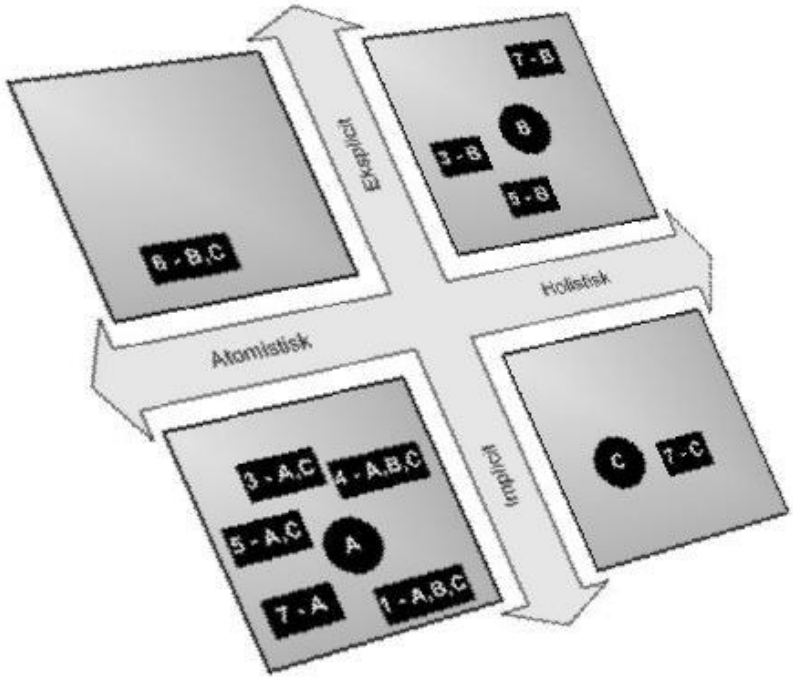
Titel: **En holistisk tilgang til adgangsstyring og autorisationskoncepter i ERP systemer**

Title: **A holistic approach to access management and authorisation concepts in ERP systems**



Kandidatafhandling for cand.merc.(dat.)

Copenhagen Business School

Skrevet af: Stefan Bendtsen Sønderup Underskrift: _____

Fødselsdato: 21-01-1980 Afleveringsdato: 29-06-2009

Vejleder: Annemette Kjærgaard

Omfang: Der er 166.636 anslag + 20 figurer (eksklusiv forside og bilag) = 79,4 normalsider, og dermed er kravet til kandidatafhandlingens omfang opfyldt.

Forord

En generel tak skal lyde til medarbejderne i Upstream og forretningsteam Sikkerhed i KMD for at lade mig foretage interviews og stille løbende opklarende og uddybende spørgsmål gennem hele forløbet.

Derudover en speciel tak til Simon Eiberg Thorup for at give mig muligheden, for at bruge KMD som case til specialet samt diskutere mulige problemstillinger i starten af forløbet, og læse afhandlingen igennem til sidst i forløbet
Derudover tak til Lars Gliskov Kristensen for hjælp med opstillingen af en figur, lægge hus til en dag med interviews og input til casen.
Tak til Annemette Kjærgaard for vejledning igennem processen og med at sikre, at afhandlingen lever op til de akademisk forventede krav.

Til sidst en kæmpe tak til Troels Lindgård for gennem hele forløbet at have været en fast hjælp, både i forhold til at stille litteratur til rådighed og diskutere opgavens problemstillinger og altid komme med relevant input og feedback, og for at invitere mig med til SAP Sikkerheds ERFA mødet, samt gennemlæse afhandlingen.

Executive Summary

The diffusion of Enterprise Resource Planning Systems (ERP) to almost all organisations has made the integration of processes and information possible. Thus, individuals often find themselves with access to, for example, financial and human resources (HR) information regardless of the department they belong to, when both Finance and HR modules are implemented in a single system. This integration of modules and systems can cause that the individual, could, intentionally or unintentionally, get unauthorised access to sensitive information. In the worst case, this could lead to, among other things, data loss and information theft. Furthermore, a breach of security could not only cause financial losses, but could also harm the organisation's reputation. In an extreme case, an organisation will face legal charges for being non compliant with the existing laws and regulations.

In order to minimise or avoid these risks, organisations need to ensure a proper access management is in place, handling which users get access to which information in their systems. Many organisations today have various different, often complex and poorly integrated authorisation concepts, and the authorisation consultants are lacking structures and concrete methodologies to develop these.
On the basis of the above, this thesis examines what factors influence an organisation's authorisation concepts, how an organisation integrates and uses the factors in the development of these concepts, and finally how these factors can be utilised in a structured way for future development of authorisation concepts.

Since most literature within access management are focusing on the technical aspects of access controls, and recent research within the literature of information systems security calls for a more holistic approach to be taken within this field, a business model for information security, inspired by the systems thinking approach, has been used to structure the way the literature have been reviewed. From this approach the 8 following factors have been construed that can influence the development of an authorisation concept:

- The prescribed requirements
- Risk analysis
- The paradigm of the authorisation consultant
- The involvement of the authorisation consultant
- Ownership model
- System integration
- The approach to Role development
- The Awareness of information security

The above identified factors have been examined through a case study that is carried out in KMD by following different approaches KMD takes in developing authorisation concepts for their customers' SAP

solutions. KMD, being the biggest Danish-based IT company and with the choice of SAP as its strategic partner, is one of, if not the biggest, SAP project in Denmark.
In the analysis it is revealed that some of the factors are handled identically through the different approaches KMD takes in developing authorisation concepts, some of the factors are handled differently, and some are not taken into consideration at all.

The research showed that most of the factors were handled in an implicit way, e.g. Segregation of duties, which is included in “The prescribed requirements”, is often carried out due to the authorisation consultants’ prior experiences, and not because of explicit requirements, which can create unnecessary implemented constraints. Furthermore, they are more often applied with an atomistic than holistic perspective, e.g. “The involvement of the authorisation consultant” happens in some of the approaches after the processes are designed and implemented. As a result, it can be difficult for the authorisation consultant to implement proper constraints, since some of these are directly related to the process definition and implementation.

It became apparent that the factors also helped in answering some fundamental questions for developing authorisation concepts, e.g. “System integration” answered what technology we have, and “Ownership model” gave an answer to who is responsible. This leads to that the factors are being grouped into a tangible and a non tangible group, according to what kind of answer they can produce. The tangible group gives answers to “what” and “who” questions and consists of: “The prescribed requirements”, “Risk analysis”, “Ownership model” and “System integration”.
The intangible group gives answers to “how” questions and consists of: “The paradigm of the authorisation consultant”, “The involvement of the authorisation consultant”, “The approach to Role development” and “The Awareness of information security”.

In an ideal world, all the factors would exist explicitly in the organisation, all relevant employees would be aware of them, and they would be used in a holistic manner as opposed to a purely atomic manner. However, the costs have to match the benefits, and since the developing of authorisations are often not the key factor of the developing projects, it should also be scoped accordingly.
One of the purposes of this thesis is to bring in more structures to access management and the development of authorisation concepts. Therefore, it is suggested first to ensure awareness exists of the tangible factors, since they provide critical input to the way the concept should be designed. According to the allocated resources in approving the use of these factors they should be transformed from implicit to explicit factors. During the development and again depending on the resource constraints, a change of the utilising of the intangible factors should be to work on changing them from an atomic perspective to a more holistic perspective.
By following these suggestions many of the problems related to developing authorisation concepts would be resolved.

Indholdsfortegnelse

1 Indledning

Enterprise Resource Planning (ERP) systemer er nu så udbredte i alle typer af organisationer, at de er blevet betegnet som indgangsprisen for at drive en forretning (She og Thuraisingham, 2007, s. 152).
Kompleksiteten af ERP systemerne er stigende, ikke mindst med de nye generationer der arbejder med web interfaces, og overfører data trådløst, og med den stigende kompleksitet og den vigtige position ERP systemerne indtager i organisationerne, bliver opmærksomheden også øget på informationssikkerheden i disse systemer (She og Thuraisingham, 2007).

Et brud på informationssikkerheden kan have omfattende konsekvenser for en organisation, det kan være alt fra direkte økonomiske tab, til manglende tillid fra kunder og leverandører. I Ernst & Youngs (2008) årlige undersøgelse af virksomheders informationssikkerhed konkluderer de, at et brud på informationssikkerheden ikke kun direkte påvirker virksomhedernes omsætning men i højere grad deres brand og omdømme.

En organisations elektroniske systemer er sårbare overfor indtrængen fra personer, der udfører skadelige handlinger såsom at stjæle information, slette data eller ændre systemopsætninger. Den skadelige hændelse kan være udført, bevidst eller ubevidst, af eksterne så vel som interne personer.
Flere forskellige metoder bliver brugt, det være sig passive teknikker med aflytning og afluring af passwords, vira hvor skadelige programmer opsnapper information, direkte forsøg på at bryde ind i systemet ved at gætte passwords eller browsing, hvor autoriserede brugere forsøger at få adgang til uautoriserede og følsomme data (Little & Best, 2003, s. 419).
Den sidstnævnte metode hvor en allerede autoriseret person, ofte en medarbejder, får adgang til uautoriserede funktioner eller systemer, har fået endnu mere relevans med ERP systemernes udbredelse i organisationerne, da ideen bag et ERP system netop er, at ét enkelt system kan håndtere mange af virksomhedens administrative processer, følger det dermed, at alle medarbejderne i en virksomhed har adgang til systemet.
Hvis vi tager HR området som eksempel, var det tidligere kun HR medarbejdere, der havde adgang til HR systemet, men nu hvor HR er inkorporeret som en komponent i ERP systemet, vil alle medarbejdere med adgang til ERP systemet potentielt kunne tilgå HR specifikke oplysninger.
Derfor er der brug for at kontrollere, at medarbejdere ikke får adgang til personfølsomme eller fortrolige oplysninger, med mindre de netop er autoriseret til dette. Dette gøres ved at have fokus på hvilke rettigheder de har i systemerne, og nærmere bestemt ved at foretage en adgangsstyring.

En virksomheds medarbejdere betegnes ofte som det svageste led inden for informationssikkerheden (Ernst & Young, 2008), og det betyder, at det er vigtigt at gøre medarbejderne bevidste om samt uddanne dem inden for sikkerhed (Desman, 2003). Dette bør dog ske i sammenhæng med, at organisationerne

kontrollerer adgangen til systemer og information, og med denne adgangsstyring sikrer, at brugerne kan deltage til produktiviteten og resultatet uden at kompromittere sikkerheden (Gartner 2007, s. 28).

Det er ikke kun internt i organisationerne, der ønskes at fokusere på adgangsstyring, men der bliver også stillet eksterne krav fra politisk besluttede regulativer og udviklede standarder. Ud over f.eks. persondataloven og DS484, der er en dansk standard for informationssikkerhed, (DS 484, 2005), stiller Sarbanes-Oxley regulativet (SOX), der blev vedtaget i kølvandet på flere amerikanske virksomhedsskandaler, med ENRON som den nok mest kendte, store krav til gennemsigtigheden i organisationernes administration. En af delene af SOX omhandler en virksomheds interne kontroller og herunder spiller adgangsstyringen i ERP systemerne blandt andet en relevant rolle (Maurizio et al, 2007, s.17).

"Because practically no methodological standards for authorizations and role structures exist, companies use an almost endless variety of solutions related to technical IT security" (Linkies & Off, 2005, s. 22).

Da informationssikkerhed sjældent er det egentlige formål med et udviklingsprojekt, men ofte et element der bliver tænkt ind i et projekt undervejs, er det ofte ikke højt prioriteret, og i forhold til udvikling og vedligeholdelse af autorisationer ses det som en gene, eller byrde, der skal håndteres på den lettest tænkelige og mindst ressourcekrævende måde. Da der samtidig eksisterer en gængs opfattelse af, at der ikke eksisterer nogen strukturer eller teoretisk funderede koncepter inden for udvikling af autorisationer, resulterer det i, at der skabes et utal af løsninger frembragt på en ad hoc basis.

Af ovenstående er det blevet klart, at organisationer bør tage stilling til adgangsstyringen i deres systemer, da en mangelfuld adgangsstyring og den medfølgende potentielle sikkerhedsrisiko ikke kun kan medføre store omkostninger ved tab af omsætning og renomme men også manglende opfyldning af standarder og lovgivning. En måde at forholde sig til adgangsstyringen er ved hjælp af et autorisationskoncept, der kan holde styr på roller og rettigheder i systemerne.

KMD er den største danskbaserede it-virksomhed, og med KMDs valg af SAP som strategisk samarbejdspartner, er det et af de største, hvis ikke det største, SAP projekt i Danmark. Gennem mit arbejde som studentermedarbejder i KMD har jeg været tilknyttet to forskellige projekter, der begge har haft at gøre med udviklingen af autorisationskoncepter, hvor det ene var i forhold til at udvikle et autorisationskoncept for udviklerne i KMD, og det andet var i forhold til at udvikle et overordnet koncept for KMDs kunders brugere i forhold til de løsninger de har købt fra KMD. Begge koncepter var i forbindelse med ERP systemet SAP.
Gennem mit arbejde har jeg erfaret, at den høje systemkompleksitet kombineret med en ad hoc tilgang og manglende struktur for adgangsstyring har resulteret i, at der hverken er klarhed over, hvad et autorisationskoncept reelt bør indeholde, eller hvilke faktorer der har indflydelse på det, hvilket har inspireret mig til denne afhandlings problemformulering, og dermed er formålet med afhandlingen at hjælpe til med at

skabe en struktur inden for udviklingen af autorisationskoncepter, så de ovenfor eksisterende problemer og ulemper for organisationerne om ikke helt kan undgås, så blive kraftigt reduceret.

1.1 Problemformulering

Hvilke faktorer påvirker autorisationskoncepter i en organisations ERP systemer, hvordan involveres faktorerne under udviklingen af autorisationskoncepter, og hvordan skal de struktureres i forhold til en fremtidig udvikling af autorisationskoncepter?

1.1.1 Begrebsdefinitioner

I dette afsnit vil de vigtigste og mest benyttede begreber blive forklaret, i forhold til hvordan de skal forstås i denne afhandling.

Autorisation: En autorisation er den lov eller rettighed, der giver en bruger adgang til at udføre funktioner eller tilgå ressourcer. (DS 484, 2005).

Koncept: I denne afhandling bliver ordet autorisationskoncept flittigt brugt, og Encarta (2009) giver 4 forskellige definitioner på hvad et koncept er: Noget tænkt eller forestillet, et vejledende generelt princip, den mest basale forståelse af noget eller en måde at gøre eller opfatte noget. I denne afhandling skal koncept forstås i forhold til, at det er et vejledende og generelt princip.

Faktor: Ligeledes kan ordet faktor betyde flere ting, Det kan være et vist niveau eller mængde af noget eller det kan være en mængde ganget med noget andet. I denne afhandling betyder en faktor dog, at det er noget der bidrager til eller influerer resultatet af noget andet (Encarta, 2009).

ERP: Et integreret IT system der giver mulighed for at samle og styre en virksomheds processer.

Autorisationskonsulent: Dette begreb dækker over den person, der arbejder med autorisationer. Selvom udtrykket konsulent bruges dækker det ikke nødvendigvis over en ekstern konsulent, men kan lige så godt stå for en intern ressource.

Informationssikkerhed: Denne definition dækker over det begreb der på engelsk bliver kaldt Information Systems Security. Der er en tendens til, at IT sikkerhed bliver brugt, når det er noget teknisk, og informationssikkerhed når fokus er mere på et organisatorisk plan. Begge ord vil blive brugt synonymt i denne afhandling, men med sidstnævnte betydning med mindre andet er specificeret.

SAP: Når SAP bliver brugt i denne afhandling, er det fortrinsvis med henblik på mySAP ERP der indeholder moduler som f.eks. SAP ERP Financials og SAP ERP HRM, det vil dog under et blive refereret som SAP. Der bliver dog også nævnt Portal der referer til SAP NetWeaver Enterprise Portal, og BI og BW, der begge refererer til SAP NetWeaver Business Intelligence.

Virksomhed vs. organisation: Hvor virksomhed ofte referer til en privat organisation, hvor hovedformålet er profitmaksimering, og organisation referer bredere, og også kan indeholde NGO'er og offentlige instanser, skelner jeg i denne afhandling ikke imellem de to ord, og de skal altså begge forstås i den bredeste forstand, med mindre andet bliver nævnt.

1.1.2 Afgrænsninger

I dette afsnit beskrives de afgræsninger der er foretaget i forhold til opgavens udstrækning.

Autorisering vs. autentificering

Der er en klar sammenhæng mellem hvem en bruger er i et system (autentificering), og hvad brugeren har adgang til i systemet (autorisering). Adgangsstyring indeholder begge dele, men det sker ofte en forvirring mellem de to dele.

Autentificering er den proces, der afgør, om en bruger virkelig har den identitet, han hævder overfor systemet. Dette gøres ved hjælp af tre, ofte kombinerede, måder, med enten noget du ved (f.eks. et password), med noget du har (f.eks. et id kort) eller med noget du er (f.eks. brug af fingeraftryk) (Ferraiolo et al., 2003, s. 3). Identity management (IdM) er en term der ofte bliver nævnt, og det har at gøre med at kunne organisere og synkronisere brugere på tværs af alle virksomhedens systemer.

Autorisering er den proces, der afgør, hvad en bruger i et system kan få adgang til. Før at autorisering kan virke korrekt, er det en nødvendighed, at autentificeringen fungerer, og lige så den anden vej. Det er nytteløst at prøve at begrænse den ene brugers rettigheder i forhold til den anden brugers rettigheder, hvis det ikke er muligt at skelne mellem brugerne, og ligeså giver det ikke værdi at bruge tid på at identificere en bruger, hvis der alligevel ikke er kontrol over, hvad brugeren kan gøre. Derfor anerkendes sammenhængen, og begge dele er lige vigtige at være bevidste og have kontrol om.

I denne afhandling er fokus på autorisering, det vil sige, hvad brugeren i systemet kan tilgå, og ikke på hvordan brugeren identificerer sig overfor systemet, så når begrebet adgangsstyring bliver brugt i denne afhandling er det med vægt på autoriseringsdelen. Dette skyldes blandt andet, at der tidligere ofte har været mere fokus på autentificeringen, og derfor findes det relevant at sætte mere fokus på autoriseringen.

SAP

Der er valgt kun at fokusere på ERP systemet SAP.[1] Da SAP er det største og mest komplekse system på markedet, er bevæggrunden, at det der kan komme frem til for dette system, også vil kunne overføres til andre systemer, dog kan det blive mere omstændeligt end nødvendigt er, men der kan ikke nødvendigvis gås den anden vej rundt. SAP bliver samtidig brugt af de fleste af de største virksomheder i Danmark (f.eks. A.P. Møller - Mærsk A/S, Vestas A/S, Novo Nordisk A/S), så konklusioner og afklaringer inden for dette problemområde vil have stor relevans. Derudover bruges SAP også af KMD, som jeg bruger som case virksomhed, og hvor jeg har adgang til og indsigt i.

Sprog

Denne afhandling er skrevet på dansk, dog er litteraturen inden for dette område udelukkende på engelsk. Nøglebegreber er blevet oversat, men citater der fremgår i afhandlingen er ikke oversat, for at sikre, at citatet fremstår med den mening der var hensigten, og derfor forudsættes det, at læseren af denne afhandling kan engelsk på et vist niveau.

1.2 Målgruppe

Afhandlingen omhandler adgangsstyring og mere specifikt autorisationskoncepter i en organisations ERP systemer, og da den arbejder med de problemstillinger, der opstår i forbindelse med disse, henvender afhandlingen sig til de medarbejdere, der konkret arbejder med sikkerhed og autorisationer, samt dem der er ansvarlige for, at sikkerheden bliver overholdt i systemerne. KMD er blevet brugt som case, og derfor henvender den sig specielt til de medarbejdere og forretningsområder, der er involveret med sikkerhed i KMD.

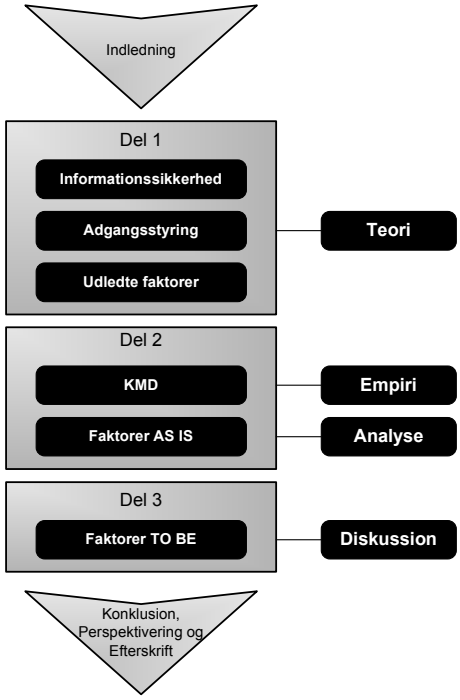
Afhandlingen har fokus på SAP, men de overordnede problemstillinger med autorisationer og adgangsstyring kan også overføres til andre ERP systemer, og derfor vil personer involveret med sådanne, også kunne læse denne afhandling med interesse.

Da det er en kandidatafhandling, henvender den sig i sagens natur også til eksaminator og censor.

[1] En pudsig information er, at et kig på Googles indikator for tidsånden for 2008, der er målt på populære søgeord inddelt i forskellige kategorier, viser at SAP indtager en fjerdeplads i "Hvad er" kategorien, kun overgået af Kærlighed, Livet og Java (Zeitgeist, 2008). Det skal dog pointeres, at tallene dækker over søgeord foretaget på google.com i USA. Selvom sådanne hitlister er poppede af natur, giver det alligevel en indikator om hvor udbredt kendskabet til SAP efterhånden er.

1.3 Disposition

Figur 1: Afhandlingens disposition



Kilde: Egen frembringelse

Indledning består af **kapitel 1 og 2**, og indeholder indledning til problemformuleringen, selve problemformuleringen, begrebsafklaringer, afgrænsninger, disposition samt metodeafsnit.

Del 1 består af **kapitel 3, 4 og 5**, hvor først emnet informationssikkerhed bliver belyst, derefter mere specifikt om adgangsstyring og til sidst bliver litteraturen om adgangsstyring gennemgået i forhold til en holistisk model, for at udlede de faktorer der påvirker et autorisationskoncept.

Del 2 består af **kapitel 6 og 7**, og her bliver casen først beskrevet, der omhandler KMDs forskellige tilgange til at udvikle autorisationskoncepter og efterfølgende en analyse af hvordan faktorerne udledt fra **del 1** er blevet involveret med disse tilgange.

Del 3 består af **kapitel 8**, og her bliver faktorerne diskuteret, i forhold til hvordan de kan struktureres og forbedres til brug for fremtidig udvikling af autorisationskoncepter.

Konklusion, Perspektivering og Efterskrift består af **kapitel 9, 10 og 11**, og her vil konklusionen svare på problemformuleringen, perspektiveringen vil se på hvor den frembragte viden ellers kan bruges, og efterskriftet vil indeholde nogle refleksioner over selve procesforløbet.

2 Metode

Dette kapitel vil gennemgå den metode, der er brugt til at besvare afhandlingens problemformulering. Først gennemgås det videnskabsteoretiske synspunkt, der anlægges gennem opgaven, dernæst hvilken teori, og til sidst hvilken og hvordan dataindsamlingen er foregået.

2.1 Videnssyn

Den videnskabsteoretiske tilgang i denne afhandling er inspireret af den moderate empirisme, hvor der ikke fokuseres så meget på hvordan teorier er opstået, men mere på hvordan de skal begrundes, og hvordan deres fordele og ulemper vurderes (Knudsen, 1994, s. 57). Selve videnssynet der anlægges, er en variant af den moderate empirisme, pragmatismen, og dens ide om handlingsbaseret viden, hvor mennesket handler i verden og viden opstår i handling. Viden skal bruges til at løse de problemer vi har, og om viden er sand afgøres af de praktiske konsekvenser den får, viden bliver derfor opfattet som et instrument til at håndtere tilværelsen i praksis (Gustavsson, 2001, s.134ff). I forhold til usikkerhedsrelationen, der er tesen om, at en undersøger altid vil påvirke det der undersøges, og dermed umuliggør en sand objektiv beskrivelse af virkeligheden (Gustavsson, 2001, s.93), fungerer pragmatismens videnssyn fint, da det ikke søger den ene endegyldige sandhed.
Da den gængse opfattelse inden for autorisationsudvikling er, at arbejdet er ad hoc, ustruktureret og mangler teoretisk funderede koncepter, giver en deduktiv fremgangsmåde en mulighed for at tage et afsæt i teorien og udforske mulighederne for at få opstillet en teoretisk ramme. Først derefter foretages en empirisk undersøgelse for at vurdere det teoretiske grundlags egnethed.

2.2 Teori

Der er blevet gennemgået relevante bøger, artikler og standarder i forhold til informationssikkerhed og ERP systemer, og specielt i forhold til adgangsstyring.
Teorien er blevet gennemgået ved hjælp af en overordnet model for informationssikkerhed. Modellen, der er inspireret af ideen om systemtænkning, bliver gennemgået trinvis, og for hvert trin identificeres hvordan adgangsstyring passer ind. På denne baggrund, er der ud fra teorien blevet skabt en teoretisk ramme, der kan bruges til at forholde sig til empirien.

2.3 Empiri

2.3.1 Case som undersøgelsesdesign

Et casestudie er valgt som undersøgelsesdesign til den empiriske dataindsamling, og selvom casestudiemetoden er blevet benævnt som en grundlæggende induktiv fremgangsmåde (Andersen, 2008, s.120), og der i denne afhandling tages en deduktiv fremgangsmåde, vil casestudiemetoden stadig blive benyttet. Et casestudie er godt, når det ikke er indlysende, hvor grænserne går mellem det fænomen der belyses, og den sammenhæng det indgår i (Andersen, 2008, s. 118). Formålet i denne afhandling er at undersøge hvordan forskellige faktorer påvirker udviklingen af et autorisationskoncept, og da det ikke er intuitivt hvordan, og om, faktorerne påvirker konceptet, passer det godt med at foretage et casestudie. Da der er anlagt et pragmatisk videnssyn, giver casestudiet også god mulighed for at belyse problemstillingen inden for dens naturlige rammer, og dermed give et bedre indtryk af hvor anvendelig teorien er.
Der er valgt et single casestudie, hvilket er oplagt, når casen er kritisk eller unik. Da KMD er en af de største SAP projekter i Danmark, giver det god mening at opfatte det som enestående i forhold til at afprøve om den generelle viden er anvendelig. Dog er en anden grund til at vælge et single casestudie, at informationssikkerhed ofte bliver behandlet fortroligt, både fordi det af natur ikke er ønskværdigt at offentliggøre hvilke tanker, der ligger til grund for ens sikkerhedskontroller og procedurer af frygt for, at de dermed lettere kan omgås, men også på grund af det dårlige omdømme der kan opstå, hvis det kommer frem, at der ikke er fuld kontrol over informationssikkerheden. Fortroligheden betyder, at det ikke umiddelbart er muligt at spørge ind til virksomheders interne sikkerhedskoncepter, men i kraft af mit arbejde i virksomheden har jeg haft mulighed for at gøre netop dette.

2.3.2 Dataindsamling

Der er foretaget en kvalitativ dataindsamling af både primære og sekundære data (Andersen, 2008, s.149ff).
Den kvalitative dataindsamlingsmetode er valgt, for at have mulighed for at få identificeret de udledte faktorer og finde ud af hvordan de bliver brugt.

2.3.2.1 Primære data

Interviews

Der er foretaget 6 delvist strukturerede interview, hvor en interviewguide med 5-10 spørgsmål er blevet sendt på forhånd til den interviewede. Under interviewet er der taget noter, og stillet opklarende og uddybende spørgsmål til de enkelte punkter for at sikre en korrekt forståelse. Umiddelbart efter interviewet er der udformet et referat, der er sendt til den interviewede for at kontrollere, at referatet er korrekt, og den interviewede kan genkende og godkende sine udtalelser (Andersen, 2008, s. 169). En enkelt af de

interviewede valgte at gøre brug af dette, og uddybede et af punkterne i interviewet. Referatet af det interview blev efterfølgende rettet til. Referaterne er vedlagt i afhandlingens bilag.
Interviewpersonerne er valgt, både ud fra de personer der deltog i at udvikle et autorisationskoncept internt for KMDs udviklingsforretning, samt dem der deltog i at udvikle et autorisationskoncept for KMDs kunder. Der er forsøgt valgt personer med forskellige profiler, så der kan komme input fra både et lavpraktisk plan såvel som et mere overordnet organisatorisk plan.

Observationer

Der er foretaget en deltagende observationsteknik med deltagelse i projektmøder, diskussioner om og udvikling af roller og autorisationer. Observationerne er foretaget åbent, da der ikke har været lagt skjult på, at forfatteren både deltog med arbejdet, men samtidig skrev kandidatafhandling, dog er nogle af observationerne foretaget indirekte, da det formentlig ikke har været alle bekendt med helt præcist hvilket formål afhandlingen har haft (Andersen, 2008, 155ff). Observationen er foregået i perioden foråret 2008 til foråret 2009.

For at supplere med input fra andre virksomheder end den der er valgt som casestudie, er der blevet deltaget i et SAP Sikkerheds ERFA møde, hvor deltagerne er en blanding af freelance konsulenter, konsulenter fra de store revisions- og SAP huse og ansatte fra nogle af de virksomheder der bruger SAP. Til mødet blev der afsat tid i agendaen både til at præsentere ideerne til og motivationen bag afhandlingen, samt at få diskuteret relevante problemstillinger i forhold til adgangsstyring. Da der deltog 14 personer, var det ikke hensigtsmæssigt kun at tage noter under mødet, så der blev også brugt en diktafon til at optage diskussionen. Deltagerne blev gjort opmærksomme på dette og fik at vide, at de ikke ville blive refereret med navns nævnelse. Efterfølgende er der udført en transskribering af den optagede diskussion og vedlagt til afhandlingens bilag.

2.3.2.2 Sekundære data

De sekundære data der er blevet brugt er årsrapporter fra KMD, revisionsrapporter fra KMD og en af deres kunder, samt interne dokumenter, guidelines og præsentationer i forhold til Den Offentlige Forretningsmodel.

Nedenstående tabel opsummerer den dataindsamling der er foretaget.

Tabel 1: Oversigt over dataindsamling

Dataindsamling	Hvad	Hvor	Hvem	Antal
Primære data	Interviews	KMD	Autorisationsassistent	1
			Forretningsspecialist	2
			SAP specialist	1
			IT-Arkitekt	1
		Andre	SAP Konsulent	1
	Observation	KMD	Generisk rollekoncept projekt	6 måneder
			OPUS Brugerstyring projekt	6 måneder
		Andre	SAP ERFA møde	1
Sekundære data	Rapporter	KMD	Årsrapport 2008	1
		Andre	Århus Kommune revisionsrapport 2007	1
	Interne dokumenter	KMD	It-revisionsmæssig gennemgang af sikkerheden i SAP Ekstern 2005	1
			Opgavestruktur for Den Offentlige Forretningsmodel	1
			Byggesten i Den Offentlige Forretningsmodel	1

2.3.3 Dataanalyse

Den indsamlede empiri vil blive belyst i forhold til den teoretiske ramme, der er opstået på baggrund af de udledte faktorer, dannet fra teorien, der påvirker et autorisationskoncept.

2.4 Metodekritik

En stor del af den litteratur der hører til adgangsstyring, og bliver gennemgået i denne afhandling, er skrevet af personer med praktisk erfaring inden for emnet, men en lille del af litteraturen indeholder eller referer til empiriske undersøgelser, der understøtter deres konklusioner.

Adgangsstyring hører inden for feltet informationssikkerhed, og det samme gør sig gældende her.

Siponen et al. (2008) analyseret 1280 artikler skrevet over en årrække på 15 år, og er kommet frem til at mere end 80 % af disse ikke indeholdt teori, og langt størstedelen af den teori der fandtes i de resterende, var matematisk teori. Derudover var langt de fleste artikler ikke baseret på nogen empiri, men understøttet af subjektive holdninger. Siponen et al. (2008) konkluderer, at enten er disciplinen informationssikkerhed ikke moden nok endnu, i forhold til andre discipliner, eller også er det fordi, der hersker en kultur hvor traditionel akademisk research, der værdsætte teori og empiriske beviser, ikke er påskønnet indenfor informationssikkerhedsfeltet (Siponen et al., 2008, s. 10).

Dette underbygges også af Ma og Pearson (2005), da de nævner, at de ikke kender til nogen tidligere forsøg på at validere de guidelines og den praksis litteraturen ofte konkluderer. De gør dog selv forsøget i forhold til at validere den internationale standard ISO 17799, der blandt andet ligger til grund for den danske standard DS 484, der bliver omtalt senere her i afhandlingen.

Ovenstående har betydning for hvilken viden, det er muligt at skabe, men jeg har netop valgt en deduktiv fremgangsmåde, for at gøre et forsøg på at tage udgangspunkt i, og skabe et teoretisk udgangspunkt, der kan bruges til at forstå empirien.
I forhold til systemtænkning passer deduktion også godt, da det ikke er muligt at få et overblik over helheden, hvis der startes med at tage udgangspunkt i detaljen. Og den model der tages afsæt i, i forhold til teorien, er netop inspireret af systemtænkning. En kritik af systemtænkningen kunne være, at det måske ikke nødvendigvis er alle handlinger, der vil påvirke alt andet. Det er selvfølgelig sandsynligt, at hvis der ændres på nogle regler i en organisation, så vil kulturen blandt medarbejderne også ændre sig, og til sidst vil det påvirke, at reglerne i organisationen ændrer sig osv., dog argumenterer teorien om løst koblede systemer for, at de to ting måske bliver påvirket af hinanden og måske gør de ikke (Weick, 1976).
Selvom jeg personligt også hælder til at indsætte et måske, dvs. at en årsag ”måske” bliver til en virkning, er modellen alligevel nyttig da formålet med at bruge den, lige så meget er at tage en holistisk indgangsvinkel til adgangsstyring, og dermed kan modellen hjælpe til med at sikre, at vi kommer hele vejen rundt om organisationen. Derudover har systemtænkningen også hjulpet til med at tegne sammenhænge mellem og visualisere problemstillinger i forbindelse med adgangsstyring.

