret i Figur 4.1.



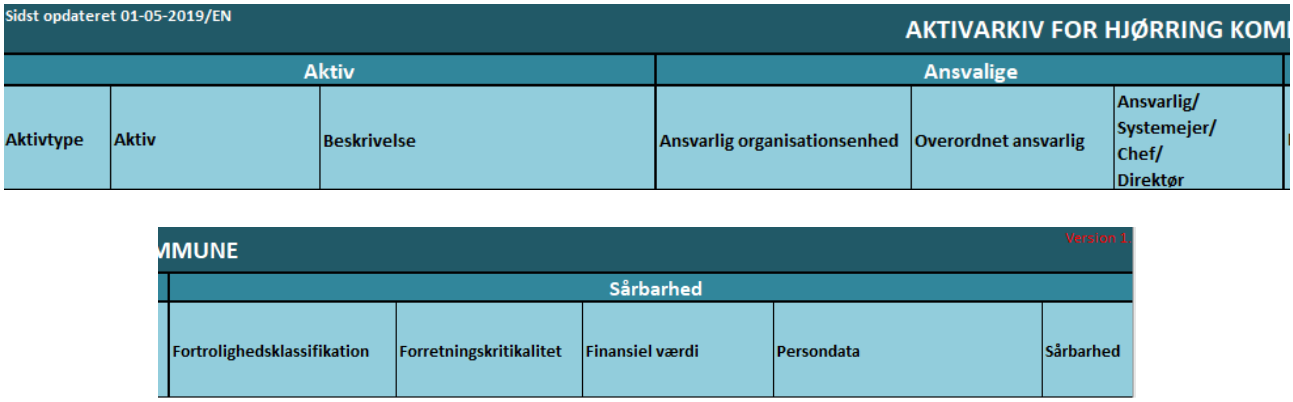
Figur 4.1: Persondata (Datatilsynet, Erhvervsstyrelsen, Justitsministeriet, & Digitaliseringsstyrelsen, 2017, s. 7).

4.1.3 Opbygning af værktøj

Designet er opbygget i Excel-mappen i tre ark, der alle tilhører minimumsdokumenteringskravet i ISO27001-standarden i forhold til risikovurdering (Digitaliseringsstyrelsen, 2015b). De tre ark har fået tildelt henholdsvis navne: *Aktivarkiv*, *Trusselskatalog* og *Risikovurdering*.

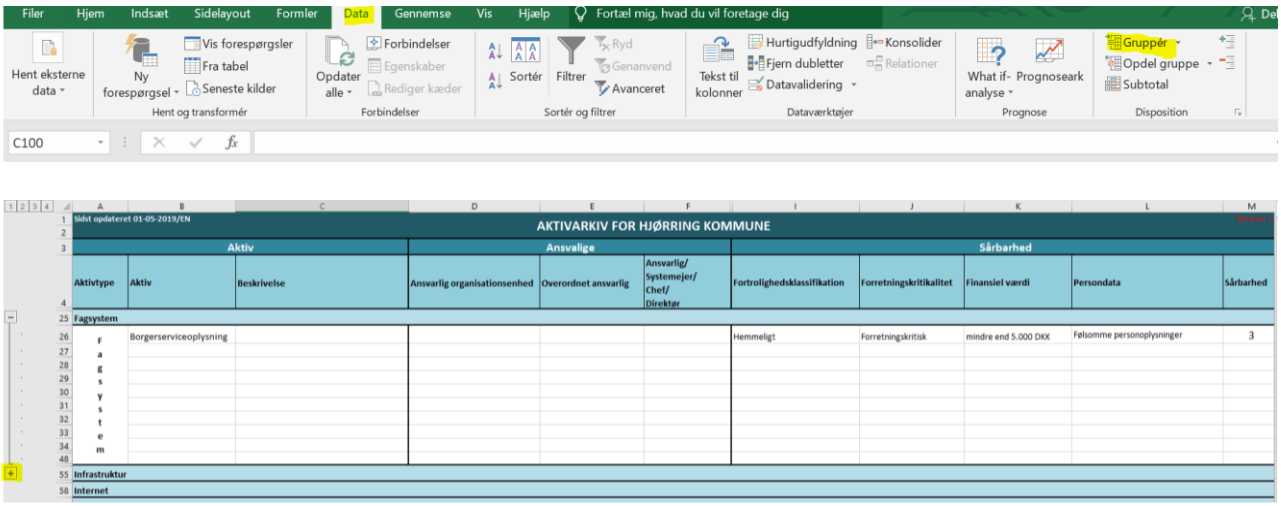
Det første ark, er aktivarkivet, som er et obligatorisk overblik over Hjørring Kommunes informationsaktiver, og samtidigt er sårbarhedsvurdering også sat ind i arkivet, da sårbarheden er vurderet ud fra det enkelte informationsaktiv. Aktivarkivet er opbygget i kolonnerne først med feltet *Aktiv*, hvor *aktivtype*, *aktiv* samt en beskrivelse af informationsaktivet bliver præsenteret. Dernæst er der kolonnen *Ansvarlige*, hvor den ansvarlige organisationsenhed, den overordnet ansvarlige og i fagsystemernes tilfælde fagsystemsejerne bliver præsenteret. Den ansvarlige organisationsenhed bliver præsenteret, da det derved er muligt at se i hvilken enhed fagsystemet bliver mest benyttet, som kan give hentydning om, hvilke arbejdsprocesser fagsystemet bliver brugt til. Hvis et fagsystem f.eks. har *Økonomi og Finans* som ansvarlig organisationsenhed, så giver det en hentydning til, at fagsystemet bliver brugt til økonomibehandling og evt. bogføring. Den overordnet ansvarlige, er den medarbejder som er ansvarlig i informationssikkerhedsfunktionen for at risikovurdering bliver fortaget, som oftest ville det være informationssikkerhedskoordinatoren. Fagsystemsejeren er den medarbejder i kommunen,

som i første omgang skal kontaktes i forbindelse med risikovurdering, og som har et ansvar for at der bliver foretaget i risikovurdering. Oplysningerne i *Aktiv*- og *Ansvarlige*-kategorierne, i forbindelse med risikovurdering af fagsystemer, stammer fra KITOS, som er kommunens digitale overblik over fagsystemer. Det næste kolonneafsnit er *Sårbarhed*, hvor oplysninger stammer fra risikovurderingerne foretaget af fagsystembrugerne og informationssikkerhedsfunktionen, hvilket læses mere om i afsnit 4.1.4 *Risikovurderingsmetode*. Sårbarhedsafsnittet er inddelt i de fire sårbarhedsklassifikationer, og et sårbarhedsvurderingsfelt, hvor sårbarheden vurderes ud fra de fire klassifikationer for derefter af blive omsat til en talværdi på mellem 1-5. Det overstående er illustreret i Figur 4.2, hvor det er beskåret således, at det er blevet delt i to for læsevenlighedens skyld.



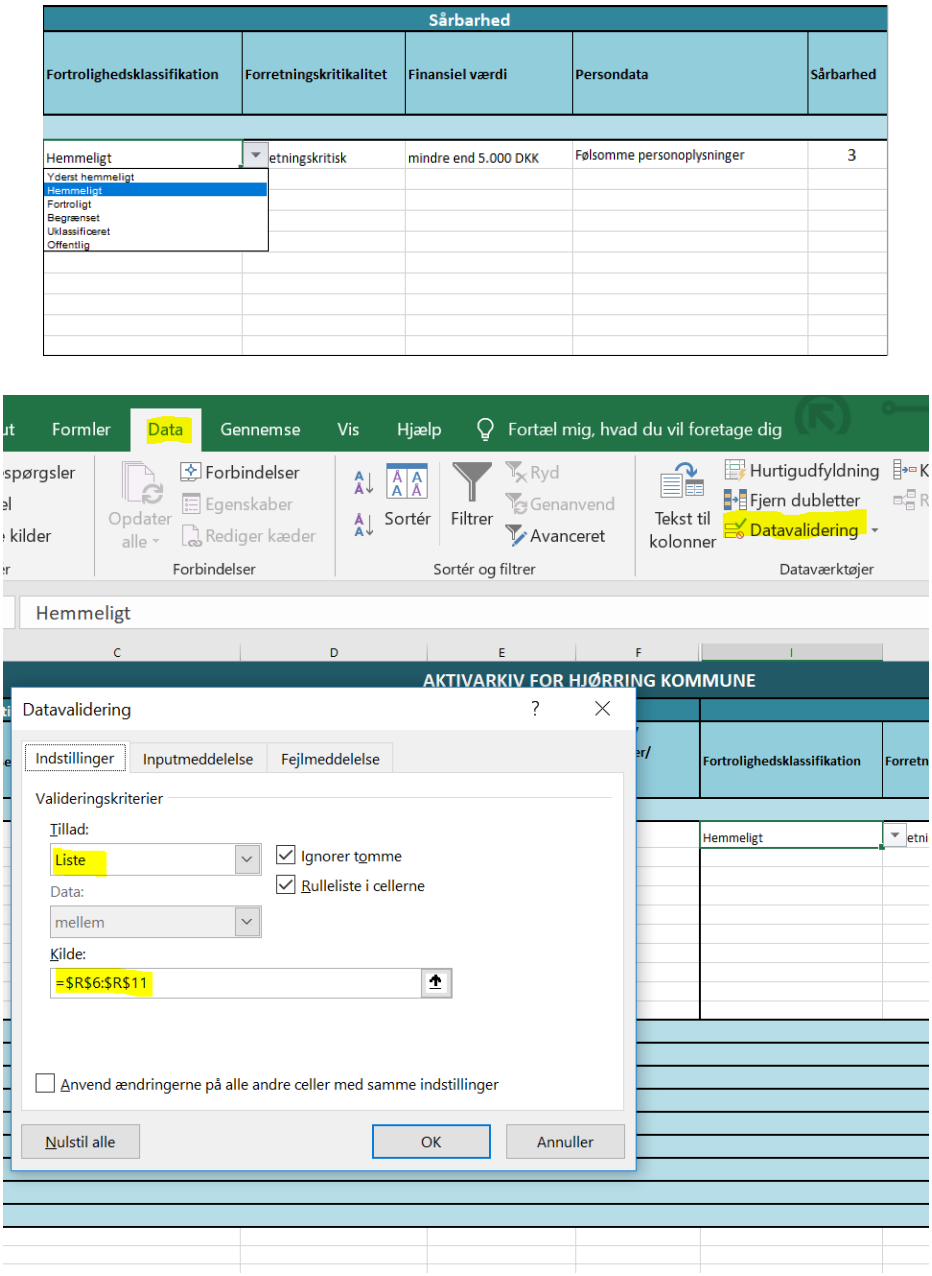
Figur 4.2: Kolonne afsnittene i Aktivarkivet

Rækkerne i Aktivarkivet er inddelt i aktivtyper, under disse er de enkelte aktiver grupperet, således, at en aktivtype kan vælges ved at trykke på det lille plus-ikon udenfor typen, og dermed kan man se de registreret informationsaktiver under den valgte type. Dette er lavet ved at markere de rækker, der ligger under aktivtyperækken, vælge fanen *Data* og derefter klikke på *Gruppér*. Det overstående er illustreret i Figur 4.3, igen er figuren beskåret i forhold til læsevenlighed.



Figur 4.3: Rækker i Aktivarkivet samt markering af, hvorledes gruppering af rækker dannes

Ved hver aktiv under sårbarhedskategorien indtastes resultatet af sårbarhedsvurderingen ved hjælp af en rullemenu, hvilket er valgt for at lette den administrative opgave. Dette er lavet ved, at lave en liste over klassifikationerne i et andet område af Excel-mappen. Derefter er der under fanen *Data* valgt *Datavalidering* under *Dataværktøjer*. I pop-up boksen, er der valgt *Liste* under *Tillad*, og derefter er cellerne med listen over klassifikationerne valgt under *Kilde*. Denne proces er illustreret i Figur 4.4.



Figur 4.4: Oprettelse af rullemenu i Excel

I det andet ark *Trusselskatalog* er kolonnerne delt op i forskellige afsnit. Det første afsnit er *Trussel* herunder *Trusseltype* og beskrivelse af truslerne. Det andet afsnit er *Hyppighed*, hvor truslernes hyppighed og trusselsårsagernes hyppighed er vurderet af informationssikkerhedsudvalget på en talskala mellem et til fem. Dernæst

er afsnittet *Konsekvens*, hvor truslernes konsekvens på *Fortrolighed*, *Integritet* og *Tilgængelighed* er vurderet af informationssikkerhedsudvalget på en talskala mellem et til fem. Det sidste afsnit er *Sammenhold med aktiver*, hvor truslerne bliver sammenkædet med de aktivtyper, som oftest vil blive påvirket af truslerne, for at gøre identifikationsarbejdet nemmere (se afsnit 4.1.4 *Risikovurderingsmetode*). Det overstående er illustreret i Figur 4.5.

