Cand.merc.aud-studiet

Institut for Regnskab og Revision

Kandidatafhandling

IT-sikkerhed i en dansk produktionsvirksomhed

Studerende:

_____
Jesper Gravlund Nielsen

Vejleder:

Per Rhein Hansen

Afleveringsdato: 7. oktober 2008

Copenhagen Business School 2008

Indholdsfortegnelse

1. English summary

The purpose of this assignment is to focus on the IT-security of a Danish manufacturing company. First of all, it is described in this assignment, that the Danish law “aktiesekskabsloven” requires members of the board of directors and the management of Danish limited companies, to assure a reasonable administration of the values in the company. This includes a reasonable administration of the IT in a company, if the existent of a company, among others, depends on IT.

This assignment is a study of IT-security in a Danish manufacturing company, which existence, among others, relies of IT, because of the complexity in the production in the company, and administration of the company.

In this study of the IT-security in the company, the assignment has its starting point of a description of how the company is working with IT. Afterwards a risk analysis is prepared and shows which areas of the IT, that needs more attention from the management of the company, or by the IT-department. The Danish standard – DS 484 – which is an approved Danish code of practice for information security management, is used as model of the preparation of a risk analysis.

The assignment includes recommendations to the company, which will insure an acceptable IT-security of the company. The main recommendation to the company is to get more commitment from the management to the issues of IT-security. This will insure an acceptable, because the commitment from the management will show the impotence of an outstanding IT-security, to the employees in the company. Leading by example, is the most effectiveness way, to show commitment.
Also, the commitment from the management insures, that the IT-department of the company, will know which IT-assets, that is the most important to protect. This priority of protection of IT-assets will not be effective, if it isn’t made by the management, because of the lack of business-understanding from the head of the IT-department.
At last, the commitment from the management insures that the company’s dependence of persons in IT-department will be reduced.
Overall, the recommendations will insure a better IT-security in the company.

2. Forord

Denne kandidatafhandling er udarbejdet, som det afsluttende projekt, på Cand.merc.aud studiet, på Handelshøjskolen i København (CBS)

Afhandlingen er udarbejdet, som et konkret studie af produktionsvirksomheden BB A/S´ IT-sikkerhed, samt anbefalinger fra DS 484 (2005). Derudover omhandler afhandlingen også perspektiveringer til henholdsvis revisors arbejde med henblik på IT-sikkerhed, samt fremtiden for IT-sikkerhed i danske produktionsvirksomheder.

Baggrunden for den valgte problemstilling skyldes, at jeg finder spørgsmålet omkring IT-sikkerhed meget relevant og aktuel, da størstedelen af mellemstore og store virksomheder er afhængig af brugen af IT-systemer.

Den 7. oktober 2008

Jesper Gravlund Nielsen

3. **Indledning**

Baggrunden for at skrive om IT-sikkerhed i kandidatafhandlingen, er interessen for problemstillingerne omkring IT-sikkerhed i danske virksomheder. Denne interesse er bl.a. opstået efter jeg har deltaget i fagene ”Revision” og ”IT-Governance og IT-revision” på Cand.merc.aud-studiet. I forbindelse med disse fag, har der været et tydeligt budskab fra undervisernes side, nemlig at IT-sikkerhed er et overset emne på direktions- og bestyrelsesniveau. Derudover har problemstillingen omkring IT-sikkerhed vagt min interesse via mit arbejde, i et af de større revisionsfirmaer i Danmark. Jeg har herigennem konstateret hvor meget, mange virksomheder, er afhængige af at deres IT-systemer er pålidelige.

For at få en idé om, hvordan problematikken omkring IT-sikkerhed bliver håndteret i en større dansk produktionsvirksomhed, er det blevet aftalt med IT-chefen for BB A/S, at lave et interview hvor der bliver forespurgt til de centrale punkter for hvordan BB A/S arbejder med IT-sikkerhed.