Afhandlingen ligger inden for emnet informationssikkerhed, og i det næste afsnit vil der redegøres for, hvad informationssikkerhed er, og hvordan det traditionelt er blevet opfattet.

3 Teori – Informationssikkerhed

Traditionelt er hjørnestenene af IT sikkerhed blevet betegnet som fortrolighed, integritet og tilgængelighed, kendt under forkortelsen CIA[2], hvor fortrolighed referer til behovet for, at information bliver holdt sikkert og privat. Integritet skal sikre, at information ikke bliver ændret af uautoriserede personer, og tilgængelighed sørger for, at information kan tilgås, når der er behov for det (Ferraiolo et al., 2003, s. 2).

Dhillon og Backhouse (2000) stiller sig kritiske overfor den ovenstående opfattelse af IT sikkerhed, da de mener CIA lægger for meget vægt på selve den information, der befinder sig på et system, og ikke den interaktion der omgiver den. F.eks. i forhold til integritet er det ikke nok kun at sikre, at tal og værdier fremstår korrekt, men at selve den måde informationen bliver opfattet og fortolket, også skal høre under IT sikkerheden.
Da virksomheder hurtigt kan ændre sig, og uforudsete hændelser kan ske, er det vigtigt, at medarbejderne kender deres ansvar og rolle i organisationen, så der hurtigt vil kunne identificeres, hvem der tager teten, når nye omstændigheder opstår. Virksomheden skal være opmærksom på, om nye medarbejdere får adgang til følsomme data, men i lige så høj grad på senior medarbejdere, da det viser sig, at medarbejderens integritet let kan ændre sig over tid, det kan f.eks. skyldes skilsmisse eller gæld, derfor bør integritet være et krav til medarbejderen. En tæt overvågning af medarbejderne er ofte hverken rentabelt, ønskværdigt, eller muligt med geografisk spredte virksomheder, og derfor er tillid et begreb, der skal tilføjes teorien omkring sikre informationssystemer. Det forventes, at medarbejdere vil handle i overensstemmelse med en etisk praksis. Dette gælder udover de allerede beskrevne regler for eksisterende procedurer, da de eksisterende regler ikke nødvendigvis dækker over nye dynamiske og uforudsigelige situationer (Dhillon og Backhouse, 2000, s. 127f). På baggrund af ovenstående foreslår Dhillon og Backhouse (2000) derfor, at der udover CIA hjørnestenene også tages højde for ansvar, integritet, tillid og etik, når der skal tages hånd om IT sikkerhed.
Dhillon og Backhouse (2000) er klar over, at virksomhederne bevæger sig i en dynamisk verden, og at medarbejderne er vigtige at inkludere for at få IT sikkerhedsligningen til at gå op.
Information er vigtig for virksomheder i dag, ikke kun for at overleve, men for at kunne trives, og IT sikkerhed er anerkendt som en vigtig spiller i denne sammenhæng. Dog ses IT sikkerhed stadig som en funktionel opgave, og tiltag inden for dette område sker alt for ofte på en reaktiv baggrund, og opfattelsen af IT sikkerhed er delt op i siloer, dvs. hver afdeling har deres eget syn på hvilken information, der er vigtig at beskytte, men da der ikke er nogen kommunikation eller sammenhæng mellem siloerne, sker det, at en forbedring af sikkerheden i én silo, i værste fald forværrer situationen i en anden silo.

Overordnet omhandler afhandlingen informationssikkerhed, men da den mere specifikt handler om adgangsstyring, vil der i det næste afsnit først blive forklaret og defineret de vigtigste begreber inden for denne disciplin, nærmere bestemt, autorisationskoncept, autorisationer og rollebaseret adgangskontrol.

[2] På engelsk: Confidentiality, Integrity og Availability, heraf forkortelsen CIA

4 Teori – Traditionel opfattelse på adgangsstyring

Langt den overvejende del af den litteratur der findes inden for området adgangsstyring, har vist sig udelukkende at have et teknisk fokus, hvor det primære er at svare på hvordan adgange kan modelleres, distribueres og grupperes på en sikker og effektiv måde (Ahn et al., 2002; Cheng, 2000; Eigeles, 2006; Goncalves & Poniszewska-Maranda, 2008; Li et al., 2007; Lin & Brown, 2000; Mohammed & Dilts, 1994; Nyanchama & Osborn, 1994; Omicini et al., 2005; Ray et al., 2004; Vanamali, 2008; Vela et al. 2007; Wainer et al., 2007; Wang et al., 2008).

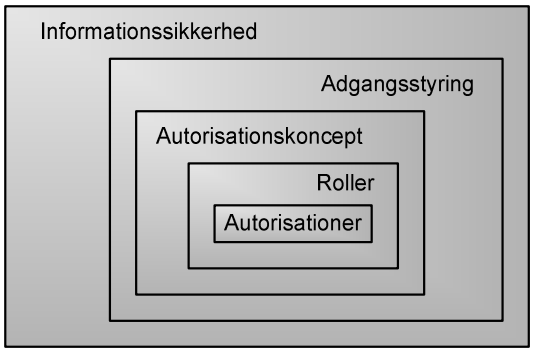
Rollebaseret adgangskontrol (RBAC) er en anerkendt og central fremgangsmåde at gribe adgangsstyring an på, og da de fleste af artiklerne ovenfor også arbejder med dette begreb, vil RBAC i dette afsnit blive gennemgået. Da Ferraiolo et al. (2003) har været med til at skabe den traditionelle RBAC metode, vil deres udgangspunkt bruges i denne gennemgang.

Ferraiolo et al. (2003) definerer 3 forskellige abstraktioner af kontrol, i forhold til adgangsstyring, hvor den første er adgangspolitikker, der beskriver de overordnede krav, der findes til hvem der må have adgang til hvilken information, under hvilke omstændigheder, og hvorfor. Den anden er adgangsmodeller, der for brugeren er den præcise kravspecifikation, og for udviklerne og leverandørerne de krav der er til design og implementering (Ferraiolo et al, 2003, s. 30). Den sidste er adgangsmekanismer, der sørger for at oversætte brugernes adgangsforespørgsler, og ved at slå op f.eks. i en tabel, kan de tillade eller nægte adgangen. Mekanismerne kræver, at der findes attributter om brugerne, i forhold til den sikkerhed der er påkrævet, for eksempel hvilket niveau af tillid der er til de forskellige brugere (Ferraiolo et al, 2003, s. 28f).
Et autorisationskoncept er en måde adgangsstyring kan operationaliseres, og bør derfor indeholde adgangspolitikker, adgangsmodeller samt adgangsmekanismer.

4.1 Autorisationskoncept

Da et koncept er et vejledende og generelt princip, bliver et autorisationskoncept et generelt princip for styringen, administrationen og kontrollen af autorisationer. Da en af de mest gængse måder at håndtere autorisationer i et system på er ved hjælp af rollebaseret adgang, bør et autorisationskoncept tage hånd om at definere, hvilke roller der skal findes på systemerne, hvad de skal indeholde og hvordan de skal tildeles, samt definere hvordan processen er for definering af roller, da dette beskriver, hvordan rollerne skal vedligeholdes, og hvordan nye roller kan tilføjes konceptet.

Figur 2: Sammenhæng fra informationssikkerhed til autorisationer



Kilde: Egen frembringelse

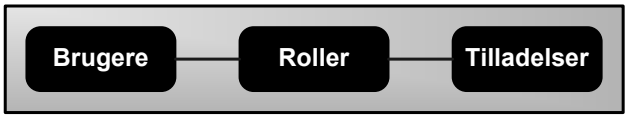
4.1.1 Autorisation

Ferraiolo et al. (2003) beskriver en autorisation, som den lov der afgør hvad brugeren må gøre. Den er en ja eller nej beslutning til, om en bruger kan få adgang til en bestemt systemressource eller handling. Denne definition understøttes af Dansk Standard, der beskriver autorisationen som en "rettighed til at udføre specifikke funktioner samt tilladelse til at anvende på forhånd tildelte ressourcer" (DS 484, 2005). Linkies & Off (2005, 191) definerer en autorisation som en form for tilladelse til at tilgå bestemte transaktioner under bestemte betingelser.

4.1.2 Rollebaseret adgangskontrol (RBAC)

Ideen med rollebaseret adgangskontrol er, at tilladelser bliver autoriseret til roller, og roller bliver autoriseret til brugere. Dermed skal der vedligeholdes to forskellige typer af associationer: bruger- og rolleassociationen, og rolle- og tilladelsesassociationen.

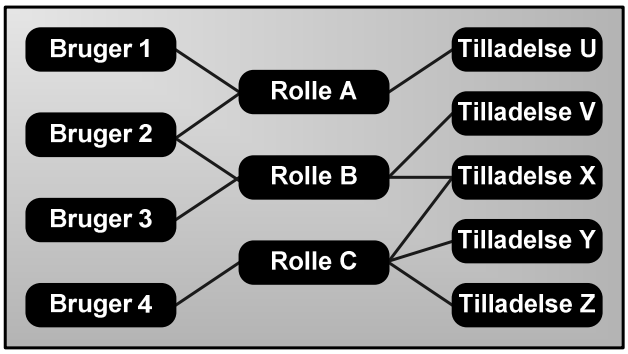
Figur 3: Relation mellem brugere, roller og tilladelser



Kilde: Egen frembringelse

Dette betyder, at når en medarbejder skifter ansvarsområde internt i virksomheden, behøver administratoren bare at fjerne associationen mellem medarbejderen og den nuværende rolle, og skabe en ny forbindelse mellem medarbejderen og den nye rolle (Ferraiolo et al., 2003, s. 23). En medarbejder kan have tilknyttet flere roller, ligesom en rolle kan have tilknyttet flere tilladelser, hvilket ses af nedenstående figur.

Figur 4: Forbindelser mellem brugere, roller og tilladelser



Kilde: Egen frembringelse

4.1.2.1 Rolleudvikling

De centrale problemstillinger ved rollebaseret adgangskontrol bliver så, hvordan rollerne skal defineres (rolleudvikling), og hvilke brugere der skal have hvilke roller (brugeradministration).
Ferraiolo et al. (2003) nævner, at en af de udfordringer der findes, er hvordan det organisatoriske skal matches med teknikken, og gør opmærksom på, at rollebaseret adgangskontrol ikke giver svaret på hvordan forbindelserne mellem brugere, roller og tilladelser skal implementeres men bare, at der skal eksistere relationer mellem brugere og roller, og roller og tilladelser.

Goncalves og Poniszewska-Maranda (2008, s. 1308f) bifalder rollebaseret adgangskontrol, men har også undret sig over, hvordan rolleudviklingen skal defineres og gøres i praksis, og kom frem til, at der ikke eksisterer nogen metodologier til dette. Dette understøttes af Ahn et al. (2002, s. 649), der påstår, at tidligere forsøg enten har været for abstrakte eller applikationsspecifikke ad hoc løsninger.

4.1.2.2 Rolleudvikling og autorisationer i SAP

I SAP er tabeller, programmer, rapporter og transaktioner beskyttet ved hjælp af autorisationstjek.
Den normale form for adgang til SAP sker ved hjælp af transaktioner. En transaktion indeholder ofte flere skærmbilleder, hvor der er mulighed for at skabe, vise, eller rette data. Bag hver transaktion ligger nogle programmer, der har indbygget autorisationstjek, der skal returnere positive svar, så længe programmerne kører. Disse autorisationstjek bruger autorisationsobjekter, der består af autorisationsfelter, hvor det er muligt at indstille, for eksempel om der må gives skrive- eller læserettigheder, eller der skal gives en begrænset adgang til en bestem firmakode. En til flere autorisationsobjekter kan samles i en rolle. Sådan en rolle er benævnt en enkeltrolle. En til flere enkeltroller kan tildeles til en anden rolle, der kaldes en samlerolle. Både samle- og enkeltroller kan tildeles brugere. (Linkies & Off, 2005, s. 188ff).

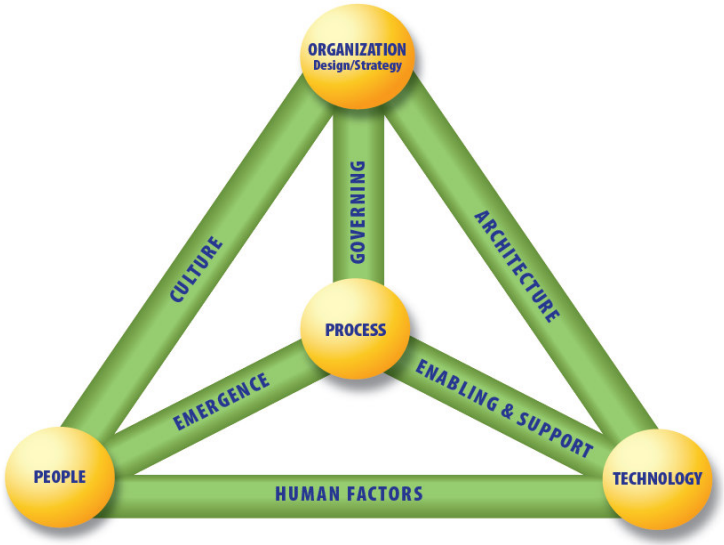
Dette kapitel har beskrevet de vigtigste begreber og termer inden for adgangsstyring, og omfatter den måde langt den største del af teorien opfatter adgangsstyring på. Det vil sige, at det vigtigste inden for adgangsstyring er at optimere hvordan RBAC skal defineres og implementeres.
I kapitel 3 kom det dog frem, at informationssikkerhed bør opfattes holistisk i forhold til en organisation, og derfor vil der gøres et forsøg på også at opfatte adgangsstyring holistisk. Derfor vil litteraturen blive gennemgået ved hjælp af ISACAs (2009) forretningsmodel for informationssikkerhed, for at se om der dermed kan skabes en holistisk tilgang til adgangsstyring. Håbet med denne holistiske tilgang er, at den kan hjælpe med at identificere og give bud på løsninger, til de problemstillinger, der eksisterer inden for adgangsstyring.

5 Teori – Holistisk syn på adgangsstyring

I de to forrige afsnit er der beskrevet, hvordan informationssikkerhed bliver opfattet, og hvad adgangsstyring indeholder. I forhold til informationssikkerhed overordnet ses det, at der forsøges at gøre et skift fra, at informationssikkerhed er noget rent teknisk over til, at det også hænger sammen med medarbejderne og forretningen.
På denne baggrund tager ISACA (2009) et holistisk syn på IT sikkerheden i en virksomhed, og inspireret af tankegangen bag systemtænkning, hvor der ses bort fra en lineær kausalitet, og i stedet fokuseres på en cirkulær kausalitet, dvs. en handling er både årsag og virkning (Senge, 2003), har de opstillet en forretningsmodel for IT sikkerhed. Deres ide med forretningsmodellen er, at IT sikkerhed ikke skal opfattes som noget teknisk, men der skal skabes en tilsigtet informationssikkerhedskultur, og selve modellen viser, hvordan en virksomheds informationssikkerhed har betydning for, og påvirker alle dele af en organisation.

Ifølge Ferraiolo et al., (2003) findes der to forskellige indgangsvinkler til, hvordan målsætningen skal defineres for adgangsstyring. Den ene går ud på, at systemressourcer skal beskyttes mod uhensigtsmæssig eller uønsket brugeradgang, og den anden tager et forretningsmæssigt perspektiv, hvor målet for adgangsstyring er at sikre den optimale deling af information.
Da adgangsstyring er en del af en virksomheds samlede informationssikkerhed, og der netop advokeres for, at informationssikkerhed ikke kun er en teknisk disciplin, vil forretningsmodellen for informationssikkerhed gennemgås, i forhold til hvordan den passer sammen med adgangsstyring.
Selvom adgangsstyring er en delmængde af en virksomheds samlede informationssikkerhed, og derfor er alle elementer eventuelt ikke lige relevante for netop adgangsstyring, så vil modellen gås igennem trinvis, for også at have en holistisk indgangsvinkel til adgangsstyringen, og dermed forsøge at undgå, at noget vil blive overset.
Selve modellen består af 4 elementer der er forbundet af 6 dynamiske sammenkoblinger. Den skal opfattes som en tredimensionel pyramide, hvor hvert aspekt interagerer med de andre, og hvis en del af modellen bliver ændret eller forvaltet forkert, er balancen i modellen potentielt i fare (ISACA, 2009, s. 14f). De dynamiske sammenkoblinger forbinder de 4 elementer og udfører en kraft der både kan skubbe og trække i forhold til de forandringer der sker. Handlingerne der foretages i sammenkoblingerne, kan bringe modellen ud af balance, eller genoprette ligevægten (ISACA, 2009, s. 16f).

Figur 5: Forretningsmodel for informationssikkerhed



Kilde: ISACA, 2009, s. 1

5.1 De 4 elementer

Hvert af de fire elementer vil blive sammenholdt, med den litteratur der findes for adgangsstyring, for at kunne udlede en faktor der kan påvirke et autorisationskoncept. Dette bliver gjort for at strukturere gennemgangen af litteraturen, og for samtidig at sikre en synliggørelse af, at adgangsstyring bliver påvirket af alle elementer fra organisationen. Denne synliggørelse bliver konkret udformet ved, at der efter hvert element bliver udledt en faktor, der kan påvirke et autorisationskoncept.

5.1.1 Organisation, design/strategi (Organization, design/strategy)

Det første element der bliver gennemgået fra modellen, er Organisation, design/strategi, hvor en organisation er et netværk af mennesker, processer og aktiver der interagerer med hinanden i forudbestemte roller mod et fælles mål. Strategien udstikker retningen virksomheden ønsker at gå, ved at formulere mål og formål, samt visionen og værdier. Designet definerer hvordan organisationen implementerer strategien (ISACA, 2009, s. 15).

5.1.1.1 Organisation, design/strategi i relation til adgangsstyring

Da et autorisationskoncept sørger for, og samtidig kontrollerer, hvilken information der bliver tilgået og af hvem, er en af præmisserne, at virksomheden er klar over, hvordan denne information ser ud, og om den er vigtig at beskytte eller ej.

En virksomheds aktiver der er relateret til IT, kan deles op i fysiske aktiver og informationsaktiver, hvor de fysiske aktiver f.eks. kan være computere, servere, netværk og kommunikationslinjer, er informationsaktiverne f.eks. medarbejdernes viden, udvikling og produktinformation, virksomhedens ry, erfaring og medarbejdernes viden. Hvor de fysiske aktivers værdi relativt let kan bestemmes ud fra købspris og afskrivninger, er det sværere med informationsaktiverne. Ikke desto mindre er det nødvendigt at gøre sig tanker om dette forud for implementeringen af sikkerhedsløsningerne for IT (Linkies & Off, 2005, 31).
Uden at kende værdien af et aktiv vil det ikke være muligt at indføre en passende sikkerhedsløsning. Det kan sammenlignes med den fysiske sikkerhed omkring ens egen bopæl og en bank, hvor banken, har flere værdier og derfor større incitament til at investere i sikkerheden. Værdierne skal dog holdes op mod den potentielle sandsynlighed for, at en utilsigtet handling måtte forekomme, så hvis ens bopæl befinder sig i et udsat område, kunne dette også være et incitament for at øge sikkerhedsforanstaltningerne.
Det samme gør sig gældende ved udvikling og implementering af autorisationer. Hvis en bestemt information godt må være offentlig tilgængelig, er der ingen grund til at indføre diverse kontroller, men er der derimod tale om fortrolig information, der ved offentliggørelse kan skade en virksomheds ry og omsætning, vil der være god grund for at have en udførlig autorisationskontrol og sikre, at det kun er autoriserede medarbejdere, der kan tilgå disse informationer. Så en forudsætning for at udvikle et autorisationskoncept er, at informationsaktiverne først identificeres, derefter skal de værdisættes, sandsynligheden for en skadelig handling indtræffer estimeres, og til sidst hvilken indvirkning det har, hvis den skadelige situation opstår.

Linkies og Off (2005, s. 181ff) har selv identificeret følgende risici inden for et SAP ERP system: Utilstrækkeligt autorisationskoncept, utilstrækkelig ansvarsstruktur, ikke fuldt defineret autorisationskoncept, tekniske problemer med autorisationer og identitetsstyring[3].
Det ses, at alle risici er relateret til adgangsstyring. Den nævnte utilstrækkelige ansvarsstruktur, vil der blive kigget nærmere på i afsnit 5.2.1 senere i afhandlingen.

5.1.1.2 Faktor der kan udledes

Af ovenstående ses det, at en risikoanalyse påvirker og ligger til grund for hvordan et autorisationskoncept bliver udviklet, da identificeringen af de forskellige risikopotentialer giver input til hvilken information, der skal beskyttes.

[3] Da tre af de omtalte risici omhandler autentificering, og der ikke er fokus på dette i denne afhandling, er de blevet slået sammen til et punkt: identitetsstyring.

5.1.2 Mennesker (People)

Det næste element i modellen er mennesker, der repræsenterer de menneskelige ressourcer, samt de sikkerhedsspørgsmål der omgiver dem. Det definerer, hvem der implementerer hvilken del af strategien i forhold til designet, og skal tage højde for adfærd, værdier og systematiske fejl (ISACA, 2009, s. 15).

5.1.2.1 Mennesker i relation til adgangsstyring

Dem der håndterer autorisationer i et system, er autorisationskonsulenterne. En autorisationskonsulent i SAP har forstand på, hvordan autorisationer implementeres i SAP systemerne, f.eks. i forhold til roller, transaktionskoder og autorisationsobjekter. Der er stadig nogen, der ser informationssikkerhed som en rent teknisk disciplin (ISACA, s. 4), og i denne gruppe hører også flere autorisationskonsulenter.

Som nævnt i indledningen af dette kapitel er Ferraiolo et al. (2003) inde på, at der er forskellige indgangsvinkler til målsætningen for adgangsstyring: et teknisk og et forretningsmæssigt perspektiv. Ved at uddybe dette, og låne noget litteratur generelt omhandlende informationsteknologi, kan det diskuteres om, autorisationskonsulenterne i virkeligheden befinder sig inden for to forskellige paradigmer. Paradigmet dækker over de grundlæggende antagelser i forhold til, hvordan adgangsstyring bør håndteres og hvad formålet med adgangsstyring og autorisationer er.
Hvor der før kun var fokus på, hvordan adgangen teknisk skulle fordeles, er der nu med øget opmærksomhed og skrappere eksterne krav en helt ny interesse for dette område. Teknologien har også udviklet sig, og det er nu muligt at tænke i integration og overordnede sammenhænge.
Friedman (1994) nævner, at der findes forskellige informationsteknologiske paradigmer, og han forudser, at det nyeste paradigme der vil komme, vil være et hvor der fokuseres på informationsteknologien i samspil med dens omgivelser. I forhold til autorisationskonsulentens verden kan dette paradigme kaldes det holistiske paradigme, det vil sige autorisationskonsulenterne skal være i stand til at tænke i de større træk og i konceptuelle baner.
Det eksisterende paradigme i 1994, som Friedman så det, er, at brugere af systemerne er kommet ind i billedet, og det gælder om at producere systemer, som brugerne reelt har brug for, eller som skaber sand værdi for organisationen (Friedman, 1994, s. 380). Oversat til autorisationskonsulentens verden bliver det til, at autorisationskonsulentens formål er at producere roller, og dermed autorisationer, som brugerne har brug for, og der dermed kan skabes værdi for organisationen. Det vil sige, det her går ud på at kende sit værktøj, og kunne arbejde effektivt med det i forhold til en brugers ønsker. Dette paradigme kan derfor betegnes som praktikerens paradigme.

Friedman gør opmærksom på, at når der tales teknologiske paradigmer, er der ofte en fejlagtig opfattelse af, at når der kommer et nyt paradigme, vil det betyde at det eksisterende vil blive udslettet (Friedman, 1994, s. 387). Oprindeligt har Kuhn (1995) da heller ikke tænkt, at der ikke kunne eksistere to paradigmer samtidigt,

tværtimod beskriver han netop, hvordan nogle tilhængere af et eksisterende paradigme aldrig vil være i stand til at acceptere et nyt paradigme. Ikke fordi de bevidst er forandringsfjendske, men simpelthen fordi de ikke kan tro, det nye paradigme vil fungere, eller rettere sagt er meningsfuldt, og at et fuldstændigt skift til et nyt paradigme ofte først sker, efter de mest trofaste medlemmer af det gamle paradigme er døde (Kuhn, 1995, s.190f).

5.1.2.2 Faktor der kan udledes

Da et paradigme har indflydelse på, hvordan verden bliver opfattet, og hvilke grundlæggende antagelser der bliver taget, er det i forhold til autorisationskoncepterne en relevant faktor, at finde ud af og være bevidst om hvilket paradigme autorisationskonsulenterne befinder sig i.

5.1.3 Proces (Process)

Det næste element i modellen er Proces, der indeholder de formelle og uformelle mekanismer, der skal sørge for, at tingene sker. De er afledt fra strategien, og sørger for at implementere den operationelle del fra organisationselementet. Processerne sørger for at identificere, styre og kontrollere risici, tilgængelighed, fortrolighed og integriteten, samt at sikre ansvarlighed (ISACA, 2009, s. 15).

5.1.3.1 Proces i relation til adgangsstyring

Når et autorisationskoncept er implementeret, skal der forefindes procedurer for, hvordan en bruger rekvirerer en adgang, hvordan den skal godkendes og hvordan den bliver fjernet igen. Der skal også findes procedurer for, hvordan vedligeholdelsen af rollerne skal foregå, det vil sige ønsker til, tilladelse af, og udførslen af ændringer, samt test og distribuering af dem (Hirao, 2004, s. 5).
Dette vil også afhænge af, hvordan virksomhedens indgangsvinkel er til åbenheden af dens data. F.eks. i forhold til om al information er fortroligt, eller om det modsatte er tilfældet. For adgangsstyringen har det betydning, i forhold til den indgangsvinkel der bør vælges, når roller skal udvikles til et autorisationskoncept (Hirao, 2004).

Der findes flere forskellige indgangsvinkler, der kan vælges, og hver af dem indebærer fordele og ulemper, blandt andet i forhold til hvor mange ressourcer det kræver at vedligeholde rollerne, og hvor godt de kan leve op til krav fra standarder og sikkerhedsprincipper.
Nedenfor gennemgås 5 forskellige indgangsvinkler til rolleudvikling med dertil hørende fordele og ulemper.

1) Adgang til alt

Denne tilgang nævner Hirao (2004) som den åbne tilgang, hvor medarbejdere har adgang til alt på nær de helt kritiske funktioner, som for eksempel rolleudvikling og brugeradministration. Fordelene er, at medarbejdere ikke bliver afbrudt i deres arbejde, fordi de pludselig mangler adgang til noget, og det vil være let at finde ud af, hvilken rolle de skal have tildelt, da der vil eksistere meget få roller. Dermed vil der ikke kræves særlig mange ressourcer til at foretage brugeradministration. Ulemperne er dog, at der risikeres at blive tildelt for bred adgang til medarbejderne, og de få roller der bliver udviklet, vil blive meget store og uoverskuelige. Derudover vil det også kræve meget arbejdskraft og være en tidskrævende proces at få udviklet rollerne, da alle transaktioner, tabeller og autorisationsobjekter skal gennemgås for at tildele den brede adgang (Hirao, 2004). Så selvom der spares ressourcer på brugeradministrationen, vil der bliver brugt mange flere på at foretage selve rolleudviklingen.

2) 1 person 1 rolle

Denne tilgang kalder Hirao (2004) den lukkede døs politik, hvor hver medarbejder får tildelt en individuel adgang, med lige netop det medarbejderen har brug for. Fordelene er, at medarbejderne præcist har adgang til det, de skal bruge. Derudover vil det kræve et minimum af brugeradministration, da hver medarbejder kun skal have tilføjet den rolle, der allerede er udviklet til ham. Ulemperne er, at det vil kræve en enorm administration at udvikle og vedligeholde rollerne, da der skal udvikles en rolle til hver enkelt medarbejder. Hvis der kun er et fåtal af brugere, vil det ikke være så stort et problem, men for hver ekstra bruger vil arbejdsbyrden stige tilsvarende, og allerede når der er et tocifret antal brugere, vil dette skabe en uoverskuelig byrde.

3) Forretningsområder

Hvor de to ovenstående tilgange er mere to ekstremer, befinder den sig i midten, i forhold til at mindske unødvendige adgange, men stadig ikke skabe en umulig arbejdsbyrde for rolleudviklerne. Ideen med denne indgangsvinkel er at oprette roller, der svarer til en virksomheds forretningsområder. Fordelene er, at forretningsområderne ofte vil være klart definerede, så det vil være let at identificere og placere en ansvarlig for rollen, samt de medarbejdere der skal have tildelt rollerne. Ulempen er dog, at selv om det er let at tilknytte roller til de medarbejdere, der er ansat inden for et bestemt forretningsområde, betyder det ikke nødvendigvis, at medarbejderen kun arbejder inden for dette arbejdsområde. Ofte tager medarbejdere del i tværorganisatoriske projekter, eller har et par enkelte ansvarsområder, der ikke ligger inden for deres primære forretningsområde. Derudover er det heller ikke sikkert, at en medarbejder der arbejder inden for et bestemt forretningsområde, har brug for adgang til alt inden for dette, og der risikeres derfor igen at blive tildelt en for bred adgang.

4) Jobfunktioner

For at komme ovenstående ulempe til livs, i forhold til en for bred tildeling af adgang til den enkelte medarbejder, kan en indgangsvinkel bruges, hvor rollerne oprettes i forhold til den jobfunktion, den enkelte

medarbejder har. Vanamali (2008) betegner denne indgangsvinkel for top-down, da den starter med at kortlægge medarbejdernes jobfunktioner, og derefter ser, hvordan rollerne skal defineres på systemerne.
Fordelene er, at medarbejderne får adgang til netop det, de har brug for til at udføre deres arbejde. Ulempen er, at det kan være svært i praksis at identificere alle medarbejdernes jobfunktioner, og det vil kræve en stærk tilpasning mellem forretningen og teknologien, før rollerne kan blive effektive.

5) Eksisterende tilladelser
Denne sidste indgangsvinkel kalder Vanamali (2008) bottom-up, og går ud på, at rollerne bliver udviklet med udgangspunkt i de eksisterende brugeres roller og rettigheder. Vanamali (2008) foreslår, at det kan gøres ved at foretage en slags data-mining på de eksisterende roller. Da rollerne bliver udviklet med afsæt i de allerede eksisterende tilladelser, burde det betyde, at medarbejderne får de adgange, de har brug for. Denne fremgangsmåde kan dog kun benyttes, når der skal udvikles roller til et system med allerede eksisterende brugere. Fordelene er, at brugerne ikke kommer til at mangle nogle adgange, da det må antages, at de roller der bliver udviklet, lever op til brugernes behov, da de bygger på deres eksisterende tilladelser. Ulemperne er, at det kan være svært, rent praktisk at udføre den data-mining der skal til, og der er stor risiko for, at brugerne har et sammensurium af tilladelser fra nuværende og tidligere jobs, og dermed giver deres nuværende tilladelser ikke et retvisende billede af, hvad de egentlig har brug for af rettigheder.

Det kan i nogle tilfælde også være muligt at kombinere flere af de ovenstående tilgange. Et typisk eksempel er f.eks., at en organisation har en stor salgsafdeling, og har opdelt dette forretningsområde i mange forskellige jobfunktioner, mens finansafdelingen er lille, og derfor ikke er opdelt, og de medarbejdere indenfor dette forretningsområde har adgang til alle processerne. Dette kan skyldes, at de forskellige forretningsområder har fået implementeret deres systemer forskudt og formentligt udført af forskellige konsulenter. Dette har medført en forskellighed, både i forhold til hvordan systemerne blev opfattet på tidspunktet for implementeringen, samt hvilken opfattelse personerne der implementerede autorisationskoncepterne havde.

5.1.3.2 Faktor der kan udledes

Det er vigtigt at slå fast, at formålet med at skabe og tildele systemroller til medarbejderne ikke er for at begrænse dem i deres arbejde men sikre, at de lige netop har adgang til det, de har brug for, til at kunne udføre deres arbejde forsvarligt.
Kunsten er at skabe rollestrukturen, så den er intuitiv, og giver plads til fleksibilitet. Dermed bliver det vigtigt at være opmærksom på, hvilken indgangsvinkel der bliver besluttet, i forhold til hvordan roller skal udvikles, da der så kan tages højde, for de fordele og ulemper dette medfører.

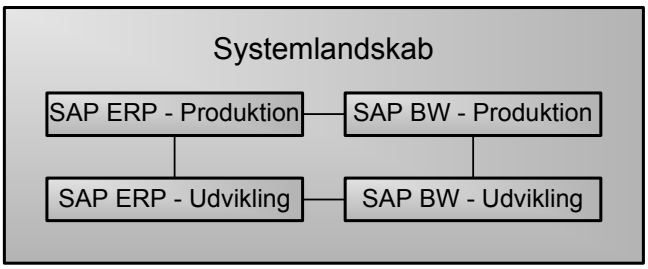
5.1.4 Teknologi (Technology)

Teknologien indeholder alle de applikationer, værktøjer og infrastruktur der gør processerne mere effektive. Teknologien oplever en stor påvirkning fra brugerne, der enten ikke har tillid til teknologien, ikke har lært at bruge den, eller simpelthen føler den er en hindring for dem (ISACA, 2009, s. 15f).