Sidst opdateret: 14-09-2018/EN	Trusselskatalog for Hjørring Kommune							Version 1.0
Trussel			Hyppighed		Konsekvens			Sammenhold med aktiver
Trusseltype	Trussel	Beskrivelse	Højeste hyppighed	Hyppighed	Fortrolighed	Integritet	Tilgængelighed	Aktivtype

Figur 4.5: Kolonneafsnit i Trusselskataloget

Rækkerne i *Trusselskataloget* er delt op i *Trusseltyper*, herunder er truslerne og trusselsårsagerne grupperet. Truslerne er rækker, hvor baggrundsfarven er blå, hvor trusselsårsagerne er hvide. Grunden til at trusselsårsagerne er taget med i *Trusselskataloget*, er at det kan være svært at sammenkoble truslerne med fagsystemerne, hvor trusselsårsagerne giver årsagerne til truslerne, og dermed en beskrivelse af, hvordan truslerne kan opstå. Dette er illustreret i Figur 4.6.

	Sidst opdateret: 14-09-2018/EN	Trusselskatalog for Hjørring Kommune							Version 1.0
3	Trussel			Hyppighed		Konsekvens			Sammenhold med aktiver
4	Trusseltype	Trussel	Beskrivelse	Højeste hyppighed	Hyppighed	Fortrolighed	Integritet	Tilgængelighed	Aktivtype
5	Fysiske og miljømæssige trusler								
28	Bruger og it-driftsmæssige trusler								
29		Brugerfejl		3		3	2	1	Proces Server Netværk Internet Serverrum Kommunikationslinje
30		Uforsætligt brugerhandlinger, fejlbehandling af medier, mangel på brugeruddannelse			2				
31		Tab af datamedier eller fysiske dokumenter	Det være sig laptops, smartphones, tablet, bærbare harddiske, USB nøgler, fysiske dokumenter og lign.		1				

Figur 4.6: Rækkerne i Trusselskataloget

I det sidste ark *Risikovurdering* er kolonnerne igen inddelt i flere afsnit. Det første afsnit *Aktiv*, hvor oplysningerne om aktivtype og sårbarhedsvurderingen fra *Aktivarkivet* indsættes. Næste afsnit er *Trussel*, hvor den identificerede trussel og den tilhørende hyppighed er indsat fra *Trusselskataloget*. Herefter er afsnittet *Konsekvens*, den vurderede konsekvens for fortrolighed, integritet og tilgængelighed er indsat fra *Trusselskataloget*. Til sidst er der *Risiko*, hvor den vurderede sandsynlighed, konsekvens og risiko er udregnet (metoden er beskrevet i afsnit 4.1.4 *Risikovurderingsmetode*). Rækkerne er opbygget af aktivtyper, herunder er de enkelte informationsaktiver, og under disse er de identificerede trusler grupperet. Dette er illustreret i Figur 4.7.

	A	B	C	D	E	F	G	H	I	J	K
1	Sidst opdateret: 01-05-2019/EN			Risikovurdering							Version 1.0
2											
3		Aktiv		Trussel		Konsekvens			Risiko		
4	Aktivtype	Aktiv	Sårbarhed	Trussel	Hyppighed	Fortrolighed	Integritet	Tilgængelighed	Sandsynlighed	Konsekvens	Risiko
5	Fagsystem										
149		Borgerserviceoplysning	3								
150	F			Leverancesvigt	3	1	3	5	3,0	3,0	9
151	a			Drifts- eller vedligeholdelsesprocesser	1	1	3	5	2,0	3,0	6
152	g										
153	s										
154	y										
155	s										
156	t										
157	e										
158	m										
159											
160											

Figur 4.7: Risikovurderingsarket

Risikovurderingsværktøjet er i første omgang designet sådan, at det kun er medarbejderne i informationssikkerhedsfunktionen, der skal arbejde med det. Derfor er der ikke taget hensyn til skrifttype, farver og layout, ud over det der er beskrevet. Farverne er valgt for at illustrere niveauerne i designet. På sigt er det meningen, at designet også skal kunne bruges som dokumentation til IT-revisionen, og derfor vil der i senere iterationer blive taget hensyn til layoutet, samt lavet ekstra ark til andre dokumentationskrav, såsom risikohåndtering og SoA-dokument, men også et ark med en vejledning til at navigere i værktøjet.

4.1.4 Risikovurderingsmetode

Metoden valgt til risikovurdering i Hjørring Kommune er inspireret af den kvalitative metode samt OCTAVE metoden, se evt. afsnit 3.3.1 *Risikovurderingsmetoder*, og inddelt i tre faser. Den første fase er inspireret af OCTAVE metoden, der starter som beskrevet med, at et analyseteam udpeger de vigtigste forretningsprocesser, og udvælger informationsaktiver herudfra. I Hjørring Kommune er analyseteamet repræsenteret ved informationssikkerhedsfunktionen, men det skal nævnes, at de første udvalgte fagsystemer til den første iteration, blev håndplukket, før informationssikkerhedsfunktionen blev oprettet af repræsentanter fra informationssikkerhedsudvalget samt informationssikkerhedskoordinatoren. Dette er sket, da informationssikkerhedsfunktionen på daværende tidspunkt skulle have fokus på udvikling af risikovurderingsmetode og -værktøj frem for udvælgelse af fagsystemer. Efter udvælgelsen af fagsystemer til vurdering, skal systembrugerne identificeres, hvilket de enkelte systemejere har ansvaret for samt have informationer omkring deres opgave i forbindelse med risikovurderingen, hvor det i den første iteration, skal foregå som en workshop.

Den næste fase handler om at vurdere fagsystemernes sårbarhed, samt identificere de trusler, som har betydning for det enkelte fagsystem. Denne fase er fagsystembrugerne en del af, og fagsystemejerne har ansvaret for, at denne fase bliver udført. Først skal fagsystembrugerne vurdere fagsystemernes sårbarhed, hvilket gøres ud fra tre klassifikationer, som er *fortrolighed*, *forretningskritikalitet* og *finansielle værdi*, hvilket står beskrevet i afsnit 4.1.2 *Risikovurderingsmetode*. Her skal fagsystembrugerne vurdere, hvilken fortrolighed fagsystemets data skal omgås med, hvor forretningskritisk er fagsystemet, altså kan kommunen fortsætte med sine arbejdsprocesser, selvom fagsystemet evt. skulle være nede og ikke tilgængeligt, samt hvad det vil koste

kommunen, hvis fagsystemet bliver ramt af en trussel, og der opstår en informationssikkerhedshændelse. Dette gøres ved at fagsystembrugerne sætter kryds ved den klassifikation af de tre begreber, de vurderer fagsystemet hører indenunder. Et tænkt eksempel kan være et fagsystem, hvor medarbejdere i borgerservice behandler fortrolige oplysninger på borgerne, hvilket kaldes *Borgerserviceoplysning*. Her vil fagsystembrugeren vurdere, at fortrolighedsklassifikationen skal være *hemmeligt*, da fagsystemets data indeholder følsomme personoplysninger. Samtidigt vurderer fagsystembrugeren at, *Borgerserviceoplysning* forretningskritikalitet, skal klassificeres som *ikke kritisk*, da fagsystemet benyttes til at bearbejde oplysninger om borgerne, som kan andet steds fra og samtidigt kan arbejdsprocesserne løses af manuelle løsninger, f.eks. i et skriveprogram. Til sidst giver fagsystembrugeren *Borgerserviceoplysning* den finansielle værdi *mindre end 5.000 DKK*, idet det ikke vil koste meget at genoprette fagsystemet, og da arbejdsprocesserne kan udføres manuelt, vil der være en lille omkostning i forhold til tabt arbejdsfortjeneste. Til slut skal fagsystembrugeren også oplyse, hvilken form for persondataoplysninger, der fremgår af fagsystemets data i forhold til persondataforordningen. I det tænkte eksempel med *Borgerserviceoplysning* er det *følsomme personoplysninger*, der er præsenteret i fagsystemets data. I den anden fase skal fagsystembrugerne også identificere trusler ud fra prædefineret trusler, som er inddelt i forskellige kategorier, se evt. afsnit 4.1.2 *Opbygning af vækrtøj*. Her vælger fagsystemsbrugerne, hvilke trusler, der er relevante for netop deres fagsystem, hvor der kan være flere forskellige trusler, der er relevante. I det samme tænkte eksempel som ovenfor, kan fagsystembrugeren af *Borgerserviceoplysning* vurdere, at *leverancesvigt* er en reel trussel for fagsystemet, idet det er en leverandør, der ejer fagsystemet og er ansvarlig for, at det kan benyttes af kommunen. Samtidigt vurderer fagsystembrugeren også, at *drift- eller vedligeholdelsesprocesser* er en trussel mod *Borgerserviceoplysning*, i og med, at en systemopdatering kan medføre, at visse funktioner ikke virker mere til brug i arbejdsprocessen omkring fagsystemet eller, at fortrolige data går tabt.

I den tredje og sidste fase, skal risikovurderingerne fra fagsystembrugerne behandles i risikostyringsværktøjet. Først bliver sårbarhedsklassifikationer for det enkelte fagsystem indsat i *Aktivarkivet*. Ud fra disse klassifikationer og indholdet i data i forhold til persondataforordningen, vurderer informationssikkerhedsfunktionen fagsystemets sårbarhed ud fra en skala fra et til fem, hvor fem er et højt sårbarhedsniveau og et er et lavt sårbarhedsniveau, altså hvor sårbart dette system er i forhold til at mulige trusler, kan forårsage en sikkerhedshændelse. I det tænkte eksempel fra ovenover, hvor fagsystemsbrugeren har vurderet, at *Borgerserviceoplysning* har en fortrolighedsklassifikation som *hemmeligt*, en forretningskritikalitetsklassifikation som *ikke kritisk* og en finansiel værdi på *mindre end 5.000 DKK* samt fagsystemet indeholder *følsomme personoplysninger*, vurderes fagsystemet sårbarhed til at være på sårbarhedsniveau tre, idet at fortrolighedsklassifikationen og det indeholdende persondata er kritisk vurderet, hvorimod forretningskritikaliteten og den finansielle værdi er vurderet som værende ikke kritisk. Det tænkte eksempel er illustreret i Figur 4.8.

Aktiv			Sårbarhed				
Aktivtype	Aktiv	Beskrivelse	Fortrolighedsklassifikation	Forretningskritikalitet	Finansiel værdi	Persondata	Sårbarhed
Afdeling							
Fagsystem							
	Borgerserviceoplysning		Hemmeligt	ikke kritisk	mindre end 5.000 DKK	Følsomme personoplysninger	3

Figur 4.8: Overblik over vurdering af sårbarhed i tænkt eksempel, hvor der er klippet i det originale design, for at vise de vigtigste funktioner.

Dernæst kopiers sårbarhedsværdien til arket *Risikovurdering* (se afsnit 4.1.2 *Opbygning af værktøj*), hvor de identificerede trusler vil blive kopieret fra *Trusselskataloget* sammen med truslernes specifikke værdier for *hyppighed* og konsekvenser for *fortrolighed*, *integritet* og *tilgængelighed*. Grunden til dette er, at det er relevant at vide, hvor hyppigt en trussel vil forekomme generelt, og sætte det i sammenhæng mellem risikoen. Samtidigt er det er krav fra ISO27001-standarden, at risikoen vurderes på baggrund af en konsekvensanalyse af truslernes konsekvens på informationsaktivernes (i dette tilfælde fagsystemer) fortrolighed, integritet og tilgængelighed (Digitaliseringsstyrelsen, 2015b). I det tænkte eksempel med *Borgerserviceoplysning* blev truslerne *leverancesvigt* og *drift- eller vedligeholdelsesprocesser* identificerede som mulige trusler, hvilket er illustreret i Figur 4.9.

Aktiv			Trussel		Konsekvens		
Aktivtype	Aktiv	Sårbarhed	Trussel	Hyppighed	Fortrolighed	Integritet	Tilgængelighed
Fagsystem							
	Borgerserviceoplysning	3					
F			Leverancesvigt	3	1	3	5
a			Drifts- eller vedligeholdelsesprocesser	1	1	3	5

Figur 4.9: Sårbarhedsværdi samt trusler indsat i risikovurderingsværktøj.

Som det fremgår af figuren så er vurderingen af truslernes hyppighed og konsekvens for fagsystemets fortrolighed, integritet og tilgængelighed illustreret ved en skala på et til fem, hvor et er mindst kritisk og fem er mest kritisk. Grunden til, at det er talværdier, der er sat ind, er på grund af valget af software. Excel er primært et regneprogram, og kan ofte kun automatisere processer, hvis det sker gennem formler, der benytter talværdier. Vurderinger af truslerne er foretaget af informationssikkerhedsudvalget samt informationssikkerhedskoordinatoren og en ekstern konsulent. Herefter bliver risikoen vurderet, ved hjælp af en udregning med bestemte formler. Risikoen bliver vurderet ud fra hver trussel, der er identificeret i forhold til fagsystemet, og i tilfældet i det tænkte eksempel, er risikoen præsenteret i Figur 4.10.