For at en større produktionsvirksomhed, samt alle andre større virksomheder, kan begå sig på markederne med stor konkurrence, kræver det at virksomheden har et fornuftigt omkostningsniveau. Dette niveau bliver bl.a. holdt nede ved en effektiv og pålidelig databehandling, som behandles af IT-systemer. Disse IT-systemer behandler eksempelvis data omkring produktionen, kreditorer, salgs- og leveringsstatus, samt personaledata. Derved bliver virksomhederne afhængig af sine IT-systemer, da førnævnte data er vigtige for driften af virksomhederne.

Når en virksomhed er meget afhængig af sine IT-systemer, skal der stilles krav til systemerne. I den forbindelse finder jeg det interessant, at finde ud af hvem der stiller disse krav og hvordan disse krav formuleres og måles. Derudover bør en virksomhed også overveje hvilke risici der er ved at være afhængig af IT.

Ved at have en aftale med IT-chefen for BB A/S, har jeg fået muligheden for at lave et konkret studie af hvordan dette selskab forholder sig til spørgsmålene omkring afhængigheden af IT.

For at se på hvordan BB A/S forholder sig til at være afhængige af IT, og dermed deres syn på hvorledes IT-sikkerheden i virksomheden skal prioriteres, tages der udgangspunkt i en vurdering af sikkerhedsrisiciene i virksomheden. Denne vurdering skal foretages metodisk, for på den måde at belyse samtlige risici i virksomheden. Vurderingen kan bygge på en risikoanalyse, som skal identificere og prioritere de risici, som virksomheden er udsat for. Denne risikoanalyse skal tage udgangspunkt i de forretningsmæssige forhold for virksomheden, således at ledelsen kan prioritere indsatsen på de forskellige områder, for at sikre et acceptabelt sikkerhedsniveau.
Ideelt set, bør der foretages flere risikoanalyser over tid, som udarbejdes på samme metodiske grundlag, således at ledelsen i virksomhederne kan se resultaterne af indsatsen i virksomheden. Derudover vil løbende risikoanalyser sætte fokus på, hvilke punkter der skal følges op på, for at sikre et fornuftigt niveau for IT-sikkerheden i den enkelte virksomhed.

Som tidligere nævnt, har budskabet i undervisningen på cand.merc.aud-studiet været, at problemstillingerne omkring IT-sikkerhed ikke har den fornødne prioritering på direktions- og bestyrelsesniveau. Dette sker, selvom mange selskaber er afhængige af IT, og ledelsen har pligt til at involvere sig i problemstillingen, da et IT-nedbrud vil være kritisk. Tab af eksempelvis data for bogføringen, vil være i strid med bogføringsloven § 10, som siger at alt bogføringsmateriale skal gemmes i 5 år, fra regnskabsårets udløb.
Derudover kan et større nedbrud, hvor selskabet lider store tab, og i værste vil gå konkurs, vil direktionen og bestyrelsen kunne drages til ansvar, da de ikke har opfyldt betingelserne i aktieselskabsloven. I Aktieselskabslovens § 54 stk. 3 står der følgende:

”*Bestyrelsen skal påse, at bogføringen og formueforvaltningen kontrolleres på en efter selskabets forhold tilfredsstillende måde. Direktionen skal sørge for, at selskabets bogføring sker under iagttagelse af lovgivningens regler herom, og at formueforvaltningen foregår på betryggende måde.*”[1]

Denne bestemmelse kan direkte overføres til problemstillingen med afhængigheden af IT. Hvis et selskabets bestyrelse og direktion ikke sørger for acceptable rammer omkring IT-driften og IT-

[1] www.retsinfo.dk

sikkerheden, overholder de dermed ikke ovenstående lov. Skulle et selskab gå konkurs pga. problemer med IT-driften, vil bestyrelsen og ledelsen kunne drages til ansvar for deres manglende fokus på IT.

Overholdes Aktieselskabslovens § 54 ikke på en tilfredsstillende måde, vil medlemmer af bestyrelsen og direktionen i selskabet kunne blive straffet efter Aktieselskabslovens § 161 med bøde.