5.1.4.1 Teknologi i relation til adgangsstyring

De værktøjer der er til rådighed samt deres indbyrdes integration, vil have en indflydelse på, hvordan autorisationskonceptet kan blive implementeret. Det vil også komme an på, hvilke tekniske systemer der findes i virksomheden, og om der skal bruges forskellige værktøjer til hvert system, eller der findes en synkronisering eller centralisering sted. Maurizio et al. (2007, s.23f) gør opmærksom på, at det er vigtigt at kontrollere konsistensen af data mellem forskellige systemer, og så vidt muligt integrere systemerne, så en automatisk distribution af information kan ske mellem systemerne. Dette gælder både på tværs af produktive systemer, men også inden for de enkelte systemmiljøer hvor hvert produktivt system, for det meste, har sit eget udviklings- og testsystem tilknyttet.
Ofte foregår forretningsprocesser på tværs af systemer, da de gør brug af de forskellige systemers teknologi til at levere den mest optimale proces for brugeren. Dette gør det yderligere komplekst, da hvert system kan have forskellige underliggende teknologier til brug for adgangsstyring. Maurizio et al. (2007) arbejder med integrationen af SAP ERP og SAP Business Warehouse (BW), og på nedenstående figur vises hvordan sammenhængen kunne se ud:

Figur 6: Eksempel på sammenhænge i en organisations systemlandskab



Kilde: Egen frembringelse

Den vertikale sammenhæng har indflydelse, da de produktive systemer kan tilgås fra de underliggende test og udviklingssystemer, og ofte er autorisationskoncepterne for sådanne systemer meget løst definerede, hvis de overhovedet eksisterer. Autorisationskoncepterne fokuserer ofte kun på adgangene i de produktive systemer, og det implementeres kun til brugerne af selve forretningsprocesserne. Dermed mangler der adgangsstyring for de funktioner der skal supportere forretningsprocessen, som f.eks.

implementeringskonsulenten der har adgang til alle systemtyper, for at kunne levere en hurtig og effektiv support.

5.1.4.2 Faktor der kan udledes

For at få et overblik over hvad autorisationskonceptet skal gælde for, kan det betale sig at kende virksomhedens systemlandskab, da dette ikke kun giver et overblik, over de forskellige teknologier der skal bruges til at udvikle roller og autorisationer, men også en mulighed for at identificere, hvor der med fordel kan genbruges på tværs af teknologier og systemer. Derudover hjælper det til med at imødekomme forskelligheden i adgangsstyringen på systemerne, så adgangen til forretningsprocesserne for brugeren bliver fyldestgørende, og der gives en ensartet adgang til data og funktionalitet på tværs af systemerne.

5.2 De 6 dynamiske sammenkoblinger

På samme måde som de 4 elementer blev gennemgået, vil de 6 dynamiske sammenkoblinger også blive gennemgået. Og på samme måde vil der efter hver sammenkobling blive udledt en faktor, der vil kunne påvirke et autorisationskoncept.

5.2.1 Regulering (Governing)

Regulering er den måde, virksomheden bliver styret på. Det sætter grænserne, indenfor hvor virksomheden kan operere. Regulering sikrer, at formål er definerede, risici styres ordentligt, og virksomhedens ressourcer bruges på den mest hensigtsmæssige måde (ISACA, 2009, s. 16).

5.2.1.1 Regulering i relation til adgangsstyring

For at styre risici ordentligt og sikre, at de medarbejdere der tilgår informationen, også er berettiget til det, bør der være klarhed over informationsejerskabet i en virksomhed. Derfor er det vigtigt at identificere og fordele ejerskabet på en virksomheds informationsaktiver, og det samme gør sig gældende, for de autorisationer der giver adgang til disse aktiver.
Austin og Darby (2003) nævner, at en leder ikke bør fokusere på den tekniske del af sikkerheden, men mere være i stand til at vurdere forretningsværdien af informationsaktiverne, afgøre sandsynligheden for, at de kan kompromitteres, og sammenkæde det med processer, der kan reducere risikoen af bestemte sårbarheder. Målet er ikke at have et 100 % sikkert system, men at minimere forretningsrisici til et minimum, og det er her, lederne har en opgave, i forhold til at identificere hvilke risici der kan give mest skade til forretningen (Austin og Darby, 2003, s. 121ff).

Et af problemerne ved adgangsstyring er, at der ofte bliver givet enten for mange eller for få autorisationer.
De værktøjer der bruges til at styre autorisationer i SAP er meget fleksible, hvilket ofte medfører et komplekst og teknisk design, der igen betyder, at efter implementeringen er det kun autorisationskonsulenterne, der har et overblik over, og evner at styre autorisationerne, men de bliver så igen overvældet af evalueringer af risici og forespørgsler på nye autorisationer. Derudover er struktureringen, mængden, typerne og selve navngivningen kompleks og teknisk, og giver ikke mening for de ansvarlige, for de områder autorisationerne vedrører (Linkies & Off 2005, s.56f).
Hirao (2004, s.3) fraråder at give ansvaret for roller og autorisationer til den øverste ledelse, da der kan opstå en situation, hvor de ansvarlige ikke har viden om de specifikke forretningsprocesser og endnu mindre om de underliggende data, og der i så fald er risiko for, at der vil blive uddelt carte blanche til samtlige forespørgsler om adgang. I stedet foreslås, at ejerskabet gives til dem, der i forvejen er ansvarlige, for den forretningsproces autorisationen vedrører.

Det er de områdeansvarlige, der har ekspertisen til at foretage afgørelser inden for deres område, samt estimere og evaluere risici, og de bliver nødt til at tage ansvaret for dette. Autorisationsmedarbejderen kan opstille rammen og opføre de basale processer, men det bør være den person, der er ansvarlig for et givent område, der også er ansvarlig for at vedligeholde de rette sikkerhedsforanstaltninger (Linkies & Off 2005, s.59f). En måde at implementere et informationsejerskab på er ved, at de enkelte afdelinger selv udvikler autorisationer, og tildeler dem til brugerne. Da den enkelte afdelings ansvarlige både har ekspertisen omkring, og ansvaret for det der bliver givet adgang til, vil de automatisk sørge for, at der kun bliver givet lige netop den adgang, der er behov for (Linkies & Off, 2005, s. 74). Denne fremgangsmåde står overfor en centralt styret, hvor ændringer alt for ofte bare bliver lig med tilføjelser til eksisterende roller. *"Changes to user authorizations are frequently carried out by simply adding more information to the profiles."* (Linkies & Off 2005, s.72).

5.2.1.2 Faktor der kan udledes

Det en vigtig forudsætning for et autorisationskoncept, at der er identificeret og uddelegeret et ejerskab for virksomhedens informationsaktiver. Mere konkret vil det være, i forhold til hvem der skal være ansvarlig for hvilke roller.

5.2.2 Det uforudsete (Emergence)

Det uforudsete referer til de handlinger og situationer, der pludselig kan opstå uden synlig grund, og hvis udfald det er umuligt at forudsige og kontrollere. Det er her, der skal indføres risikostyring, forandringskontrol og tilpasning af procesforbedringer (ISACA, 2009, s. 17).

5.2.2.1 Det uforudsete i relation til adgangsstyring

En ofte uforudset situation sker, når rollerne, og dermed processerne, ikke er godt nok testet, f.eks. kan der være handlinger, der kun skal foretages ved kvartals- eller årsafslutninger. Disse handlinger bliver ofte udført i forhold til en stram deadline, og derfor bliver rollerne oftest tildelt uforholdsmæssigt meget ekstra autorisation, for at sikre, at processen kan gennemføres. Efterfølgende bliver der ikke evalueret på, hvad der egentlig er brug for af autorisation, til at foretage de ønskede handlinger, og derved bliver rollerne ikke tilpasset, og beholder den brede autorisation.
Et velfungerende autorisationskoncept vil forhåbentligt medvirke til, at der sker færre uforudsete situationer. Et af formålene med et autorisationskoncept er at sikre, at medarbejderne kan tilgå de ressourcer de har brug for, i forhold til det arbejde de skal udføre, og til dette eksisterer der to kendte sikkerhedsprincipper: det mindste privilegiums princip og separation af opgaver.

Det mindste privilegiums princip

Det mindste privilegiums princip og separation af opgaver er to velkendte sikkerhedsprincipper inden for adgangsstyring (Omicini et al., 2005, s. 68).
Hirao (2004) opstiller de to ekstremer; den åbne tilgang, hvor alle som udgangspunkt har adgang til alt, og derefter fjerner man specifikke rettigheder, og overfor denne står den lukkede dørs politik, hvor ingen har adgang til noget som helst, og der så bliver åbnet op for lige netop det der er brug for.
Den sidstnævnte fremgangsmåde bliver kaldt det mindste privilegiums princip, og er en praksis, hvor en bruger kun får adgang til netop det, han har brug for i forhold til at udføre sin jobfunktion. Fordelen ved denne praksis er, at en bruger ikke har ekstra unødvendig adgang, og derved ikke har mulighed for at udføre fejl eller potentielt skadelige handlinger udenfor sit jobområde.
Udfordringen er dog at identificere præcist hvad en bruger har brug for, dette kræver en del administration. Hvis det skal følges stringent, bør der også ses på brugerens behov i forhold til forskellige tidspunkter, hvilket vil give en ekstra byrde til i forhold til administrationen (Ferraiolo et al, 2003, s. 5).

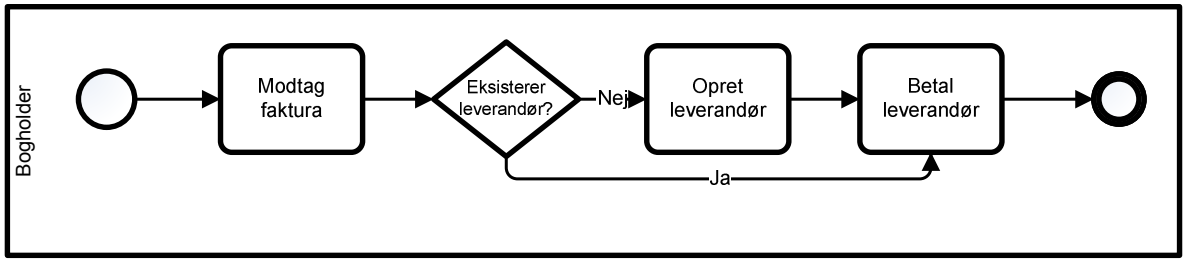
Separation af opgaver

Separation af opgaver er en betegnelse for det at have flere personer involveret til udførelsen af en, ofte følsom eller kritisk, opgave (blandt andre: Omicini et al., 2005; Little & Best, 2003).

På nedenstående figur ses et BPD[4], der kunne være designet i forbindelse med en løsning til et økonomimodul. Diagrammet viser en proces for modtagelse og betaling af en faktura. Dette procesdiagram er selvfølgelig forenklet og alt efter hvilken og hvor stor en virksomhed, vil der være flere aktiviteter involveret, det kunne eventuelt være, at der kontrolleres om et produkt eller ydelse er leveret før fakturaen betales.

[4] Business Process Modeling Notation (BPMN) er en notationsform, der kan bruges til at udvikle Business Proces Diagrams (BPD). Notationsformen er brugbar, fordi den bruger elementer fra standard UML, der gør den genkendelig og let at forstå. Den arbejder med få og enkle objekter, men er kompleks nok til at vise også tekniske processer. Den er udfærdiget med henblik på at have en notationsform der kan skabe diagrammer der både kan læses og forstås af ledelsen samt af mere teknisk personale. BPMN kan bruges til at beskrive B2B, men også interne forretningsprocesser (White, 2004).

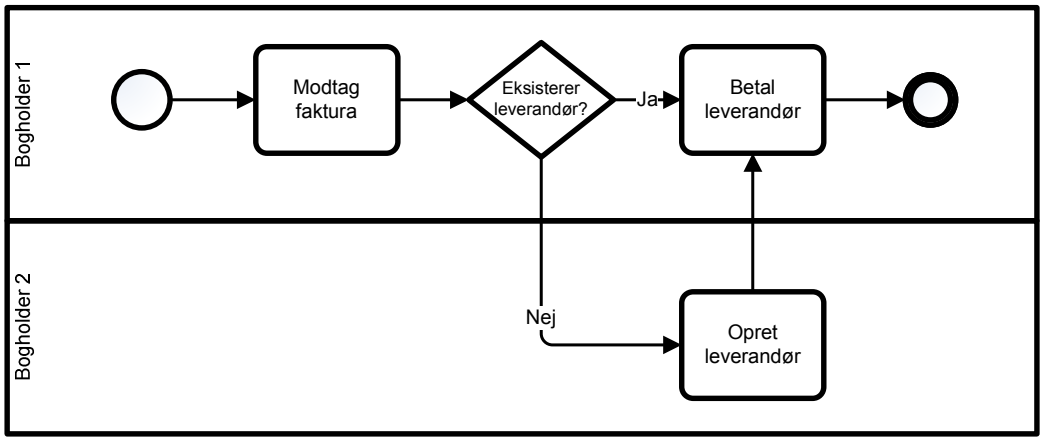
Figur 7: Modtagelse og betaling af faktura uden funktionsadskillelse



Kilde: Egen frembringelse

I forhold til at overholde separationen af opgaver, er det ikke god skik, at den samme person kan vedligeholde master data og samtidig foretage posteringer (Little & Best, 2003, s. 421). I dette eksempel vil det sige, at den samme person ikke må oprette en leverandør, og samtidig betale fakturaen.
Det vil nemlig betyde, at personen kan opfinde en fiktiv leverandør og derefter udbetale penge. For at mindske denne risiko skal opgaven deles ud på to personer, det vil sige, processen så skulle designes som på figuren nedenfor Dette mindsker risikoen, da begge de to involverede personer i så fald skal være med til at udføre bedrageriet.

Figur 8: Modtagelse og betaling af faktura uden funktionsadskillelse



Kilde: Egen frembringelse

Dette princip gør sig selvfølgelig også gældende i forhold til processer, der har med adgangsstyring at gøre, f.eks. i forhold til styring af adgangsrettigheder er det vigtigt, at den person der udvikler en rolle, ikke er den samme, der kan tildele rollen. Ved at indføre denne adskillelse sikres det, at en person ikke kan udvikle en rolle, der giver adgang til sensitive data og derefter tildele rollen til sig selv.

5.2.2.2 Faktor der kan udledes

Et velfungerende autorisationskoncept vil netop medvirke til, at der sker færre uforudsete situationer, men det er selvfølgelig begrænset, hvor meget uforudsete situationer kan undgås, da det jo netop er uforudset, og derfor ikke er forventet. Det vigtigste er at være opmærksom på at uforudsete handlinger kan opstå, og så kunne håndtere dem, når det sker. Ved at følge gældende sikkerhedsprincipper kan nogen af de uforudsete handlinger forhåbentligt kommes i forkøbet.

5.2.3 Kultur (Culture)

Kulturen er et mønster af adfærd, tro, antagelser, attitude og måden at gøre tingene på. Kulturen bygger på nogle fælles tidligere oplevelser der ligger til grund for fremtidig forventet adfærd. Det giver sig til udtryk i uskrevne regler, der bliver en norm for dem der deler den samme kultur. Kulturer kan findes i mange lag, og bliver skabt både af interne og eksterne faktorer (ISACA, 2009, s. 16).

5.2.3.1 Kultur i relation til adgangsstyring

Kulturen har indflydelse på, hvordan autorisationskonsulentens arbejde bliver opfattet, og mere konkret hvornår det skal involveres i et projektforløb. Skal autorisationskonsulenten involveres i et SAP projekt fra starten, eller skal han først involveres til slut, når processerne allerede er defineret. Ulempen ved den sidste måde er, at hensynet til informationssikkerhed har indflydelse på, hvordan processer skal defineres, og dermed medfører en for sen involvering, at det ikke er muligt at have denne indflydelse. En af forudsætningerne for at udvikle et ordentligt autorisationskoncept er netop at kende processerne på forhånd (Esch & Junold, 2009, s.26ff)
Et eksempel er den proces, der allerede er beskrevet i afsnit 5.2.2.1, hvor der bliver modtaget en faktura fra en ny leverandør. Hvis autorisationskonsulenten blev involveret fra starten, ville han kunne gøre opmærksom på, at processen var kritisk, og der skulle finde en separation af opgaver sted for at involvere to personer i processen.
Grunden til det er vigtigt at få en eventuel separation af opgaver på plads under designet af processerne og ikke efterfølgende er, at når en proces først er implementeret i en teknisk løsning, er det ikke sikkert den uden videre kan ændres igen. Dette kan skyldes at både oprettelsen og betalingen af leverandøren sker i samme skærmbillede i systemet. Desuden kan det være, at det underliggende autorisationstjek ikke er differentieret nok til at imødekomme organisationens ønsker, eller de love den er underlagt, derfor skal der i programmerne indlægges autorisationstjek, der netop sikrer, at disse ønsker og love overholdes.

I SAP bliver sådanne processer implementeret ved hjælp af transaktionskoder og autorisationsobjekter, og da roller netop indeholder transaktionskoder, vil en separation af opgaver ikke kunne lade sig gøre, hvis

begge aktiviteter befinder sig i den samme transaktionskode, og autorisationsobjektet ikke kan differentiere adgangen til aktiviteterne. Dermed vil opgaven ikke kunne deles ud til to forskellige personer.

5.2.3.2 Faktor der kan udledes

Fra denne dynamiske sammenkobling kan det udledes, at autorisationskonsulenten skal involveres allerede under defineringen af processerne for, at alle krav til adgangsstyring bliver klarlagt i forbindelse med defineringen af forretningsprocesserne. Dermed sikres, at informationssikkerhed bliver tænkt ind i processerne fra start af, og ikke bare er noget, der bliver koblet på til sidst, eventuelt fordi det bliver påpeget af revisionen.

5.2.4 Aktivering og støtte (Enabling & Support)

Denne sammenkobling går mellem proces og teknologi, og ved at lave procedurer brugervenlige og simple, kan det hjælpe til med, at mennesker også følger dem. Standarder, politiker og brugervejledninger skal designes så de hjælper til med at mindske interessekonflikter (ISACA, 2009, s. 16f).

5.2.4.1 Aktivering og støtte i relation til adgangsstyring

Procedurer og retningslinjer bliver udført i forhold til at sikre, at aktiviteter bliver udført på en korrekt og hensigtsmæssig måde. Det behøver ikke kun være korrekt i forhold til den enkelte virksomheds egne præferencer, men bunder ofte i eksterne krav fra lovgivning, f.eks. persondataloven, og sikkerhedsstandarder, f.eks. DS 484, som virksomheden ønsker, eller skal, leve op til.

IT standarder – DS 484

DS 484 er en dansk standard for informationssikkerhed. Denne standard ligger ofte til grund for en virksomheds interne sikkerhedspolitikker, der igen vil indeholde krav til, hvordan informationsaktiver skal tilgås, og dermed har indflydelse på, hvordan autorisationskonceptet må agere.
Standarden har både til formål at udgøre et generelt grundlag for en virksomheds sikkerhedsmålsætning, samt være referenceramme for virksomhedens brug af IT systemer og give et tillidsgrundlag til virksomhedens interne og eksterne informationsbehandling (DS 484, 2005, s. 11).
Standarden beskriver 12 forskellige områder og dertil hørende krav inden for informationssikkerhed. Disse områder dækker blandt andet fysisk sikkerhed, styring af netværk og drift og beredskabsstyring. Her fremhæves kun de to mest relevante områder for den nærværende problemstilling.

1) Styring af informationsrelaterede aktiver

Formålet er *"at sikre og vedligeholde den nødvendige beskyttelse af virksomhedens informationsaktiver"* (DS 484, 2005, s. 32). Der skal udpeges en ejer for alle identificerede informationsaktiver, og informationerne skal klassificeres i forhold til deres betydning, samt der skal udarbejdes retningslinjer for, hvordan informationer kan tilgås og bruges (DS 484, 2005, s. 32ff).

Ad 2) Adgangsstyring

Det overordnede formål med adgangsstyringen er at kontrollere hvem der får adgang til hvilke informationer og hvordan og dermed forhindre misbrug eller fejl. Administration af brugeradgange er en vigtig del af dette, for at forhindre uautoriseret adgang og sikre autoriserede brugeres adgange. Ved registrering af brugere skal både tildeling og afbrydelse af brugeradgang være beskrevet i en formaliseret forretningsgang, og derudover bør det overvejes at definere typiske brugerprofiler for at lette administration og opfølgning (DS 484, 2005, s. 62f). Der bør også være en mulighed for at tidsbegrænse adgange, adgangen til informationer bør begrænses, og der skal være kontrol med de enkelte brugeres rettigheder (DS 484, 2005, s. 70ff).

Persondataloven

Ifølge Datatilsynet (2009) så er persondataloven hovedloven i forhold til, hvornår og hvordan en virksomhed, organisation eller myndighed skal behandle personoplysninger. Den dikterer blandt andet, at oplysninger skal opdeles i forhold til om de er følsomme eller ikke-følsomme, og at den dataansvarlige skal have truffet de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger blandt andet i forhold til at undgå at de kommer til uvedkommendes kendskab.

I indledningen bliver SOX nævnt, og selvom det kun er virksomheder, der er børsnoteret i USA, f.eks. Novo Nordisk A/S, eller datterselskaber af sådanne, f.eks. Microsoft Danmark ApS, der er direkte underlagt SOX, har dele af SOX dannet best practice og bør derfor tages seriøst af alle organisationer (DocTech, 2006). Dog gennemgår jeg den ikke nærmere her, da de vigtigste punkter nogenlunde er indeholdt i DS 484.

5.2.4.2 Faktor der kan udledes

Den faktor der kan udledes her, er de forskellige nedskrevne krav, der bliver stillet til et autorisationskoncept. Kravene kan både være eksterne og interne, hvor de eksterne krav, f.eks. lovgivning, er uden for virksomhedens direkte indflydelse, kan virksomheden direkte influere de interne krav, f.eks. en virksomheds sikkerhedspolitik. Dermed ikke sagt, at en virksomhed ikke kan påvirke et eksternt krav, f.eks. er der i forbindelse med udarbejdelsen af standarder mulighed for at udføre lobbyarbejde, og omvendt kan en intern faktor være en så indgroet del af virksomheden, at det vil være for omkostningsfuldt at ændre eller påvirke den. Under ét er det valgt at kalde de ovenstående for de foreskrevne krav.

5.2.5 Menneskelige faktorer (Human Factors)

Denne sammenkobling er mellem mennesker og teknologien, og er kritisk i forhold til informationssikkerheden, da det er her de interne trusler som misbrug, tyveri eller læk af data kan opstå, det er derfor vigtigt at træne medarbejderne i relevante færdigheder (ISACA, 2009, s. 17).

5.2.5.1 Menneskelige faktorer i relation til adgangsstyring

Flere har de sidste år gjort opmærksom på, at den største trussel i forhold til informationssikkerheden ikke er om teknikken eller procedurerne er gode nok, men om medarbejderne udfører, bevidste som ubevidste, skadelige handlinger (Desman, 2003; Dhillon & Backhouse, 2000; Ernst & Young, 2008; Kent, 2008; Nosworthy, 2000).
Desman (2003) gør opmærksom på, at da informationssystemer bliver udviklet til mennesker og brugt af mennesker, bør kommunikationen til disse mennesker være det vigtigste punkt indenfor informationssikkerheden (Desman (2003, s.40).

Selv det bedst designede autorisationskoncept vil komme til kort, hvis medarbejderne ingen bevidsthed har om, hvordan deres handlinger influerer informationssikkerheden. For eksempel hvis en medarbejder i bogholderiet lader en salgsassistent bruge hans bruger ID, så er værdien i at udvikle roller på systemerne ved at være forsvindende lille.
Derfor er det vigtigt, at medarbejderne er bevidste om, hvordan de skal reagere, hvis de for eksempel har brug for adgang til et system, eller deres sidemand har brug for adgang. For nogen kan det være en selvfølge at låne sidemandens bruger ID, eller også kopierer sidemanden bare hans egne adgangsrettigheder til den kollega, der har brug for dem. Dette har især været et problem i SAP, da der har været præcedens for, at udviklere har haft tilknyttet brugerprofilen SAP_All, der gav adgang til alt, og dermed har de også haft adgang til rolle- og brugeradministration, hvormed den situation kunne opstå, at en kollega kopierede hans egen adgang til en anden kollega. Hack (2008) beskriver problemet med SAP_All i forhold til batch brugere, men det er samme problemstilling, der også gør sig gældende med alle andre brugere.

Den ovenfor beskrevne situation opstår ofte ikke af ond vilje, men fordi det er den nemmeste, når medarbejderne står i situationen. Ovenstående tilfælde kan løses ved at fjerne SAP_All profilen fra alle medarbejdere, men der vil altid kunne opstå situationer, hvor medarbejdernes handlinger får indflydelse på informationssikkerheden.

5.2.5.2 Faktor der kan udledes

At medarbejdernes bevidsthed om informationssikkerhed, er en af de vigtigste forudsætninger for at undgå et brud på informationssikkerheden, betyder ikke, at et autorisationskoncept ikke har sin berettigelse,

snarere tværtimod, da et sådan vil minimere risikoen for, at medarbejderne kan udføre skadelige handlinger. Dette sker netop ved at sikre, at medarbejderen kun har adgang til det han skal bruge, og på det tidspunkt han skal bruge det for at udføre sit job (Kent, 2008, s.6).
Det ene udelukker altså ikke det andet, men er vigtige suppleringer til hinanden. Og derfor vil et autorisationskoncept kun kunne blive en succes, hvis der bliver støttet op om det, med en kampagne der sikrer, at medarbejderne arbejder og opfører sig forsvarligt i forhold til informationssikkerheden. Dette gælder for alle medarbejdere, det vil sige også for autorisationskonsulenterne og deres arbejde med autorisationskoncepterne.

5.2.6 Arkitektur (Architecture)

Sikkerhedsarkitekturen omfatter de mennesker, processer, politikker og teknologier virksomhedens sikkerhedspraksis består af. Designet af sikkerhedsarkitekturen beskriver, hvordan sikkerhedskontroller placeres, og hvordan de hænger sammen med den overordnede IT arkitektur. Arkitekturen letter sikkerhedsfunktioner på tværs af organisationen, og sikrer en konsistent og omkostningseffektiv måde for virksomheden at være proaktiv med beslutninger vedrørende sikkerhedsinvesteringer (ISACA, 2009, s. 17).

Esch og Junold (2009, s. 23) nævner, at autorisationskonceptet netop skal integreres med den overordnede IT arkitektur, og ikke blive opfattet som et isoleret koncept.
""Enterprise arkitektur" er ikke en ny term, men det er først de senere år at den har vundet indpas bredt. Tidligere var "it arkitektur" brugt, i stort set samme betydning." (OIO, 2009). IT arkitektur kan både være løsnings- og holistisk orienteret, og alt efter hvem man er, kan fokus være vidt forskelligt. Derfor bliver der ofte brugt begreberne Løsnings og Enterprise Arkitektur i stedet. Det falder dog uden for denne afhandlings omfang at gå i dybden med en diskussion om arkitektur, men umiddelbart indeholder arkitekturen alle de andre elementer og dynamiske koblinger, og den bør mere opfattes som en ramme for alle de resterende faktorer i stedet for en sidestillet faktor, og derfor bliver der ikke udledt en særskilt faktor fra denne dynamiske kobling.

5.3 Opsamling af udledte faktorer

Alle elementer og dynamiske koblinger er nu gået igennem for forretningsmodellen for informationssikkerhed, og på den baggrund er der blevet udledt faktorer, der kan påvirke eller have indflydelse på et autorisationskoncept.

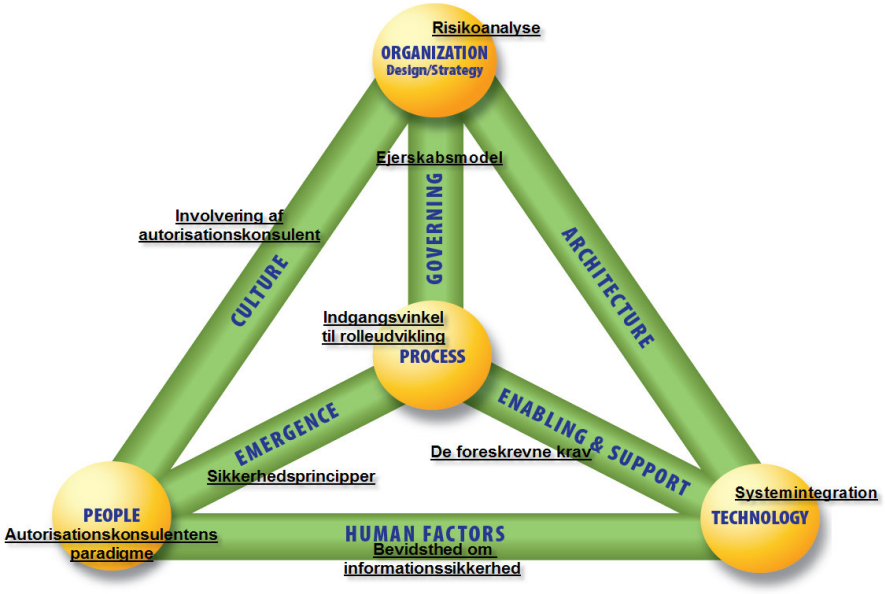
Fra modellens elementer er følgende faktorer identificeret:

- Risikoanalyse (udledt fra Organization, design/strategy)
- Autorisationskonsulentens paradigme (udledt fra People)
- Indgangsvinkel til rolleudvikling (udledt fra Process)
- Systemintegration (udledt fra Technology)

Og fra modellens dynamiske koblinger er følgende faktorer udledt:

- Ejerskabsmodel (udledt fra Governing)
- Involvering af autorisationskonsulent (udledt fra Culture)
- De foreskrevne krav (udledt fra Enabling & Support)
- Sikkerhedsprincipper (udledt fra Emergence)
- Bevidsthed om informationssikkerhed (udledt af Human Factors)

Figur 9: Forretningsmodel for informationssikkerhed med udledte faktorer



Kilde: Egen tilpasning af ISACA, 2009, s. 1

I forhold til de identificerede faktorer, vil der ikke efterfølgende blive skelnet mellem, om de er udledt fra et element eller en dynamisk kobling i modellen. Den vigtigste betydning i forhold til modellen har været at få dem udledt, og derfor er det sekundært, hvor de er kommet fra.

5.3.1 Redundans mellem faktorerne

Der findes også en vis redundans mellem de forskellige faktorer. For eksempel med Ejerskabsmodel og De foreskrevne krav, så går den første ud på, at der skal være et overblik over, hvem der har ansvaret for hvilke informationsaktiver, mens den anden dækker over de krav, der kommer fra for eksempel standarder inden for informationssikkerhed. DS 484 er en sådan standard, og i den, er et af kravene netop, at informationsaktiver skal have tildelt en ejer (DS 484, 2005, s. 32ff). Da Ejerskabsmodel er afhængig af hvordan den enkelte organisation strukturer sig selv, og specifikt kombinerer processer, personer og informationsaktiver, bliver den bibeholdt som selvstændig faktor.

De foreskrevne krav og Sikkerhedsprincipper overlapper også hinanden, da de to sikkerhedsprincipper går igen i både DS 484, SOX og persondataloven, samt ofte er at finde i virksomhedernes sikkerhedspolitiker. Derudover er sikkerhedsprincipperne så anerkendte, at det kan argumenteres for at de burde blive opfattet som krav og ikke bare principper. Derfor har jeg valgt at slå disse to faktorer sammen under navnet De foreskrevne krav og principper.

5.3.2 Faktorernes indbyrdes afhængigheder

Flere af faktorerne har en direkte afhængighed af eller indflydelse på hinanden. Dette er naturligt, set i forhold til, at den model de er blevet udledt fra, er skabt med baggrund i systemtænkning, og dermed netop foreskriver, at et objekt, eller en faktor, ikke kan fungere isoleret.

Et eksempel på deres afhængigheder er for eksempel, hvis vi sammenligner Indgangsvinkel til rolleudvikling og de to sikkerhedsprincipper, der hører til faktoren De foreskrevne krav og principper.
Afhængigt af den indgangsvinkel der vælges til udviklingen af roller, giver det mulighed for at leve op til det mindste privilegiums princip, da roller kan udvikles, så de netop kun kan udføre de ønskede funktioner, hvilket ifølge Nyanchama og Osborn (1994) vil give optimal sikkerhed, da der er sammenhæng mellem hvad der er tilsigtet med en rolle og hvad den reelt kan udføre.
Igen afhængig af hvilken indgangsvinkel der vælges, er der mulighed for at understøtte separation af opgaver. Dette gøres ved at udvikle to roller, der begge er nødvendige for at udføre en opgave, og så sørge for, at den samme person ikke kan blive tildelt begge roller (Omicini et al., 2005, s. 68). På nedenstående tabel, ses hvordan de forskellige indgangsvinkler for rolleudvikling, beskrevet i kapitel 5.1.3.1 lever op til de nævnte sikkerhedsprincipper.

Tabel 2: Oversigt over de forskellige indgangsvinkler i forhold til de to sikkerhedsprincipper

	Adgang til alt	1 person 1 rolle	Forretnings-områder	Jobfunktioner	Eksisterende tilladelser
Mindste privilegium	Nej	Ja	Nej	Ja	Måske
Separation af opgaver	Nej	Ja	Nej	Måske	Måske

5.3.3 Berettigelse for faktoren Autorisationskonsulentens paradigme

Denne faktor arbejder med udtrykket paradigme. Kuhn (1995) udviklede teorien om paradigmer i forbindelse med videnskabens praktisering og udvikling. Derfor kan det diskuteres, om det kan overføres til denne situation, hvor den bruges i forbindelse med, hvordan medarbejderne opfatter arbejdet med autorisationer inden for informationsteknologi i en organisation, og om der er at gå for vidt i forhold til Kuhns oprindelige hensigter med ordet paradigme (Kuhn, 1995).