Aktiv			Trussel		Konsekvens			Risiko		
Aktivtype	Aktiv	Sårbarhed	Trussel	Hyppighed	Fortrolighed	Integritet	Tilgængelighed	Sandsynlighed	Konsekvens	Risiko
Fagsystem										
	Borgerserviceoplysning	3								
F			Leverancesvigt	3	1	3	5	3,0	3,0	9
a			Drifts- eller vedligeholdelsesprocesser	1	1	3	5	2,0	3,0	6

Figur 4.10: Risikovurdering for Borgerserviceoplysning.

Risiko anses i ISO27001-standarden for produktet af *sandsynlighed* og *konsekvens*, hvilket i en formel vil skrives som $Risiko = Sandsynlighed * Konsekvens$ (Digitaliseringsstyrelsen, 2015b). For at vurdere sandsynligheden, tages gennemsnittet af det specifikke fagsystems sårbarhed og hyppigheden for den tildelte trussel, grundet, at sandsynlighed for, at risikoen bliver til en informationssikkerhedshændelse, er større jo mere sårbart fagsystemet er, og hvor hyppigt fremkommende en trussel er. I en formel vil det således se sådan ud: $Sandsynlighed = \frac{Sårbarhed+Hyppighed}{2}$. Konsekvensen vurderes som gennemsnittet af truslens konsekvens for fortrolighed, integritet og tilgængelighed, og vil i en formel se således ud: $Konsekvens = \frac{Fortrolighed+Integritet+Tilgængelighed}{2}$. I det tænkte eksempel med *Borgerserviceoplysning*, er sårbarheden vurderet til 3, og hyppigheden for truslen *Leverancesvigt* er vurderet til 3, hvilket vil sige at $Sandsynlighed = \frac{3+3}{2} = 3$. Truslens konsekvenser for fortrolighed er vurderet til 1, for integritet vurderet til 3 og for tilgængelighed vurderet til 5, hvilket medfører at $Konsekvens = \frac{1+3+5}{3} = 3$, og dermed kan risikoen udregnes til $Risiko = 3 * 3 = 9$.

Da risikoen er et produkt af sandsynligheden og konsekvensen, vil risikoen have en talværdi på mellem 1-25, hvor værdierne 1-4 angiver en risiko som er kritisk, værdierne 5-18 angiver en risiko som er ret kritiske og værdierne 19-25 angiver en risiko som er alvorlig kritisk. Det skal påpeges, at den udregnede risiko, kun er en vurdering og et forslag til et risikoniveau, som informationssikkerhedsudvalget dernæst skal vurdere, om de er enige i dette forslag. Efterfølgende kan informationssikkerhedsudvalget vælge om de vil godkende det vurdere risikoniveau, eller om risikoniveauet skal hæves eller sænkes.

4.2 Sammenhæng mellem design og fagsystembrugere

Dette afsnit tager udgangspunkt i forbedringspotentialepunktet 3: *Der skal overvejes, hvordan fagsystemsbrugernes risikovurderinger indgår i risikovurderingsværktøjet.* Afsnittet starter med en præsentation af den valgte designmetode som er storyboard og begrundelse herfor. Derefter bliver storyboardet præsenteret med tankerne bag idéen om, hvor der kan skabes en sammenhæng mellem risikovurderingsværktøjet og fagsystembrugernes risikovurdering.

4.2.1 Metode

Det der gør interaktionsdesign unikke er, at det forestiller en person der interagerer med et system over tid og vedkommendes adfærd herom. Elementet tid opfanger storyboards som en serie af diskrete billeder, der visuelt fortæller, hvad der foregår scene efter scene. Der findes fire typer af storyboards, hvor den første type er sekventielle storyboards (Sequential Storyboards), som introducerer storyboardet som en visuel fortælling der fanger nøgleidéer som en sekvens af rammer, der udfolder sig over tid. Den anden type er tilstandsovergangsdiagrammet (The State Transition Diagram) som formaliserer storyboardet, og repræsenterer interaktionstilstande, som overgang udløst af interaktioner og beslutningsvejen gennem storyboardet. Den tredje type er

forgreningsstoryboardet (The Branching Storyboard) er en måde at visuelt illustrerer beslutningsveje, der opstår over tid. Den sidste type af storyboards er det narrative storyboard (Narrative Storyboard) som fortæller en historie om interaktionskonteksten, hvilket vil sige det fysiske miljø, menneskelige handlinger samt behandlinger, der udfolder sig over tid (Greenberg, Buxton, Carpendale, & Marquardt, 2011, s. 145). I dette speciale er det narrative storyboard benyttet.

Det narrative storyboard

Det narrative storyboard bidrager med en illustration af kontekst gennem brug af en sekvens af billeder til at fortælle en mere komplet historie om brugernes interaktion over tid, hvor hvert billede i storyboardet repræsenterer en bestemt begivenhed. Disse sekvenser af billeder kommunikerer information om, hvor interaktionen finder sted, præsenterer brugerne som personligheder og giver oplysninger om andre brugerhandlinger, der sker, når brugerne interagerer med designet (Greenberg, Buxton, Carpendale, & Marquardt, 2011, s. 167).

4.2.2 Fra skema til risikovurdering

Det er besluttet fra informationssikkerhedsfunktionens side, at risikovurderingsværktøjet kun skal benyttes af medarbejderne i informationssikkerhedsfunktionen. Dette er bestemt for at til dels at minimere fejlændringer i værktøjet, men også fordi, at informationsfunktionen har det overordnet ansvar for risikovurderingerne, og kan derfor have behov for at ændre i vurderingerne, inden de videresendes til godkendelse hos informationssikkerhedsudvalget. Derfor skal systembrugerne indsende et udfyldt skema, som sendes via Hjørring Kommunes interne medarbejderportal, medarbejderweb, og derefter bliver automatisk journaliseret i kommunens journaliseringssystem SBSYS, og en medarbejder fra informationssikkerhedsfunktionen indsætter resultatet i risikovurderingsværktøjet. Selve idéen er, at systembrugerne deltager i første omgang på en workshop, hvor de bliver præsenteret for risikovurdering og den udviklede risikovurderingsmetode, og samtidigt udfylder skemaet. Næste gang de skal lave en risikovurdering, får de valget om at deltage i en ny workshop, deltage i en interviewseance med en medarbejder fra informationssikkerhedsfunktionen, eller at udføre risikovurderingen på egen hånd med hjælp fra vejledninger på medarbejderweb. I Figur 4.11 er det illustreret, hvordan risikovurderingsskemaet bliver udfyldt og bliver videresendt for at til sidst at ende i risikovurderingsværktøjet.

Figur 4.11: Storyboard som viser risikovurderingsproces

I Figur 4.11 er det i det første billede konteksten der er illustreret, som er Hjørring Kommune præsenteret ved kommunens våbenskjold. I det andet billede bliver problemet præsenteret, hvor en medarbejder hos kommunen er blevet identificeret som fagsystembruger, og skal derfor udføre en risikovurdering, men medarbejderen ved

ikke hvordan man udføre sådan en risikovurdering. Dernæst i tredje billede bliver inputtet illustreret ved, at medarbejderen kommer med til en workshop sammen med andre fagsystembrugere og på workshoppen lærer medarbejderen om, hvordan en risikovurdering udføres. I fjerde billede bliver feedbacken illustreret ved, at medarbejderne i forbindelse med workshoppen kan udfylde et risikovurderingsskema på medarbejderweb og derved sende det videre til det sidste billede, som illustrerer resultatet, som er en udført risikovurdering i risikovurderingsværktøjet.

5 Fase 3 – Afprøvning i praksis

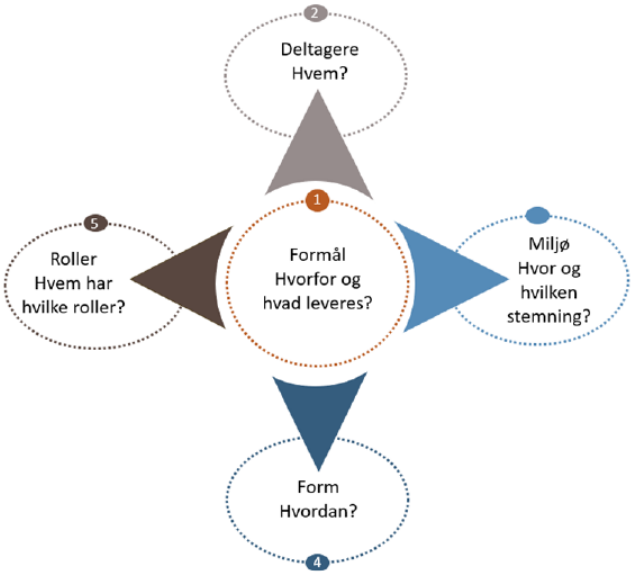
Dette kapitel tager udgangspunkt i forbedringspotentialepunktet 4: *I forbindelse med risikovurderingen skal fagsystembrugerne, og i en hvis grad fagsystemejerne, undervises i risikovurdering ud fra Illeris' teori om voksenlæring og principperne om tilpasningsorienteret og udviklingsorienteret læringstilgange.* Dette gøres med metoden facilitering, som bliver præsenteret i starten af kapitlet. Derefter bliver de didaktiske overvejelser med teoretisk baggrund af afsnit 3.2.3 *Voksenlæring* præsenteret først i form af en designstjerne og dernæst som en drejebog.

5.1 Metode

Facilitering handler om at skabe resultater og ejerskab gennem involvering, som kan bestå af møder, workshops, seminarer og andre processer, hvor en gruppe mennesker skal nå et fælles mål. Facilitering ledes af en facilitator, der skal styre formen og målet for faciliteringen. Facilitering er ofte en del af en større forandringsopgave, og derfor skal facilitatoren mestre en række forskellige fokusområder, for at opnå et godt resultat på en workshop. Facilitatoren skal have fokus på både interaktionen på selve workshoppen, samt hvordan workshoppen passer ind i et overordnet forløb, og samtidig have fokus på både organisationen og den interpersonelle dimension i samme procesbegreb. Der er tre grundlæggende komponenter i facilitering som er design af processen, selve facilitering og opfølgning og sikring af faciliteringens effekt (Van Loon, Andersen, & Larsen, 2016, s. 19-30). I dette kapitel vil designet samt selve facilitering blive præsenteret. Først vil konteksten, hvori processen skal foregå kortlægges ved hjælp af designstjernen (afsnit 5.2 *Kontekst*), dernæst planlægges og designes workshoppen ved hjælp af en drejebog (afsnit 5.3 *Planlægning og design af workshop*). Kortlægning af konteksten samt planlægning og design af workshoppen er udarbejdet gennem flere møder med informationssikkerhedsfunktionen. Selve opfølgningen, som i dette speciale bliver kaldt evaluering præsenteres i kapitel 6 *Fase 4 - Evaluering*.

5.2 Kontekst

I den første del af designfasen af workshoppen, benyttes designestjernen til at kortlægge konteksten (Van Loon, Andersen, & Larsen, 2016, s. 49). Designstjernen er illustreret i Figur 5.1.



Figur 5.1: Designstjernen (Van Loon, Andersen, & Larsen, 2016, s. 49)

Det fremgår af Figur 5.1 , at designstjernen er delt op i fem kategorier: formål, deltagere, miljø, form og roller. Disse fem kategorier bliver præsenteret samt med de valg informationssikkerhedsfunktionen har foretaget i forbindelse med kategorierne.

5.2.1 Formål

Formålet er designstjernens kerne og retningsgiver for resten af designprocessen, og placeres derfor først i processen. Formålet i denne sammenhæng er det produkt, der tilblives i workshoppen, og skal være meningsskabende for deltagerne (Van Loon, Andersen, & Larsen, 2016, s. 51). I denne facilitering kan formålet deles op i to dele. Den ene del handler om at afprøve risikovurderingsmetoden og samtidigt lave en undersøgelse, som kan være med til at klargøre om workshop er den rette metode til at hjælpe fagsystembrugerne til at lære og forstå risikovurderingsmetoden, og udvikle kompetencer til at foretage en risikovurdering. Den anden del er et formål, som kan virke meningsskabende for deltagerne, idet det formål tjener, at fagsystembrugerne deltager i længerevarende proces, hvor risikovurderingsrelateret kompetencer udvikles gennem assimilativ læring. Grunden til at det skal ske gennem assimilativ læring, er at her indoptages og indpasses sanseindtryk som tilføjelser og udbygninger af etablerede mentale skemaer (Illeris, 2015, s. 61). Dette kan være til gavn i forhold til deltagernes motivation, idet de ikke selv har valgt at skulle lære om risikovurderingsmetoder, men er blevet udvalgt af en fagsystemejer, hvilket ifølge Illeris (2003, s. 103) kan svække følelsen af medbestemmelse og mindske den indre motivation. Det kan styrke deltagernes motivation, hvis læringen tager udgangspunkt i deres egen hverdag på arbejdspladsen og de arbejdsopgaver deltagerne arbejder med til daglig, hvor læringen med risikovurderingsmetoden gennem assimilativ læring optages i allerede etablerede skemaer omhandlende arbejdslivet. Dette vil også blive præciseret i afsnit 5.3 *Planlægning og design af workshop*.