Bestemmelserne i Aktieselskabslovens § 54 har tidligere været anvendt, når direktion og bestyrelse ikke har levet op til deres pligter i selskaber og der er derfor ingen tvivl om, at paragraffen håndhæves. Derfor bør denne paragraf tages alvorligt af ledelsen i virksomhederne, også når det kommer til at tage sig sine forholdsregler omkring IT-sikkerheden.

4. Problemformulering

Formålet med denne afhandling, er at belyse IT-sikkerheden i en dansk produktionsvirksomhed og undersøge i hvilket omfang virksomheden forholder sig til at være afhængig af IT. Derudover har opgaven til formål, at komme med konkrete løsningsforslag til hvordan produktionsvirksomheden kan reducere de risici der er forbundet med at være afhængig af IT.

Formålet giver følgende overordnede problemstilling:

- Hvorledes forholder BB A/S sig til at være afhængige af IT, og hvilke handlinger vil kunne reducere risiciene ved at være afhængige af IT?

For at besvare den overordnede problemstilling, er følgende arbejdsspørgsmål udarbejdet:

- Hvordan er BB A/S afhængig af IT?
- Hvordan opgøres afhængigheden af IT i BB A/S og risiciene ved at være afhængig af IT?
- Hvilke risici for IT-sikkerheden er der konstateret i BB A/S?
- Hvilke IT-sikkerhedsforanstaltninger gør BB A/S brug af, for at reducere de konstaterede risici?
- Hvad burde der gøres, for at reducere de konstaterede risici, i IT-sikkerheden?

Derudover søger opgaven at perspektivere følgende spørgsmål:

- Hvad bør revisor være opmærksom på, når en produktionsvirksomhed er afhængig af IT?
- Hvorfor vil der i fremtiden være et stigende behov for IT-sikkerhed i produktionsvirksomheder?

5. Afgrænsning

Det er fundet hensigtsmæssigt, ved udarbejdelsen af denne kandidatafhandling, at afgrænse sig fra at skrive om andre virksomheder end BB A/S. Dette skyldes at kravet til denne opgaves omfang, ikke gør det muligt at komme med sammenligninger til andre virksomheder, samtidig med at der stadig er fokus på de enkelte emner.

Dermed skal læser være opmærksom på at denne opgave ikke giver et entydigt svar på samtlige problemstillinger omkring IT-sikkerhed, men derimod har til hensigt at beskrive og kommentere på hvorledes en enkelt virksomhed arbejder med problematikken. Derudover søger opgaven at komme med konkrete løsningsforslag til den konkrete virksomhed, hvor de i opgaven udarbejdede forslag, ikke nødvendigvis kan bruges i andre virksomheder.

6. Metode[2]

Metoden for udarbejdelse af denne kandidatafhandling, har haft til hensigt, at være velegnet til opnåelse af viden, indenfor de rammer, som formålet med afhandlingen har opstillet. Formålet for afhandlingen har været, at lave et konkret studie af IT-sikkerheden i en dansk produktionsvirksomhed. Når afhandlingen udelukkende fokuserer på en enkelt dansk produktionsvirksomhed, er det en snæver tilgang til at tilegne sig viden omkring hvorledes virksomheder generelt i Danmark arbejder med IT. Derved tilsigter afhandlingens emne og konklusion ikke en universal løsning på samtlige IT-sikkerhedsmæssige problemstillinger.
Der arbejdes udelukkende med en enkelt virksomhed, og indledes med en risikoanalyse, for at kunne påpege de væsentligste problemområder, dvs. for at kunne specificere behovet for IT-sikkerhed.

Den danske standard for informationssikkerhed, DS 484 (2005) er valgt, dels som model for udarbejdelse af en risikoanalyse i produktionsvirksomheden BB A/S, samt udgangspunkt for formulering af anbefalinger vedrørende forbedret sikkerhedsforanstaltninger. Dette skyldes, at DS 484 (2005) har været den mest oplagte standard, frem for eksempelvis rammeværktøjer, som COSO ERM (2004) eller CobIT (2007), da disse ikke er ligeså operationelle. DS 484 (2005) kommer med konkrete løsningsforslag til konkrete problemstillinger, og dermed har denne standard de bedste forudsætninger til at anskueliggøre problemstillingerne og løsningsforslagene, indenfor formålet af denne kandidatafhandling.