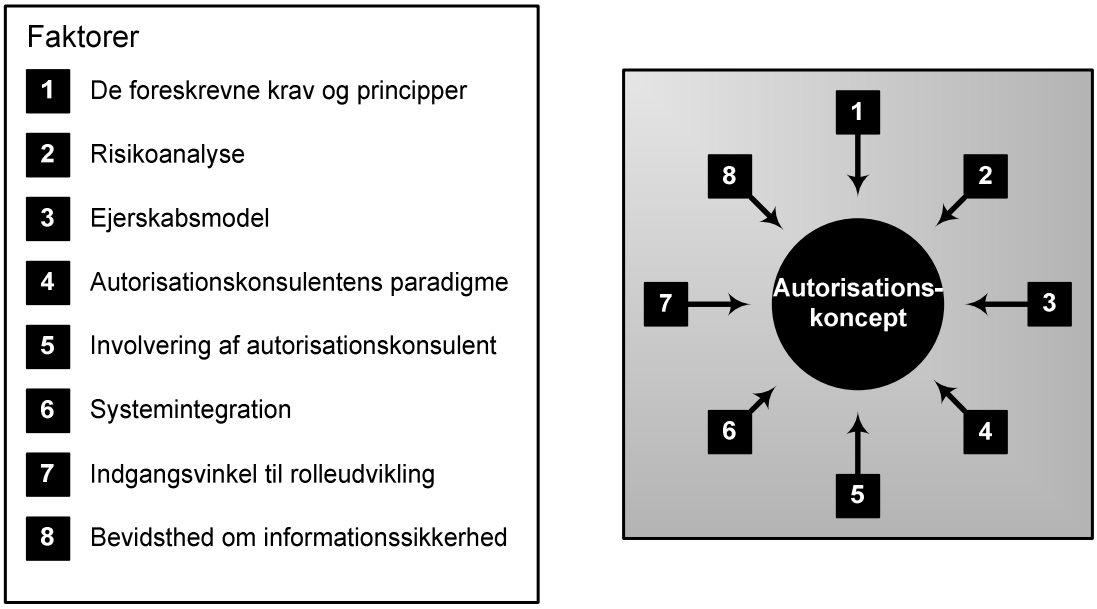
"Some language purists feel that among "business philosophers" and advocates of any type of change whatsoever, the term paradigm is widely abused and in that context bears no meaning whatsoever." (Websters, 2009)

På trods af den ovenfor citerede skepsis, mener jeg godt, jeg kan forsvare brugen af paradigmebegrebet i forhold til autorisationskonsulenternes opfattelse af arbejdet med autorisationer som en ren praktisk genstand, eller om autorisationer i virkeligheden skal gribes an med en holistisk og mere overordnet tilgang. Og i forhold til autorisationskoncepterne er det derfor stadig en relevant faktor at finde ud af, og være bevidst om hvilket paradigme autorisationskonsulenterne befinder sig i.

5.4 Udledte faktorer

Det er tidligere nævnt, at adgangsstyring primært bliver opfattet i forhold til rollebaseret adgangskontrol. Det vil sige, hvilke roller skal findes, og hvordan skal de udvikles. Dette er stadig en essentiel part, men som det er blevet vist, er der mange andre faktorer, der spiller ind i forhold til at udvikle et autorisationskoncept.
Formålet med at forholde sig til litteraturen om adgangsstyring i forhold til Forretningsmodellen for Informationssikkerhed, var at få foretaget en struktureret gennemgang, og netop ved at bruge en model der tager en holistisk indgang til informationssikkerhed, har den hjulpet til med at identificere faktorer, der ikke umiddelbart ellers ville blive identificeret. Dermed bliver det også klart, at nok er en vigtig del af et autorisationskoncept, hvordan roller bliver udviklet, men det er kun en enkelt brik i det puslespil, hvor det gælder om at ligge et autorisationskoncept. På figuren nedenfor ses de udledte faktorer, der påvirker et autorisationskoncept.

Figur 10: Faktorer der påvirker et autorisationskoncept



Kilde: Egen frembringelse

5.5 Modellens anvendelighed

Forretningsmodellen der bliver brugt ovenfor, er både relativ ny og uprøvet, og gør selv opmærksom på, at de næste skridt bliver at arbejde mere i dybden med de enkelte punkter i modellen (ISACA, 2009, s. 19). Alligevel har jeg gjort brug af den, og den har været til gavn, da den har hjulpet til med at få ting frem, der ellers ikke umiddelbart ville komme frem. At den overvejende litteratur centrerer sig om rollebaseret adgangskontrol bliver også synligt, i forhold til, at den faktor der relaterer til dette, Indgangsvinkel til rolleudvikling, også tager mere plads, end de andre faktorer. Der skal dog også gøres opmærksom på, at selvom en mere holistisk tilgang til adgangsstyring er ønskværdig, skal der stadig være styr på de basale principper, og RBAC er nu engang den tilgang, der bruges indtil videre. Formålet med at udlede faktorerne er dog stadig at arbejde hen imod, at der bliver favnet mere bredt, så der også bliver taget højde for andre ting, og det er netop her, de udledte faktorer kan hjælpe.

Det der kan risikeres ved at følge en holistisk model, og ”tvinge” litteraturen til at passe med den er, at der bliver udledt faktorer på et for tyndt, eller en for kunstigt konstrueret baggrund. Hvis det ikke umiddelbart er muligt at udlede en faktor fra f.eks. en dynamisk kobling på baggrund af litteraturen indenfor adgangsstyring, er det så fordi det punkt ikke er relevant i forhold til adgangsstyring? Dette svarer til diskussionen om hønen og ægget, fordi findes der ikke litteratur, fordi det ikke er relevant at vide noget om inden for adgangsstyring, eller vides der ikke noget om det inden for adgangsstyring, fordi det ikke findes i litteraturen. Alt skal

selvfølgelig afbalanceres, men her var formålet netop at forsøge med en holistisk indgangsvinkel til adgangsstyring, og de udledte faktorer der er kommet ud af det, må så efterprøves i forhold til deres anvendelighed og relevans.

I det næste afsnit beskrives hvordan der i KMD har været, og stadig bliver, taget forskellige tilgange til det at udvikle autorisationskoncepter. I det efterfølgende kapitel vil de forskellige tilgange blive analyseret i forhold til de netop udledte faktorer, dermed kan faktorerne blive efterprøvet i forhold til om de eksisterer, og om de er relevante.

6 Case – KMD

6.1 Baggrund om KMD

KMD er med omkring 3000 ansatte og en omsætning på mere end tre milliarder kr. den største danskejede IT virksomhed. KMD leverer primært IT og konsulentydelser til det offentlige marked i Danmark, og står bag en række af danmarkshistoriens største IT projekter, som for eksempel it-kommunalreformen, Nemkonto, Netborger, e-Boks og lønadministration til Københavns Kommune.

KMD har valgt at basere alle sine nye IT løsninger til kommunerne på ERP suiten fra SAP.
Der er omkring 600 personer direkte involveret i udviklingen af løsningerne til kunderne, derudover er et tilsvarende antal involveret i drift og service af disse løsninger.
KMDs udfordring er, at man med valget af SAP som platform for sine fremtidige løsninger, skal integrere alle relevante processer og data. Dette bevirker f.eks., at alle processer som foretager udbetaling, skal bruge den løsning, forretningsområdet for udbetaling stiller til rådighed. Derved bliver flere og flere forretningsprocesser afhængige af hinanden og afhængige af, at de kan tilgås ensartet af kundernes brugere.

Med valget af SAP som platform valgte KMD også at indføre en Enterprise Arkitektur for at strømline og ensarte defineringen af forretningsprocesser og de omkringliggende elementer, der skulle være kernen i de løsninger som KMD implementerede i SAP. Som en del af dette forløb er der blevet udviklet en model kaldet Den Offentlige Forretningsmodel (DOF). Denne model er udviklet af KMD i samarbejde med væsentlige interessenter, og er KMDs bud på, hvordan en arkitektur kan se ud for den offentlige forretning. Den er altså KMDs produktforretnings opfattelse af den del af den offentlige sektor, der ønskes at udvikles produkter til med SAP. Modellen indeholder 31 forskellige opgaveområder med sammenlagt 103 tilknyttede opgaver. Hver af disse opgaver har defineret en række forretningselementer f.eks. forretningsobjekter, forretningshændelser, forretningsprocesser, aktiviteter, aktører, roller, software komponenter og eksterne snitflader. Disse forretningselementer er produktforretningens udgangspunkt til alt udvikling til KMDs SAP baserede løsninger.

6.2 KMD og autorisationskoncepter

I forbindelse med udviklingen af autorisationskoncepter har Den Offentlige Forretningsmodel også haft stor betydning, og da der har fundet en overordnet strukturering og koordinering sted, af de løsninger der bliver solgt til kommunerne, har der også været interesse for og blevet gjort en indsat for at strukturere hvordan adgangsstyring, og mere specifikt hvordan autorisationer og roller bliver koordineret på tværs af de forskellige løsninger, der bliver, og allerede er, solgt til kommunerne. Der har været gjort et forsøg på, ved

hjælp af den allerede definerede offentlige forretningsmodel, at skabe et generisk autorisationskoncept, der skulle fungere på tværs af forretningsområder og kommuner. Dette var dog ikke vellykket, eller i hvert fald blev forsøget droppet igen, da det skulle udrulles til den første kommune, og i stedet blev et mere individuelt autorisationskoncept taget i brug.

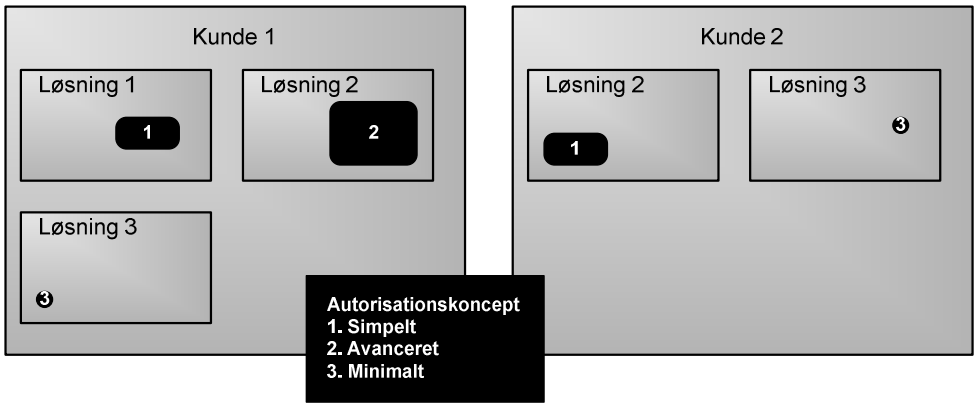
I det følgende er casen delt op i forhold til tre forskellige tilgange, hvor den første tilgang beskriver situationen, hvor hvert forretningsområde havde deres eget autorisationskoncept, og der ikke var nogen sammenhæng forretningsområderne imellem i forhold til autorisationskoncepter. Dette foregår, for så vidt stadigvæk, men ved slutningen af 2007, bliver det besluttet at prøve at strømline autorisationskoncepterne og dermed skabe et generisk autorisationskoncept på tværs af forretningsområderne, dette er den anden tilgang. Den tredje tilgang beskriver en mere individuel tilgang til autorisationskoncepterne, der blev besluttet i 2009 i stedet for den generiske tilgang. Den individuelle tilgang blev besluttet, da der manglede en tro på, at det generiske koncept kunne lade sig gøre i praksis.

6.2.1 Den fragmenterede tilgang

Produktforretningen i KMD var tidligere opdelt i forretningsområder, for eksempel løn, HR og økonomi, der hver især udviklede deres egne produkter, og også definerede deres egne autorisationskoncepter.

Dette gav flere og flere udfordringer, da antallet af løsninger hele tiden udvidedes, og derved forøgedes afhængigheden på tværs af forretningsprocesserne. Dette gav specielt udfordringer, når de enkelte forretningsområders autorisationskoncepter var forskellige i opbygningen, da det derved var forskelligt, hvordan rollerne var defineret, så som indhold, størrelse osv.. Desuden har udrulningen af autorisationskoncepter også været ad hoc baserede hvilket betød, at der ikke var en ensartet tilgang til, hvordan autorisationskoncepterne skulle defineres, hvilket igen ville sige, at hver kunde for hver løsning havde et forskelligt autorisationskoncept. Disse løsninger var også forskellige, alt efter hvor modne de forskellige forretningsområder var, det vil sige, at for økonomiområdet kunne en kunde få udleveret et excel ark over hvilke overordnede roller der burde eksistere, men det var op til kunden selv at finde ud af hvad der skulle fyldes på disse roller, hvorimod på HR området kunne kunderne få en oversigt over roller, og hjælp til at få udviklet de nødvendige roller.
Der var roller, der gik igen imellem kunderne, men der fandtes ikke noget overblik over hvor de passede, og hvor autorisationskoncepterne var forskellige.

Figur 11: Fragmenteret autorisationskoncept



Kilde: Egen frembringelse

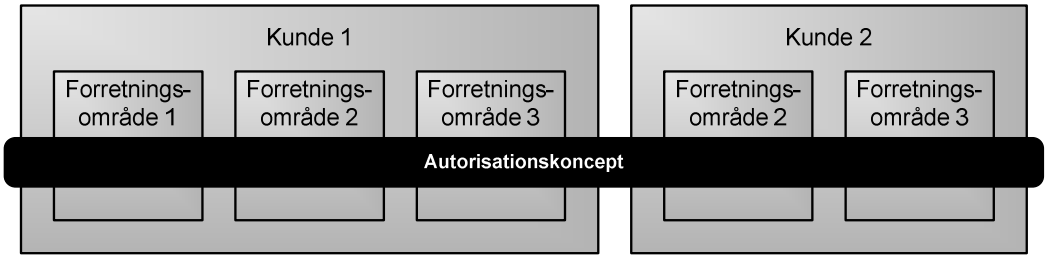
6.2.2 Den generiske tilgang

I forbindelse med forretningsområdet for sikkerhed skulle lancere et nyt Identity Management produkt, blev det valgt, også at ensrette defineringen af roller, ved at kortlægge og forbinde de eksisterende tekniske roller, som fandtes i de forskellige SAP systemer, med forretningsroller som var defineret i Enterprise arkitekturen. Dette blev valgt, da man med Identity management systemet fik mulighed for at kunne tildele disse forretningsroller til brugerne. Forretningsrollerne svarer til en jobfunktion. Måden denne tilpasning mellem tekniske roller og forretningsroller blev gjort på, var over flere workshops, hvor der var repræsentanter fra forretningsområderne samt autorisationsfolk.

Ved hjælp af denne tilpasning blev der skabt et generisk autorisationskoncept, der skulle være udgangspunktet i alle fremtidige udrulninger af løsninger til kunderne. Målet var, at 90 % af indholdet i autorisationskoncepterne imellem kunderne skulle være ens. Begrundelserne for det generiske autorisationskoncept var flere, men de primære var:

- Stordrift ved udrulninger af nye løsninger til kunderne
- Stordrift ved vedligehold af roller
- Overblik over hvilke roller der er i brug hos kunder
- Muliggøre implementering af nye produkter indenfor risikostyring af adgange

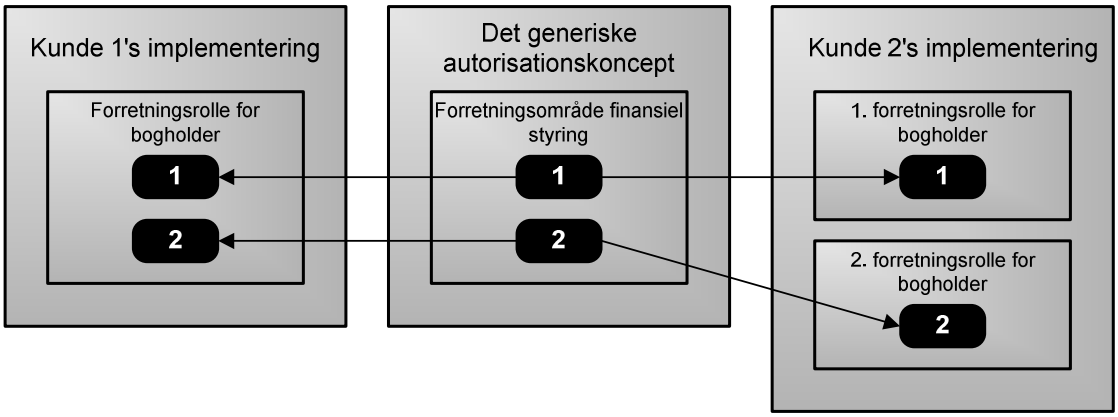
Figur 12: Det generiske autorisationskoncept



Kilde: Egen frembringelse

Så selve ideen med det generiske koncept var at få defineret nogle "byggesten", der ville gøre det intuitivt, når roller skulle implementeres hos kunderne. Disse "byggesten" skulle defineres tilpas småt, til at kunne passe til behovene hos de store kunder. F.eks. vil en mindre kunde, måske kun have én bogholderstilling, hvor en større kunde kan have delt nogle af opgaverne op, og dermed have to forskellige bogholderstillinger. Konceptet hjælper til med, at den lille kommune kan samle de to bogholder-byggesten i én rolle, hvor den store kunde kan oprette 2 forskellige roller, en for hver "byggesten", se evt. nedenstående figur.

Figur 13: Implementering af det generiske autorisationskoncept



Kilde: Egen frembringelse

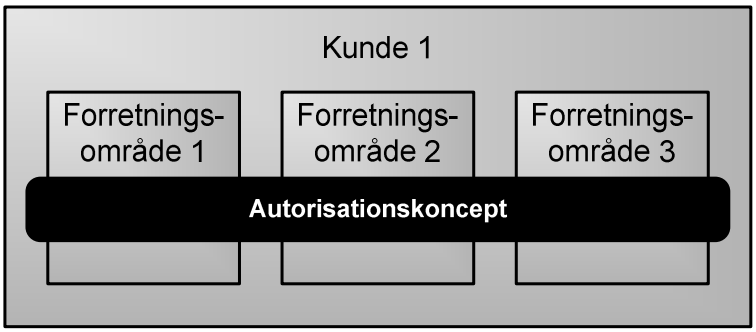
6.2.3 Den individuelle tilgang

Da udrulningen af Identity management systemet skulle ske for den første kunde, blev det generiske autorisationskoncept dog fravalgt, da forretningsområderne ikke følte, at det var fyldestgørende, i forhold til at kunne understøtte individualiserede kunder. Den primære bekymring gik på, at forretningsrollerne som var defineret igennem de afholdte workshops var for brede og, at det derfor var alt for store byggesten, som ville komme til kort, når konceptet skulle rulles ud til store kunder som f.eks. Århus Kommune med 25.000 SAP brugere.

I stedet blev der i samarbejde med den enkelte kunde defineret et individuelt autorisationskoncept på tværs af alle tekniske systemer. Dette blev gjort med en ad hoc baseret tilgang, hvor den enkelte kundes brugere og deres roller på systemerne, blev koblet sammen med nogle stillinger, der blev defineret af kunderne. På denne måde blev der skabt nogle forretningsroller på tværs af de tekniske systemer.

Reelt var man tilbage til den første tilgang og det fragmenterede autorisationskoncept, det vil sige forskellige autorisationskoncepter for hver kunde, dog med en tilføjelse af et ekstra lag, i form af forretningsrollerne, så konceptet dækkede flere af kundens forretningsområder.

Figur 14: Individuelt autorisationskoncept



Kilde: Egen frembringelse

I dette kapitel er der blevet gennemgået de tre forskellige tilgange, KMD har haft foretaget til at udvikle autorisationskoncepter. I det næste kapitel vil der blive identificeret hvordan, og hvor de udledte faktorer fra forrige kapitel er blevet brugt i hver af de forskellige tilgange.

7 Analyse – De udledte faktorer i forhold til KMD

Ud fra gennemgangen af casen i forrige kapitel er det blevet tydeliggjort, at KMD har brugt tre forskellige tilgange til, hvordan de udvikler autorisationskoncepter. I kapitel 5 blev der udledt 8 faktorer, og de vil nu blive gennemgået i forhold til at få belyst hvordan KMD forholder sig til dem i forhold til de forskellige tilgange. Der bliver også brugt eksempler fra ERFA mødet for SAP Sikkerhed og fra de sekundære kilder for at understøtte analysen.
Hvor der er forskel, på den måde en faktor bliver brugt i forhold til de 3 tilgange, vil faktoren blive gennemgået særskilt for hver af de tilgange, ellers vil faktoren blive gennemgået samlet for alle tilgangene. Formålet med at lave denne analyse er at finde ud af, om faktorerne er blevet brugt, og om de har haft nogen relevans. Hver faktor bliver indledt, med en kort repetition af hvad faktoren indebærer. Den første faktor der bliver set på, er De foreskrevne krav og principper.

7.1 De foreskrevne krav og principper

Denne faktor omhandler de nedskrevne og konkrete krav, f.eks. fra DS 484, der findes til et autorisationskoncept.

I forhold til KMDs tre tilgange er der ikke forskel, i forhold til hvordan kravene og sikkerhedsprincipperne bliver håndteret. Derfor vil faktoren blive behandlet under et. En forretningsspecialist formulerer blandt andet følgende:

"Den måde, at autorisationskoncepter og roller blev udviklet på var, at autorisationskonsulenten havde en tidligere erfaring, og den bragte han med ind i projektet. Hvorfor er det, vi laver en opdeling? Vi har ikke regler for det, det er mere noget, vi gør på baggrund af erfaring, f.eks. at den samme person ikke må kunne oprette en leverandør, og så også betale ham."

Kilde: Forretningsspecialist fra KMD

Dette betyder, at der bliver taget højde for de krav der kommer, f.eks. fra standarder eller lovgivning, på en implicit måde. Det vil sige, det er i forhold til, hvad autorisationskonsulenterne allerede kender, og hvordan de mener, det bør være, og ikke fordi disse krav er eksplicitte, inden udviklingen af autorisationskonceptet går i gang. Dette bliver også tydeliggjort af en af mødedeltagerne til ERFA mødet for SAP sikkerhed:

"Så er du tilbage til, at vi fortæller ledelsen, hvordan de skal tænke. Det er jo egentlig ikke meningen med alt det her. Det er jo meningen, at vi skal spørge ledelsen, hvad de havde forestillet sig,"

Kilde: Mødedeltager fra ERFA møde for SAP Sikkerhed

Når kravene ikke er eksplicitte fra starten, kommer der netop sådan en situation som nævnt ovenfor.
De manglende krav kommer også til udtryk i det følgende citat fra en Forretningsspecialist fra KMD, der taler om, at dem der stiller kravene til løsningerne, ikke er bevidst om, hvilke krav de bør stille til de sikkerhedsmæssige aspekter.

"Det overlader han til autorisationskonsulenten at definere, og da autorisationskonsulenten per automatik ikke kender processerne, ved han ikke hvilke regler og love de er underlagt."

Kilde: Forretningsspecialist fra KMD

I forhold til om kravene bliver overholdt, hjælper for eksempel revisionen til. Da det netop er sådanne krav, der ligger til grund, når der foretages en IT revision. Hvis vi tager et kig på en revisionsrapport for Århus Kommune, en af KMDs kunder, så bliver der gjort opmærksom på følgende i forhold til adgangsstyring i SAP:

- *"Det er vores opfattelse, at der er tildelt for brede adgange til for mange brugere i SAP."*
- *"Der er identificeret 86 brugere med SAP_ALL (administratorrettighed), hvilket er et væsentligt større antal, end vi ville forvente i en organisation af Århus Kommunes størrelse. Det er fra kommunen oplyst, at det udelukkende er KMD, som kan tildele og fjerne disse rettigheder."*[5]
- *"Generelt er resultatet, at de faktisk tildelte adgange i SAP ikke understøtter den forventede funktionsadskillelse i forretningsgangene."*
- *"Det er endvidere konstateret, at der ikke er etableret processer inden for eksempelvis tildeling af uforenelige roller, løbende opfølgning og nødprocedurer."*

(Århus Kommune, 2008, s. 9ff)

Som det kan ses af ovenstående punkter, rammer revisionsrapporten plet i forhold til nogle af de centrale problemstillinger. Der tildeles alt for bred adgang til brugerne, og der finder ikke en ordentlig separation af opgaver sted (funktionsadskillelse), der jo netop er et af sikkerhedsprincipperne.
For at kunne overholde de krav, der stilles, er det vigtigt også at have kendskab til dem. Det ses, at de fleste krav og principper er nogen, der eksisterer implicit. Det vil sige, de findes på baggrund af autorisationskonsulenternes tidligere erfaring. Hvilket så igen betyder, at alt efter hvilke individer der deltager i et bestemt projekt, vil autorisationskonceptet blive udviklet efter deres overbevisninger.

"Der er selvfølgelig de overordnede rammer, men ikke noget konkret, så dem der er med i projektet, har en enorm indflydelse i forhold til, hvor meget de synes brugerne skal måtte kunne."

Kilde: Autorisationsassistent fra KMD

[5] Dette er dog ikke korrekt. En SAP_All adgang giver adgang til alt, og dermed vil en bruger med SAP_All netop kunne fjerne disse rettigheder. Men om brugeren, og dermed kunden, er bevidst om dette, og om hvordan, er en anden sag.

7.2 Risikoanalyse

Denne faktor indebærer, at der foretages en analyse af de risici der findes, da dette vil både give input til, hvad autorisationskonceptet bør beskytte, men også en ide om hvor mange ressourcer der skal bruges på at udvikle autorisationskonceptet.

Der var ikke forskel på hvordan denne faktor blev håndteret under de forskellige tilgange, og den bliver derfor gennemgået samlet i forhold.

Der eksisterer en viden om, at det er vigtigt at identificere risici, hvilket ses af nedenstående citat.

"Du skal vide hvad det er vigtigt eller kritisk, så du kan definere dine autorisationer ud fra det. Men så skal du også vide hvad der ikke er kritisk, så du ikke bruger en masse ressourcer på at formindske adgangen til noget alle gerne må have adgang til. Dvs. hvis du ikke ordentligt har defineret hvad der er vigtigt og ikke er vigtigt, ved du ikke om det arbejde du laver giver noget værdi."

Kilde: Forretningsspecialist fra KMD

Men når der blev spurgt konkret ind til, hvordan risici blev analyseret ved de tre forskellige tilgange til udviklingen af autorisationskoncepter, så var der ikke så stor viden om dette.

"Jeg fandt aldrig ud af, om der var en standardiseret måde at gøre det på. Andre steder har man ofte gjort det mere på bagkant, men i KMD har man ikke rigtigt gjort noget."

Kilde: Forretningsspecialist fra KMD

Derudover blev der heller ikke skelnet mellem for eksempel en risikoanalyse og sikkerhedsprincippet separation af opgaver.

"Først og fremmest tænkes der SoD (Segregation of Duties). *Der skulle kunne bindes noget op på noget konkret. Det var SAP kasserne man kiggede på."*

Kilde: Forretningsspecialist fra KMD

Der skete en sammenblanding i forhold til at identificere og evaluere risici (risikoanalyse), og så de måder der efterfølgende kan tages højde for de allerede identificerede risici (separation af opgaver).

Hvis dette er en faktor, der er blevet taget højde for, så har den i hvert fald ikke været eksplicit formuleret.

7.3 Autorisationskonsulentens paradigme

Denne faktor dækker over, hvordan autorisationskonsulenten overordnet opfatter selve arbejdet med autorisationer.

Der blev ikke identificeret et forskelligt paradigme i forhold til de tre tilgange, derfor bliver det behandlet under et i dette afsnit.

Under indsamlingen af empirien blev hver respondent spurgt, hvordan de opfatter et autorisationskoncept, og her var svarene ikke entydige, og afviger en del i abstraktionsniveau, hvilket selvfølgelig også kan hænge sammen med respondentens primære arbejdsområde, hvor IT arkitekten vil fokusere på et højere abstraktionsniveau end autorisationsudvikleren, der vil fokusere mere på det operationelle niveau.

I den første tilgang var autorisationskonsulenterne praktikere, og der blev heller ikke forventet andet. I den næste tilgang, blev der forsøgt arbejdet med en mere generisk tilgang til autorisationskoncepter i forhold til den overordnede rammearkitektur. Den generiske tilgang lykkedes dog ikke, måske netop fordi autorisationskonsulenterne stadig befandt sig i praktikerens paradigme.

For at efterprøve paradigmepåstanden, blev der også spurgt ind til dette i det SAP Sikkerheds ERFA møde, der blev deltaget i, og her blev det konstateret, at der var uenigheder i forhold til hvordan folk opfattede en autorisationskonsulent, både i forhold til hvad der burde kunne forventes af en sådan, og hvilket ansvarsområde han burde have.
Det blev dog synliggjort, at der stadig er en stor del, af dem der arbejder med autorisationer, der ikke har en holistisk indgangsvinkel, men kun fokuserer på det enkelte system og teknikken heri. Da der blev diskuteret i forhold til, om autorisationskonsulenten har en teoretisk tilgang i forhold til hans arbejde, handlede det stadig om, hvad de konkret laver, og om andre kan forstå det. Det vil sige, metodologi blev blandet sammen med dokumentation, hvilket også vises af nedenstående citat fra en af mødedeltagerne:

”Uanset hvad, så er det jo nok meget godt at have en metode, for det er jo det, du så gerne vil have, og uanset om vi har den samme metode, eller hver vores, men en metode der bliver overleveret til kunden, så de forstår, hvorfor ser konceptet ud som det gør, og kan vedligeholde det derefter... Jeg tror, at hvis man kigger lidt på den her håndværker og teoretiker skelnen, så er meget af det vel også, at vi går ud og har noget dokumentation, og en masse metode, men er det forståeligt for andre? Og hvis det kun er forståeligt for os selv, så er vi måske lidt mere håndværkere end teoretikere.”

Kilde: Mødedeltager fra ERFA møde for SAP Sikkerhed

7.4 Involvering af autorisationskonsulent

Denne faktor indebærer, at autorisationskonsulenten skal involveres allerede når processer bliver defineret, og ikke først til sidst eller bagefter.

I forhold til de forskellige tilgange var der forskel på hvordan involveringen fandt sted, og derfor vil de blive gennemgået hver for sig.

7.4.1 Manglende involvering

Ved både den fragmenterede og individuelle tilgang, bliver autorisationskonsulenterne først involveret efter en bestemt løsning er udviklet.

"Rent forståelsesmæssigt at kunne se, at sikkerhed bare er noget, der skal integreres, og er en integreret del af det, man gør, det kræver et vidst modenhedsniveau, ellers er det bare noget, man laver til sidst. Hvilket jo også viser sig her, i sidste ende er det også noget, vi laver til sidst."

Kilde: IT-Arkitekt fra KMD

Den manglende involvering medfører netop den problemstilling, at autorisationskonsulenten ikke har mulighed for at have indflydelse eller ændre på allerede definerede processer, hvilket også bliver eksemplificeret af en af mødedeltagerne fra SAP Sikkerheds ERFA mødet:

"Man skal typisk lave det én gang. Så ringer man til autorisationsmanden, når alle beslutningerne er taget, og så bliver han altså håndværkeren, om han vil det eller ej. Ellers skal personen have meget gennemslagskraft, hvis han skal kunne spole tiden tilbage, og så stille nogen krav til en ledelse som har truffet en beslutning om at implementere SAP."

Kilde: Mødedeltager fra ERFA møde for SAP Sikkerhed

Desuden var det for nogen autorisationskonsulenter opfattelsen, at de selv skulle definere, hvad autorisationerne skulle give adgang til, da ingen andre kunne forstå det. Dette kom også frem under ERFA mødet for SAP Sikkerhed:

"Så du siger, at der er nogen uden for autorisationerne, der gider at beskæftige sig med autorisationer. Det har jeg aldrig hørt før."

Kilde: Mødedeltager fra ERFA møde for SAP Sikkerhed

Derfor kunne autorisationskonsulenten opfinde begrænsninger fordi det er hans opgave, mens disse opfundne begrænsninger reelt ikke svarede til de eksisterende krav.

7.4.2 Øget involvering af autorisationskonsulent

Under udarbejdelsen af det generiske autorisationskoncept, blev autorisationsmanden involveret fra starten, sammen med både forretningsområderne, og de ledere der var ansvarlige. Dette skete i forbindelse med de workshops der blev afholdt.

7.4.3 Opsamling på faktoren Involvering af autorisationskonsulent

Ved at koble alt der har med autorisationer på til sidst, eller efter et udviklingsprojekt er færdigt, bliver der skabt en opfattelse af, at informationssikkerhed er noget, der kan til- eller frakobles, det vil sige, det er en slags knap, vi kan slå til, når vi har brug for at "tænde op" for sikkerheden.

Ulempen ved denne fremgangsmåde er, at informationssikkerhed og i dette tilfælde adgangsstyring og autorisationer bliver opfattet som en ren teknisk disciplin, og når autorisationskonsulenten bliver involveret sent i projektet, er det sværere at få indflydelse og have mulighed for at tilpasse de processer, der allerede er definerede, og dermed bliver de fleste sikkerhedsløsninger skabt på en ad hoc basis.
Under den generiske tilgang sås det, at autorisationskonsulenterne blev involveret tidligt i udviklingen, men alligevel gik det ikke godt med denne tilgang, når det kom til stykket. En af grundene kan være, at selv om alle parter deltog, havde de ikke, eller følte de ikke, de havde mandat til at udtrykke deres ønsker og behov.
Det kan også være, at de stadig var fanget i det gamle paradigme, og derfor ikke var i stand til at forlige sig med et generisk koncept. Det vil sige, der opstår en klar sammenhæng imellem denne faktor, og faktoren der omhandler autorisationskonsulentens paradigme, så hvis ikke autorisationskonsulenten er skiftet væk fra det gamle paradigme, så vil det måske alligevel ikke hjælpe at involvere ham tidligere i processen.

7.5 Ejerskabsmodel

Ejerskabsmodellen går ud på at få identificeret og defineret, hvem der skal være ansvarlig for hvilke roller.

I de tre tilgange sås en forskellighed i forhold til, om der eksisterede, og blev tænkt i ejerskab, så derfor bliver der i det følgende gennemgået, hvordan ejerskabsmodellen så ud for hver af de forskellige tilgange.