5.2.2 Deltagere

I forhold til deltagerne, der skal engageres i workshoppen, er der tre spørgsmål, facilitatoren skal have svar på. De tre spørgsmål er:

1. *Hvem kan sikre, at vi når formålet med processen?*
2. *Hvem er deltagerne?*
3. *Hvilket niveau af involvering skal deltagerne have i processen?* (Van Loon, Andersen, & Larsen, 2016, s. 61).

Svaret på det første spørgsmål findes i organiseringen af informationssikkerhedsarbejdet (se afsnit 3.3.2), hvor det fremgår, at det er fagsystembrugerne, som skal udføre risikovurdering. Fagsystemejerne skal samtidigt også have muligheden for at deltage, i og med de gennem samme læringsproces, kan støtte fagsystembrugerne videre i processen, og medbringe viden, som kan være essentiel i forhold til risikovurderingen.

Svaret på spørgsmål to er, at deltagerne er medarbejdere i Hjørring Kommune. Da der er tale om fagsystembrugerne er deltagerfeltet meget bredt i forhold til uddannelsesniveau, alder og køn. Fagsystemerne spænder fra at være uddannet sundhedsplejersker til it-medarbejdere og er alt fra akademisk uddannet til faguddannet. Samtidigt er aldersgruppen også mellem 18-67, og begge køn er ligeledes også præsenteret. Ifølge Illeris (2015) spiller uddannelsesniveau, alder og køn en stor rolle i forhold til læringen. Uddannelsesniveau har betydning, da det kan forklare, hvordan deltageren deltager i læringen. Hvis deltageren har en faguddannelse, som er praksispræget gennem elevtid eller praktik, så vil man være tilbøjelig til at have en praktisk tilgang til læring. Hvis deltageren derimod har en akademisk uddannelse, har deltageren en erfaring med læring, der har en teoretisk tilgang, og deltageren vil gå mere analytisk og refleksivt til læringen. Alder har også en betydning idet de yngre deltagere, der lige er kommet ud på arbejdsmarkedet, vil have en åben tilgang til læring, idet de er vant til en åben og kompetenceudviklende tilgang til læring gennem deres uddannelsesproces. De ældre deltagere vil være mere lukket mod læring, da de har været vant til en færdighedsudviklende tilgang til læring, måske endda indeholdende udenadslære. Til sidst kan køn have en stereotyp tilgang til læring, f.eks. har mænd en større praktisk og rationel præference, hvor kvinder har en relationel og kreativ præference i forhold til læring (Illeris, 2015, s. 40-46). Derfor skal der i designet af workshoppen tænkes i, hvordan indholdet kan tilpasses til alle deltagerne uanset uddannelsesniveau, alder og køn, og samtidigt have et motiverende aspekt.

Til at svare på spørgsmålet om graden af deltagernes involvering benyttes Senges involveringsniveauer som består af *telling*, *selling*, *testing*, *consulting* og *co-creation* (Van Loon, Andersen, & Larsen, 2016, s. 38). I denne workshop benyttes først *telling*, da det er her formålet med risikovurderingen bliver præsenteret. Formålet med risikovurdering er fastlagt, og kan ikke ændres, men har betydning for deltagerne. Formålet er fastlagt ud fra ISO27001-standarden som Hjørring Kommune skal efterleve gennem Den fællesoffentlige digitaliseringsstrategi. Dernæst benyttes *testing*, da *testing* benyttes, når der er udarbejdet et bud på en løsning

som deltagerne skal teste (Van Loon, Andersen, & Larsen, 2016, s. 39). I denne workshop skal deltagerne teste informationssikkerhedsfunktionens bud på en risikovurderingsmetode. Til sidst benyttes *co-creation* som benyttes til at tale om en åben proces, hvor der samskabes løsninger og beslutninger (Van Loon, Andersen, & Larsen, 2016, s. 40). I denne workshop skal deltagerne i samarbejde komme med idéer til, hvordan processen med risikovurderingen skal foregå i fremtiden, om risikovurderingsskemaet skal udfyldes i forbindelse med en workshop, interview eller gennem e-læring eller andre måder, som deltagerne finder på. Ifølge Illeris (2003, s. 101) kan involvering på *co-creation*-niveauet være gavnligt for de voksne deltageres læring, idet de har en følelse af medansvar (betydningen af medansvar for voksnes læring kan læses mere om i afsnit 3.2.3).

5.2.3 Miljø

Miljøet omkring denne workshop er bestemt ud fra, at det skal foregå på arbejdspladsen. Her er problemet pladsmanglen, som Illeris (2003) også nævner. Det har været meningen, at deltagerne skulle sidde samlet i små grupperinger, for at skabe et uformelt miljø, hvor samarbejde er i fokus. Dette kunne ikke lade sig gøre i de lokaler, der kunne bookes på grund af størrelsen. Derfor skal deltagerne sidde i en hestesko, hvilket giver god mening i forhold til de forskellige præsentationer af begreberne, da alle deltagere vil have mulighed for at se. I gruppearbejdet vil deltagerne så skulle flytte sig, så de sidder over for hinanden. Dette kan resultere i forstyrrelser, der kan forsinke gruppearbejdet, hvilket skal tænkes ind i designet. For at byde deltagerne velkommen i et rart miljø, vil de blive mødt af en velkomstplakat, de vil blive budt velkommen, der bliver sørget for kaffe og kage til deltagerne, og samtidig vil formål og dagsorden hele tiden være synligt på en flipover. Disse virkemidler er valgt for at skabe et rart læringsmiljø (Van Loon, Andersen, & Larsen, 2016, s. 74).

5.2.4 Form

Formdimensionen omhandler hvilke metoder, der skal anvendes for at nå målet og for at skabe involvering og mening for deltagerne. Metoderne anvendes, så der skabes variation, som er med til at sikre deltagernes engagement (Van Loon, Andersen, & Larsen, 2016, s. 83). Metoderne benyttet i denne workshop, bruges til at præcisere hvilken del af risikovurderingen, der er i gang med at blive præsenteret, sårbarhed og trusselsidentifikation, og til sidst ved *co-creation* seancen. Den første metode er *individuel refleksion*, som benyttes ved sårbarhedsdelen, hvor deltagerne skal vurdere deres fagsystems sårbarhed i forhold til fortrolighed, forretningskritikalitet og finansiel værdi. Dette vælges, således at alle deltagere har mulighed for at få tid til at notere deres tanker og spørgsmål, samt at bidrage til fællesskabet (Van Loon, Andersen, & Larsen, 2016, s. 84). Dernæst benyttes metoden *samtale i lille gruppe*, hvor deltagerne vil sidde sammen to og to, eller tre og tre alt efter hvordan det går op med deltagerantal, for at hjælpe hinanden med at identificere truslerne mod deres fagsystem. Dette kan være med til at skabe tryghed for deltagerne og give lov til at flere synspunkter kommer i spil. Det er dog vigtigt at sikre sig, at grupperne fungere og alle føler sig trygge. Dette sker under workshoppen, hvor man kan hjælpe gruppen på vej ved at stille spørgsmål eller dele gruppen op (Van Loon, Andersen, & Larsen, 2016, s. 84). I *co-creation* seancen benyttes metoden *produktion i grupper*, hvor deltagerne bliver

inddelt i grupper på 3-6 deltagere. Her skal de komme med input til, hvordan processen med udfyldningen af risikovurderingsskemaet skal foregå i fremtiden. Det gode ved *produktion i grupper*, er at deltagerne kan komme med mange bud ad gangen som bliver en del af en fælles beslutning (Van Loon, Andersen, & Larsen, 2016, s. 85). Hver opgave slutter af med en *runde*, som er en metode, hvor alle kommer til orde. Et opmærksomhedspunkt er, at *runden* kan tage lang tid, og der derfor skal sættes tid af til dette (Van Loon, Andersen, & Larsen, 2016, s. 85). Ifølge Illeris (2015, s. 145-146) kan disse metoder, hvis det bliver til deltagerstyrede systemer, fører til social læring, som har indvirkning på den individuelle læring. Da deltagerstyrede systemer opererer i et spændingsfelt mellem kreativitet, magt og ansvarlighed som leder til læring gennem handling, refleksivitet, kommunikation og samarbejde.

5.2.5 Roller

Det er vigtigt at forventningsafstemme roller i forhold til projektleder og medfacilitatorers roller. Projektlederen har overblik og styrer processen, imens medfacilitatorene skal have specifikt definerede roller (Van Loon, Andersen, & Larsen, 2016, s. 94). Rollerne deles ud mellem medarbejderne i informationssikkerhedsfunktionen, således at den studerende, der skriver dette speciale, er projektleder, en anden medarbejder står for at dele tingene ud til opgaverne i processen og have et praktisk overblik. Den sidste medarbejder sørger for at notere detaljer ned omkring processen, som kan benyttes til evaluering af workshoppen gennem deltagerobservation.

5.3 Planlægning og design af workshop

Til at planlægge og designe workshoppen bliver der benyttet en drejebog, hvor formålet er at få gennemtænkt, hvordan formålet opnås, fordelingen af roller og ansvaret samt hvordan processen skal ledes. Derudover er der flere praktiske ting, som der skal tages stilling til, såsom længden af workshoppen og mængden af pauser, stemningen samt hvilke materialer, som skal anvendes. Drejebogen er samtidig med til at give tryghed, og giver mulighed for at vide, hvor tid kan spares undervejs, hvis det skulle blive nødvendigt (Van Loon, Andersen, & Larsen, 2016, s. 102-103). Workshoppen i forbindelse med dette speciale varer 2 timer og er delt op i fire faser: præsentation, sårbarhed, trusler og en afsluttende del. Disse dele vil blive præsenteret samt tankerne bag.

5.3.1 Præsentation

Præsentationen varer 10 minutter, hvor deltagerne bliver præsenteret for informationssikkerhedsfunktionen, hvilken afdeling vi hører til og hvilke opgaver vi arbejder med i forbindelse med informationssikkerhed. Derefter bliver deltagerne præsenteret for formålet og en flipover med dagsordenen præsenteres. Præsentationen af informationssikkerhedsfunktionen er valgt for at skabe en begyndende relation mellem informationssikkerhedsfunktionen og fagsystemsbrugerne, som skal udvikle sig over længere sigt. Formålet og dagsorden bliver præsenteret, så deltagerne er bevidste omkring, hvad de skal lære på workshoppen og da dagsorden er på en flipover, kan de hele tiden følge med i, hvad næste skridt i processen er. Herefter er der et oplæg, hvor deltagerne bliver bevidste om, hvorfor de skal til at udføre risikovurderinger. Dette er præget af en

udviklingsorienteret læring, da hele kommunen bliver påvirket af risikovurderingerne, og der opstår flere problemstillinger omkring informationssikkerhed, som en risikovurdering kan være med til at forebygge.