Strukturen på opgaven har til formål at guide læseren igennem opgaven. Det tilsigtes, at opgaven har en "top-down" fremstilling, hvor der i starten beskrives hvorledes ledelsen i BB A/S forholder sig til problemstillingerne omkring IT-sikkerhed. Derefter bliver der fokuseret på niveauet under ledelsen, som er den daglige IT-drift, herunder hvorledes IT-afdelingen arbejder med IT-sikkerhed og hvorledes de daglige brugere arbejder med IT-systemerne.

Den i opgaven udarbejdede risikoanalyse, samt forslag til forbedringer i BB A/S, udgør hoveddelen af afhandlingen. Denne del er opbygget på baggrund af DS 484 (2005), som er sekundær litteratur. Derfor

[2] Metodeafsnittet er skrevet på baggrund af bogen: ”Den skinbarlige virkelighed”, samt følgende artikel: http://da.wikipedia.org/wiki/Videnskabelig_metode

har behovet for anden sekundær litteratur været mindre end hvis opgaven havde været opbygget på andre måder. Derved gør omfanget af afhandlingen, at det er fundet hensigtsmæssigt at begrænse søgningen af sekundær litteratur. Som alternativ, kunne hoveddelen af afhandlingen have taget udgangspunkt i de enkelte informationsaktiver, hvorfor en anden tilgang til valg af metoden, ville være en fordel.

Som primær kilde til opgavens problemstilling er der anvendt interview, samt løbende samtaler, med IT-chefen for BB A/S[3]. Derudover er der gennemført et mindre interview, og der har været løbende samtaler med medarbejderen PP, som er ansat for en koncernforbundet virksomhed, hvor IT-chefen for BB A/S ligeledes er IT-chef. Det er blevet vurderet, ud fra samtale med både IT-chefen, PP, samt vejleder for denne opgave, at PPs udsagn er ligeså gyldige som en ansat hos BB A/S. Grunden til at PP er udvalgt, skyldes bl.a. at PP tidligere har været ansat i BB A/S i mere end 15 år og først indenfor det sidste år, har skiftet arbejdsplads til EE A/S, der ligesom BB A/S ejes af den irske koncern CC plc.

Beskrivelsen af BB A/S´ arbejde med IT-sikkerhed, tager udgangspunkt i et delvist struktureret interview lavet med IT-chefen d. 16. april 2008. IT-chefen for BB A/S har det daglige ansvar for IT-sikkerheden mm. i virksomheden. Interviewet blev lavet, ved at stille spørgsmål om BB A/S, med udgangspunkt i DS 484 (2005). For at komme endnu mere i dybden, end de direkte spørgsmål lægger op til, blev der ved slutningen af interviewet lagt op til, at IT-chefen selv kunne komme med supplerende bemærkninger, som der ikke var snakket om, under det struktureret forløb af interviewet. Under denne del blev tiden brugt til at snakke om diverse emner omkring virksomheden generelt, samt at uddybe emner der allerede var diskuteret. Derudover blev der berørt forhold der ikke tidligere var belyst, for at få yderligere kommentarer, der ikke tidligere var blevet snakket om.
Det har i forbindelse med udarbejdelsen af denne afhandling ikke været muligt at komme i kontakt med ledelsen af BB A/S, selvom dette var stillet i sigte. I den forbindelse, ville det havde været interessant at lave et interview med ledelsen, for at få dens syn på, og overvejelser omkring, IT-sikkerheden i BB A/S. Derudover ville det være interessant at høre hvilke forudsætninger ledelsen har for at arbejde med IT-sikkerhed, samt få dens holdninger om hvorledes IT-sikkerhed i BB A/S skal prioriteres.

[3] Se bilag 1 – Interviews i forbindelse med afhandling

Denne afhandling er anonymiseret, da oplysningerne i opgaven kan være kritiske for virksomheden. Vejleder for denne afhandling er bekendt med virksomhedens identitet.