7.5.1 Ustrukturerede ejerskabsmodeller

Under den fragmenterede tilgang findes der ikke entydige ejerskabsmodeller. Det er medarbejderens nærmeste leder der godkender de rettigheder, der er brug for, men eftersom lederen altid er interesseret i, at medarbejderen skal kunne udføre sit arbejde, og samtidig forventer, at de rettigheder der bliver efterspurgt, også er nogen, der reelt er behov for, vil lederen altid godkende forespørgslen. Dette hænger også sammen med, at der sjældent er nogen konsekvens, hvis en bruger får for meget adgang, og/eller misbruger de brede rettigheder.
Da den individuelle tilgang gik væk fra at bruge Den Offentlige Forretningsmodel, kunne ejerskabsmodellen herfra heller ikke anvendes længere, og der er indtil nu endnu ikke fastsat en ejerskabsmodel for denne tilgang.

7.5.2 Nedarvet ejerskabsmodel

For den generiske tilgang findes der allerede et ejerskab på de enkelte opgaveområder fra Den Offentlige Forretningsmodel, og derfor bliver dette ejerskab overført, og brugt i forhold til hvilke roller der bliver tilknyttet hvilke opgaveområder.
Dette blev udført på de workshops, hvor forretningsroller og de tekniske roller blev forbundet til hinanden. Der var enkelte generelle roller, der faldt uden for opgaveområderne, f.eks. dem der giver adgang til at logge på systemer osv. og ansvaret for disse roller bliver placeret hos et nyt forretningsområde, der tager sig af basis funktionalitet til KMDs platform af SAP løsninger.

7.5.4 Opsamling på faktoren Ejerskabsmodel

I kapitel 5.2.1.1 bliver det nævnt, at det er bedre at have uddelegeret ejerskabet til de specifikke forretningsområder, da det er her ekspertisen er, i forhold til de ting der ønskes adgang til, i forhold til en leder der ikke har viden om de forskellige sensitive tabeller og transaktionskoder, og dette passer netop med den ejerskabsmodel der blev brugt i den generiske tilgang.

7.6 Systemintegration

Denne faktor hjælper med at give et overblik over hvilke teknologier autorisationskonceptet skal gælde for, så der gives en ensartet adgang til data og funktionalitet på tværs af systemerne.
Da denne faktor blev opfattet forskelligt i de forskellige tilgange, vil de blive behandlet separat nedenfor.

7.6.1 Manglende integration

Under den fragmenterede tilgang bliver systemer ikke tænkt i forhold til hinanden, og der findes ikke en teknologi til at understøtte dette. Det vil sige, der findes ikke et krydstjek af, om de rettigheder der bliver givet på et system, giver mening i forhold til de rettigheder, der bliver givet på et andet, eller som det bliver formuleret af en forretningsspecialist i KMD:

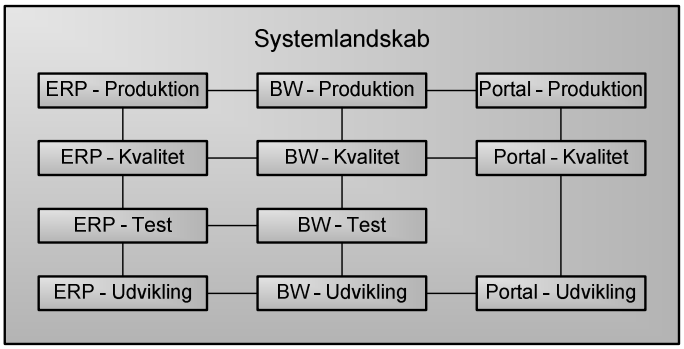
"Det var det, der var lidt mærkeligt med autorisationskoncepterne. På ERP skal man have adgang til nogle omkostningssteder som leder, der svarer til den afdeling, man er leder for, og på BI skal man have adgang til profitcentre, der svarer til den afdeling, man er leder for. Jeg har aldrig hørt om et koncept, der husker at tage højde for det her."

Kilde: Forretningsspecialist fra KMD

7.6.2 Forsøg på integration

Den generiske og den individuelle tilgang forsøger at tage højde for denne faktor, eller der er i hvert fald identificeret hvordan sammenhængene mellem de overordnede forretningsroller passer både med ERP, BW, og Portal systemerne. Systemlandskabet for det generiske koncept ser ud som på figuren ovenfor, men da dette koncept kun dækker kundens brugere, og de kun bruger produktionssystemerne, bliver der ikke taget højde for, hvilken indflydelse den eksisterende systemintegration har på autorisationskonceptet. Det vil sige i forhold til, at integrationen fra udvikling til produktion giver mulighed for uønsket adgang i produktionen for implementeringskonsulenterne, der kun skal have adgang til udviklings- og testsystemer.

Figur 15: Systemlandskab



Kilde: Egen frembringelse med inspiration fra kollegaer fra KMD

I SAP findes der flere forskellige måder at integrere systemerne på, og ofte er de alle sammen i brug, da de har forskellige funktioner. F.eks. transporter der bruges til vedligeholdelse, RFC der muliggør, at brugere kan "hoppe" fra system til system osv.

7.6.3 Opsamling på faktoren Systemintegration

Når autorisationskonceptet skal implementeres, er der brug for en oversigt over hvilke systemer og komponenter der eksisterer. For at kunne skabe dette overbliksbillede, og dermed også kunne gennemskue, hvordan og hvor roller og adgange kan standardiseres, og hvilke grænser autorisationskonceptet skal have, kan det betale sig at lave et visuelt overblik over systemlandskabet.

"Så spiller heterogeniteten af systemlandskabet også en stor rolle. Jo mere komplekst et systemlandskab og jo flere teknologier der er i spil, jo sværere er det konceptuelt at lave noget, der går på tværs."

Kilde: IT-Arkitekt fra KMD

Systemlandskabet i KMD er komplekst og indeholder flere lag, men det har mærkeligt nok vist sig, at der ikke eksisterer et sådant visuelt overbliksbillede over samtlige systemer og komponenter i SAP.

7.7 Indgangsvinkel til rolleudvikling

Denne faktor indebærer, hvordan roller skal udvikles. Da faktoren har været brugt forskelligt under de forskellige tilgange beskrevet i casen, vil den nedenfor blive undersøgt separat for hver tilgang.

7.7.1 Ad hoc rolleudvikling

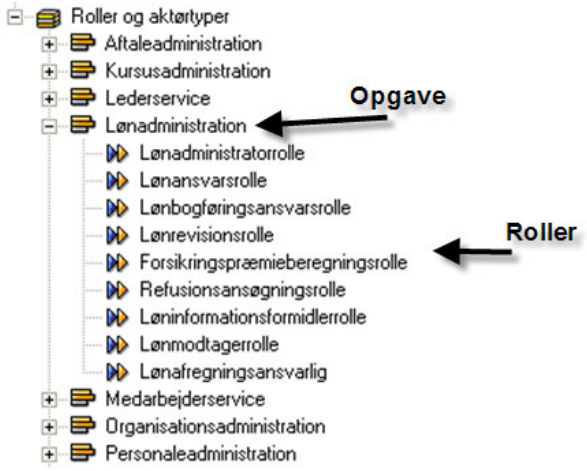
Der er ikke bevidst valgt en indgangsvinkel til, hvordan rollerne skal udvikles, men der er fokus på, at den enkelte bruger skal have adgang til det, han har brug for, og derfor bliver tilladelser givet på en løbende og ad hoc basis, decentralt styret både med hensyn til systemerne og forretningsområderne.
I kapitel 5.1.3.1 bliver beskrevet forskellige indgangsvinkler, og dem der kommer tættest på, er de to yderligheder. Den ene er den, hvor der gives adgang til alt for brugeren. Dette sker, når brugeren får tildelt rollen SAP_All. Den anden grøft, der også blev arbejdet ud fra var, hvor det næsten endte op med, at der blev udviklet én rolle pr. person. Dette skete på grund af de utallige og ustrukturerede ændringer der blev foretaget, og da fokus er på, at der vigtigste er, at brugeren kan udføre opgaven, så hellere give en tilladelse ekstra, hvis brugeren efterspørger det.

7.7.2 Tekniske roller koblet til Den Offentlige Forretningsmodel

Ved den generiske tilgang, blev der valgt en kombination af roller defineret for jobfunktioner og eksisterende roller i systemerne, nærmere beskrevet i kapitel 5.1.3.1. Fordelene ved dette er, at det bliver intuitivt, hvordan roller skal fordeles til medarbejderne.
Måden det blev gjort på, var ved at forbinde eksisterende systemtekniske roller med overordnede forretningsroller, der var udledt fra Den Offentlige Forretningsmodel.

For at vise et eksempel på hvordan dette fandt sted, er der valgt en enkelt opgave fra Den Offentlige Forretningsmodel, nemlig opgaven Lønadministration der hører under opgaveområdet Løn og Personale. Lønadministration er blot én af tolv opgaver, der hører under Løn og Personale, f.eks. er Rekruttering, Personaleudvikling og Personaleadministration også opgaver inden for dette område.
I opgaven Lønadministration er der defineret 9 forretningsroller, se figuren nedenfor. En forretningsrolle dækker over en gruppe af medarbejdere, der kan udføre bestemte aktiviteter.

Figur 16: Forretningsroller under opgaven Lønadministration



Kilde: Udsnit af skærmdump fra SAP Solution Composer i KMD med egen tilføjelse af pile

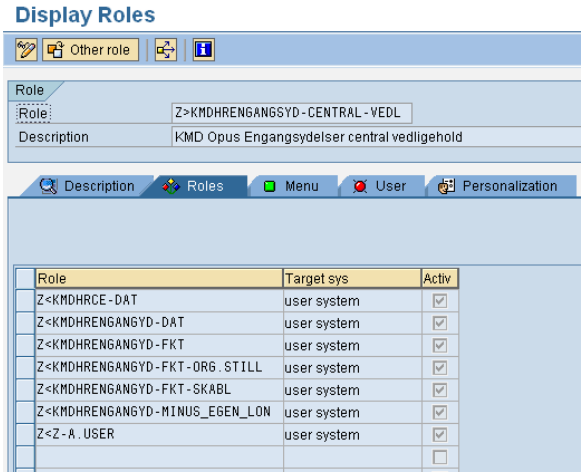
Hver af disse forretningsroller bliver forbundet, til de roller der findes på de forskellige systemer, så hvis der zoomes ind, og denne gang kigges på Lønadministratorrollen, så blev det besluttet på de workshops, der blev holdt, at den skulle forbindes til de 4 følgende tekniske samleroller:[6]

- Z>KMDHRANS-MAXI_(ROLLE_1)
- Z>KMDHRANS-UDMOENT-VEDL
- Z>KMDHRENGANGSYD-CENTRAL-VEDL
- Z>KMDHRENGANGSYD-VEDL

Hver af disse tekniske samleroller består af tekniske enkeltroller, og hvis vi kigger nærmere på Z>KMDHRENGANGSYD-CENTRAL-VEDL, der er en rolle, der giver mulighed for at vedligeholde engangsydelser for medarbejdere, ses det af nedenstående figur, at den igen består af 7 tekniske enkeltroller.

[6] For ikke at gøre eksemplet alt for komplekst, har jeg set bort fra organisatoriske og strukturelle dataafgrænsningsroller.

Figur 17: Samlerollen Z>KMDHRENGANGSYD-CENTRAL-VEDL og dens tilhørende enkeltroller



Kilde: Udsnit af skærmdump fra SAP

Hver af disse enkeltroller giver adgang til nogle transaktionskoder, der igen bliver kontrolleret ved hjælp af nogle autorisationsobjekter, men i dette eksempel gives der slip ved enkeltrollerne, og det var da også på det niveau, at sammenbindingen foregik på de workshops, der forbandt forretningsrollerne med de tekniske roller.
Efter denne øvelse var blevet gjort i forhold til alle forretningsroller for de forskellige opgaver, var der nu lavet en direkte forbindelse fra kommunernes forretning til teknologien.

Af figur 16 ses, at ud over Lønadministratorrollen under opgaven Lønadministration, så findes der roller med så imponerende navne som for eksempel Løninformationsformidlerrolle, Lønbogføringsansvarsrolle, Lønafregningsansvarlig. Det er umiddelbart ikke særligt intuitivt, hvad en medarbejder med Løninformationsformidlerrolle udfører af aktiviteter. Det viste sig da også, da de ovenfor nævnte workshops blev gennemført, at der var forskellige meninger om hvad de forskellige roller indebar, og som det blev formuleret af en forretningsspecialist fra KMD, i forhold til hvad de enkelte roller indeholdt: *"Det var der ligeså mange meninger om, som der var mennesker rundt om bordet."*
Da der var disse uklarheder omkring flere af rollerne, blev det besluttet at splitte dem op eller ændre dem senere. Det er selvfølgelig et problem, at der på den ene side ønskes, at der skal ske en kobling fra de tekniske systemer til forretningen, for netop at gøre det mindre kompliceret og dermed mindske risikoen for fejl, men definitionen af forretningsrollerne på den anden side, så ikke lever op til forventningerne.

7.7.3 Tekniske roller koblet til ad hoc definerede forretningsroller

I den individuelle tilgang blev der valgt den samme kombination af indgangsvinkler som i afsnittet ovenfor, det vil sige en kombination af roller defineret for jobfunktioner og eksisterende roller i systemerne. Dog er den væsentligste forskel her, i forhold til den generiske tilgang, at de forretningsroller de tekniske roller bliver forbundet til, ikke stammer fra Den Offentlige Forretningsmodel, men derimod er nogen, der er specificeret af en autorisationskonsulent fra KMDs konsulentenhed, og ikke udviklingsenheden, i samarbejde med den enkelte kommune.

7.7.4 Opsamling på faktoren Indgangsvinkel til rolleudvikling

Ulemperne ved den tilgang, der bliver brugt under den fragmenterede tilgang, er, at der ikke er stordriftsfordele at hente, da hver bruger bliver individualiseret. Der mistes også hurtigt overblikket over, hvem der har adgang til hvad, og ikke mindst hvorfor de har denne adgang.
Ved den generiske tilgang, er fordelen ved at bruge forretningsrollerne, at ikke bare er de defineret af og for alle forretningsområderne, men de hører også til de overordnede rammearkitekturer, og dermed bliver linket skabt mellem tekniske systemer og forretningsopgaver med dertil hørende processer.
Derudover burde det også være mere intuitivt at identificere, hvilke roller der hører til hvad. Hvor de tekniske roller hurtigt bliver komplekse og svære at gennemskue, er forretningsrollerne anderledes intuitive. Eller det burde de i hvert fald være. Desuden kunne man også bruge den allerede definerede ejerskabsmodel til også at omhandle de tekniske roller.

Ud over de allerede beskrevne problemstillinger kan der påpeges en fundamental fejl ved den valgte fremgangsmåde, der blev brugt til at udvikle rollerne, og denne fejl vil kunne underminere hele ideen om et generisk koncept. Den sammenkobling der bliver gjort, hvor forretningsroller bliver forbundet med eksisterende tekniske roller, er i og for sig fin nok, men som det netop bliver påpeget under gennemgangen af den fragmenterede tilgang, så er der tidligere fundet en ad hoc tilgang sted ved udviklingen og vedligeholdelsen af disse tekniske roller. Derudover indeholder hver rolle op til flere autorisationsobjekter, der ikke er blevet kortlagt i den ovenstående proces. Det vil sige, reelt er det bare nogle sorte bokse, der er blevet koblet sammen, uden bevidsthed om indholdet, bortset fra navnene uden på boksene. Der har selvfølgelig været involveret autorisationskonsulenter i de forskellige workshops, og de må formodes at have kendskab til indholdet i, i hvert fald en del af, de tekniske roller. Men eftersom de tekniske roller ikke er blevet udviklet efter en klar og stringent fremgangsmåde, betyder det, at der er en stor risiko for, at de byggeklodser der er brugt i forhåbning om at skabe et solidt fundament er, om ikke fordærvede, så i det mindste møre i kanterne.

Dermed ikke sagt, at det ikke kan gøres på denne måde, da man jo også bliver nødt til at starte et eller andet sted, og det måske ville kræve for mange ressourcer i forhold til udbyttet at foretage en fuldstændig udrensning af roller og begynde helt fra bunden med at genopbygge det hele. Problemet her er dog, at der ikke er taget højde for det, hvilket betyder, at der bliver udrullet et koncept, der måske, måske ikke, vil fungere efter hensigten.

7.8 Bevidsthed om informationssikkerhed

Denne faktor handler om medarbejdernes bevidsthed i forhold til informationssikkerhed, det vil sige om de arbejder, og opfører sig forsvarligt i forhold til den.

I forhold til de tre tilgange fra casen, kunne denne faktor ikke differentieres, og der var gennemgående den samme holdning til, f.eks. hvordan en adgang kan opnås til et system.

Projektgruppen der skal udvikle det nye autorisationskoncept, har brug for adgange til de systemer autorisationskonceptet skal indeholde, så de har mulighed for at identificere, hvad der allerede eksisterer af brugere og rettigheder på systemerne. Følgende fremgangsmåde blev brugt til dette.
Først identificerer medlemmerne af projektgruppen, hvilke systemer de hver især allerede har adgang til, i kraft af deres arbejde fra tidligere projekter. For hvert system de allerede har adgang til, og hvis deres egen adgang giver mulighed for det, kopierer de deres egne adgangsrettigheder til de projektmedlemmer, der endnu ikke har adgang til systemet.
Dernæst er næste skridt nu at finde de kollegaer i nærheden, der har adgang til de systemer, der endnu ikke er opnået adgang til og gentage samme fremgangsmåde som ovenfor.
Først til sidst og i forbindelse med de systemer der endnu ikke er givet adgang til, bliver der identificeret, hvordan denne adgang kunne erhverves gennem de officielle procedurer og eksisterende autorisationskoncepter.[7]

I forbindelse med udviklingen af autorisationskoncepterne er der ikke fokus på at øge bevidstheden om adfærd og informationssikkerhed, men KMD har derimod på et overordnet plan valgt at sætte fokus på dette område, hvilket kan ses af følgende uddrag fra KMDs årsrapport for 2008:

"KMD forvalter store mængder både administrative og personfølsomme data for vores kunder. Sikkerhed har på den baggrund altid stået højt på dagsordenen i KMD, og for at sætte yderligere fokus på området afsluttede vi året med en intern kampagne, som skulle sikre øget fokus blandt medarbejderne på de sikkerhedsmæssige aspekter i forhold til det daglige arbejde."

(KMD Årsrapport, 2008, s. 17)

Vi har så stadig til gode at se de positive følger af dette inden for udviklingen af autorisationskoncepter.

Et af formålene med et autorisationskoncept er at styre den måde, hvorpå der bliver givet adgange til virksomhedens informationer og systemer. Derfor er det tankevækkende, at de involverede personer i et

[7] Denne fremgangsmåde var især udbredt under et andet projekt, der gik ud på, at udvikle et internt autorisationskoncept

projekt hvor formålet netop er at udvikle et autorisationskoncept, ikke følger de allerede eksisterende procedurer for dette. Et af argumenterne er ofte, at formålet med det nye autorisationskoncept jo netop er at forhindre, at personer kan gøre disse handlinger, men man kan alligevel undre sig over om det, at man er i gang med at forny en procedure, er grund nok til ikke at ville overholde de eksisterende.

7.9 Faktorerne AS IS

I de foregående afsnit er de 8 udledte faktorer blevet analyseret, for at finde ud af hvordan de bliver brugt af de tre tilgange, der findes til at udvikle autorisationskoncepter i KMD. I dette afsnit vil faktorerne blive sammenholdt for at give et overordnet AS IS billede af, hvordan de bliver brugt.

I tabellen nedenfor ses, en opsamling af faktorerne i forhold til hvordan de blev brugt for hver af de tre tilgange.

Tabel 3: Sammenligning af faktorer og tilgange

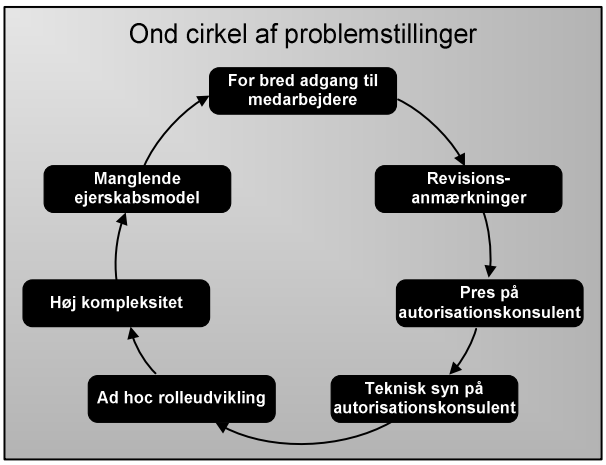
Tilgange / **Faktorer**	**Den fragmenterede tilgang**	**Den generiske tilgang**	**Den individuelle tilgang**
De foreskrevne krav og principper	Implicit kendskab	Implicit kendskab	Implicit kendskab
Risikoanalyse	*Ikke taget højde for*	*Ikke taget højde for*	*Ikke taget højde for*
Ejerskabsmodel	Ikke struktureret	Struktureret	Ikke struktureret
Autorisationskonsulentens paradigme	Praktikerens	Praktikerens	Praktikerens
Involvering af autorisationskonsulent	Til sidst	Fra starten	Til sidst
Systemintegration	*Ikke taget højde for*	Delvis integration	Delvis integration
Indgangsvinkel til rolleudvikling	Ad hoc	Jobfunktioner fra rammearkitektur	Selvopfundne jobfunktioner
Bevidsthed om informationssikkerhed	*Ikke taget højde for*	*Ikke taget højde for*	*Ikke taget højde for*

Det ses, at under alle tilgangene findes der faktorer, der ikke er taget højde for, og de to faktorer Risikoanalyse og Bevidsthed om informationssikkerhed, er der ikke taget højde for i nogen af tilgangene.
Der er blevet identificeret flere problemstillinger, ved den måde de udledte faktorer bliver brugt på. Det ses også, at faktorerne påvirker hinanden indbyrdes, og dermed har de problemstillinger, der er tilknyttet dem også direkte eller indirekte indflydelse på hinanden. I forhold til systemtænkningen, der er beskrevet i indledningen til kapitel 5, hvor en årsag også samtidig kan blive en virkning, kan følgende sammenhæng sættes op mellem de identificerede problemer.

Der bliver tildelt for brede adgangsrettigheder til medarbejderne, hvilket giver revisionsanmærkninger, hvilket så giver et øget pres på autorisationskonsulenterne for at få afklaret problemet, hvilket så medfører et teknisk syn på autorisationskonsulenten i forhold til at han skal trykke på de rigtige knapper for at løse problemet, hvilket medfører, at der bliver udført brandslukning i forhold til at kontrollere adgange, så roller bliver ændret på en ad hoc og ustruktureret måde, hvilket medfører, at det bliver komplekst og uoverskueligt, hvilket igen medfører, at det er svært at finde ud af, hvem der er ansvarlig, og hvad de er ansvarlige for, hvilket til sidst igen medfører, at roller alt for let bliver givet til medarbejdere, og dermed er vi tilbage hvor vi startede.

Nedenstående figur opsummerer denne onde cirkel af problemstillinger.

Figur 18: Ond cirkel af problemstillinger



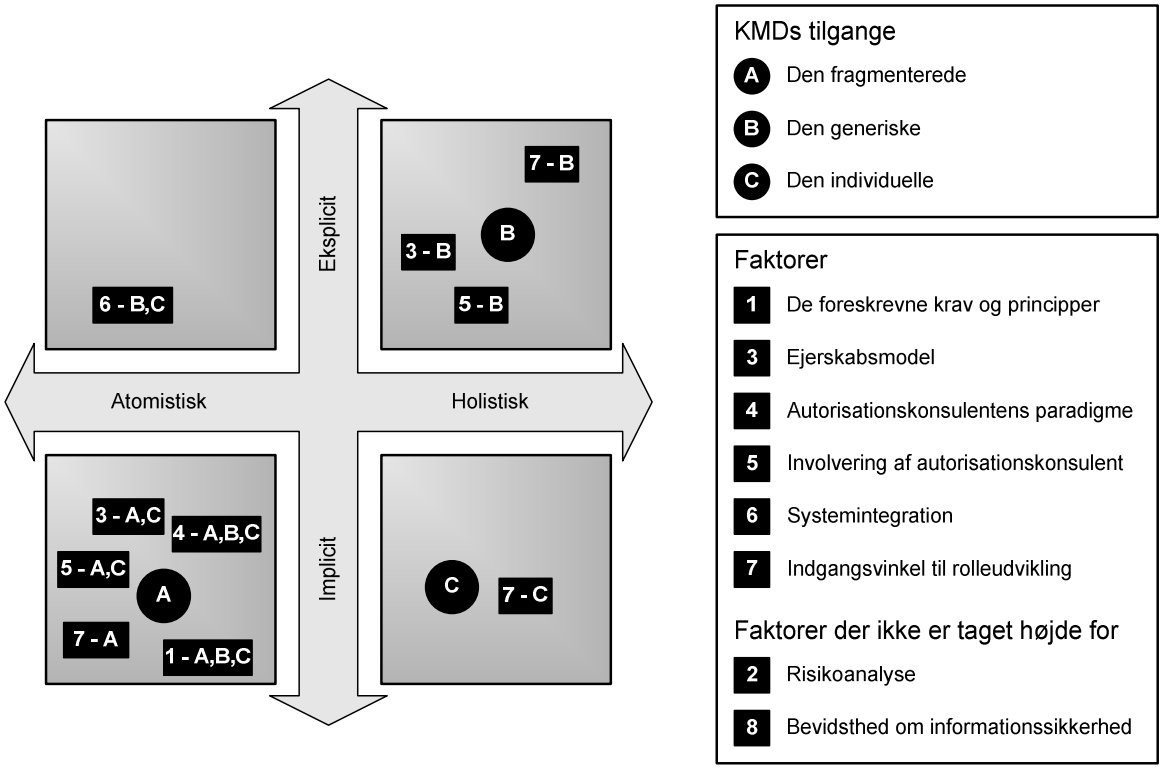
Kilde: Egen frembringelse

Det har vist sig, at den måde faktorerne er blevet brugt, og de problemstillinger det har medført, ligger sig op af en klassisk problemstilling i forhold til teknologi og forretning, netop hvordan samspillet og sammenhængen er mellem disse to. En anden gennemgående tendens har været, at flere af dem har været brugt, hvis ikke ubevidst, så på en tilfældig og ustruktureret måde.

På baggrund af disse to forhold kan faktorerne, og dermed tilgangene KMD har taget til at udvikle autorisationskoncepter fordeles i forhold til følgende to dimensioner: Atomistisk overfor Holistisk og Implicit overfor Eksplicit.
Atomistisk overfor Holistisk afhænger af hvilket startpunkt, man tager afsæt i. Hvor der med Atomistisk menes, at der tages afsæt i de enkelte dele (atomer), i dette tilfælde ofte den enkelte teknologi på det enkelte system, og først derefter sættes de sammen, til en helhed der kan opfattes (Den Store Danske, 2009). Hvor Holistisk betyder, om der bliver taget en overordnet tilgang, her i forhold til om der tænkes sammenhæng mellem forretning og teknologi.
Implicit overfor Eksplicit dækker over hvilken indfaldsvinkel, der tages til tingene, dvs. er det på en ad hoc basis, og er det bare noget, vi gør, fordi vi ved det plejer at være sådan, eller er vores handlinger gennemsigtige og utvetydige.

På nedenstående figur er faktorerne og KMDs tilgange indsat i forhold til, hvordan de passer med disse to dimensioner. Som nævnt ovenfor er der to faktorer, der slet ikke er taget højde for, så de er ikke plottet ind på figuren. Da faktorerne er brugt forskelligt i de forskellige tilgange, er de indsat sammen med det bogstav, der passer med den tilgang, de er blevet brugt i.

Figur 19: AS IS – Faktorer og de nuværende tilgange



Kilde: Egen frembringelse med inspiration fra kollegaer fra KMD

Af ovenstående figur ses det, at den første og fragmenterede tilgang til autorisationskoncepterne befinder sig overvejende under Atomistisk og Implicit, hvilket blandt andet skyldes den indgangsvinkel, der var valgt til rolleudvikling, den manglende involvering af autorisationskonsulenten under processen, samt de krav der blev stillet, fandtes implicit hos autorisationskonsulenterne.
Derimod befinder den generiske tilgang sig under Holistisk og Eksplicit, da der her blev gjort et forsøg på at koble de tekniske dele på den arkitektur, der var defineret for forretningen, og autorisationskonsulenterne blev indblandet under udarbejdelsen af konceptet.
Den individuelle tilgang befinder sig under Holistisk og Implicit, da den godt nok også tager udgangspunkt i at koble tekniske dele sammen med forretningen, dog er det til lejligheden opfundne roller, og dermed ryger den ned under Implicit, da der ikke er en struktureret eller gennemsigtig måde disse roller er fremkommet på.
Der var ingen af tilgangene der passede i forhold til Atomistisk og Eksplicit. En sådan tilgang kunne for eksempel være de af SAP definerede autorisationskoncepter, hvor de tydeliggør hvordan roller og autorisationsobjekter kan sættes sammen, men hele fokus ligger på det teknologiske plan på de enkelte delsystemer.

Det er nu blevet klarlagt hvordan faktorerne bliver brugt, og hvilken indflydelse de har, men i det næste kapitel, vil der fokuseres på, hvordan der bør blive arbejdet med disse faktorer ved fremtidige projekter.

8 Diskussion – Faktorerne TO BE

Den traditionelle opfattelse af adgangsstyring har haft et teknisk fokus omkring blandt andet optimering af RBAC, men igennem de forrige kapitler er der ved hjælp af en holistisk indgangsvinkel blevet udledt faktorer, der påvirker udviklingen af autorisationskoncepter, og det er blevet påvist, hvordan de konkret bliver brugt, og hvordan de har indflydelse på koncepterne. Det er også kommet frem, at nogen af dem ikke bliver brugt, eller der i hvert fald ikke bliver taget højde for dem. Især for de faktorer, hvor det ikke umiddelbart lod sig gøre at identificere deres brug, men for så vidt også for de andre faktorer, bør der i efterfølgende undersøgelser ske en yderligere validering af dem. Det kan ske af både en kvantitativ og kvalitativ karakter.

Det der har vist sig som et gennemgående træk, i forhold til brugen af faktorerne er, at de er blevet brugt mere eller mindre tilfældigt, og mere eller mindre bevidst. Dette skyldes blandt andet, at der ofte ikke har været overblik over hvilke faktorer, der eksisterede fra starten af, og dermed er de i løbet af udviklingsprocessen dukket op mere eller mindre tilfældigt, og der er derfor også blevet taget højde for dem på en ad hoc basis. Dette har betydet, at der gang på gang er blevet løbet ind i de samme problemstillinger i forhold til autorisationskoncepterne. Derudover har disse problemstillinger så været selvforstærkende i forhold til at påvirke hinanden. Netop denne indbyrdes påvirkning betyder, at det ikke er nok kun at tage højde for enkelte af faktorerne.
Dog skal det huskes, at udviklingen af et autorisationskoncept, stadig er en lille del, af en meget højere enhed, og dermed er det ikke sikkert, at afkastet kan stå mål med indsatsen, hvis der kræves, at samtlige faktorer skal være gjort eksplicitte på forhånd, og alle autorisationskonsulenterne skal have gennemgået et paradigmeskift. I forhold til at komme til forståelsen af hvor mange ressourcer der bør bruges på dette, er det dog tankevækkende, at netop risikoanalysen, der er den faktor, der påvirker i forhold til at identificere om udbyttet vil stå mål med omkostningerne, slet ikke så ud til at eksistere eksplicit under udviklingen af autorisationskoncepterne.
Figur 19 i forrige kapitel, kan umiddelbart blive opfattet normativt, det vil sige, at det bedste sted for faktorerne er at befinde sig under den holistiske og eksplicitte dimension.
At holistisk bliver favoriseret over atomistisk, kan også skyldes den forudfattede mening, denne afhandling allerede indeholder, ekstra forstærket af, at øvelsen der blev gjort, hvormed faktorerne blev udledt, netop skete ved hjælp af en holistisk model. Det vil sige, selve faktorerne har et holistisk ophav.

For Autorisationskonsulentens paradigme kan der argumenteres for, at fordelen ved at autorisationskonsulenterne skifter væk fra at opfatte dem selv som praktikere, ville betyde, at de var mere modtagelige overfor, og ville have større lyst til at tænke i integration og helheden, og dermed anlægge en mere holistisk tilgang til at få skabt rammeværktøjer og metodologier til det at udvikle autorisationskoncepter, og dette ville efterfølgende medføre en struktureret og mere eksplicit udvikling af fremtidige autorisationskoncepter. Måske giver det ikke mening i forhold til alle faktorerne, at en holistisk indgang er

bedre end en atomistisk. Hvis vi kigger på Ejerskabsmodel, er det så også bedst hvis den er holistisk? Måske ville den fungere lige så godt, selvom den havde en mere atomistisk indgang, her er det måske mere vigtigt, at der findes en eksplicit ejerskabsmodel. Svaret på dette kan findes ved at kigge nærmere på de fundamentale spørgsmål, vi bør stille os selv, inden vi går i gang med at designe et autorisationskoncept, og som det har vist sig, at faktorerne hver især kan, eller burde kunne, give svar på. Nedenfor er faktorerne endnu engang opstillet, og denne gang med det spørgsmål de kan give svaret på i parentes.

- De foreskrevne krav og principper *(Hvad bliver der krævet af os?)*
- Risikoanalyse *(Hvad skal beskyttes?)*
- Autorisationskonsulentens paradigme *(Hvordan tænker og opfatter vi?)*
- Involvering af autorisationskonsulent *(Hvordan involverer vi hinanden?)*
- Ejerskabsmodel *(Hvem er ansvarlig?)*
- Systemintegration *(Hvilken teknologi har vi?)*
- Indgangsvinkel til rolleudvikling *(Hvordan skal vi gøre det?)*
- Bevidsthed om informationssikkerhed *(Hvordan opfører vi os?)*

Resultatet af disse spørgsmål vil kunne produceres i forskellige niveauer, hvilket bliver mere tydeligt, hvis vi grupperer faktorerne efter det spørgsmål, de hjælper os med at svare på.