5.3.2 Sårbarhed

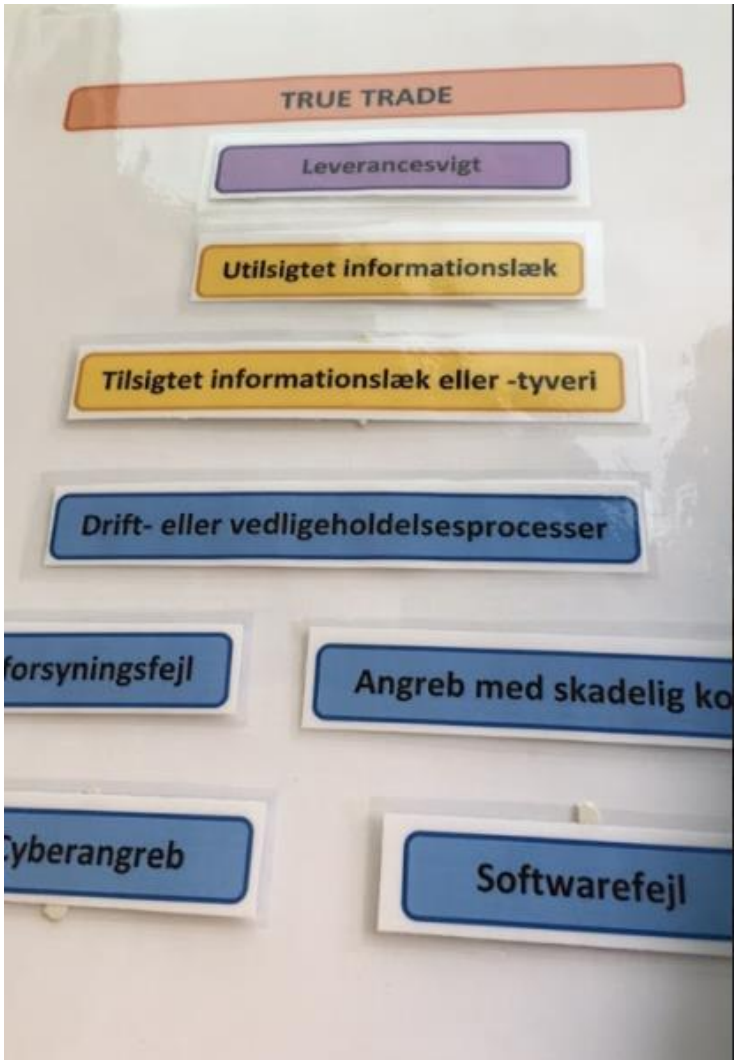
Sårbarhedsfasen starter med et oplæg omkring sårbarhed, workshopsdeltagerne bliver præsenteret for sårbarhedsklassifikationerne med tilhørende praksiseksempler som varer 10 minutter. Dette er valgt for at have en tilpasningsorienteret læringstilgang, hvor deltagerne bliver præsenteret for en bestemt metode til at vurdere sårbarhed. Det sparer tid i forhold til, hvis deltagerne selv skal udvikle metoden, men også for at gøre deltagerne trygge gennem en foruddefineret metode. Derefter skal deltagerne arbejde med metoden sammen i par, hvor de skal udfylde et skema som er illustreret i Figur 5.2.

Figur 5.2: Sårbarhedsvurdering

Denne opgave er valgt for, at deltagerne får fornemmelsen af, hvordan det vil se ud, når de skal sidde med risikovurderingsskemaet. Deltagerne skal arbejde sammen i par, så de kan diskutere de forskellige klassifikationer, hvilket de har 10 minutter til. Herefter diskuteres deltagernes refleksioner i plenum, således at læringstilgangen igen bliver udviklingsorienteret, da det bliver diskuteret, hvordan det i fremtiden skal foregå, hvilket der er afsat 10 min til. I denne diskussion er det meningen at klassifikationerne skal diskuteres i forhold til deres brugbarhed i en risikovurdering.

5.3.3 Trusler

Trusselsfasen starter med en præsentation af trusselstyperne, og hvilke trusler der tilhører disse typer, hvilket varer 10 minutter. Herefter skal deltagerne i par identificere truslerne gennem et puslespil, hvor deltagerne får udleveret truslerne som brikker. Truslerne er skrevet med forskellig farvet skrift, så det passer til de før præsenteret trusselstyper, så deltagerne kan bruge den viden de har lært omkring trusselstyperne. Her tages igen udgangspunkt i en tilpasningsorienteret læringstilgang, hvor deltagerne igen bliver præsenteret for en bestemt metode og udvalgte trusler. Der er sat 15 minutter af til opgaven, og et eksempel på et resultat kan ses i Figur 5.3.



Figur 5.3: Resultat af trusselsopgaven

Puslespillet er valgt på baggrund af, at deltagerne kan diskutere og reflektere over de forskellige trusler og tilhørende typer i forhold til fagsystemer. Efter opgaven er der diskussion i plenum, som varer 10 minutter, hvor deltagerne bliver præsenteret for de mest hyppige trusselstyper mod fagsystemer som er leverandørrelaterede trusler og bruger- og it-driftsmæssige trusler.

5.3.4 Afsluttende del

I et fem minutters oplæg bliver deltagerne præsenteret for risikovurderingsværktøjet, hvor et eksempel på en risikovurdering bliver præsenteret. Dette er valgt for at vise deltagerne, hvad deres arbejde bliver brugt til efter de har afleveret risikovurderingsskemaet. Herefter er der en brainstorming opgave, hvor deltagerne i større grupper i 20 minutter skal give bud på, hvordan de i fællesskab med informationssikkerhedsfunktionen kan foretage risikovurderinger i fremtiden. Deltagerne skriver deres idéer ned på små sedler. Denne opgave er valgt for at give deltagerne ejerskabsfornemmelse for en del af processen og samtidigt lade dem selv styre, hvordan de vil indgå i et lærings- og udviklingsforløb i forbindelse med risikovurdering, som Illeris beskriver det (Illeris, 2003, s. 97-101). Samtidigt er dette også en udviklingsorienteret læringstilgang, da der bliver reflekteret over, hvordan risikovurderingsprocessen skal foregå i fremtiden. Derefter er der en 10 minutters afsluttende opsamling, hvor deltagernes bud bliver diskuteret og de bud, hvor flest er enige, bliver skrevet ned, så informationssikkerhedsfunktionen kan udvikle på idéerne til næste iteration, og deltagerne bliver mindet om, at de får tilsendt et evalueringsskema, hvor de skal være med til at evaluere workshoppen.

6 Fase 4 – Evaluering

Dette kapitel omhandler forbedringspotentialepunktet 5: *I forbindelse med undervisningen skal risikovurderingsmetoden afprøves og evalueres for at metoden kan videreudvikles.* Den første del af dette kapitel vil evaluere på, om workshops kan bruges som undervisningsgrundlag for risikovurderinger, hvilket undersøges gennem interviews med workshopsdeltagerne. Den anden del evaluerer på selve risikovurderingsmetoden, som undersøges gennem deltagerobservationer, hvor de tre medarbejdere fra informationssikkerhedsfunktionen har observeret workshoppen. Til sidst præsenteres forbedringspotentialet til næste iteration.

6.1 Evaluering af workshop som grundlag for risikovurdering

Et af formålene med workshoppen er, at finde ud af om workshop er en passende metode til at udføre risikovurderingen fremover eller om der er andre metoder der kan være mere passende ifølge fagsystembrugerne.

6.1.1 Metode

For at undersøge om workshop er en passende metode til at udføre risikovurdering benyttes interview af workshopsdeltagerne. Grunden til dette er, at et interview kan være med til at opnå viden om menneskers livssituation, meninger, holdninger og oplevelser (Tanggaard & Brinkmann, 2015, s. 53). I dette speciale, er det blevet prioriteret at få så mange workshopsdeltagernes mening omkring workshoppen, på grund af den store diversitet mellem deltagerne, og derfor har der til denne interviewundersøgelse været en alternativ tilgang. Grunden til dette er for det første, at det vil tage lang tid at udføre 22 interviews, især i forhold til udførelsen og transskribering af interviewene, og det vil heller ikke være muligt at udføre klassiske interviews med workshopsdeltagerne, idet at deltagerne har andre og højere prioriterede arbejdsopgaver, og det derfor var svært for deltagerne at afsætte tid til et interview. Samtidigt har informationssikkerhedsfunktionen en deadline i forhold til at få rapporteret resultatet og skal i gang med næste iteration. En anden begrundelse for at ikke vælge det klassiske interview er, at intervieweren er en del informationssikkerhedsfunktionen, og derfor også var til stede og en del af workshoppen. Det kan derfor være svært for informanterne, at give ærlige svar, hvis de sidder overfor én af dem, der var med til at skabe workshoppen og risikovurderingsmetoden.

Deltagerne har fået tilsendt et link på mail, som ledte videre til en Google Analyse formular, som minder om et spørgeskema (resultatet kan ses i Bilag A). Denne måde er valgt, da det er med til at samle svarene et sted, så analysen af svarene bliver mindre tidskrævende. Herefter bliver deltagerne bedt om at give deres samtykke til, at besvarelsen kan indgå som en del af dette speciale samt at svarene vil fremgå anonym i specialet. Derefter bliver de præsenteret for selve interviewguiden, som består af to spørgsmål. De to spørgsmål er inspireret af feedbackmetoden til evaluering af facilitatoren (Van Loon, Andersen, & Larsen, 2016, s. 199), hvor deltagerne skal først give feedback omkring, hvad der fungerede godt i workshoppen og hvorfor, og herefter det der fungerede mindre godt og hvorfor. Valget på disse spørgsmål er valgt på grund af, at det er workshopsdeltagernes mening omkring workshoppen, der undersøges for at finde ud af om denne metode er værd at benytte

videre i risikovurderingsprocessen. Spørgsmålene minder om et semistruktureret interview i forhold til de åbne spørgsmål, men da intervieweren ikke kan stille opfølgende spørgsmål til informanten er interviewet i sin egentlig udgave struktureret. Svarene er herefter analyseret på baggrund af en meningskondensering som er datadrevet, der er valgt som analyseteknik grundet specialets postfænomenologiske retning (kodningen af besvarelserne kan findes i bilag B). Meningskondenseringen er foregået ved, at interviewsvarene først er gennemgået og derefter inddelt i meningsbærende afsnit, hvorefter der er skrevet fortolkende noter til hvert afsnit. Fortolkningerne er foretaget ud fra de didaktiske overvejelser i designet af workshoppen, men samtidigt også de observationer, jeg som deltager som observatør, har observeret som en del af workshoppen.

I stedet for Google Analyse, kunnet der med fordel være benyttet e-mailinterview, da det vil give intervieweren mulighed for at stille opfølgende spørgsmål, og dermed gå dybere ind i informanternes mening og opfattelse af workshoppen. Dette er ikke valgt grundet tidsforbruget i forhold til at følge op på alle svarene, og samtidigt går den anonyme fordel væk. Ved et e-mailinterview ved intervieweren, hvem informanten er, og kan derfor have forudbestemte forestillinger omkring informantens person, hvilket undgås ved Google Analyse, idet alle informanter er anonyme fra start af.

6.1.2 Resultat

Der var 12 ud af 22 workshopsdeltagere, som svarede på interviewet. En begrundelse kan være, at der er en kort svarfrist, og nogle af deltagerne havde andre højere prioriteret opgaver. Det er heller ikke alle deltagere, som har svarede på alle spørgsmål. En forklaring kan være, at det kan være svært for nogle at beskrive meninger og oplevelser på skrift, og derfor har sprunget disse spørgsmål over, hvor man skulle beskrive, eller de ikke mente, de havde nogle oplevelser eller meninger at bidrage med. Parenteserne i næste afsnit henviser til bilag A.

Det første spørgsmål lød: ”*Hvad fungerede godt i workshoppen og hvorfor?”*. Her er der flere af deltagerne, der beskriver at vekslen mellem oplæg og gruppearbejde fungerede godt. En deltager beskriver det således: *” Jeg synes, at det var rart, at workshoppen var godt planlagt, opgaverne i gruppeopgaverne var overskuelige, og tiden passede. Der var en god variation mellem oplæg og gruppeopgaver.”* (interview, spg. 1, svar 1). Hvilket betyder, at tanken med den vekslende læringssituationer har passet godt til deltagerne, og samtidigt kan det også betyde, at flere af deltagerne har brug for at diskutere emnerne i grupper, før de ytrer deres mening i gruppediskussioner, hvilket en deltager beskriver: ”*Vekslen mellem oplæg og opgaver, hvor der blev plads til diskussion i mindre grupper”* (interview, spg 1, svar 9). Det kan derfor være en idé, at risikovurderingsprocessen skal være præget af gruppearbejde, hvor fagsystembrugerne kan diskutere f.eks. identificering af trusler med hinanden og dermed viden- og erfaringsdele med hinanden. Flere af deltagerne har også haft udbytte af de følgende diskussioner efter opgaverne, hvor en deltager beskriver det således: *” En god struktur med diskussion fra alle om hvordan vi griber risikovurdering/konsekvensberegningen an.”* (interview, spg. 1, svar 3). Altså kan det være en idé at tænke vidensdeling i større grupper ind i risikovurderingsprocessen. En sidste del

af deltagerne har haft stort udbytte af de forskellige oplæg fra underviseren, hvor en deltager beskriver det således: *" Der var en fin gennemgang af de forskellige trusler"* (interview, spg. 1, svar 6) og en anden deltager beskriver det meget kort: *" Oplæg – Dejligt med forklaring"* (interview, spg 1, svar 11). Svarene på dette interviewspørgsmål indikerer, at det vil passe deltagerne i en risikovurderingsproces, at der er forskellige læringstilgange, som både omfatter traditionel undervisning, gruppearbejde samt vidensdeling og diskussioner i større grupper. En løsning på dette kan være, at alle medarbejdere, der skal foretage en risikovurdering først skal igennem en introworkshop, og derefter i næste risikovurdering selv bestemme om risikovurderingen skal foretages gennem en undervisningsseance, gruppearbejde, vidensdeling med andre eller på egen hånd. På denne måde imødeses også voksne lærendes behov for medbestemmelse i læringen som Illeris beskriver det ((Illeris, 2003, s. 123-124).