7. Kildekritik

Det er især den primære kilde til opgaven, IT-chefen, hvor det er nødvendigt at forholde sig kritisk til de oplysninger, han er kommet med, i forbindelse med interviewet. IT-chefen har en interesse i at fremvise virksomhedens positive sider, idet denne selv er ansat i virksomheden og at det er ham der har ansvaret for driften af IT i BB A/S.

Det er dog min opfattelse, via interviewet der er lavet med IT-chefen, at han har været ærlig og kritisk overfor sit eget arbejde. IT-chefen har under interviewet selv bragt problemstillinger op, som har været problematiske for BB A/S.

Undervejs i de løbende samtaler og under interviewet, har IT-chefen beskrevet ledelsens synspunkter på forskellige problemstillinger. Disse beskrivelser er anvendt i opgaven med skepsis, men i og med, at en del af beskrivelserne har været kritiske overfor IT-afdelingen generelt og ham selv i særdeleshed, er det vurderet at beskrivelsernes validitet har været gode nok, til at kunne bruges i denne afhandling.

8. Terminologi

Anneks B i DS 484 (2005) indeholder et eksempel på hvordan en virksomhed skal gribe en risikovurdering an for IT-sikkerheden. Det er vigtigt at understrege, at når der bliver snakket risiko for en virksomhed ved at anvende IT, snakkes der om hvor stor sandsynligheden for forekomster af uregelmæssigheder er, gange konsekvensen af uregelmæssigheden. Det vil sige følgende:

Risiko = Sandsynlighed x Konsekvens

Det anbefales i anneks B, at virksomheder laver en risikoanalyse. I denne analyse bør der oplistes potentielle trusler, for derefter at blive vurderet en efter en. Denne vurdering skal gå på hvor stor sandsynlighed der er for at truslen bliver til virkelighed, samt hvor stor en konsekvens der vil være forbundet med at truslen rammer virksomheden.

Forretningsmæssige risici for en virksomhed, er de risici, der er forbundet med virksomhedens brug af IT. Det vil sige de potentielle skadende situationer, der med en vis sandsynlighed skader virksomheden, hvis der sker et brud på IT-sikkerheden.

En trussel for en virksomhed, er defineret som ”en skadevoldende eller sikkerhedstruende hændelse, der potentielt kan medføre skade for en virksomhed”[4]. Der skal dog som hovedregel være tale om en potentiel betydelig skade, som der kan opstå, inden en hændelse kan karaktiseres som en trussel.

[4] DS 484:2005, side 104

9. Præsentation af BB A/S[5]

Som nævnt i indledningen af denne afhandling, er det lykkes at få en aftale med BB A/S, om at skrive omkring IT-sikkerhed i denne virksomhed. BB A/S fremstiller betonelementer, primært til industrien, i forbindelse med opførsel af nye byggerier. Selskabet er ejet af den irske koncern, CC plc., som har en samlet omsætning, på mere end 700 mia. kr. og flere end 60.000 medarbejdere.

BB A/S havde i 2006 en omsætning på ca. 635 mio. kr., et resultat før skat på ca. 74 mio. kr. og havde knap 600 medarbejdere. De knap 600 medarbejdere er fordelt på seks fabrikker, fordelt rundt om i Danmark. Selskabets primære marked er det danske, men selskabet eksportere også betonelementer, hvor det især er det nordtyskland marked, der aftager produkterne.

Produktionen af betonelementer foregår i store produktionshaller, hvor alt fra start til slut styres af virksomhedens IT, eksempelvis blandingsforhold af ingredienser i betonen, samt lagerstyring og produktionsrækkefølgen.

BB A/S tegner, i samarbejde med virksomhedens egne arkitekter, de enkelte elementer, der skal bruges til byggerierne. Dette sikrer at kunderne altid kan lave deres byggerier ud fra egne ideer og ikke udelukkende via standardløsninger. Arkitekterne benytter sig af programmer på computere, til at tegne de enkelte elementer, ud fra kundernes ønsker og behov. Hvis ikke tegnerne kan få adgang til computerne på arbejdspladsen, vil det være umuligt for dem at tegne de skabeloner, der skal bygges elementer ud fra og derved vil produktionen gå i stå.