Den første gruppe er dem, hvor svaret er noget håndgribeligt, dvs. hvad, hvem og hvilken. De følgende faktorer svarer på sådanne spørgsmål:

- De foreskrevne krav og principper *(Hvad bliver der krævet af os?)*
- Risikoanalyse *(Hvad skal beskyttes?)*
- Ejerskabsmodel *(Hvem er ansvarlig?)*
- Systemintegration *(Hvilken teknologi har vi?)*

Dette betyder, at svaret på alle de ovenstående spørgsmål, kan være noget konkret, altså et fysisk objekt, som for eksempel, Systemintegration. Svaret på hvilken teknologi vi har, kunne for eksempel være en oversigt over et systemlandskab, hvor der kan ses teknologier og tilhørende komponenter.
Det der har været problemet, med de ovenstående faktorer er, at de har været håndteret implicit eller helt ignoreret. For at sikre, at deres indflydelse er hensigtsmæssig, bliver de derfor nødt til at blive eksplicitte, så der kan undgås de problemer, de tidligere har medført, for eksempel når der bliver implementeret nogle procedurer, der slet ikke er brug for på grund af, at autorisationskonsulenten bruger sin egen erfaring fra tidligere projekter, og kravene kun har eksisteret implicit i projektet. Igen, skal der afvejes hvor mange ressourcer der vil bruges i forhold til at kræve, at de ovenstående faktorer findes eksplicitte i organisationen, da dette vil være et stort ressource- og tidskrævende arbejde.

Nedenfor ses de resterende faktorer, der alle giver svar på et hvordan spørgsmål:

- Autorisationskonsulentens paradigme *(Hvordan tænker og opfatter vi?)*
- Involvering af autorisationskonsulent *(Hvordan involverer vi hinanden?)*
- Indgangsvinkel til rolleudvikling *(Hvordan skal vi gøre det?)*
- Bevidsthed om informationssikkerhed *(Hvordan opfører vi os?)*

Svarene på ovenstående spørgsmål er ikke umiddelbart håndgribelige, da de vedrører, hvordan vi tænker og handler. Derfor kan vi heller ikke umiddelbart give svar på disse spørgsmål ved hjælp af et dokument eller et diagram, da de har med at gøre hvordan vi opfører os, det vil sige, de er mere kulturelt betingede. Der bliver altså nødt til at blive arbejdet med disse faktorer, da det ikke er muligt at udarbejde en model, og så sige, sådan her skal vores bevidsthed om informationssikkerhed se ud. Det vil sige, vi kan godt udforme sådan et dokument, og disse dokumenter findes da også, men det er ikke det samme som, at de bliver efterlevet, hvilket allerede tidligere er blevet påvist i denne afhandling.
De to grupperinger af faktorerne er også med til at give en ide om, hvordan de kan blive valideret af senere undersøgelser, hvor den første gruppe vil kunne valideres af en kvantitativ undersøgelse, da der kan svares målbart på disse spørgsmål, bør den anden gruppe af faktorer undersøges mere kvalitativt.

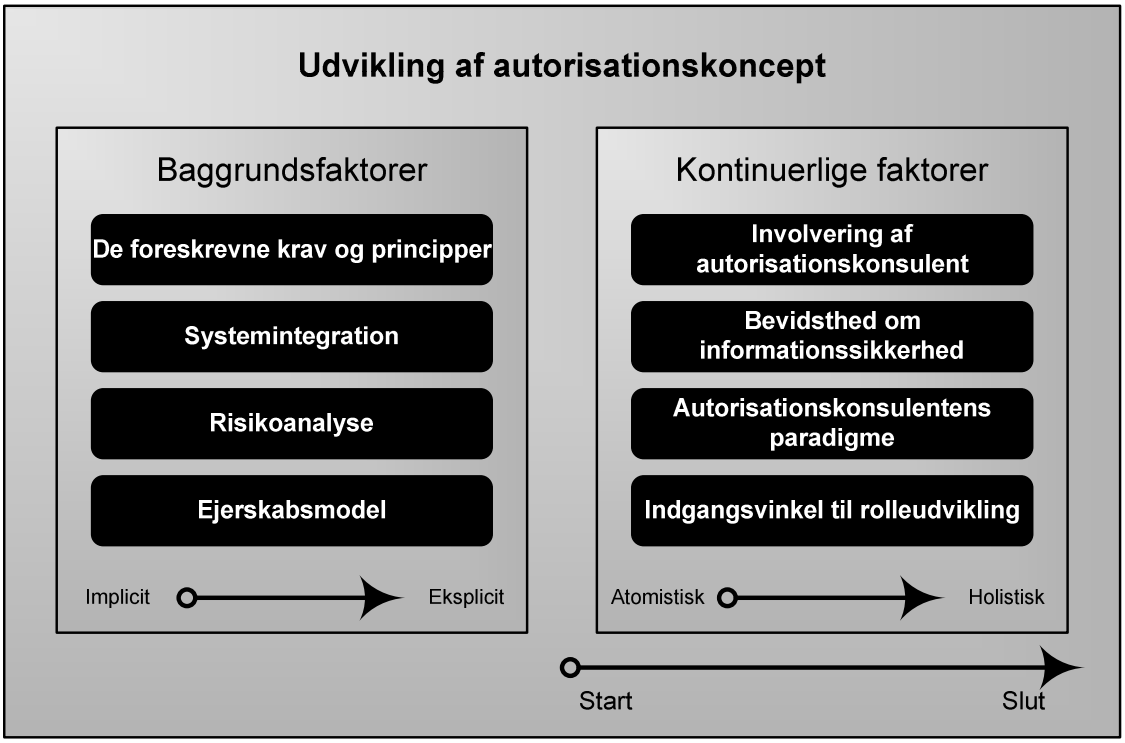
Det viser sig dermed, at ikke bare findes der flere faktorer, der påvirker udviklingen af et autorisationskoncept, men de bliver også nødt til at blive håndteret forskelligt. Der er tidligere nævnt, at der mangler en overordnet struktur for, hvordan at autorisationskoncept bliver udviklet, som også bliver støttet af følgende citat:

"Vi mangler begrebsapparatet, vi mangler metoden eller referencerammen. Der har vi nok kun hver især vores egen, når vi kommer ud."

Kilde: Mødedeltager fra ERFA møde for SAP Sikkerhed

Et af de overordnede problemer har været at der manglede noget struktur, og som et bidrag til dette, har jeg udviklet nedenstående figur til brug for udviklingen af autorisationskoncepter.
Ideen er, at de håndgribelige faktorer, bør være på plads, inden projektet går i gang, da de er selve den platform der ligger til grund for hele konceptet, og derfor har jeg valgt at kalde dem baggrundsfaktorer. Er disse faktorer ikke på plads, er konceptet nyttesløs. Tidligere er det set, at godt nok er der taget højde for disse faktorer, men de har eksisteret implicit. Alt afhængig af hvor mange ressourcer der ønskes sat af til det, bør der arbejdes på, at disse faktorer går fra at være implicitte til eksplicitte.
De resterende faktorer har jeg valgt at kalde de kontinuerlige faktorer, da disse faktorer kan få mulighed for at udvikle sig selv i løbet af projektet, og det er tanken, at de hver især skal gå fra at være på et atomistisk niveau til et mere holistisk niveau.

Figur 20: TO BE – Strukturering af faktorer til udvikling af autorisationskoncepter



Kilde: Egen frembringelse

Ideelt skulle ingen af de ovenstående faktorer udvikle sig i løbet af et projekt, men derimod være på plads fra start, men der hvor vi står i dag, og som der er kommet frem i afhandlingen, ville en simpel bevidsthed og indsats i forhold til bare halvdelen af faktorerne være en stor forbedring.

I kapitel 5.2.6 blev der valgt ikke at udlede sikkerhedsarkitektur som en sidestillet faktor med de andre. Det kunne dog tyde på, at det netop er sådan en overordnet faktor, eller nærmere overordnet rammeværk, der kan være brug for. Dette kan måske være løsningen på at få gjort faktorerne eksplicitte, og få lukket hullet mellem det atomistiske og holistiske. Jeg vil dog lade det være op til en efterfølgende undersøgelse at følge op på sikkerhedsarkitekturen.

9 Konklusion

Litteraturgennemgangen inden for adgangsstyring viste, at en stor del af litteraturen er centreret om tekniske løsninger, og dermed vidner det om, at området stadig er meget fokuseret på at finde tekniske løsninger på de udfordringer der findes, og som ofte har med mennesker at gøre.
Litteraturen viste sig overvejende at handle om effektivisere rollebaseret adgangskontrol (RBAC). Samtidig bliver der, efterhånden, konkluderet overordnet indenfor informationssikkerheden, at problemerne vedrørende dette område ikke kun kan løses ved hjælp af teknik.
Derfor blev en holistisk model brugt til at gennemgå litteraturen, og derigennem blev der udledt følgende 8 faktorer, der påvirker et autorisationskoncept i en organisations ERP systemer:

- De foreskrevne krav og principper
- Risikoanalyse
- Autorisationskonsulentens paradigme
- Involvering af autorisationskonsulent
- Ejerskabsmodel
- Systemintegration
- Indgangsvinkel til rolleudvikling
- Bevidsthed om informationssikkerhed

Ved at undersøge tre forskellige tilgange KMD har taget til udviklingen af autorisationskoncepter, er det kommet frem, at to af faktorerne er blevet brugt identisk på tværs af tilgangene, det er Autorisationskonsulentens paradigme og De foreskrevne krav og principper, fællesnævneren for disse er dog, at de foregår både implicit og med manglende overblik over overordnede sammenhænge.
4 af faktorerne er blevet håndteret forskelligt under de tre tilgange, og det er Involvering af autorisationskonsulent, Ejerskabsmodel, Systemintegration og Indgangsvinkel til rolleudvikling. Dog er disse stadig overordnet, præget af at blive brugt implicit, og med få undtagelser bliver de også brugt uden at tage højde for de overordnede sammenhænge.
De sidste to faktorer og dem der ikke bliver taget højde for under udviklingen, er Risikoanalyse og Bevidsthed om informationssikkerhed.
Netop en risikoanalyse bør være en fundamental del at have på plads, før udviklingen af et autorisationskoncept startes, og det var derfor interessant, at denne ikke umiddelbart kunne identificeres.

Ud fra analysen af faktorerne, er det blevet muligt, at sammenholde dem på to dimensioner i forhold til hvordan de bliver involveret under udviklingen af autorisationskoncepter: en Implicit-Eksplicit dimension, og en Atomistisk-Holistisk dimension. Der er en tendens til at disse dimensioner skal opfattes normativt i forhold

til, at hvis en faktor bliver involveret Holistisk og Eksplicit, er det bedre end hvis en faktor bliver involveret Atomistisk og Implicit.

Det viste sig også, at hver af de 8 faktorer gav svar på følgende fundamentale spørgsmål i forhold til udviklingen af et autorisationskoncept, spørgsmålet står i parentes efter faktoren:

- De foreskrevne krav og principper *(Hvad bliver der krævet af os?)*
- Risikoanalyse *(Hvad skal beskyttes?)*
- Autorisationskonsulentens paradigme *(Hvordan tænker og opfatter vi?)*
- Involvering af autorisationskonsulent *(Hvordan involverer vi hinanden?)*
- Ejerskabsmodel *(Hvem er ansvarlig?)*
- Systemintegration *(Hvilken teknologi har vi?)*
- Indgangsvinkel til rolleudvikling *(Hvordan skal vi gøre det?)*
- Bevidsthed om informationssikkerhed *(Hvordan opfører vi os?)*

Ud fra disse spørgsmål kan faktorerne grupperes efter, om de kan give svar på noget håndgribeligt (hvad/hvem/hvilken spørgsmål), eller om det handler om noget mere uhåndgribeligt i forhold til vores adfærd og overbevisninger (hvordan spørgsmål).

Ved fremtidig udvikling af autorisationskoncepter bør der fokuseres på at få gjort de håndgribelige faktorer eksplicitte, inden projektet går i gang, da de ligger grundstenene til hele formålet med at have sådanne koncepter. Og derefter kan der arbejdes med de uhåndgribelige faktorer løbende gennem projektet for at få dem bevæget fra at være atomistiske til at være holistiske, det vil sige fra at fokusere på de enkelte dele til at fokusere på en overordnet helhed.

10 Perspektivering

I forbindelse med implementeringen af store IT systemer, har fokus ofte været på forandringsledelse i forhold til brugerne af systemerne. I forhold til afhandlingen har det vist sig, at der også bør være fokus på de IT konsulenter der udfører udviklingen og implementeringen, og hvordan de burde opfatte deres opgaver i et mere overordnet forretningsperspektiv.
ERP systemer bliver ofte solgt i forhold til, hvordan de kan håndtere forretningsprocesser, men efterfølgende er implementeringen og driften meget teknisk orienteret. Dette gør sig også gældende inden for SAP, hvor de betydningsfulde SAP konsulenter, benævnes ud fra, hvilke SAP tekniske kompetencer de har, frem for deres forretningsmæssige forståelse indenfor SAP. Dette bevirker, at det ikke kun er autorisationskonsulenten, der skal bevæge sig fra en atomar og teknisk forståelse op til en mere overordnet forståelse, dette gælder også alle de andre IT konsulenter involveret i implementering og driften af ERP systemerne.

Indførelsen af en Enterprise Arkitektur kan være med til at bryde denne barriere, men da Enterprise Arkitektur stadigvæk kun i begrænset omfang bruges af alle områder, og primært kun indenfor delområder og systemer, vil transformationen fra denne til at få en bedre forretningsforståelse tage lang tid.

Denne afhandling har taget udgangspunkt i KMD, der er leverandør til en masse ensartede kunder, men konklusionerne fra denne opgave kan også bruges af andre organisationer, f.eks. i forhold til en koncern med flere forskellige datterselskaber, hvor de enkelte datterselskaber ofte bliver betragtet som kunder for koncernens IT afdeling.
Det er tidligere blevet nævnt, at KMDs SAP projekt er et af Danmarks største, og måske også et af de mest komplekse. Dog kan andre organisationer og deres SAP projekter drage nytte af, at være bevidste om, og strukturere de faktorer der påvirker udviklingen af deres autorisationskoncepter. I mindre SAP projekter, vil alt arbejdet relateret til dette dog ofte foregå blandt de samme 2-3 personer, så derfor kan det være lidt mindre åbenlyst, hvordan faktorerne påvirker, på grund af, at der er så få personer involveret, vil de hver især varetage flere ansvarsområder på samme tid under udviklingen, og derfor kan det være lidt sværere at identificere hvornår og hvad den enkelte faktor påvirker, og netop derfor, er det endnu mere vigtigt at få dem gjort eksplicitte og arbejde med dem struktureret. Dette er ikke kun gældende for SAP men også for arbejdet med adgangsstyring i andre integrerede systemer.

11 Efterskrift

Da jeg startede med denne afhandling, var jeg af den overbevisning, at der ikke fandtes et generisk autorisationskoncept for SAP, der både omfavnede en organisations SAP systemer og brugere i bredden, så vel som i dybden helt ned på transaktions- og autorisationsobjektniveau, og derfor ville jeg skabe et sådant generisk koncept. Jeg startede derfor med en udforskende tilgang, for at finde ud af hvilke problemer der eksisterede i forbindelse med udviklingen af autorisationskoncepter, og for selv at få en forståelse af hvad sådan et koncept indebar. Jeg havde forventet på den baggrund at kunne gå direkte over til at løse problemerne ved at give mit bud på hvordan autorisationskonceptet skulle se ud. Jeg opdagede dog, at der var et misforhold mellem forståelsen af de grundlæggende problemstillinger inden for adgangsstyring, i forhold til de nyligt opdagede skisma gældende for informationssikkerheden generelt, og derfor opstod et behov for at kunne forstå og forklare hvordan disse hang sammen med og influerede på adgangsstyring. Så fokus på afhandlingen blev at få dette på plads først, før næste skridt kan tages mod at udvikle et generisk koncept, der kan tage hånd om organisationens problemstillinger i forhold til adgangsstyring.

Da fokus for området ændrede sig, og der først blev identificeret, hvilke faktorer der påvirkede udviklingen af autorisationskoncepter, for derefter at validere dem i forhold til empirien, blev det klart, at en kvantitativ dataindsamling kunne have været brugt til at understøtte denne validering. Dog kræver en kvantitativ dataindsamling, at det ligger helt klart hvad der søges efter, når dataindsamlingen går i gang, og på trods af en overordnet deduktiv fremgangsmåde er arbejdet med denne afhandling foregået i en løbende iterativ proces mellem teori og empiri. Derfor blev det for sent i processen klart, hvordan en kvantitativ dataindsamling også kunne tilføje værdi. For at kompensere for dette blev der i stedet deltaget i et møde med deltagere fra 14 virksomheder, så det stadig var muligt at få verificeret enkelte af faktorerne i en bredere forsamling, men dog stadig med en kvalitativ, og dermed fortolkende tilgang.

12 Litteraturliste

Artikler og bøger

(Ahn et al., 2002)
Ahn, Gail-Joon, Seung-Phil Hong & Michael E. Shin
Reconstructing a formal security model
Information and Software Technology 44, 2002, s. 649-657

(Andersen, 2008)
Andersen, Ib
Den Skinbarlige Virkelighed
Samfundslitteratur, 4. udgave 2008

(Austin & Darby, 2003)
Austin, Robert D. & Christopher A. R. Darby, 2003
The Myth of Secure Computing
Harvard Business Review, june 2003

(Cheng, 2000)
Cheng, Edward C.
An object-oriented organizational model to support dynamic role-based access control in electronic commerce
Decision Support Systems 29, 2000, 357-369

(Desman, 2003)
Desman, Mark B.
The Ten Commandments of Information Security Awareness Training
Information Systems Security, January/February 2003, s. 39-45

(Dhillon & Backhouse, 2000)
Dhillon, Gurpreet & James Backhouse
Information System Security Management in the New Millennium
Communications of the ACM, vol. 43, no. 7, July 2000, s. 125-128

(DS 484, 2005)
Standard for informationssikkerhed
1. udgave, DS 484:2005
Dansk Standard

(Eigeles, 2006)
Eigeles, Dan
Intelligent authentication, authorization, and administration (I3A)
Information Management & Computer Security, Vol. 14, Nr. 1, 2006, s. 5-23

(Esch & Junold, 2009)
Esch, Martin & Anja Junold
Authorizations in SAP ERP HCM
Galileo Press, 1st edition, 2009

(Ernst & Young, 2008)
Ernst & Young
Global Information Security Survey - 2008
Ernst & Young

(Ferraiolo et al., 2003)
Ferraiolo, David, Richard Kuhn & Ramaswamy Chandramouli
Role-Based Access Control
Artech House, Incorporated, 2003

(Friedman, 1994)
Friedman, Andrew L.
The Information Technology Field: Using Fields and Paradigms for Analyzing Technological Change
Human Relations, Vol. 47, No 4, 1994, s. 367-392

(Gartner, 2007)
Gartner, 2007
Identity and Access Management Technologies Defined, 2008
Gartner

(Goncalves & Poniszewska-Maranda, 2008)
Goncalves, Gilles & Aneta Poniszewska-Maranda

Role engineering: From design to evolution of security schemes
The Journal of Systems and Software 81, 2008, s. 1306-1326

(Gustavsson, 2001)
Gustavsson, Bernt
Vidensfilosofi
Forlaget Klim, 2001

(Hack, 2008)
Hack, Dylan
Address Problem Users for Compliance
GRC Expert Online, 2008

(Hirao, 2004)
Hirao, Joey
The Do's and Don'ts of SAP Security: Strategies for Team Selection, Ownership, and Role Creation
SAPtips Journal, August/September 2004 Vol. 2 Issue 4

(ISACA, 2009)
ISACA
An Introduction to the Business Model for Information Security
ISACA, 2009
www.isaca.org

(Kent, 2008)
Kent, Michelle
Strengthening the weakest link
su53 Solutions White Paper, www.su53.com, 2008

(Knudsen, 1994)
Christian Knudsen
Økonomisk metodologi, Bind 1
Videnskabsteori & Forklaringstyper
Jurist- og Økonomforbundets Forlag, 1994

(Kuhn, 1995)
Kuhn, Thomas
Videnskabelige revolutioner (uddrag), oversat fra amerikansk af Knud Haakonssen, 1995
Kompendium til Informationsvidenskabsteori, for CMD, DØK 2. år, DØK merit
Samfundslitteratur, forår 2005

(Li et al., 2007)
Li, Celia, Cungang Yang & Richard Cheung
Key management for role hierarchy in distributed systems
Journal of Network and Computer Applications 30, 2007, s. 920-936

(Lin & Brown, 2000)
Lin, A. & R. Brown
The application of security policy to role-based access control and the common data security architecture
Computer Communications 23, 2000, s. 1584-1593

(Linkies & Off, 2005)
Linkies, Mario & Frank Off
SAP® Security and Authorizations
SAP Press, 2005

(Little & Best, 2003)
Little, Adam & Peter J. Best
A Framework for separation of duties in an SAP R/3 environment
Managerial Auditing Journal 18/5, 2003, s. 419-430

(Ma & Pearson, 2005)
ISO 17799: "Best Practices" in Information Security Management?
Ma, Qingxiong & J. Michael Pearson
Communications of the Association for Information Systems, Vol. 15, 2005, s. 577-591

(Maurizio et al., 2007)
Maurizio, Amelia, Louis Girolami & Peter Jones
EAI and SOA: factors and methods influencing the integration of multiple ERP systems (in an SAP environment) to comply with the Sarbanes-Oxley Act
Journal of Enterprise Information Management, Vol. 20 No. 1, 2007, s. 14-31

(Mohammed & Dilts, 1994)
Mohammed, Imtiaz & David M. Dilts
Design for dynamic user-role-based security
Computers & Security, vol. 13, 1994, s. 661-671

(Nosworthy, 2000)
Julie D. Nosworthy
Implementing Information Security In The 21st Century — Do You Have the Balancing Factors?
Computers & Security, 19, 2000, s. 337-347

(Nyanchama & Osborn, 1994)
Nyanchama, Matunda & Sylvia Osborn
Access Rights Administration in Role-Based Security Systems
To appear in Database Security VIII: Status & Prospects, August 1994

(Omicini et al., 2005)
Omicini, Andrea, Alessandro Ricci & Mirko Viroli
RBAC for Organisation and Security in an Agent Coordination Infrastructure
Electronic Notes in Theoretical Computer Science 128, 2005, s. 65-85

(Ray et al., 2004)
Ray, Indrakshi, Robert France, Na Li and Geri Georg
An aspect-based approach to modeling access control concern
Information and Software Technology 46, 2004, s. 575–587

(Senge, 2003)
Senge, Peter M.
Den femte disciplin
Forlaget Klim, 2003

(She & Thuraisingham, 2007)
She, Wei & Bhavani Thuraisingham
Security for Enterprise Resource Planning Systems
Information Systems Security, 16:152-163, 2007

(Siponen et al., 2008)
Siponen, Mikko, Robert Willison & Richard Baskerville
Power and Practice in Information Systems Security Research
International Conference on Information Systems (ICIS) 2008 Proceedings, paper 26
Association for Information Systems, 2008

(Vanamali, 2008)
Vanamali, Srinivasan
Role Engineering: The Cornerstone of RBAC
JournalOnline Information System Control Journal, 2008

(Vela et al. 2007)
Vela, F.L. Gutiérrez, J.L. Isla Montes, P. Paderewski Rodríguez, M. Sánchez Román & B. Jiménez Valverde
An architecture for access control management in collaborative enterprise systems based on organization models
Science of Computer Programming 66, 2007, s. 44-59

(Wainer et al., 2007)
Wainer, Jacques, Akhil Kumar & Paulo Barthelmess
DW-RBAC: A formal security model of delegation and revocation in workflow systems
Information Systems 32, 2007, s. 365–384

(Wang et al., 2008)
Wang, Xinyu, Jianling Sun, Xiaohu Yang, Chao Huang & Di Wu
Security Violation Detection for RBAC Based Interoperation in Distributed Environment
IEICE TRANS. INF & SYST, vol. E91-D, nr. 5, may 2008, s. 1447-1456
The Institute of Electronics, Information and Communication Engineers

(Weick, 1976)
Weick, Karl E.
Educational Organizations as Loosely Coupled Systems
Administrative Science Quarterly, vol. 21, March 1976, s. 1-19

(White, 2004)
White, A. Stephen
Introduction to BPMN
White paper, IBM Corporation, 2004
www.bpmn.org

Rapporter og beretninger

(Århus Kommune, 2008)
Århus Kommune
Beretning nr. 9
Beretning om revision af åbningsbalance pr. 1. januar 2007, statusafstemninger og IT-sikkerhed
Ernst & Young, marts 2008

(KMD Årsrapport, 2008)
KMD Årsrapport for 2008
http://aarsrapport2008.kmd.dk

Internetsider

(Datatilsynet, 2009)
Kort om persondataloven
http://www.datatilsynet.dk/offentlig/kort-om-persondataloven/

(Den Store Danske, 2009)
Den Store Danske, Gyldendals åbne Encyklopædi
Definition af atomisme
http://www.denstoredanske.dk/Livsstil,_sport_og_fritid/Filosofi/Oldtidens_filosofi/Atomisme

(DocTech, 2006)
Document Technology Systems ApS (DocTech)
Introduktion til Sarbanes-Oxley Act (SOX), 2006
http://www.doctech.dk/Sarbanes_Oxley_Act.html

(Encarta, 2009)
Encarta
http://encarta.msn.com

(kmd.dk, 2009)
KMD
http://www.kmd.dk

(OIO, 2009)
OIO Enterprise Arkitektur
http://ea.oio.dk/arkitektur-faq

(Websters, 2009)
Definition af paradigme
http://www.websters-online-dictionary.org/pa/paradigm.html

(Zeitgeist, 2008)
Google Zeitgeist, 2008
http://www.google.com/intl/en/press/zeitgeist2008/mind.html

13 Bilag

Interview med konsulent fra Applicon Solutions A/S

Hvad er et autorisationskoncept? Hvad indeholder/omfatter et autorisationskoncept?

Alt og ingenting. Jeg har set autorisationskoncepter i alle udformninger og kompleksitetsniveauer. Nogen projekter har været uden brugeradministration, og andre med.
For mig personligt omfatter et autorisationskoncept alt: design af roller, procedurer omkring udvikling og ændring af roller
Procedure omkring projekter kan enten starte med implementering af SAP og udviklingen af roller, eller det kan være løbende projekter, hvor roller skal ændres
Der skal være et projektkoncept, der senere kan ændres til et driftkoncept, hvor der kan udvikles en guide til brugeradministrationen. Hvis brugeradministrationen skal automatiseres, vil det kræve et helt projekt for sig selv. Det er komplekst at få automatiseret brugeradministration
Udvikling af roller og brugeradministration bliver nødt til at hænge sammen, ellers svarer det til, at den ene hånd gør noget, og den anden hånd gør det modsatte, og derved opnår vi ikke den effekt at få en bedre sikkerhed. Det er lige meget om rollerne er fantastiske, hvis de bliver givet til brugerne tilfældigt, og det er heller ikke godt, hvis der ikke bliver uddelt nogen roller overhovedet

Hvorfor have et autorisationskoncept?

Du bliver nødt til at kunne dokumentere hvad du gør. Det skal afspejle den sikkerhedspolitik eller strategi virksomheden har valgt
For at kunne dokumentere, at man har forsøgt at efterleve sikkerhedsstrategien, er man nødt til at lave et koncept. Der kan komme spørgsmål om, om konceptet skal ændres, hvis sikkerhedsstrategien ændres.
Autorisationskonceptet kan hjælpe til at sikre at forretningen overholder den del af strategien. Autorisationskonceptet skal være en dokumentationscontainer til at bygge bro mellem IT sikkerhedsstrategien, over mod autorisationer og senere over mod forretningerne.

Hvad er de største udfordringer i forbindelse med at implementere og vedligeholde autorisationer?

Der er mange udfordringer, og det er forskelligt fra virksomhed til virksomhed, men for de mindre virksomheder, vil det være at få fokus på, at alle ikke skal have adgang til alt.

For de større virksomheder kan der skulle udvikles tusindvis af roller, og dermed skabes en kæmpe kompleksitet. Hvordan sikrer man sig, at det der er udviklet holder vand?
Derudover mangler der generelt at blive testet på autorisationerne. Har folk rent faktisk fået det de vil have. Det er utroligt svært at få folk til at teste systematisk.
SAP har udviklet standardroller og defineret standardprocesser, og folk mener ikke, at de bliver nødt til at teste det, hvis det er en standard, så de forventer vi kan sætte det op, uden at de behøver at teste det. Dermed bliver der ikke allokeret tid til at teste.
Folk har ikke forstået kompleksitetsniveauet og hvilken indflydelse det har på driften af projektet. De tror man lige kan sætte en administrator på, der kan fikse det, og han skal helst ikke forstyrre de andre. Det gælder om at få ledelsen til at forstå, at enten kan de vælge nul sikkerhed, eller også skal de bruge 1-1,5 million på det. Det er svært for ledelsen at forstå. 3 ud af 4 steder skal dette diskuteres, og hvor der er modstridende opfattelser af, hvad der skal bruges for at lave noget fornuftigt.

Gælder udfordringerne kun for SAP?

Det skal lige siges, at jeg kun har erfaring med SAP, men når jeg møder folk der skifter til SAP fra et andet ERP system, bliver de ofte overraskede over hvad der kræves med hensyn til autorisationer. Min opfattelse er, at SAP kan mere med hensyn til sikkerheden, og ikke bare kan, men kræver mere, og det er vigtigt at notere. Du kan vælge at alle kan alt, eller også kan du lave roller. Du kan ikke bare øge sikkerheden med 10 %. Hvis du har sagt a, skal du sige b. Det kræver at du udvikler roller, tester dem osv.
Du skal forvente 10 % af budgettet skal gå til sikkerhed. For store virksomheder måske en 3-4 %, da der er nogle stordriftsfordele. En rolle tager lige mange ressourcer at udvikle og teste, uafhængigt af om der vil være 3 eller 500 brugere, der vil få den tildelt, så hvis du er en lille virksomhed, koster det det samme at sætte det tekniske fundament op, og dermed bliver det relativt dyrt pr. antal bruger.

Interview med forretningsspecialist fra KMD

Er de seks potentielle risici udpeget af Kommunernes Revision i den IT-revisionsmæssige gennemgang af sikkerheden i SAP ekstern i 2005 stadig gældende?[8] *(Viser listen fra rapporten)*

Alle er stadig gældende, og i forhold til det andet punkt, så er det ikke komplekst, da alle har SAP All.

Hvad er de største udfordringer i forbindelse med at implementere og vedligeholde autorisationer?

Manglende forståelse fra kravstillerens side i forhold til hvad det egentlig er, vedkommende efterspørger. Udfordringen mellem, at en teknisk person skal omsætte teknikken til noget forretningsmæssigt, og omvendt. Det er det største. Hvis du ser på det i et større perspektiv, så er det næste, at der er mange kravstillere på et enkelt system. Dvs. du kan have mange forskellige regler for tildeling. Det manglende koncept og struktur gør, at du ikke kan ensarte definering af autorisationer, så kravstillerne kan stille alle mulige krav, der ikke nødvendigvis passer i det overordnede sikkerhedskoncept.
Derudover er det også en udfordring, at når der sker organisationsændringer medfører det sjældent, eller stort set aldrig, ændringer i autorisationskoncepterne.

Gælder dette kun for SAP?

Jeg har kun arbejdet med SAP, men hvad jeg har hørt fra andre er, at SAPs autorisationssystem er det mest komplekse

Hvad er et autorisationskoncept?

Det er en beskrivelse af hvilken adgang og hvordan du vil give adgang til en bruger af et system eller en afgrænset funktionalitet.
Under dette kommer dokumentationen af hvad rollerne indeholder og hvordan de er udviklet. Autorisationskonceptet bliver tit misforstået med et sikkerhedskoncept. Det er en fejl. Et autorisationskoncept favner jo ikke alt det der har med sikkerhed at gøre. Autorisationskoncepter generelt er ofte projektbaserede,

[8] De seks risici: 1) Utilstrækkelige regler for sikring af ensartet sikkerhedsmæssig systemopsætning, administration og drift. 2). Kompleksiteten i konceptet for systemautorisationer. 3) Manglende forståelse for og kendskab til konceptet med hensyn til adskillelse af opgaver og funktioner. 4) Der tildeles for bred adgang til brugere frem for at tildele adgangsrettigheder i relation til jobindholdet. 5) Utilstrækkelig adskillelse mellem de enkelte SAP-miljøer. 6) Manglende eller utilstrækkelige interne reviews og opfølgninger på sikkerhedsarbejdet og det fastlagte sikkerhedsniveau efter idriftsættelse af systemerne

og projekter er jo ofte defineret efter hvordan projektchefen ser verden. Der findes ikke nogen bøger der indeholder et autorisationskoncept. Derfor indeholder de ofte alt muligt. Dette er også en af præmisserne for dit speciale, at teorien er så sporadisk indenfor autorisationskoncepter.

Kunne det tænkes der findes et overordnet autorisationskoncept, men at KMD ikke er klar over det?