Det andet interviewspørgsmål er *" Hvad kunne være anderledes i workshoppen og hvorfor?"*. Her svarer en af deltagerne, at det kan være idé at opdele deltagerne på forvaltningsniveau: *" […] Men skulle jeg pege på noget, ville det måske fungere ligeså godt, hvis det kun havde været Borgerservice – vi har systemer nok at tage fat på. Der var måske ikke så meget input fra de andre forvaltninger."* (interview, spg. 2, svar 1). En anden deltager svarer i denne sammenhæng også, at der skulle bruge mere tid på at undersøge deltagernes forudsætninger: *" Hmnnn, I kunne gøre endnu mere ud af at undersøge deltagernes forudsætninger, så I rammer endnu mere præcist"* (interview, spg 2, svar 4). Det vil derfor være en idé at inddele medarbejderne, der skal udføre en risikovurdering ind på forvaltningsniveauer, hvilket også vil gøre det nemmere at undersøge deltagernes forudsætninger, da de vil arbejde med flere af de samme arbejdsopgaver. Samtidigt kan det også føre til en samhørighed blandt deltagerne, og de vil næste gang de skulle foretage en risikovurdering kunne mødes internt i forvaltningen og hjælpe hinanden. En udfordring ved dette er, at ikke alle forvaltninger er ansvarlige for lige mange forretningskritiske fagsystemer, og her skal flere forvaltninger deltage sammen for at opnå vidensdeling på tværs. Der var også flere af deltagerne, der gav udtryk for en frustration over de forskellige begreber, især sårbarhedsklassifikationerne. En deltager beskriver det således: *" Lidt mere uddybende i fortrolighedsklassifikation"* (interview, spg. 2, svar 10). Et løsningsforslag er, at gennemse sårbarhedsklassifikationerne og lave bedre beskrivelser af begreberne så de bliver præcise og praksisnære. En idé kan være at lave et univers på medarbejderweb, hvor medarbejderne kan orientere sig omkring risikovurdering og lære begreberne, så de kan være bedre forberedte til en risikovurdering. Til sidst er der en deltager, der ikke er motiveret for workshoppen i og med, at der ikke er foretaget en risikovurdering eller sat en deadline for en risikovurdering. Deltageren beskriver det således: *" Jeg er stadig meget i tvivl om hvorfor man har valgt at lave en workshop nu, når man ikke er klar til at gå i gang med risikovurderingerne på de enkelte systemer endnu. Jeg vil personligt gerne have ventet med workshoppen til vi havde en konkret opgaven/deadline at forhold os til."* (interview, spg. 2, svar 6). For at undgå dette i næste skridt i risikovurderingsprocessen, kan omdrejningspunktet og formålet med workshoppen være, at deltagerne i sidste ende får foretaget en risikovurdering.

6.2 Evaluering af risikovurderingsmetoden

Det andet formål med workshoppen er, at afprøve risikovurderingsmetoden på fagsystembrugerne og om hvorvidt begreberne er forståelige og meningsfulde i forhold til risikovurderingen.

6.2.1 Metode

For at undersøge om risikovurderingsmetoden kan bruges af fagsystembrugerne benyttes metoden deltagerobservation, hvor fokus er på sårbarhedsbegreberne og -klassifikationerne samt om identificering af trusler mod fagsystemer giver mening. I dette speciale er den overordnet metode deltagerobservation, hvor observationstypen deltageren som observatør er benyttet, hvorimod i sammenhængen med workshoppen er observationstypen observatøren som deltager benyttet. Grunden til dette er, at workshoppen har varet to timer, og der er derfor begrænset af tid til at observere og samtidigt er observatørerne også facilitatorer. Observationen er foregået ved, at tre medarbejdere fra informationssikkerhedsfunktionen har observeret. Én af observatørerne har samtidigt haft rollen som underviser på workshoppen, en anden observatør har skulle stå for de praktiske ting ved workshoppen, som f.eks. at uddele opgavemateriale og stå for forplejning, og den sidste observatør har kun haft observatørrollen, men har ikke kunnet fuldt ud deltage i den ene af de to workshops.

Fordelene ved at være tre observatører har været, at observationen ikke kun er begrundet i en observatørs subjektive oplevelse af workshoppen, men at flere observatører har kunnet bidrage med deres oplevelser og samtidigt har kunnet verificere hinandens oplevelser. Samtidigt har det også været nødvendigt med flere observatører grundet de forskellige roller to af observatørerne har haft i forbindelse med workshoppen. En ulempe ved de tre observatører er, at alle observatører er en del af informationssikkerhedsfunktionen og dermed har en aktie i risikovurderingsværktøjet og -metoden. Dermed kan observatørerne have et blindt øje i forhold til metoden, og derfor have en oplevelse af workshoppen, som er tæt knyttet med risikovurderingsmetoden og dermed have svært ved at sætte sig ind i fagsystembrugernes negative oplevelser med risikovurderingsmetoden. En løsning på dette problem kunne have været at optage workshoppen enten ved hjælp af lydoptager eller et kamera, således at observatørerne kunne gennemse workshoppen igen og derved få et andet perspektiv på workshoppen, som vil være mere ude fra og ind på workshoppen. Dette er valgt fra, da det ikke var muligt at booke de mødelokaler, som blev brugt til de to workshops, god tid i forvejen, således at det var muligt at opstille det nødvendige udstyr. Samtidigt deltog 22 fagsystemsbrugere og -ejere i de to workshops, som alle skulle give lov til at optage og bruge optagelserne i evalueringsarbejdet, hvilket vil have taget lang tid, og hvis én deltager ikke ville give lov til optagelse, kunne det ikke lade sig gøre. En anden løsning på blind spot-problemet kan være at inddrage workshopsdeltagerne i denne del af evalueringen, men det er blevet vedtaget, at holde dem ude, for at de ikke skulle deltage i for mange interviews, og fordi det er vurderet, at denne del af workshoppen ville have været svært at svare på i forhold til den form for interview, som der har været tid til at foretage.

Observationerne fra de tre observatører er diskuteret på møder, som er placeret i forlængelse af workshoppen, efter at deltagerne har forladt lokalerne. Derefter er observationerne analyseret og fortolket på baggrund af viden indsamlet i kapitel 3: Fase 1 – Domænekendskab.

6.2.2 Resultat

Deltagerobservationerne har fokus på især to dele, sårbarhed og trusler, da disse to er det som fagsystembrugerne skal vurdere i forbindelse med risikovurderingen. Generelt oplevede observatørerne, at fagsystembrugerne og -ejerne var motiverede i forhold til risikovurderingen.

De første observationer, med henblik på risikovurderingsmetoden, er i forbindelse med den første opgave, hvor deltagerne skal klassificere deres fagsystem i forhold til fortrolighed, forretningskritikalitet og finansiel værdi. Her har observatørerne oplevet, at der var stor forskel på de valgte fagsystemer og især særdeleshed deres kompleksitet. De fagsystemer, som er forbundet særligt til få arbejdsprocesser, som f.eks. True Trade, som er et e-handelssystem, oplevedes som nemmere at klassificere i forhold til fagsystemer, som var forbundet til mange arbejdsopgaver så som SBSYS, som er kommunens journaliseringssystem på forskellige forvaltningsområder. Her passede risikovurderingsmetoden ikke til de store og komplekse fagsystemer. Samtidigt fandtes det også, at nogle af fagsystemer ikke er forretningskritisk. Et eksempel er Microsoft Office-pakken, som er med i workshoppen, hvor de data, der generes gennem dette fagsystem ikke lagres i systemet, men på kommunens servere. Samtidigt kan Microsoft Office-pakken mere kaldes et værktøj frem for et fagsystem, da det bruges som skriveredskab eller regneark.

I opsamlingen efter sårbarhedsopgaven er begreberne diskuteret. Fortrolighedsklassifikationen har en klassifikation, der mindede for meget om fortrolighedsklassifikationer, som de ses ved f.eks. forsvaret, som ikke er tilpasset en kommune, og flere af deltagere giver udtryk for, at denne klassifikation ikke er passende i forhold til en risikovurdering af fagsystemer. Den finansielle værdi giver heller ikke mening for deltagerne. De deltagerne der er fagsystembrugere af et forretningskritisk fagsystem har alle en høj finansiel værdi, hvilket betyder, at et loft på 100.000 DKK eller mere ikke giver et fyldestgørende billede af fagsystemernes værdier. Den sidste klassifikation, forretningskritikalitet, giver ikke mening for deltagerne. Både ordet forretningskritikalitet og klassifikationen passer ikke til kommunens behov, og samtidigt er det svært for informationssikkerhedsfunktionen at forklare klassifikationen, således at den giver mening for deltagerne.

Det andet, der er observeret er trusselsidentifikationsopgaven. Her er det tydeligt, at deltagerne har stor værdi i at samarbejde omkring denne opgave. Det giver også mening for deltagerne, at de kan vælge en trussel, snakke om den sammen med andre og derefter vælge om truslen er reel for deres fagsystem. Flere nævnte på workshoppen, at det er nemmere sammen med andre, end det vil være at identificere truslerne alene, da de får sat flere øjne på fagsystemerne. Det kan betyde, at risikovurderingsmetoden er afhængig af, at fagsystembrugerne har mulighed for at diskutere truslerne med andre for at identificere dem. Det kan også betyde, at i første

omgang er det bedst at identificere truslerne igennem en samtale, men efter fagsystembrugerne får mere erfaring, bliver det en opgave som de kan udføre alene.

6.3 Forbedringspotentiale

Efterfølgende på et møde i informationssikkerhedsfunktionen er resultaterne for hhv. interviewene og observationerne diskuteret og har resulteret i følgende forbedringspunkter til næste iteration:

- Sårbarhedsklassifikationen fortrolighed skal defineres præcist og være praksisnært.
- Sårbarhedsklassifikationerne forretningskritikalitet og finansiel værdi skal udskiftes med tilgængelighed og integritet, således at klassifikationen følger Hjørring Kommunes informationssikkerhedspolitik, hvor der står, at kommunen arbejder med informationssikkerhed med fokus på fortrolighed, integritet og tilgængelighed.
- På medarbejderweb skal der under informationssikkerhed være en afdeling omkring risikovurdering, hvori der vil være et begrebsopslag til orientering om risikovurderingsbegreberne og læringsvideoer, hvor risikovurdering bliver beskrevet nærmere, som fagsystembrugerne kan benytte i forbindelse med risikovurdering.
- Fagsystembrugerne inviteres til en introduktionsworkshop, hvor formålet er at få udført en risikovurdering. De bliver opdelt på forvaltningsområder, undtaget de forvaltninger med få fagsystemer, som bliver slået sammen for at kunne dele viden på tværs.
- Ved næste risikovurdering kan fagsystembrugerne vælge mellem at få udført en risikovurdering gennem en workshop, en gruppeøvelse, interviewøvelse med informationssikkerhedsfunktionen eller på egen hånd.
- Risikovurderingsværktøjet skal opdateres med de nye sårbarhedsklassfikationerne. Samtidigt skal værktøjet gøres så automatisk så muligt, således at der ikke skal bruges unødigt tid på administrative processer i forbindelse med risikovurdering af de mange fagsystemer.
- Der skal udvikles et skema til risikovurdering af fagsystemer til benyttelse af fagsystemsbrugerne.

7 Diskussion

I dette kapitel diskuteres risikovurderingsmetoden og -værktøjets generaliserbarhed, undersøgelsens validitet samt den gennemgående metode deltagerobservation.

7.1 Designets generaliserbarhed

I forhold til designets generaliserbarhed, kan der diskuteres generaliserbarheden for to ting: risikovurderingsmetoden og risikovurderingsværktøjet.

Risikovurderingsværktøjet er et værktøj, hvor det er muligt at tilpasse værktøjet til den enkelte organisation, da det er designet i Microsoft Excel, hvilket gør det fleksibelt i forhold til ændringen af designet. Man kan tænke sig, at et lille privat firma ikke har brug for alle truslerne i trusselskataloget, da de har outsourcet mange af deres databehandlingsopgaver, og derfor hurtigt kan fjerne et par af trusselstyperne, hvis de ikke er aktuelle for dem. Samtidigt kan en organisation som ikke vil bruge samme sårbarhedsklassifikation eller talskala til at vurdere risiciene hurtigt lave disse om, uden det kræver den store viden indenfor brugen af Excel, og denne proces vil samtidigt gøres nemmere ved at udvikle en brugervejledning. Den største ulempe ved Microsoft Excel, er at der i risikoværktøjet er en række prædefineret formateringer som hvis de ændres for meget, kan tage det automatiserede og "smarte" væk fra risikovurderingsværktøjet. Det er muligt at låse disse formateringer, men det kan også påvirke designets generaliserbarhed negativt. En løsning kan være at låse formateringer i celler, hvor det vurderes, at værdierne i cellerne ikke ændre på af andre organisationer. Derefter kan en brugervejledning formuleres til de formateringer, som er i celler med værdier, det vurderes, at andre organisationer har behov for at ændre på, for at tilpasse risikovurderingsværktøjet til netop deres organisation.

Risikovurderingsmetoden har ifølge undersøgelsen i kapitel 6 *Fase 4 - Evaluering*, nogle ulemper i forhold til generaliserbarhed, som skal ændres, hvis det skal være muligt at benytte metoden i andre organisationer. Her tænkes især på, at undersøgelsen viste, at risikovurderingsmetoden har svært ved at håndtere komplekse fagsystemer, såsom Hjørring Kommunes journaliseringssystem SBSYS. Her kan det tænkes, at organisationer, der er større end Hjørring Kommune og har flere komplekse fagsystemer vil opleve problemer ved brug af denne risikovurderingsmetode. Samtidigt er det også i et fremtidsperspektiv et problem, da det ifølge ISO27001-standarden ikke kun er fagsystemer, der skal laves en risikovurdering på, men også andre informationsaktiver, såsom arbejdsprocesser og servere, som kan være mere komplekse end fagsystemer. Derfor er det vigtigt, at dette problem bliver taget op i en videre iteration, således at risikovurderingsmetoden bliver i stand til at håndtere disse komplekse informationsaktiver.

7.2 Undersøgelsens validitet

Validitet omhandler hvorvidt undersøgelsens resultater reelt belyser forskningsspørgsmålet, eller i dette tilfælde problemformuleringen (Justesen & Mik-Meyer, 2010, s. 40). I dette speciale er det igennem specialet gået fra en stor fokus på risikovurderingsmetoden og risikovurderingsværktøjet til stadig fokus på

risikovurderingsmetoden, men derudover samspillet mellem informationssikkerhedsfunktionen, fagsystembrugerne og risikovurderingsmetoden. I kapitel 6 *Fase 4 – Evaluering*, er det workshoppen som didaktisk værktøj i forhold til at hjælpe fagsystembrugerne med at udføre en risikovurdering og selve risikovurderingsmetoden, der bliver evalueret og ikke risikovurderingsværktøjet. Det er der tre hovedgrunde til.

Den første hovedgrund er, at selvom risikovurderingsværktøjet er det digitale produkt og omdrejningspunktet for dette speciale, så kan værktøjet ikke eksistere uden risikovurderingsmetoden. Derfor giver det mest mening at evaluere på metoden, således at begreber og klassifikationer er på plads inden værktøjet bliver videreudviklet. Samtidigt hører risikovurderingsværktøjet og -metoden sammen, så når der skal laves ændringer i metoden, vil der også ske ændringer i værktøjet. Den anden hovedgrund er, at risikovurderingsværktøjet skal kun benyttes af informationssikkerhedsfunktionen, som også har været med til at udvikle og designe værktøjet og derfor vil en evaluering muligvis være fyldt af blinde pletter, da informationssikkerhedsfunktionen i forvejen er tilfredse med værktøjet. Den sidste hovedgrund er, at dette speciale har et fænomenologisk perspektiv, og derfor vil evalueringsundersøgelser bære præg af, at det er informanternes oplevelse af sociale fænomener, som der bliver undersøgt. En undersøgelse af værktøjet kan tænkes at have flere positivistiske træk, hvor det er selve funktionerne i værktøjet der bliver undersøgt gennem kvantitative data, f.eks. brugertest, hvor det ses på, hvor gode brugerne er til at benytte værktøjet.

I et fænomenologisk perspektiv er der en variation af validitet, som kaldes respondentvalidering, hvor dele af analysen præsenteres for informanterne, der har bidraget til det empiriske materiale, og de har så mulighed for at kommentere og korrigere på forskerens analyse og fortolkning af deres udsagn (Justesen & Mik-Meyer, 2010, s. 47). Dette har ikke været muligt, idet at informanterne i interviewundersøgelsen har været anonyme, og derfor kan det ikke vides hvem af workshopsdeltagerne som har responderet. En løsning kan være at sende analysen til alle workshopsdeltagerne og lade dem kommentere, men det er vurderet til at tage for lang tid i forhold til processen med at udarbejde speciale.

7.3 Metode

I dette speciale har den overordnet metode været deltagerobservationer med den primære rolle som deltager som observatør. Begrundelsen for dette har været, at jeg har haft Hjørring Kommune som samarbejdspartnere og udviklet risikovurderingsmetoden og -værktøjet for dem, imens jeg har været ansat som studentermedhjælper. Dette har bevirket, at jeg har haft adgang til viden, som studerende med en samarbejdspartner ikke har haft, i og med jeg haft har min daglige gang på rådhuset. Derfor er flere informationer, især i forhold til afsnit 3.3.2 *Organisering af informationssikkerhedsarbejdet* og kapitel 5 *Fase 3 – Afprøvning i praksis* samt kapitel 6 *Fase 4 – Evaluering* indhentet gennem denne metode, ved at være en del af dagligdagen på rådhuset. Dette giver fordele i og med, jeg har opbygget relationer til informanterne og har været en del af et sæt uskrevne normer, men samtidigt kan det også have den effekt, at jeg har haft skyklapper og derfor haft blinde punkter i forhold til designet af risikovurderingsmetoden og risikovurderingsværktøjet, men også i forhold til afprøvning

af designet og den senere evaluering, som derfor ikke er belyst i dette speciale, og kan have en påvirkning på resultatet af undersøgelsen.

8 Konklusion

Specialet er udarbejdet ud fra et fænomenologisk perspektiv med Design-Based Research som overordnet metodologi for at besvare problemformuleringen:

> *Hvordan kan en risikostyringsmetode med tilhørende værktøj designes og implementeres i Hjørring Kommune således, at metoden og værktøjet kan understøtte kommunens arbejde med implementering af principperne fra ISO27001-standarden? Herunder udvikle færdigheder og kompetencer hos medarbejderne således, at de kan udføre en risikovurdering på kommunens fagsystemer?*

Den iterative tilgang til specialet har givet anledning til at problemstilling er besvaret gennem fire faser.

Den første fase er domænekendskab, hvor målet har været at skabe en kontekst hvori designprincipper kunne opstå. I denne fase er undersøgelsesspørgsmålene også forsøgt besvaret. Det første undersøgelsesspørgsmål *Hvordan har Hjørring Kommune indtil videre arbejdet med risikovurdering?* er besvaret gennem et feltstudie, som er udført i efteråret 2018. Her konkluderes det, at der er en række forbedringspotentialer i forhold til, hvordan kommunen arbejder med risikovurdering, bl.a. udvikling af risikovurderingsmetode og tilhørende værktøj, oprettelse af en struktureret risikovurderingsproces og uddannelse af medarbejdere, så disse kunne udføre en risikovurdering. Det andet undersøgelsesspørgsmål *Hvilke krav er der til risikovurdering i ISO27001-standarden?* dette er undersøgt gennem Digitaliseringsstyrelsens vejledninger, hvor det blev klargjort, at risikovurderingsværktøjet skal indeholde et informationsaktivarkiv, et trusselskatalog og en risikovurdering. Gennem Calder og Watkins' forskning er det belyst, at den optimale risikovurderingsmetode i forhold til principperne i ISO27001-standarden er en kvalitativ metode, hvor de relevante medarbejdere i kommunen inddrages i risikovurderingsprocessen. Det tredje undersøgelsesspørgsmål *Hvordan kan læring foregå på en arbejdsplads?* er besvaret ud fra et konstruktivistisk læringssyn og Illeris' forskning, hvor medarbejderne skal have medbestemmelse i læringssituationen og undervisningen skal bære præg af en tilpasnings- og udviklingsorienteret læringstilgang. Til sidst er der udviklet en Plan-Do-Act-Model for Hjørring Kommunes risikovurderingsproces og nye forbedringspotentialer er formuleret.

I fase 2 er designet udviklet. Første del af designet er udviklet på baggrund af forbedringspotentialepunkterne 1: *Der skal udvikles en risikovurderingsmetode, der kan benyttes af både informationssikkerhedsfunktionen og fagsystemsbrugerne* og 2: *Til at understøtte risikovurderingsmetoden skal der udvikles et risikovurderingsværktøj til brug af informationssikkerhedsfunktionen.* Først er der udviklet begreber til brug ved klassificering af fagsystemernes sårbarhed. Grunden til dette er, at Digitaliseringsstyrelsens vejledninger og Calder og Watkins' forskning fremstillede vigtigheden i at benytte

de specifikke begreber til risikovurderingen, således at resultaterne bliver sammenlignelige. Herefter er risikovurderingsværktøjet designet med et informationsaktivarkiv, et trusselskatalog og en risikovurdering i en Microsoft Excel-mappe. Herefter er risikovurderingsmetoden designet, med henblik på, at risikoen er et produkt af en sårbarhed og en trussel. Sårbarheden klassificeres ud for fortrolighed, forretningskritikalitet og finansiel værdi. Derefter er der i designfasen tænkt over forbedringspotentialepunktet 3: *Der skal overvejes, hvordan fagsystemsbrugernes risikovurderinger indgår i risikovurderingsværktøjet*. Her er der ved metoden storyboard udviklet en idé, hvor fagsystemsbrugerne tager til en workshop, hvor de få viden om, hvordan de skal udføre en risikovurdering og udfylder et risikovurderingsskema. Herefter sendes risikovurderingsskemaet til informationssikkerhedsfunktionen, hvor det derefter bliver behandlet i risikovurderingsværktøjet, hvor der i sidste ende vil være en komplet risikovurdering af fagsystemet.

I fase 3 er risikovurderingsmetoden afprøvet i praksis på baggrund af forbedringspotentialepunktet 4: *I forbindelse med risikovurderingen skal fagsystemsbrugerne, og i en hvis grad fagsystemsejerne, undervises i risikovurdering ud fra Illeris' teori om voksenlæring og principperne om tilpasningsorienteret og udviklingsorienteret læringstilgange.* Her er facilitering benyttet som metode og de didaktiske overvejelser er gennemarbejdet ved en designstjerne og en drejebog. De didaktiske overvejelser har især været fokuseret omkring deltagerne og vekslen mellem aktiviteter i workshoppen. Det har været vigtigt at planlægge aktiviteter, hvor deltagerne har mulighed for at viden- og erfaringsudveksle med hinanden, og samtidig give dem mulighed for medbestemmelse i næste del af iterationen.

I den sidste fase er designet og workshoppen evalueret ud fra forbedringspotentialepunktet 5: *I forbindelse med undervisningen skal risikovurderingsmetoden afprøves og evalueres for at metoden kan videreudvikles*. Her er workshoppen som didaktisk understøttelse i forbindelse med fagsystembrugernes risikovurdering evalueret gennem et skriftligt interview. Her har deltagerne nævnt, at de er tilfredse med vekslen af undervisning og opgaver i workshoppen, og muligheden for vidensdeling i løbet af workshoppen. Deltagerne synes, at workshoppen skal være delt op på forvaltningsniveauer, og der skal fra facilitatorernes side være mere fokus på deltagernes forudsætninger. Samtidigt synes deltagerne også, at sårbarhedsklassifikationerne er svære at benytte, og det ville give mere mening, hvis de skulle udføre en risikovurdering i forbindelse med workshoppen. Derudover er risikovurderingsmetoden evalueret ud fra deltagerobservation, hvor tre medarbejdere fra informationssikkerhedsfunktionen har evalueret på metoden. Her er resultatet, at sårbarhedsklassfikationerne ikke fungerer, og at fagsystembrugerne kan have stor værdi i at udføre risikovurderinger sammen med hinanden. Til sidst er nye forbedringspotentialepunkter præsenteret til næste iteration:

- Sårbarhedsklassifikationen fortrolighed skal defineres præcist og være praksisnært.

- Sårbarhedsklassifikationerne forretningskritikalitet og finansiel værdi skal udskiftes med tilgængelighed og integritet, således at klassifikationen følger Hjørring Kommunes informationssikkerhedspolitik, hvor der står, at kommunen arbejder med informationssikkerhed med fokus på fortrolighed, integritet og tilgængelighed.
- På medarbejderweb skal der under informationssikkerhed være en afdeling omkring risikovurdering, hvori der vil være et begrebsopslag til orientering om risikovurderingsbegreberne og læringsvideoer, hvor risikovurdering bliver beskrevet nærmere, som fagsystemsbrugerne kan benytte i forbindelse med risikovurdering.
- Fagsystemsbrugerne inviteres til en introduktionsworkshop, hvor formålet er at få udført en risikovurdering. De bliver opdelt på forvaltningsområder, undtaget de forvaltninger med få fagsystemer, som bliver slået sammen for at kunne dele viden på tværs.
- Næste risikovurdering kan fagsystemsbrugerne vælge mellem at få udført en risikovurdering gennem en workshop, en gruppeøvelse, interviewøvelse med informationssikkerhedsfunktionen eller på egen hånd.
- Risikovurderingsværktøjet skal opdateres med de nye sårbarhedsklassfikationerne. Samtidigt skal værktøjet gøres så automatisk så muligt, således at der ikke skal bruges unødigt tid på administrative processer i forbindelse med risikovurdering af de mange fagsystemer.
- Der skal udvikles et skema til risikovurdering af fagsystemer til benyttelse af fagsystemsbrugerne.