Der findes ikke noget. Vi har haft møder med SAP, og de har ikke selv nogen skabelon for hvordan det skal gribes an. De har en del eksempler, men de ligner ikke hinanden.
Autorisationskonceptet er den mærkelige ting, at i sig selv er de ikke noget, de er bare skaller, men de er relationer til teknologi eller funktionalitet, og det vil sige, at du kan have mange syn på hvordan en autorisation skal bygges op. Du kan have et teknisk syn på hvordan systemet er bygget op, eller et forretningsmæssigt syn i forhold til, at det er sådan her processen er, eller du kan have et organisatorisk syn. Problemet er, at du altid har det tekniske syn på det, i stedet for at have det organisatoriske. Det er det autorisationer lider under. Personer der arbejder med autorisationer er håndværkere der arbejder med meget tekniske ting, som f.eks. hvordan du giver adgang til noget specifikt, men de har ikke et overblik hvordan man ensartet tildeler og vedligeholder autorisationer, fordi de mangler de overordnede retningslinjer. Deres fokus er ad hoc løsninger på dag til dag problemer. De har fokus på at løse det enkelte problem frem for at skabe et ensartet koncept for udvikling og tildeling af roller. Det er ikke nødvendigvis dem der skal udvikle konceptet, men det er de eneste, der arbejder med det.
Du har tre led med organisationen, processen og autorisationerne. Ofte vil der opstå en konflikt mellem processen og autorisationen. En proces er både vist rent forretningsmæssigt, men også defineret i systemet rent teknisk. Hvilket niveau bør udvikling og tildeling af autorisationer ske?
Man har troet, at man bare kunne hyre en mand til at løse et problem og så kunne han gå ud af døren igen.
F.eks. i løbet af en 10 årig periode har du haft 10 forskellige konsulenter der har haft 10 forskellige måder at arbejde på. Der har måske været 3-4 forskellige kravstillere. Det er måske endda lavt sat. Jeg har f.eks. arbejdet med det her i 2,5 år i KMD og jeg har haft 4 chefer.
Vi har en kravstiller der ejer en proces. Han definerer kravene for implementeringen af forretningsprocessen og adgangskoncept. Så har du ham der får ansvaret for at implementere processen, vi kalder ham IT konsulenten. Til sidst har du autorisationskonsulenten, der skal implementere adgangskonceptet.
Hver gang du har nogen, der skal kommunikere med hinanden, er der risiko for fejl og misforståelser, og du mangler nogen folk til at binde tingene sammen, f.eks. at have adgang til at betale løn, betyder, at du skal have adgang til en bestemt transaktionskode, der igen skal sættes op med bestemte værdier. Dette kræver både stor organisatorisk og teknisk indsigt. I Danmark mangler kravstilleren ofte en indsigt i hvilke sikkerhedsmæssige krav han skal stille til sin løsning. Det overlader han til autorisationskonsulenten at definere, og da autorisationskonsulenten per automatik ikke kender processerne, ved han ikke hvilke regler og love de er underlagt.
Et stort problem er, at SAP ikke leverer prædefinerede autorisationskoncepter.
Et endnu større problem er, at SAP ikke kan levere en tegning, over de processer der findes. Måske kan du få dem på et overordnet salgsniveau, men ikke på det tekniske niveau. Det er jo absurd, at du køber en best

practice proces, men rent teknisk kan du ikke se, hvad du laver i den. Jeg kan ikke forstå hvordan SAP er blevet verdens største softwareleverandør, når du ikke kan se standardprocesserne. Det er ok, at lønprocessen er kompliceret, da der findes så mange reguleringer og alle lande har det forskelligt, men f.eks. med brugeradministrationen, så er den jo stort set det samme alle vegne, så det burde ikke være svært. I USA er det lov at alle offentlige organisationer skal have en enterprise arkitektur, så der er nogle helt eksplicitte krav for at de kan dokumentere deres forretningsprocesser.

Hvorfor er et autorisationskoncept vigtigt?

For det første set fra den administrative side er det vigtigt, at folk ved hvad de skal gøre for at tildele autorisationer, og når der kommer krav om hvordan de skal vedligeholdes, skal de kende begrundelserne for hvorfor man giver adgang til en specifik funktionalitet i en rolle, så man ved hvor man skal placere funktionalitet og udvidelser.
Den anden side er brugerne. Ofte er det rent ansvarsmæssigt lederens ansvar, at medarbejderen kun har adgang til det han har brug for, for at udføre sit job, men det sker ofte at medarbejderen siger, at han har brug for dette for at udføre sit job, og så godkender lederen det. Men medarbejderen skal nemt kunne beskrive hvad han skal have adgang til. Problemet i SAP er, at brugeren kender Transaktionskoderne og kan sige han skal have adgang til denne og denne transaktionskode, og det er fint nok, men transaktionskoden kan ligge i flere forskellige roller, og så er det ikke klart hvad brugeren skal have. I stedet for skal autorisationskonceptet bygges op, så det forretningsmæssigt giver mening.
Derudover har revisionen også et krav og IT standarder som DS484 kræver også at medarbejderen kun har adgang til det han har brug for, for at udføre sit arbejde.
Du skal vide hvad det er vigtigt eller kritisk, så du kan definere dine autorisationer ud fra det. Men så skal du også vide hvad der ikke er kritisk, så du ikke bruger en masse ressourcer på at formindske adgangen til noget alle gerne må have adgang til. Dvs. hvis du ikke ordentligt har defineret hvad der er vigtigt og ikke er vigtigt, ved du ikke om det arbejde du laver giver noget værdi.

Har KMD et autorisationskoncept?

Vi har mange forskellige som i mere eller mindre grad er eksplicitte. De er i hvert fald ikke krystalklare, i forhold til, at du både som rolleudvikler forstår dem, og at kravstilleren også forstår dem, og at du fra brugernes side kan forstå hvad du skal have adgang til.
Meget af det er implicit, også fordi det er et underprioriteret område, så der er ikke brugt tid på at dokumentere det, så viden er forsvundet gennem tidens løb, både med udskiftning af medarbejdere og chefer og ved organisatoriske ændringer generelt. Det er heller ikke klart hvem der har ansvaret for hvad. Det er ikke klart hvad kravene er i forhold til autorisationskonceptet. Hvad er det vi prøver at begrænse og udvikle adgang til?

Hvilke faktorer påvirker et autorisationskoncept?

Organisation og processer. Modenhed og forståelse i forhold til sikkerhed. Lovgivning. Ofte brancher eller geografiske lokationer, f.eks. har amerikanske virksomheder større krav til hvordan autorisationskoncepter skal udvikles i forhold til i Danmark, hvor der ikke er de store krav. Problemet med disse krav er dog ofte, at det mere er krav om dokumentation for dokumentationens skyld. Derudover er der det menneskelige. Når der ikke er nogen generel forståelse for autorisationskoncepter, er det også styret af hvem der for øjeblikket er ansvarlig for udførelsen af koncepterne. Manglende teori og metode gør, at det bliver endnu mere præget af hvem der lige netop nu er kravstiller og hvem der implementerer løsningerne

Det er svært umiddelbart at opstille en business case for et autorisationskoncept, det vil sige hvad virksomheden får ud af det, f.eks. når det gælder tab, bedrageri eller ineffektive processer. De ineffektive processer går ud på, at hvis folk har for bred autorisation kan de mere eller mindre udføre processen som de har lyst til, og ikke som den var tiltænkt. Et godt autorisationskoncept skal også hjælpe med at processer er strømlinede. Hvis du har folk der har adgang til alt og går ind og laver noget de ikke er uddannede i, kan det være utrolig dyrt for virksomheden i forhold til fejl og udbedring af fejl. Det er svært at måle dette, og identificere hvem der har skylden for det, og du kan heller ikke ordne det hele med autorisationer. Man har ikke tradition for at måle dette fordi det er en støtteproces. Ofte måler man kun på kerneprocesserne.

Hvilke forudsætninger skal være til stede for at kunne designe et autorisationskoncept?

Man skal kende sin organisation. Man skal kende sine processer. Man skal kende sine sikkerhedsmæssige krav til processerne såsom funktionsadskillelse, kritiske data og kritisk funktionalitet. Man skal kunne finde ud af at omsætte det forretningsmæssige til teknikken. Det er ofte det sidste der halter.

Det her med autorisationer er en klassisk problemstilling mellem at sammenstille forretningen og IT. Meget software kommer fra en teknisk baggrund, dvs. de har et teknisk view på tingene, og får lige pludseligt et forretningsmæssigt view på tingene, men det sker ofte kun med salg og management, men du mangler nogen med en forståelse for at binde det hele sammen. Det store problem her og alle andre steder er, at man tror man kan købe sig til det. Men det kan du ikke, for det det bunder i er at du har nogen interne folk der forstår hvilke processer du har og ejer, og hvordan det skal bindes til teknikken.

Interview med IT-Arkitekt fra KMD

Hvad er de største udfordringer i forbindelse med at implementere og vedligeholde autorisationer?

Det ligger i forhold til hvordan spørgsmålet er stillet. For hver tilgangsvinkel er der specifikke udfordringer. Så når man skal lave autorisationer, så er mit perspektiv at sikre, at det bliver på et fundament der sikrer den rette fordeling af effektivitet og konsistens, dvs. forretningsarkitekturen skal på plads, det er råskelettet, visionen om hvor vi skal hen, og det procesmæssige skal være på plads.
Den største udfordring i mit perspektiv er at få form på et autorisationskoncept så alle kan forstå det

Gælder dette kun for SAP?

Nej, det er et universelt udviklingsparadigme. Men det der er i relation til SAP er, at mange af de SAP kompetencer der er involveret, har deres egen terminologi og deres egen arkitektur, der står over for standardrammearkitekturen. Det i sig selv kan være en udfordring, at man skal få de to verdener, standardrammearkitekturverdenen og SAP verdenen til at blive enige om hvornår man taler om det ene og hvornår man taler om det andet.

Hvad er et autorisationskoncept?

Hovedskitsen i et koncept er, at det er en primær taktisk model for at udvikle noget sammenhængende, og efterhånden som den bliver udviklet bliver den operationel og før den kan blive operationel, skal der tages strategisk stilling til den.
Selve autorisationskonceptet er født som en model for, hvordan autorisationer skal tildeles, og hvilken systematik der er og hvilken metode. Sammenhængen for hvordan autorisationer håndteres i organisationen. Det er ikke nok, at det er en model, det skal også vise noget af vejen.
I forhold til KMD ville det helt overordnet være fantastisk, hvis vi havde et overordnet koncept der øverst oppe var platformsuafhængigt, så de operationelle koncepter stammer fra det samme koncept. Sådan som det er nu, så bliver der lavet flere forskellige autorisationskoncepter. Der bliver lavet noget for udviklingen, noget for produktion, og noget for de enkelte systemer. Der ville det være bedre med en overordnet skabelon, der siger hvordan autorisationskonceptet skal se ud forretningsmæssigt.

Hvorfor er et autorisationskoncept vigtigt?

Internt er det vigtigt, når konceptet er født, at man ved hvad man arbejder hen imod, at man ved hvordan det hænger sammen og skal se ud.

Eksternt er det for at sikre, at der er konsistens i de produkter man leverer, så man kan sikre, at der er noget sikkerhedsmæssig styring på de produkter og, at konceptet er operationaliseret på en form, så det kræver mindst mulig administration. Jo mindre model og konceptmæssigt autorisationer bliver tildelt, jo mere administration kræver det og du vil skulle have mange bolde i luften.

Har KMD et autorisationskoncept?

Vi har mange. F.eks. til BI. Det er et meget operationelt koncept, hvor det konceptuelle og modelmæssige er lidt svært at få øje på. Det er nede i noget meget detaljeret.

Hvilke faktorer påvirker et autorisationskoncept?

Inden for udviklingen vil jeg nok sige den ledelsesmæssige forståelse, accept og buy in er rimelig vigtig fordi autorisationskonceptet går på tværs af alle forretningsområder, og hvis dem der er interesseret i at udvikle autorisationskonceptet ikke har et ledelsesmæssigt mandat, er det håbløst at gå ud og bede forretningsområdet bruge ekstra tid på at lave sikre løsninger og ikke bare lækre løsninger. Sikkerhed er jo sådan en kedelig faktor og kedeligt ekstraarbejde og meget komplekst
Derudover skal man have tjek på sine processer, på sin forretningsarkitektur, ellers famler du i blinde. Hvis du ikke har en forretningsarkitektur, er du rent reaktiv, så skal du tage stilling til alle behov når de kommer ind, og det er administrativt tungt.
Så spiller heterogeniteten af systemlandskabet også en stor rolle. Jo mere komplekst et systemlandskab og jo flere teknologier der er i spil, jo sværere er det konceptuelt at lave noget, der går på tværs.
Den generelle kultur og modenhed i organisationen er også ret vigtig. Rent forståelsesmæssigt at kunne se, at sikkerhed bare er noget, der skal integreres, og er en integreret del af det, man gør, det kræver et vidst modenhedsniveau, ellers er det bare noget, man laver til sidst. Hvilket jo også viser sig her, i sidste ende er det også noget, vi laver til sidst.
For Produktionen gælder de ovenstående og derudover er man i spil mod kunderne, og der kan det godt være at konceptet ikke er det kunderne har ønsket sig, måske vil de have flere frihedsgrader end det der ligger i konceptet, så derfor er kunderne en vigtig faktor, så det er vigtigt at have en forretningsmodel i forhold til hvordan man definerer sikkerhed, hvor bøjeligt må konceptet være, og hvor meget må det i så fald koste.

Hvilke forudsætninger skal være til stede for at kunne designe et autorisationskoncept?

De faktorer jeg har nævnt før er også forudsætninger, sådan noget som at man har en forretningsarkitektur, og ledelsesmæssig opbakning, at man har sine tilstødende koncepter på plads, i forhold til kunderne, og i forhold til interne roller. At man har sin interne sikkerhed på plads. Dette er også en forudsætning for, at konceptet i sidste ende holder.
Og helt basalt, at man har de kompetencer der skal til for, at man rent faktisk kan lave det.

Interview med autorisationsassistent fra KMD

Hvad er de største udfordringer i forbindelse med at implementere og vedligeholde autorisationer?

Det er de brugere, der skal bruge dem. De skal vide hvorfor der er brug for et koncept. De tror man begrænser dem i deres arbejde.

Gælder dette kun for SAP?

Det ved jeg ikke. Jeg har kun erfaring med SAP

Hvad er et autorisationskoncept?

Det skal sikre, at brugerne ikke gør mere end det de må. At have styr på hvem der har adgang til de forskellige systemer.

Hvorfor er et autorisationskoncept vigtigt?

For at undgå tab. Det der er mest spændende, er inden for de finansielle markeder, hvor der er tabt virkelig mange penge. Jeg kender ingen IT virksomheder der er gået fallit pga. en brist i deres autorisationskoncepter.
Det er vigtigt fordi du kan komme til at brænde nallerne. f.eks. ENRON, jeg tror de havde SAP, og medarbejderne havde SAP_All adgang, så mellemlederne kunne selv rette i deres regnskaber, og i sidste ende krakkede det fordi regnskaberne ikke passede. Herinde er vi jo også bange for økonomiske tab. Det er derfor vi laver det. Ellers er det jo lige meget. Men hvorfor er det så vigtigt med sikkerheden, og standarder som DS 484? Man er vel bange for de økonomiske tab. Også i forhold til at undgå insiderhandler. Man skal sikre segregation of duties, dvs. den person der laver en rolle, må ikke være den samme der tildeler den til en bruger.

Har KMD et autorisationskoncept?

Næ, men det får de vel. Jo, det har de vel på nogen af systemerne, f.eks. på BI.

Hvilke faktorer påvirker et autorisationskoncept?

Overordnet er der nogle love, f.eks. bestemmelser man skal leve op til. Så er der datatilsynet og datalovgivningen, f.eks. skal alle læger ikke have adgang til alle journaler.

Den enkelte afdeling i virksomheden er også en faktor, da de ikke gider at blive tjekket af de andre afdelinger i forhold til hvad de laver. Og man ønsker ikke at alle har adgang til det samme, så der bliver slettet til højre og venstre og man ikke ved hvem der har gjort hvad.
Der er også dem der er med til at skabe autorisationskonceptet. De påvirker det i forhold til hvor lempelige de synes det skal være. Deres syn på sikkerhed har en kæmpe betydning. Specielt når der ikke ligger faste rammer for hvad det skal indeholde. Der er selvfølgelig de overordnede rammer, men ikke noget konkret, så dem der er med i projektet, har en enorm indflydelse i forhold til, hvor meget de synes brugerne skal måtte kunne.

Hvilke forudsætninger skal være til stede for at kunne designe et autorisationskoncept?

En overordnet jobbeskrivelse af hvad hvem laver, og hvem der har ansvaret for de forskellige jobtyper. Nogen skal tage ansvar for de forskellige afdelingers jobtyper. Hvis man kender ansvaret fra dag 1, er det meget lettere, fordi så kan de ansvarlige guide i forhold til at lave konceptet. F.eks. med mit arbejde i forhold til at vedligeholde roller, ville det være enormt godt, hvis jeg kendte folks jobtyper, eller jobtyperne rollerne tilhører. Det er meget vigtigt, at folk ved hvad de er sat i verden for at lave, i stedet for at det er dem der laver konceptet der skal gætte på hvad folk går rundt og laver.

Interview med SAP specialist fra KMD

Er de seks potentielle risici udpeget af Kommunernes Revision i den IT-revisionsmæssige gennemgang af sikkerheden i SAP ekstern i 2005 stadig gældende? (Viser listen fra rapporten)

Punkt 4 holder stadig stik internt

Hvad er de største udfordringer i forbindelse med at implementere og vedligeholde autorisationer?

Det er at få folk til at gøre det rigtigt. Folk gør det på deres egen måde. Ligesom en udvikler har sin personlige måde at skrive kode på, og økonomen har sin egen måde at regne nøgletal ud på. Det gælder om at få styret det, da der ikke er en skarp opdeling i autorisationsverdenen, er der mere mulighed for frihedsgrader, og så er det med at få lavet koblingen, mellem hvad folk har brug for, og få det specificeret så det kan omsættes til implementering, f.eks. få en udvikler til at sige, at han har brug for adgang til sådan og sådan, eller få en bogholder til at sige, at han har brug for at lave dette og vedligeholde dette.

Gælder dette kun for SAP?

Det vil jeg ikke formode. I langt de fleste virksomheder skal man overvåge en medarbejder i 14 dage, for at vide hvad han laver, og det er ikke behageligt for medarbejderen. Som arbejdskulturen er nu, laver vi mange forskellige ting, så det er ikke så simpelt at finde ud af hvad den enkelte medarbejder laver.

Hvad er et autorisationskoncept?

Det er en beskrivelse af hvad man har tænkt og hvilke retningslinjer der er, samt hvilke særtilfælde der kan være. Det er ikke en kogebogsopskrift, for det er ikke en opskrift, der fortæller at du skal gøre sådan og sådan, men det er en beskrivelse af alt hvad der vedrører autorisationer, som skal sætte udenforstående i stand til at forstå hvad der er tænkt og ment, og sætte dem i stand til at agere korrekt fremadrettet.
Formålet med autorisationskonceptet er, at hvis jeg bliver ramt af en bus i morgen så skal andre kunne tage det og forstå hvad der skal ske. Det skal skrives på et niveau så konceptet kan overholdes, selvom dem der har været med til at lave det ikke er der længere.
Derudover indeholder det procedurebeskrivelser for hvad man gør, hvis man ønsker at få udført opgaver, som man ikke selv har rettigheder til at løse.
Dette er også en vigtig ting ved et autorisationskoncept, fordi det sætter andre i stand til at vurdere hvordan de skal agere eller hvem de skal kontakte for at få hjælp til deres opgaver.

Hvorfor er et autorisationskoncept vigtigt?

Det er vigtigt, fordi man f.eks. her i virksomheden har decentrale autorisationsfunktioner, og for at ensarte rolleudviklingen er det vigtigt, at alle ved hvilke retningslinjer der er gældende.
For dem som er underlagt autorisationer kan det være en hjælp til at forstå hvorfor man har underlagt dem regler, f.eks. kan en udvikler være irriteret over hvorfor der er noget han ikke må, men hvis han læser konceptet kan han forstå hvorfor han ikke må det. Det er ikke nødvendigvis meningen, at en udvikler skal læse det, men nogen vil få gavn af at læse det, i forhold til hvis de mangler nogen rettigheder, da konceptet også vil indeholde beskrivelser af roller.

Har KMD et autorisationskoncept?

Godt spørgsmål. Der er ikke et overordnet autorisationskoncept der dækker alt. Der er flere. Det giver også ok mening da man håndterer forskellige situationer og miljøer i KMD. F.eks. er der lavet et til BI. Der er også kundevendte autorisationskoncepter for Løn.

Hvilke faktorer påvirker et autorisationskoncept?

Systemlandskabet, f.eks. hvor mange systemer har man, hvor mange klienter, taler vi ERP, CRM eller BI? Hvad er med, og hvad er ikke med?
Anvendelse, er det en løsning du bruger til at lave en web service, så eksterne brugere kan logge på og købe varer, eller er det et lønsystem? Er det et internt system? Hvad er det det skal bruges til?
Antal brugere. Hvor kvalificeret er dine brugere, er det superbrugere, eller er det nybegyndere? Nogen der ikke er erfarne skal begrænses mere, så de ikke kommer galt af sted. Man skal ikke komme til at kunne kigge på noget ved et uheld fordi man ikke vidste hvad man lavede. Hvis jeg nu er udvikler, kan jeg finde på at justere på ledige systemprocesser, hvilket jeg så sætter tilbage igen, men hvis jeg er ny, kan jeg komme til at pille i noget, der kan genere andre kolleger.
Hvor følsomme er de data man har?
Hvordan er virksomhedens opbygning? I nogen virksomheder er det okay, at man roder i hinandens arbejdsopgaver, og så har man nogle virksomheder med vandtætte skodder.
Økonomien, hvor meget vil man betale for at have et autorisationskoncept. Jo mere granulært det skal være, jo dyrere bliver det at vedligeholde.
Lovgivningen påvirker selvfølgelig også, da det skal være lovligt, og derudover kan ledelsen også påvirke i forhold til økonomien og omfanget.

Hvilke forudsætninger skal være til stede for at kunne designe et autorisationskoncept?

Du er nødt til at specificere hvad det er, der er behov for, det ved du jo ikke som autorisationsmand/dame. Så er du nødt til at have en forankring i virksomheden, der gør, at det er en prioriteret opgave for andre en dig.

Det er vigtigt at man har en change management proces, eller en ledelsesforankring som gør, at det bliver accepteret, når konceptet bliver implementeret, fordi normalt vil det betyde ændringer for den enkelte bruger, at man lige pludselig vedtager retningslinjer, og normalt vil det medføre restriktive ændringer. Det har aldrig været nemt at begrænse brugerne. Der er aldrig nogen der er glade for at afgive rettigheder. Man vil gerne afgive arbejdsopgaver, men man vil gerne stadig have muligheden for at udføre dem, hvis nu man får brug for det.

Interview med to forretningsspecialister fra KMD

(Den ene af forretningsspecialisterne er allerede blevet interviewet én gang før)

Hvordan startede det med KMD og SAP?

1: Omkring 1998 skal KMD lave et nyt løn og personale system, og da de ikke selv vil udvikle det, kigger de omkring hvad der findes, og beslutter til sidst at vælge at bruge SAP til det. I April 2005 offentliggøres det, at SAP er blevet valgt som den strategiske platform hvor alt skal udvikles på. Dette var også interessant for SAP, da det ikke havde noget modul for offentlig forvaltning.
For at kunne gøre dette, finder vi ud af, at der er brug for en enterprise arkitektur. Og det bliver besluttet at i 2006 skal alle forretningsområder have defineret deres enterprise arkitektur, herunder helt ned til aktiviteter i processer, forretningsobjekter og forretningsroller.

Blev der taget højde for de jobfunktioner der skulle udføres? Hvordan blev rollerne udviklet?

1: Man startede med at have nogle forretningsroller, men de blev hurtigt forurenet, i forhold til, at man sagde, nogen gange skal Knud kunne det her, og Bente det her, så det hele blev hurtigt meget småt, og det vigtigste var, at de kunne udføre deres opgaver, og ikke så meget i forhold til f.eks. hvad en controller skulle være i stand til at kunne gøre.

2: I SAP R/2, hvor det hele var teknisk, og hver rolle var lavet til én bruger, og hvor man ikke brugte et rollekoncept, det var mere et adgangsprincip, hvor man fik en hard kodet adgang til det man skulle kunne. Så kom R/3, hvor SAP lavede deres systemer om, så de lavede en rollebaseret indgang, men fokus blev, at man skulle gøre det så smart som muligt.

1: Teknologien var dog ikke helt klar til at definere forretningsroller, igen fordi SAP er en platform, der består af flere forskellige systemer, mens rolleteknologien var begrænset til hvert enkelt system
F.eks. en budgetteringsproces starter i budgetteringssystemet, og bagefter kommer det over i finanssystemet for at kunne styre det. Det vil sige, at en bruger skal have adgang til begge systemer. Så han skal have roller både på det ene og på det andet system.

2: Tanken var god nok, men teknologien var ikke klar. Tanken var at lave integrationen, men man havde ikke en platform at gøre det på. Man lavede en CUA *(central user administration)*, men kun inden for SAP platformen, man havde ikke noget der kunne række ud over SAP, ikke før Portalen bliver købt, og derfor kunne der ikke kobles resten af forretningen sammen med det

Hvordan var informationsejerskabet fordelt?

2: Man havde prøvet at tænke noget ejerskab ind, men der var ingen procedurer til rådighed, du kunne ikke forbinde til en der sad ude i forretningen og ejede de ting.

1: Du har et projekt, der udvikler et system, der tilhører nogle processer, men ham der er projektchef er jo ikke ham der er ejer over processerne, det er han måske, når projektet er i gang, men hvad med bagefter? Man tænkte ikke så meget i ejerskabsmodeller.

2: Man kunne godt se, det var smart, men det kunne ikke rigtigt lade sig gøre.

Var det taget stilling til risici?

1: Jeg fandt aldrig ud af, om der var en standardiseret måde at gøre det på. Andre steder har man ofte gjort det mere på bagkant, men i KMD har man ikke rigtigt gjort noget.

2: Først og fremmest tænkes der SoD *(Segregation of Duties)*. Der skulle kunne bindes noget op på noget konkret. Det var SAP kasserne man kiggede på. Andre steder har man bestilt revisionen til at lave en overordnet gennemgang.

1: F.eks. i KMD, hvor der var SAP kasserne. Løn og Personale, det er HR modulet. Men er det nu det? F.eks. Strukturelle autorisationer der bliver brugt i HR, det hører til i Basis løsningen.

2: Hvert modul var projektopdelt, typisk FI/CO *(finans og controlling)*, og så var der nogen i gang med at lave HR, og så kom CRM og BW senere. F.eks. da SAP releasede CRM glemte de autorisationsobjekter for CRM, det vil sige det virkede kun, hvis du have SAP_All, det vil sige rigtig bred adgang til tabellerne.

1: Det viser, at fra SAPs side har der heller ikke været så meget fokus på det, og kunderne var heller ikke så opmærksomme på det.

Så risici og separation af opgaver blev opfattet som det samme?

1: Den måde, at autorisationskoncepter og roller blev udviklet på var, at autorisationskonsulenten havde en tidligere erfaring, og den bragte han med ind i projektet. Hvorfor er det, vi laver en opdeling? Vi har ikke regler for det, det er mere noget, vi gør på baggrund af erfaring, f.eks. at den samme person ikke må kunne oprette en leverandør, og så også betale ham.

Der er andre, der har nævnt et BI autorisationskoncept, hvordan hænger det sammen med dette projekt?

1: BI *(Business Intelligence)* konceptet blev lavet i 2007, men det var mere på et teknisk plan. Der var en ny teknologi, og vi skulle finde ud af hvordan det fungerede, på det tidspunkt var det ikke klart for mig, at der var

en rammearkitektur, og at jeg skulle kende til den. Det var det første forsøg på at lave et eller andet tværgående, da her var en boks, hvor der umiddelbart var et behov for at lave et teknisk skarpt adskilt autorisationskoncept, da alle kunder kom ind på den samme klient. Men forretningsmæssigt, var der ikke viden om hvordan det skulle hænge sammen.

Var der et overblik over systemlandskabet?

1: Det var det, der var lidt mærkeligt med autorisationskoncepterne. På ERP skal man have adgang til nogle omkostningssteder som leder, der svarer til den afdeling, man er leder for, og på BI skal man have adgang til profitcentre, der svarer til den afdeling, man er leder for. Jeg har aldrig hørt om et koncept, der husker at tage højde for det her. Man har ikke haft værktøjer til det her, man har ikke kunnet se alle roller, der er tildelt en bruger på hele SAP platformen.

Hvornår blev autorisationsmanden involveret i processen?

1: Efter systemerne var i produktion, det vil sige, sikkerhed fik ikke mulighed for at have indflydelse på hvordan processerne blev designet.

2: Det var en reaktiv proces, du havde ikke mulighed for at påvirke tingene fremadrettet.

Hvad ændrede ved ovenstående opfattelse af autorisationskoncepterne?

1: I slutningen af 2007 eller begyndelsen af 2008, startede forsøget på at lave et generisk autorisationskoncept. På dette tidspunkt havde vi også DOF'en *(Den Offentlige Forretningsmodel)*. Meningen med DOF'en var, at det var ens business blueprint. Der var dog ikke nogen der brugte det. Det kan være mangel på forståelse af enterprise arkitektur, både på et specialist- og lederniveau.
Lederen skal jo sikre, at de gør det på den rigtige måde. At de følger de processer og metoder, der er for udvikling.

Hvordan var informationsejerskabet fordelt?

1: Det er blevet lidt nemmere med DOF'en, hvor komponenter fra KMDs rammearkitektur bliver mappet med komponenter fra SAP. Det er dog ikke fuldstændig stringent i forhold til, hvem der ejer hvad. Og der er ikke nogen overordnet ansvarlig. Der var forskellige sikkerhedsvejledninger for de forskellige forretningsområder selvom det var på samme system.

Hvordan blev rollerne udviklet?

1: På workshops blev samleroller fra systemerne mappet med forretningsroller fra DOF'en. Det vi gjorde var at tage udgangspunkt i de forretningsroller, der var defineret i rammearkitekturen, stod der f.eks. Lønadministrator. Hvad er det? Hvad indeholder det? Det var der ligeså mange meninger om, som der var mennesker rundt om bordet. Der er heller ikke beskrivelser tilknyttet alle sammen.
Vi fandt også en masse ting der skulle rettes på disse workshops. F.eks. hvis man følte, at en forretningsrolle var for bred, og skulle deles op i flere forretningsområder, så blev det henlagt til at skulle ændres senere, men det blev aldrig gjort, igen fordi det ikke er nogen af cheferne, der føler et ansvar for at få dette her på plads. Som udgangspunkt var det roller fra DOF'en, men hvis de ikke var gode nok, blev der defineret nogle nye. De forretningsroller der blev defineret her under det generiske autorisationskoncept, skulle være så små, så man kunne bygge koncepter både til de mindste og til de største kunder, det vil sige de små roller skulle bruges til de store kunder, da disse er mere specialiserede. Kunderne skulle stadig kunne specialisere til deres egne behov, det vil sige en bogholder i Århus og en bogholder i Randers er forskellig, men de underlæggende roller er de samme. En bogholder i Randers er både fakturaopretter og fakturagodkender, mens der i Århus er to forskellige stillinger. Dvs. i Randers er der kun en bogholderstillingsrolle, og i Århus er der to bogholderstillingsroller

Var det taget stilling til risici?

1: Den laveste fællesnævner er SoD, det er den nemmeste at forstå, du må ikke kunne det her, og det her.

Blev der taget højde for de job funktioner der skulle udføres?

1: Der blev ikke tænkt stillinger, det blev ikke verificeret i forhold til f.eks. Århus kommune, det var i forhold til hvordan forretningsområderne så de mindste byggesten.

Blev der taget højde for standarder?

1: På det her tidspunkt bliver man også klar over, at man skal være compliant, så man troede, man kunne lave et quick fix, ved at tilføje et dokument ved, at hvert forretningsområde skulle lave en sikkerhedsrisikovurdering. Der er ikke nødvendigvis sammenhæng, mellem det man skriver i sikkerhedsrisikovurderingen og det tekniske. Der er lavet et dokument, men det hænger ikke nødvendigvis sammen med rammearkitekturen.

Hvornår blev autorisationskonsulenten involveret i processen?

1: Det gode ved det her var, at alle der vidste noget om det, og skulle tage af på det, var samlet. Det vil sige på de workshops der blev holdt skulle det hele kunne blive aftalt, men desværre ville folk ikke tage det ansvar de burde.

Var der et overblik over systemlandskabet?

1:Autorisationsudvikleren i finans, vidste ikke hvilke roller der matchede på portalen, det samme gjaldt med BI. Man fik fordelt noget ansvar, og overfor cheferne fik man synliggjort, hvor der manglede ejerskab, eller hvad der ikke faldt ind i den umiddelbare ejerskabsmodel, der var defineret. Det er her hvor forretningsområder havde ansvaret for forskellige moduler i SAP. Men der var de her teknologiske platforme, som Portalen og BI der faldt lidt uden for.

Hvorfor gik man væk fra det generiske?

1: Fordi forretningsområderne ikke kunne stå inde for det generiske autorisationsrollekoncept. De følte ikke det var granuleret nok til at kunne dække alle kundernes behov. Byggestenene var ikke blevet små nok.
Det der måske manglede var, at ansvarsfordelingen mellem forretningsområderne og Service ikke var helt klar, dvs. hvor stor er Services rolle i forhold til at definere autorisationskoncepter ude hos kunden?
Og kan Service overhovedet finde ud af at tænke koncepter, og tænke enterprise arkitektur, fordi det har de ikke lært.
Der ligger den potentielle konflikt i, at service siger de ved, hvordan det er ude hos kunderne, mens forretningsområderne ikke nødvendigvis har informeret dem, om alt det de skal vide.
Hvor går skellet mellem udvikling og Service? Nogle steder laver Service helt nye roller for kunden, og andre steder laver de dem kommunespecifikke

Hvordan blev rollerne udviklet?

1: Service og kunden har sammen defineret nogle overordnede forretningsroller og nogle specialfunktionsroller, uden hensyntagen til noget andet, andet end hvordan de eksisterende roller er hos kunden.