Risikovurderingsmetoden og -værktøjet samt workshoppen skal tilpasses og redesignes til næste iteration, hvor der med fordel kan være fokus på at få udført risikovurdering på nøje udvalgte fagsystemer.

Bibliografi

Boolsen, M. W. (2015). Grounded Theory. I S. Brinkmann, & L. Tanggaard, *Kvalitative metoder: en grundbog* (2 udg., s. 241-272). København: Hans Reitzels Forlag.

Calder, A., & Watkins, S. G. (2007). Information Security Risk Management for ISO27001/ISO17799: Implementing ISO27001. Hentet fra https://library-books24x7-com.zorac.aub.auu.dk/toc.aspx?site=G45VZ&bookid=36118

Christensen, O., Gynther, K., & Petersen, T. B. (2012). Design-Based Research - introduktion til en forskningsmetode i udvikling af nye E-læringskoncepter og didaktisk design medieret af digitale teknologier. *Læring & Medier, 5*(9), s. 1-20.

Datatilsynet, Erhvervsstyrelsen, Justitsministeriet, & Digitaliseringsstyrelsen. (oktober 2017). Databeskyttelsesforordningen. Hentet 3. maj 2019 fra https://www.datatilsynet.dk/media/6559/generel-informationspjece-om-databeskyttelsesforordningen.pdf

Digitaliseringsstyrelsen. (september 2015a). Guide til implementering af ISO27001. København. Hentet 4. april 2019 fra https://digst.dk/media/13668/guide-til-implementering-af-iso27001-september-2015.pdf

Digitaliseringsstyrelsen. (februar 2015b). Vejledning i it-risikostyring og -vurdering. København. Hentet 5. april 2019 fra https://digst.dk/media/13717/vejledning-it-risikostyring-og-vurdering_februar-2015.pdf

Digitaliseringsstyrelsen. (februar 2015c). Vejledning i informationssikkerhedsstyring (ISMS). København. Hentet 5. april 2019 fra https://digst.dk/media/13682/vejledning-i-informationssikkerhedsstyring-isms_februar-2015.pdf

Digitaliseringsstyrelsen. (Juni 2016). Vejledning i planlægning af sikkerhedsarbejdet. København. Hentet 5. april 2019 fra https://digst.dk/media/13777/vejledning-i-planl%C3%A3-gning-af-sikkerhedsarbejdet_juni-2016.pdf

Digitaliseringsstyrelsen. (u.d.). Hvad er ISO27001? Hentet 10. april 2019

Engward, H. (2013). Understanding Grounded Theory. *Nursing Standard, 28*(7), s. 37-41.

Greenberg, S., Buxton, B., Carpendale, S., & Marquardt, N. (2011). Sketching user experiences: The workbook. Hentet fra https://ebookcentral.proquest.com

Illeris, K. (2003). *Voksenuddannelse og voksenlæring.* Frederiksberg: Roskilde Universitetsforlag.

Illeris, K. (2015). *Læring* (3 udg.). Frederiksberg: Samfundslitteratur.

Illeris, K., & Samarbejdspartnere. (2004). *Læring i arbejdslivet.* Frederiksberg: Roskilde Universitetsforlag.

Jacobsen, B., Tanggaard, L., & Brinkmann, S. (2015). Fænomenologi. I S. Brinkmann, & L. Tanggaard, *Kvalitative metoder: en grundbog* (2. udg., s. 217-239). Hans Reitzels Forlag.

Justensen, L., & Mik-Meyer, N. (2010). Videnskabsteori, perspektiver og kvalitative metodeer. I L. Justensen, & N. Mik-Meyer, *Kvalitative metoder i organisations- og ledelsesstudier* (s. 11-36). Hans Reitzels Forlag.

Justesen, L., & Mik-Meyer, N. (2010). *Kvalitative metoder i organisations- og ledelsesstudier.* København: Hans Reitzels Forlag.

Larsen, H., Sørensen, T. B., & Devantier, N. (2018). *Danskernes infomationssikkerhed.* Kgs. Lyngby: DelC.

Nøhr, E. J. (2018). *Praktikrapport: Et casestudie på en kommunes risikovurderingsproces.* Aalborg: Aalborg Universitet.

Shattuck, J., & Anderson, T. (2013). Using a design-based research study to identify principles for training instructors to teach online. *International Review of Research in Open and Distance Learning, 14*(5), s. 187-210. doi:10.19173/irrodl.v14i5.1626

Szulevicz, T. (2015). Deltagerobservation. I S. Brinkmann, & L. Tanggaard, *Kvalitative metoder: en grundbog* (2 udg., s. 81-96). København: Hans Reitzels Forlag.

Tanggaard, L., & Brinkmann, S. (2015). Interviewet: Samtalen som forskningsmetode. I S. Brinkmann, & L. Tanggaard, *Kvalitative metoder: en grundbog* (2. udg., s. 29-53). Hans Reitzels Forag.

Van Loon, C., Andersen, H. H., & Larsen, L. (2016). *Facilitering - Skab resultater gennem involvering.* Jurist- og Økonomforbundets Forlag.

Bilag A

Interviewspørgsmål og svar

Tidsstemple	Hvad fungerede godt i workshoppen og hvorfor?	Hvad kunne være anderledes i workshoppen og hvorfor?
26/11/2018 11.46.09	Jeg synes, at det var rart, at workshoppen var godt planlagt, opgaverne i gruppeopgaverne var overskuelige, og tiden passede. Der var en god variation mellem oplæg og gruppeopgaver.	Jeg har svært ved at pege på noget, der kunne være anderledes. Men skulle jeg pege på noget, ville det måske fungere ligeså godt, hvis det kun havde være Borgerservice - vi har systemer nok at tage fat på. Der var måske ikke så meget input fra de andre forvaltninger.
26/11/2018 12.48.57	Flere samlet og fælles videndeling	Mere rammesætning omkring vurderinger - hvad er stor risico f.eks.
26/11/2018 13.30.47		
26/11/2018 13.58.04	En god struktur med diskussion fra alle om hvordan vi griber risikovurdering/konsekvensberegningen an.	Vi justerede i løbet af workshoppen, hvis der skulle ændres noget f.eks. om det var de rigtige systemer m.m., måske det skulle ha været vurderet inden mødet så vi fra starten vidste hvilke systemer der skulle vurderes.
26/11/2018 14.17.28	I var rigtig godt forberedte og havde tænkt over hvad I ville, og så fik I det leveret godt. Jeg synes også at I ramte rigtigt i forhold til det I underviste i.	Hmnnn, I kunne gøre endnu mere ud af at undersøge deltagernes forudsætninger, så I rammer endnu mere præcist.
26/11/2018 17.44.37	Godt at få sikker IT sikkerheden på dagsorden	Bedre/ mere fyldestgørende intro til emnet og til jeres afdeling og arbejdsområde
27/11/2018 08.54.44	Det var en fin gennemgang af de forskellige trusler	Jeg er stadig meget i tvivl om hvorfor man har valgt at lave en workshop nu, når man ikke er klar til at gå i gang med risikovurderingerne på de enkelte systemer endnu. Jeg ville personligt gerne have ventet med workshoppen til vi havde en konkret opgave/deadline at forholde os til.
27/11/2018 11.23.24	Jeg deltog via tlf og fik udbytte af gennemgang samt efterfølgende drøftelse	Mulighed for at deltage via Skype/videomøde hvis man ikke kan være fysisk tilstede, så kan man være mere med i dialogen
28/11/2018 09.32.13	gruppearb.	lidt mere uddybende i fortrolighedsklassifikation
28/11/2018 10.13.59	Vekslen mellem oplæg og opgaver, hvor der blev plads til diskussion i mindre grupper	Jeg kan ikke lige finde på
28/11/2018 10.54.09	God vekslen mellem oplæg og gruppearbejde	Det kunne have fremgået tydeligere, hvad målet med workshoppen var.
03/12/2018 09.51.23	Oplæg - Dejligt med forklaring	

Bilag B

Interviewkodning

Udskrift af interviewsekvens		Meningskondensering	Kategorisering, analyse, fortolkning
I	Hvad fungerede godt i workshoppen og hvorfor?	Vekslen mellem oplæg og opgaver. Gruppearbejde med plads til diskussion	**Vekslen mellem oplæg og opgaver** Det har passet deltagerne, at der var vekslen i workshoppen, hvilket også kan have været en motivationsfaktor i forhold til læringen. **Diskussioner i grupper** Jf. tanken om, at ikke alle er klar til at ytre sig i en stor gruppe, kan dette have været godt for mange af deltagerne, at de har kunnet diskutere det med andre. Det kan også føres videre og bruges som metode i risikovurderingsprocessen. **Fælles videndeling** Deltagerne har haft udbytte af en fælles videndeling og erfaring – der skabes et fællesskab omkring risikovurderingen. **Oplæg** Flere fik stort udbytte i at blive undervist af 'eksperter' på området og forklaring af risikovurdering og trusler.
1	Jeg synes, at det var rart, at workshoppen var godt planlagt, opgaverne i gruppeopgaverne var overskuelige, og tiden passede. Der var en god variation mellem oplæg og gruppeopgaver.		
8	Gruppearb.		
9	Vekslen mellem oplæg og opgaver, hvor der blev plads til diskussion i mindre grupper		
10	God vekslen mellem oplæg og gruppearbejde		
2	Flere samlet og fælles vidensdeling	Fælles videndeling og diskussion i forhold til emnet.	
3	En god struktur med diskussion fra alle om hvordan vi griber risikovurdering/konsekvensberegningen an.		
7	Jeg deltog via tlf og fik udbytte af gennemgang samt efterfølgende drøftelse		
4	I var rigtig godt forberedte og havde tænkt over hvad I ville, og så fik I det leveret godt. Jeg synes også at I ramte rigtigt i forhold til det I underviste i.	Oplæg fungerede godt	
5	God at få IT sikkerheden på dagsorden.		
6	Der var en fin gennemgang af de forskellige trusler		
11	Oplæg – Dejligt med forklaring		
I	Hvad kunne være anderledes i workshoppen og hvorfor?		

1	Jeg har svært ved at pege på noget, der kunne være anderledes. Men skulle jeg pege på noget, ville det måske fungere ligeså godt, hvis det kun havde været Borgerservice – vi har systemer nok at tage fat på. Der var måske ikke så meget input fra de andre forvaltninger.	Deltagernes sammensætning og forudsætning	**Deltagernes sammensætning** Det tyder på, at deltagerne gerne vil være delt ud på forvaltningsområder. Dette giver mening i forhold til at deres praksiserfaring muligvis er mere ens – og så skaber det et fællesskab indenfor forvaltningen. **Deltagernes forudsætning** Et større arbejde med deltagernes forudsætning – det kan muligvis også løses ved at have samme forvaltninger
4	Hmnnn, I kunne gøre endnu mere ud af at undersøge deltagernes forudsætninger, så I rammer endnu mere præcist		
2	Mere rammesætning omkring vurderinger – hvad er stor risico f.eks.	Vurdering af systemer og bedre præcisering af begreber	**Systemer og begreber** Dette betyder, at begreber har været upræcise i defineringen, hvilket der skal laves om på til næste gang. Samtidigt skal fagsystemerne analyseres, så det kun er de mest kritiske systemer, der bliver valgt ud.
3	Vi justerede i løbet af workshoppen, hvis der skulle ændre noget f.eks. om det de rigtige systemer m.m., måske det skulle ha været vurderet inden mødet så vi fra starten vidste hvilke systemer der skulle vurderes.		
5	Bedre/mere fyldestgørende intro til emnet og til jeres afdeling og arbejdsområde		
10	Lidt mere uddybende i fortrolighedsklassifikation	Workshoppen havde fungeret bedre, hvis der blev lavet en risikovurdering	**Deadline** Det kan være motiverende, hvis deltagerne ved, at der venter en deadline i, hvor de skal bruge viden til noget. Dette kan gøres ved, at risikovurderingerne bliver lavet på workshoppen.
6	Jeg er stadig meget i tvivl om hvorfor man har valgt at lave en workshop nu, når man ikke er klar til at gå i gang med risikovurderingerne på de enkelte systemer endnu. Jeg vil personligt gerne have ventet med workshoppen til vi havde en konkret opgaven/deadline at forhold os til.	Mulighed for anden tilstedeværelsen	**Anden tilstedeværelse** Det kunne også være et udtryk for, at ikke alle kan afsætte et par timer til dette, og der skal være andre alternativer til dem.
9	Mulighed for at deltage via Skype/videomøde hvis man ikke kan være fysisk tilstede, så kan man være mere med i dialogen.		