Blev der taget højde for de job funktioner der skulle udføres?
1: Ja, det blev der. Det generiske koncept gik ud på, at lave nogle fornuftige grupperinger, altså en slags lim, ved at indskyde et ekstra niveau i koncepter, som også kunne gå på tværs af systemerne. Det der nu skete var, at man gik tilbage til det første fragmenterede koncept, men med en ekstra kompleksitet i forhold til forretningsrollerne. Og der blev igen ikke taget højde for eller stilling til risici

Hvordan var informationsejerskabet fordelt?
1: Det er ikke relateret til noget i KMD. KMD siger bare det er kundens ansvar.

Var der et overblik over systemlandskabet?
Der er 3 systemer. Og konceptet dækker alle 3. Det der er problemet med dette ad hoc, er at der mangler en proces, det vil sige det er uklart hvordan defineringen af roller skal foregå når der kommer nye systemer på.

ERFA møde for SAP Sikkerhed

Mødedeltagerne vil blive refereret som M1, M2 osv.

Påstand

Traditionelt er medarbejdere, der tager sig af autorisationer "håndværkere" og ikke teoretikere. Dette medfører lav interesse for at skabe strukturer og teoretisk funderede koncepter

Diskussion

Er ovenstående korrekt, og i så fald er det et reelt problem? Gør det noget, hvis der ikke er teoretisk funderede koncepter?

M1: Jamen, et eller andet sted føler jeg mig da også som håndværker, når man kommer ud. Nu siger du håndværker i modsætning til teoretiker? Nogle af de flotteste huse jeg har set, det er murermestervillaerne, så et eller andet sted så skal der en plan til, og det tror jeg de fleste af os, når vi kommer ud til kunden arbejder ud fra, eller det er vores foretrukne arbejdsform. Men den måde man arbejder på, i hvert fald som ekstern konsulent, altså det eksterne konsulentmarked er lidt en luderbranche, altså man kommer ud og man bliver bedt om at løse en eller anden konkret opgave, og jeg har da prøvet at komme ud, hvor der er en kunde der har købt et SAP best practice system, hvor jeg får at vide, at jeg har to dage til at lave roller, og de skal bare have standard roller punktum. Ja, hvad med ham udvikleren der sidder der skal han ikke?… De skal bare have standard roller, det er det, de har købt. Så laver man standardroller. Så kan man jo argumentere nok så meget, og gør det også gerne, det tror jeg de fleste af os gør, men jeg tror de fleste af os, har været ude i de situationer, hvor vi bliver bedt om at lave noget, og også rent tidsmæssigt, vi ved godt det her, det holder ikke, og vi kan også fortælle kunden, at det holder ikke, men branchen er jo også sådan at, jamen, han vil betale to dage, du har to dage, that is it, og er det ikke dig der laver det, så er det en anden der laver det.

M2: Altså, jeg ser det også lidt sådan, at man er en del håndværker, selvfølgelig er man det, men jeg ser det da også sådan, at man også er teoretiker, og det tror jeg også du er, i det øjeblik du rent faktisk står i virksomheden, for de har jo ikke rigtig nogen ide om hvordan det skal være. De har tænkt tankerne, de har lavet strukturen og konceptet, og så beder de dig om at implementere det. Hvis du bare implementerer det uden at stille dig kritisk, eller stille spørgsmål, jamen, så bliver du håndværker, hvis du derimod går ind og udfordrer dem, og prøver at foreslå dem noget andet, eller prøver at foreslå noget smartere, fordi du har tænkt over de her ting, så bliver du også teoretiker. Så på den måde, så vil jeg helst gerne være brobygger mellem teoretikerne og håndværkerne, være der imellem hvor jeg både er håndværker og teoretiker, fordi alt teori den skal selvfølgelig være anvendbar, og implementerbar, og der ser jeg ofte, at virksomheden og revisionen måske er teoretikerne, som går ind og siger, vi har de her regler og de her rammer, og det skal være sådan her, hvor man som konsulent kan gå ind og give et modspil til det. Jeg tror egentlig, at det er meget korrekt, at de fleste, altså hvis ikke man tager fat i sig selv, så bliver man lidt en håndværker, så laver

man det man får besked på. Det er da et problem. Så er det vi får de her tilsandede koncepter, og roller der ikke rigtig giver mening.

M3: Der er et sted deroppe, man kan dele det i to. Der hvor du skriver, at det er medarbejdere, der tager sig af autorisationer. Der er to roller, der tager sig af autorisationer, typisk. Det ene det er at lave selve designet omkring det, og at have forståelsen for det, og det andet det er fysisk at gå ned og lave tastearbejdet. De to ting, hvis de er separeret til to forskellige personer, så vil jeg sige, at så har man ikke problemet, hvis man har taget de to rigtige personer. Men man starter med at have en eller anden funktion der skal udføres, eller en eller anden systemadministrator, hvor man har hyret en praktiker ind, og der har man glemt den første fase, man har kun kigget på det operationelle, det vil sige selve opsætningen, det er sådan en person man har hevet ind, og sætter til opgaven. Hvis man så glemmer, at designfasen også er der, og pålægger den opgave sådan uformelt, så stille og roligt kommer den ind over, så bliver det et problem, fordi de forudsætninger har man egentlig ikke ansat vedkommende til. Hvis der i organisationen i forvejen er nogle andre, der tager sig af den del af det, så er det ikke noget problem. Sådan ville jeg formulere det, hvis man har hyret den rigtige person, eller de to personer, måske, og det ser man jo mere nu, at man deler den rolle til to personer, eller hyrer en der kan begge dele, og ikke bare tror, at den ene eller anden person faktisk kan løse det.

M4: Jeg tror de fleste af os, når vi kommer ind, under alle omstændigheder har en holdning til arkitekturen, og til den teoretiske del også i projektet.

M5: Problemet er, at vi mangler altså en teori, vi mangler en gængs teori, ikke, at en teori kan afdække alt, men der kan afdække det meste af det, også for at kunne have en eller anden form for hjul, for at have en kontinuerlig proces i forhold til at forbedre og vedligeholde dit koncept. Der er jo ingen, der har nogle modeller for, hvordan er det lige vi vedligeholder de her koncepter og opdaterer. De sander til med det samme, fordi den måde vi også dokumenterer på, det er utroligt kedeligt, og der er ikke nogen værktøjer til at hjælpe os med at gøre de her ting, så du ved vi kan ikke rigtig... Ja vi mangler en teori

M4: Vi mangler begrebsapparatet, vi mangler metoden eller referencerammen. Der har vi nok kun hver især vores egen, når vi kommer ud

M6: Det er delvist rigtigt, fordi der er nogle der har bygget nogle gigantrammer op, problemet er bare, at de ikke er håndterbar. Sarbanes-Oxley, hvor end meget man måtte hade konceptet, så tager den jo funktionsadskillelse ud, og udpensler den til et eller andet niveau, hvor du skal have tusind medarbejdere for at lave et eller andet, det er jo kompromiset, du skal køre sammen og vedligeholde det. I Danmark, der kan du sige, det er ikke kommet så langt, der kommer nogle euro-sox tiltag her over det næste stykke tid, hvor vi begynder at se på det, men i USA, jamen, du har Sarbanes-Oxley, du har organisationer der tager sig af governance strukturer og den stil, det er jo noget af det, der kommer ind, der er OSEC, som har nogen ganske udmærkede modeller for det, men det man ser, det er jo, at det ikke er sådan, at der bliver lavet en

model til SAP, der bliver lavet nogle overordnede modeller for integrerede systemer, eller store kasser, det vil sige, der kommer noget, der også dækker over ORACLE, eller ORACLE og SAP blandede platforme. De bliver teoretiske, men de bliver gigantiske, og de er jo gearet til at tage sig af store størrelser. Det man også kan sige, når man tager fat i de her store størrelser, det er, at man vil have et værktøj, eller en begrebsmodel, som ligesom kan koge nogle af de her ting ned. Hvor er dit acceptable niveau i forhold til dine funktionsadskillelser? Det nytter jo ikke noget at gå ud, som jeg har set nogen, at tage de her kæmpe store kasser, og når de så skal ud og implementere dem i et eller andet datterselskab, hvor der i stedet for 100 mand i bogholderiet, sidder 10 mand. Det kan ikke lade sig gøre, fordi der skal være 100 mand, det siger deres model, men hvad er det så, der er acceptabelt, hvornår skal du sige, det her er acceptable risici, og hvornår skal du kompensere for det? Det er stadig det samme koncept, og efterhånden som du modner, så skal du selvfølgelig stå inde for en løbende vedligeholdelse af dine koncepter, ligesådan som du skal tage din modning og sige, hvad er det i grunden, der er vigtig for den her virksomhed at beskytte, fordi hvad der er vigtigt for én virksomhed at beskytte, det er ikke nødvendigvis det samme i en anden virksomhed. Det vil sige, en af de vigtigste ting det er at sige, hvad er det denne her virksomhed vil beskytte? Hvad er kritisk for denne her virksomhed? Det er det, der er core business for den her virksomhed eller konkurrenceparameteren.

M5: Det kan bare gøres meget mere simpelt, hvis man bare kigger på den proces og metode der ligger bag, lad os sige, at vedligeholde en rolle. Efter du danner dit autorisationskoncept i dit projekt, så følger du en eller anden metode. Gør du det? Næ, det går du måske ikke. Så går vi over i vedligehold. Følger det en metode der, ved du hvor kravene er, har du overhovedet styr på dine krav fra starten, da du lavede dit implementeringsprojekt? Har du styr på om du må rette det efterfølgende, altså bare en helt gængs procesmodel altså det er sådan her, vi gør det, vi har den her sporbarhed op til kravene, vi har mappet alle tingene, så de her krav bliver til sådan her, til den her proces der bliver til de her transaktionskoder, der bliver til de her autorisationsobjekter, du ved helt derned, det er sådan nogle ting, hvor jeg mener, at det hjælper Sarbanes-Oxley jo heller ikke med at gøre. De stiller jo bare nogle krav ikke?

M6: Jo, jo, præcist, men hvad er din del af teorien, er det governance, hvordan du styrer dine autorisationsstyringer, eller er det hvad du vil bygge? I SAP, der kan du bruge Solution Manager, og den kan du bruge på mange måder. Det er et værktøj, den kan en del af det du sidder og siger, man gerne vil, men der er mange, der vælger at bruge det på en anden måde. Det er jo igen det, at alle værktøjskasser det er et spørgsmål om valg.

M5: Men du har ikke det holistiske perspektiv, helt oppe fra det forretningsmæssige, enterprise arkitektur, eller hvor det nu er, du har dine krav og så hele vejen ned til systemet, så du ved, hvorfor det er, tingene ser ud som de gør.

M6: I nogle tilfælde vil jeg sige, det er et spørgsmål om kommunikation.

M4: Det er måske også en fejl i projektet, at man skal bare aflevere derhenne. Der skal du aflevere, og der skal dine roller være færdige, og så forsvinder projektet ligesom, og så starter der et nyt liv af rollerne bagefter, som ikke var det samme, som der var i projektet, og det er jo der hvor, hvis man var en teoretiker fra starten af, så ville man se 5 år frem, i stedet for at se til den deadline vi har til marts næste år.

M1: Jeg tror man skal holde fast i, at der er meget stor forskel fra organisation til organisation, jeg tror det er meget vigtigt, at det man kommer ud med, er meget tilpasset til den organisation, man kommer ud til.
Der er ikke nogen tvivl om at køre autorisationskoncepter hos KMD, er noget anderledes end at køre autorisationskoncepter hos Børglums Børstefabrik med 10 SAP brugere, og i øvrigt en regnskabschef der har fået ansvaret for at passe deres SAP system ved siden af. Han ringer en gang i mellem, når der er noget brugerne ikke kan. Han vil gerne have et nogenlunde sikkert system. Men hvordan autorisationskoncepter, og sådan noget overhovedet er bygget op. Det interesserer ham egentlig ikke, og det er slet ikke noget han har tid til, eller vil bruge sin tid på. Det er et spørgsmål om stadig at kunne sætte kravene. Der er det spørgsmålet om at holde, når vi kommer ud og skal hjælpe med at implementere, at få lavet nogle koncepter der er tilpasset, det vil sige, at i små organisationer nogle simple koncepter, der gør, at Søren vil kunne komme ind dagen efter mig, kigge på det, og sige, der er de her 5 roller, fint, det kræver ikke det store. I forhold til KMD, hvor man kommer ind i et begrebsapparat af en helt anden størrelse.

M4: Jo, men så har du som konsulent også taget et valg for kunden. Du har hjulpet ham, og påvirket ham, hvorimod hvis du havde trukket i en anden retning, og sagt se lige her, det kan godt være det virker det næste år, men hvis du lige laver nogle statistikker her, og skriver noget her, så er der mulighed for at vokse, og gøre de her ting, men hvis du designer det nu, er det lidt mere besværligt, men så gør det, at det måske lever 3 år til med den her model, og så er det måske ikke så utilfredsstillende, og det er sådan noget, man først er begyndt at høste, når der er gået et år eller to, så er det de siger, der var der nogen, der tænkte sig om.

M1: Det kræver også, at når du så afleverer det til kunden, så tjekker, at du også afleverer et begrebsapparat, der gør, han kan vedligeholde, så det ikke når du kommer tre år frem, er sandet fuldstændig til.

M5: Ville det så ikke have en rigtig stor værdi, hvis vi alle sammen havde den samme proces, eller metode og begrebsapparat. Et koncept vi kunne bruge ude hos kunderne, så vi vidste, hvordan er det, tingene er dokumenteret, hvordan er det, de hænger sammen, så man kan se, her er kravene, og her på børstefabrikken, der har de valgt ikke at have nogen krav, så det er derfor, det ser sådan her ud.

M2: Uanset hvad, så er det jo nok meget godt at have en metode, for det er jo det, du så gerne vil have, og uanset om vi har den samme metode, eller hver vores, men en metode der bliver overleveret til kunden, så de forstår, hvorfor ser konceptet ud som det gør, og kan vedligeholde det derefter.

M1: Helt banalt, bare et eller andet sted hvor man ved, at her der ligger der noget dokumentation. Jeg tror de fleste af os oplever at komme ud, og dokumenta… hvad for noget? Den er stort set ikke eksisterende, men vi har nogen roller her, der er nogen, der har lavet engang, og så har vi nogle andre roller her, der er nogle andre, der har lavet engang, og så er der i øvrigt nogen, der har været inde og lavet noget helt tredje, og hvis vi nu får alt det sammen, så kan man gøre sine ting.

M2: Jeg tror, at hvis man kigger lidt på den her håndværker og teoretiker skelnen, så er meget af det vel også, at vi går ud og har noget dokumentation, og en masse metode, men er det forståeligt for andre? Og hvis det kun er forståeligt for os selv, så er vi måske lidt mere håndværkere end teoretikere. Tanken er vel også, at det man efterlader, skal være en åbenbaring, for den man efterlader det til, dem der skal vedligeholde det, og andre der kommer senere hen. Så man netop kan arbejde videre med det. Det er vigtigt, at man hurtigt kommer ind i den tankegang, ellers forstår man det måske ikke, og så laver man et eller andet, som kunden måske har forestillet sig, eller har implementeret sit eget koncept oven i det eksisterende, så man lige pludselig har 2 halve koncepter. Det har jeg da oplevet. De store virksomheder er ofte meget slagfaste. De ved hvad de vil have, og de har nogle krav. Det kan godt være, at kravene ikke er i sync med konceptet, men så får man implementeret det, og så er det, at konceptet skrider, så er det, vi sidder med en sandkasse.

Påstand

Man kan ikke få ledelsen involveret og til at tage ansvar for og forstå ting på de tekniske niveauer.

Diskussion

Er ovenstående korrekt, og bør ledelsen overhovedet forstå ting på de tekniske niveauer?

M7: Omkring påstanden der mener jeg ikke, at ledelsen skal involvere sig i det tekniske niveau, men at det er håndværkeren, eller konceptmageren, eller hvad vi nu kalder ham, autorisationsmandens, eller kvindens, ansvar at kunne oversætte de tekniske ting til noget forståeligt for ledelsen. Det er så også ledelsens ansvar at tro på, om de her mennesker er i stand til at gøre det, sådan så de kan stole på det der efterfølgende bliver lavet. At ledelsen skal kunne forstå tekniske ting nede i SAP, det giver ikke nogen mening. Hvis ledelsen kan det, så fokuserer de forkert.

M5: Jeg vil lige tale imod, det du siger. Igen, det er det der bottom up, at det er autorisationsmanden, der skal komme med tingene. Det er ledelsen, der skal sætte kravene.

M7: Nu tager jeg udgangspunkt i teknik, og det er derfor, jeg tager fat om det først. Jeg er fuldstændig enig i, at der er ledelsen, der skal sætte kravene.

M8: Men jeg må lige spørge, kan de forstå, at der er en bruger, der må bogføre i den kode, og ikke i den kode, er det forståeligt for ledelsen?

M1: Vi siger det på en anden måde end den firmakode og den firmakode. Må du bogføre i dit firma i Sverige? Må du bogføre for KMD i Ballerup og KMD i Aalborg? Det ved de godt. Det er deres verden. Men man er nødt til at kommunikere med ledelsen i det sprog.

M6: Det er derfor, man nogle gange har tolke med. Altså helt bogstaveligt, så er det typisk, at der er procesejere med, som har en detaljeret procesviden. Når du sidder med din teknik-Jørgen, og du bygger et eller andet op, så har du brug for en, der også taler ledelsens sprog, og ind imellem skal det oversættes til noget lidt andet, også fordi du er ude i et væsentligt mere komplekst billede, så du skal have nogen, hvor du kan sige, jeg stoler på, du ved det her, hvis du giver mig grundessensen her. Typisk dem der tager ansvar for de forskellige processer, de deltager jo også i det her forløb, så der er en kobling fra ledelsen til overordnede betragtninger til detaljerede betragtninger, altså udførelsen. Det er sådan set rimeligt vigtigt, at der er det ejerskab undervejs.

M7: Vi talte om, hvornår er det teknik, og hvornår er det ikke teknik? Det er også vigtigt at definere her. Hvornår taler vi egentlig teknik? En company code, er det teknik? Det blev vi så enige om, det ikke var. Det skulle forretningen, i et eller andet omfang kunne forholde sig til.

M5: Er en transaktionskode så teknik?

M7: Ja, det er et godt spørgsmål, og det vil sikkert blive defineret forskelligt, om det er teknik, eller det ikke er teknik, om man vil tage ansvaret som autorisationsmand for at definere transaktionskoden, eller om man mener, at det er forretningens ansvar.

M4: Transaktionskoden har jo en beskrivelse, som måske er mere forståelig for dem. De ved jo ikke lige, hvad de hedder, men vi kan måske heller ikke altid antage, at vi har den på dem alle sammen, men ofte vil de jo, kunne forstå dem, i hvert fald er det nok en god ide med en tolk, altså sådan en der har et eller andet fingerspitzgefühl for, hvad der egentlig rører sig i SAP, altså ikke en total tekniknørd, men netop forstår transaktionsniveau, og som måske kan forklare det videre.

M6: Skal du bogføre, kan det være, at der er 3 transaktionskoder for at bogføre, som er en god ide, men når du skal fortælle det til ledelsen, så er det bogfør eller ikke bogfør. At du så i praksis har en parker dokument, frigiv dokument, verificer dokument, bogfør dokument, eller hvad du nu ellers kan have, det er nede på et niveau, hvor vi kan diskutere, hvordan deler du de detaljerede processer op, men på et overordnet ansvar, så er det at kunne sige, at manden kan bogføre. Det er jo et spørgsmål, om at kunne oversætte de her transaktioner til handlinger, og der er nogen af dem, der er meget simple, og nogle af dem er meget detaljerede, alt efter hvor man er i SAP.

M2: Det er jo også det, at du har ledelsen, og så har du dine oversættere i form af mellemledere og procesejere, og som til sidst havner nede hos dig, og der er jeg enig i, at ledelsen skal ikke tage stilling til de her ting. De skal sætte de overordnede krav, som måske går ned i organisationen, hvor der bliver sat nogle detaljerede krav, som så går videre ned, hvor de bliver oversat til noget teknisk implementeret. På samme måde som når man skal cirkle opad, så har man nogen procesejere, som kan forstå den tekniske del, som man kan rådføre sig med, og så bliver det gjort mere og mere overordnet, jo længere man kommer op.

M1: Der har vi som autorisationsfolk, når du kommer nedefra og op til procesejerne, en opgave i at hjælpe dem med at oversætte de her objekter, altså helt lavpraktisk, så får vi jo mange gange en eller anden der siger, jeg har en transaktionskode, jeg kan ikke gøre et eller andet her. Det viser sig så, at manden har forsøgt at bogføre i en anden firmakode, må han så det, ja eller nej. Jeg kan ikke sende et objekt ud til en procesejer, og spørge om en eller anden må få adgang til objektet, men jeg kan lave oversættelsen, Peter har bedt om at få lov til at bogføre i firmakode 3000, er det okay? Det kan procesejeren tage stilling til. Den oversættelsesopgave har vi, men på det tekniske niveau, nu kan jeg se, men det er måske en provokation, men det er jo decideret autorisationsobjekter, du har taget med på din slide. Det er jo hardcore teknik, som aldrig forlader autorisationskonsulenten. Nogen gange kunne man da håbe, at der var et par programmører, der kunne nogen af dem, men det er så en anden snak.

M5: Det er da meget sejt, det I har ude i DONG.

M9: Vi har sådan et dataråd, hvor de snakker om forskellige kritiske felter, hvor de diskuterer, hvem må vedligeholde det her, hvad er validt, og hvad er ikke? Det er forretningen, der er faktisk ikke IT ressourcer med i det her.

M6: Det er jo også tegn på stor modenhed inden for løsningen, man er nået dertil, at man kan tage stilling til dataindholdet.

M1: Der har man jo egentlig også adskilt de tekniske niveauer fra forretningsdelene. Jeg går ud fra, I bare får at vide, at Peter må ikke vedligeholde de 3 felter, kan I få det til at virke?

I er rimeligt enige om, at ledelsen ikke behøver at kende autorisationsobjekterne, og det lyder også let nok, at der bare er en der oversætter, og så spiller det hele. Er det også jeres erfaringer? At ledelsen er fuldstændig klar over, hvad de er ansvarlige for, og der skal bare være den der tolk.

M1: Min erfaring mange gange er, at det er svært at få ledelsen involveret i det niveau de bør involvere sig på. Det kan være en lidt hårdere kamp mange gange end at tage en snak med procesejeren.

M2: Jeg synes også, at den her oversættelsesopgave den ligger hos os, fordi den ikke kan ligge andre steder, ikke fordi vi er bedre til det, det er vi måske, men det er vores opgave at oversætte det her til et forståeligt forretningssprog, som gør det muligt for procesejere at tage stilling til de spørgsmål de har.

M5: Det er jeg faktisk direkte uenig i. Fordi hvis du sidder og oversætter det. Så kan de ikke tage det ansvar. Så tager du det ansvar fra procesejerne i at forstå deres processer. De skal forstå hvordan de autoriserer til dem, for at kunne stille de reelle krav. Det er mere som et joint venture, du skal hjælpe dem med at komme med ideerne, og de skal stadig forstå, hvad er deres kritiske objekter, kritiske værdier, inden for deres procesområde.

M10: En af de indbyggede faldgrupper der kan ligge i, at de slet ikke forstår teknikken, det er, at risici slet ikke går op for dem. Spørger du lederne, så er de mange gange slet ikke klar over, at man kan sidde i Danmark og bogføre i Kina, nå, kan man det i et SAP system? Det var da spændende. Kan de så også i Kina bogføre i Danmark? Ja, det kan de også. Det må de ikke. Nå, okay. Det er fordi, de ikke forstår teknikken, de forstår ikke opbygningen af SAP

M6: Det er tilbage til en gammel diskussion. En af de ting vi skal gøre, er jo at høre efter, den simple logik de har, at det her må man bare ikke kunne, fordi det er forskellige juridiske ting, de måske heller ikke mener, man skal forklare ned. Det er to forskellige kasser. Det er lidt sådan, jeg ser det.

M7: jeg sidder og tænker på, at vi er gået tilbage til slide 1, omkring de her diskussionspunkter der siger, er vi håndværkere eller er vi konceptmagere, eller hvad er vi? Er vi overhovedet tæt på denne her ledelse, når det her foregår? Nej, det er vi typisk ikke. Vi ligger og har måske projektledelsen at snakke med, men det er typisk ikke ledelsen. Så spørgsmålet er, om vi snakker teknik med procesejerne, men det er jo sjældent, at det er oppe på ledelsesniveau, dem vi snakker med, for er projektet gået i gang, så har ledelsen godkendt og blåstemplet projektet, og så gider de ikke høre mere om det, så har de andre ting at beslutte. Hvis det er store virksomheder vel at mærke. Spørgsmålet er hvad vi egentlig diskuterer her? Diskuterer vi op imod procesejere, diskuterer vi drift, diskuterer vi projekt, hvad er det egentlig, vi diskuterer? Fordi det er nogle forskellige mennesker vi skal have til at involvere, og skal have til at tage ansvar, og træffe nogle beslutninger, og hvis vi går tilbage til udgangspunktet, er vi så de her håndværkere, der kommer ind, når alle beslutningerne er taget, og bliver sat ind i projektet, og skal til at arbejde, eller står vi egentlig og er med til at præge, hvad det er for et projekt, der skal sættes i gang, og hvad det er for nogen forudsætninger, der skal være for det. Fordi derude, uden for KMD, der bliver ikke brugt lige så meget krudt på at sætte sig ned, og lave store evalueringer af hvordan kan vi lave det her, fordi man skal ikke lave det så mange gange. Man skal typisk lave det én gang. Så ringer man til autorisationsmanden, når alle beslutningerne er taget, og så bliver han altså håndværkeren, om han vil det eller ej. Ellers skal personen have meget gennemslagskraft, hvis han skal kunne spole tiden tilbage, og så stille nogen krav til en ledelse som har truffet en beslutning om at implementere SAP.

M6: Der er en af de store forskelle. Vi sidder 3 grupper ved bordet. Om end man kan lide det eller ej. Den interne ressource har en væsentlig bedre føling, med hvad der sker i biksen. Det får man. Den eksterne kommer ind, hyret til en opgave der er defineret på forskellige måder, det kan være som håndværker eller være hyret ind tidligere som assistance. Og så kommer de store og slemme til sidst, og i mange tilfælde siger, at i det her har I nogen store huller. Har I tænkt over det her? Kigger revisionsrapporterne igennem, og siger, de her står pivåbne. Det er ikke godt, I har et problem. Den rolle kommer jo også ind. Når vi sidder her, så er vi jo ikke kun konsulenter, der sidder her, vi kommer ind med forskellige vægtstange. Der er nogen forskellige faser.

M11: Der er to forskellige ting, som jeg ser det, om man kan få ledelsen involveret. Det er, om de ser det som et IT system, det er IT, så det er teknik, eller om de ser SAP som et forretningsprojekt. Så bliver det nemmere, sådan som jeg ser det, at få involveret ledelsen, for så ved de, at denne her del af SAP det er mit område, fordi det er en del af min forretning,

M1: Jeg har gode erfaringer med at få ledelsen involveret ved at komme ud og sige, ved I hvad, jeg skal bare bruge 20 minutter, vi skal lige have fastlagt de overordnede retningslinjer for det her. Du starter med folk længere nede i organisationen, så kan du sagtens, som konsulent og også som intern, lave et dokument på 1-2 sider, som du kan præsentere for en styregruppe, det her det er de helt overordnede retningslinjer for jeres sikkerhed og for jeres system, og mange gange så læser de det igennem, og indrømmet engang imellem så nikker de og siger, det ser meget fint ud, men fint, så er det blevet besluttet på styregruppen et eller andet sted, og så behøver de ikke være involveret længere, og når der så kommer nogen bagefter og siger, jeg skal have SAP All, så kan man sige til dem, jamen for 9 måneder siden besluttede de på det og det møde, at det er der ikke nogen der har, men du kan gå op og banke på oppe ved direktøren, og hvis han siger, at det er ok, at vi laver beslutningen om, så får du det. Du kan være sikker på, at manden går aldrig op og banker på, men du er fri for at tage diskussionen, du får de overordnede rammer, du skal have.

M7: Så er du tilbage til, at vi fortæller ledelsen, hvordan de skal tænke. Det er jo egentlig ikke meningen med alt det her. Det er jo meningen, at vi skal spørge ledelsen, hvad de havde forestillet sig,

M1: Måske at spørge organisationen, hvordan er jeres kultur, hvordan ønsker I, det her skal strikkes sammen? Og så få det her faciliteret og så ligge det op til ledelsen som så blåstempler det. Fordi mange gange når du kommer ned i organisationen, så ved de godt, hvad retningslinjerne er. Altså er det her en virksomhed, hvor man ikke må se på tværs af cost centrene, er det her en virksomhed hvor man ikke må kunne se lønposteringerne, eller gå over i FI delen, hvad er det her for en gesjæft?

M5: Diskussionen ville også være skarpere, hvis der i stedet for at stå ledelsen stod forretningen overfor IT.

M3: Jeg tænkte bare, at diskussionen ville have været lidt anderledes, hvis man havde formuleret det, eller havde sagt, er ovenstående korrekt og bør ledelsen overhovedet forstå værdien, af det man kommer ind i de

tekniske niveauer? For mig handler det om, at hvis de forstår, at det input man putter i der, hvor vigtigt det er, så vil de også ligge mere pres på, at de folk der sidder med processerne i forretningen, gider at sætte sig ind i det, og så får man det input, til den der sidder og udvikler det, som sætter konceptet op, som man egentlig mangler. Ledelsen skal forstå værdien af, at den her funktion vi putter ind, at den er rigtig. Så har man det på plads.

Her til sidst lige for at følge op på det fra før, er det så en dårlig ting at være håndværker, eller er det ikke en dårlig ting? I sagde, at man får besked på at lave noget, og så laver I det, men er det ikke også godt nok? Altså, der var det med kontinuitet, og overlevering, men det kan man vel stadigvæk gøre.

M7: Jeg synes jo egentlig, at det er fint, at man skelner imellem det, at man ser folk med forskellige kompetencer som noget godt. Nu har jeg været i konsulentbranchen i en del år, og jeg har altid set det som en fordel, hvis man har et team, hvor der er nogen, der er mere teknisk funderede, og nogen der er mindre teknisk funderede, nogen der er mere ovre mod projektledelse, nogen der er mere ovre mod at lave metode, strategi og koncepter og så videre, og så egentlig bruge de forskellige kompetencer til at få lavet det, i stedet for, at man kræver af folk, at de skal kunne det hele, det er typisk meget svært for folk, at både kunne bore sig langt ned i teknikken men så samtidig også lave konceptet. Så derfor synes jeg det er en fin deling. Den kan måske så endda fininddeles mere.

M3: Det kommer an på hvor man er, altså hvis man er så langt, som de for eksempel er ude ved Heidi, jamen der får man klart beskrevet, hvad det er, du skal lave. Det her det er opgaven. Gør det. Så er det jo håndværkeren, man har brug for. Hvis opgaven er meget mere udefineret, så er det ikke nok med en håndværker.

M7: Jeg synes altid, et eller andet sted, man har brug for det, for der er altid brug for at udfordre, det der engang er lavet, udfordre det eksisterende koncept. At kunne sige, SAP har lavet om på deres måde at tænke på, okay måske skulle vi lave om på vores koncept. Derfor er det ikke sådan, at man bare siger, vi skal bare bruge en håndværker, og så kører vi med det de næste 20 år, men at man løbende har den der dialog enten fordi, at man er en sammensat person, der både kan tænke koncepter og lave håndværket, eller man er et team, der har forskellige kompetencer.

M3: Hvis det nu er en proces, altså man har lagt det ud, at procesejerne har påtaget sig det ansvar, og har taget den dialog altså med at følge med, og nu sker det noget nyt, nu er der nogle ændringer, at de tilpasser sig, okay nu er det sket noget her, det her skal vi have lavet om. I princippet også, jamen, der er kommet et nyt objekt, der skal lægges ind, og sender den information ned til håndværkerne.

M7: Så du siger, at der er nogen uden for autorisationerne, der gider at beskæftige sig med autorisationer. Det har jeg aldrig hørt før.

M10: Jeg tror det er helt nødvendigt, at det er håndværkerne. Hvis du tager en universitetsuddannet professor i revisionsteori, og siger til ham, du har to dage til at lave de her roller, det kan jo ikke lade sig gøre, så alene af den årsag, er det mere en teoretisk diskussion.

M1: Et eller andet sted så har jeg det sådan, at det er vel okay at være håndværker. Jeg vil da sætte pris på, at den håndværker der kommer hjemme hos mig siger, at jeg har skimmelsvamp, og ikke bare lukker hullet, og det mener jeg da, er vores pligt, når vi kommer ud til kunder som håndværkere, at sige, hov, du skal være opmærksom på sådan og sådan.

M4: Du spurgte sådan ligefrem, om det var godt eller skidt at være håndværker. Jeg synes, det er et sjovt spørgsmål. Begge dele er godt.

Det jeg prøvede at komme frem med, var at fordi der er mange håndværkere, så mangler der også koncepter. Og hvad så? Gør det noget?

M4: Det er ikke kun inden for autorisationer, det er SAP verdenen generelt. Det gør noget, ja, der skal struktur på.

M2: I virkeligheden så har vi også denne her situation, hvor vi har projekter der bliver implementeret løbende, og så har vi nogle driftperioder. I driftperioderne der er behov for håndværkerne. Man laver et autorisationskoncept, det kører et par år, og så laver man et nyt. Så håndværkeren er god i mellemperioden, og teoretikeren er god, når der skal laves noget nyt, så det afhænger vel også af, hvilken situation man er i. Hvis man skal lave et eller andet stort og konceptuelt, så nytter det jo ikke noget at have en teoretiker, så skal man have en håndværker, der kan lave de lavpraktiske ting.