Derudover har BB A/S også en udviklingsafdeling, som i samarbejde med ingeniører og entreprenører udvikler elementer, så de kan leve op til nye standarder, indenfor eksempelvis varmeisolering, holdbarhed og reaktioner på brand. Processen med udvikling af betonelementer, sker blandt andet med hjælp fra IT, idet resultaterne af udviklingen gemmes og bearbejdes, inden nye udviklingsinitiativer påbegyndes. Dermed er hele udviklingsafdelingen afhængig af en stabil IT-drift.

[5] Informationerne omkring BB A/S er hentet fra virksomhedens hjemmeside, selskabets årsrapport for 2006, samt i forbindelse med interviewet af IT-chefen i BB A/S.

BB A/S´ fokusområde er produktion af betonelementer, men kan også være behjælpelig med montering og transportering af elementerne, til byggepladser. Disse processer kræver intens planlægning, som skal koordineres meget struktureret. Dette foretages fra hovedkontoret i Jylland. For produktionen, gælder det blandt andet om, at have adgang til computerne, hvis der skal laves blandingsforhold for betonen til skabelonerne, som afviger fra standarden. Hvis IT-driften går ned, vil produktionen godt kunne fortsætte i kortere tid, idet der altid er skabeloner, som produktionen kan gå i gang med. Dog kan produktionen blive ramt, hvis IT-systemerne er nede i mere end en dag.

For at BB A/S kan få succes på det konkurrencepræget marked for betonelementer, er det vigtigt at produktionen er stabil, således at kunderne kan regne med de leveringstider, der bliver fastlagt ved indgåelsen af kontrakten. Denne stabilitet skal blandt andet sikres, ved at have pålidelige IT-systemer, således at virksomheden ikke pludselig må holde en ufrivillig produktionspause, på grund af fejl ved IT.

BB A/S er ligeledes afhængig af, at der ikke slipper fortroligt materiale ud til hverken kunder eller konkurrenter. Hvis dette sker, kan det betyde at virksomheden går glip af ordrer, da eksempelvis arkitekttegnede tegninger, vil kunne misbruges af konkurrenter. Derudover kan bud på ordrer blive marginalt underbudt, hvis oplysningerne kommer til kendskab for kunder eller konkurrenter.

BB A/S står stærkt til udfordringerne i fremtiden, hvor de generelle betingelser for den danske byggebranche bliver dårligere, som følge af især den globale økonomiske nedtur. Derudover regner virksomheden med at der kommer strengere krav til blandt andet isolering fra myndighedernes side, hvilket giver flere omkostninger til BB A/S. Dermed bliver det dyrere at bygge nye domiciler for virksomheder og nye boligbyggerier, hvilket vil gøre det mindre attraktivt at bygge nyt.

Disse udfordringer, som virksomheden står overfor, forventes at have en indflydelse for den fremtidige arbejdsgang, hvor BB A/S blandt andet vil prøve at effektivisere produktionen. De nye udfordringer stiller også store krav til stabiliteten af produktionen, hvorfor IT-området vil have en nøglerolle for at sikre denne stabilitet.

10. IT-rammeværktøjer

Når en virksomhed beslutter sig for at sætte fokus på IT-sikkerheden, er der flere indgangsvinkler til hvorledes dette kan foregå. Valg af rammeværktøj, eller standard, har betydning for i hvilket omfang detaljeringsgraden af anbefalingerne bliver, indenfor IT-sikkerhed. I dette afsnit vil nogle af de værktøjer der findes, blive beskrevet.

Set fra et internationalt perspektiv, er der sket en udvikling i løbet af de sidste 10-15 år, hvor IT-sikkerheden er kommet mere og mere i fokus. Denne udvikling kan ses, når man kigger nærmere på de tre internationalt anerkendte rammevæktøjer, COSO Internal control – Integrated framework fra 1992, COSO Enterprise risk management – Integrated framework fra 2004 og CobIT framework version 4,1 fra 2007.

COSO fra 1992 fokuserer på rutinerne omkring intern kontrol, der defineres, som en proces, der er udarbejdet af ledelsen i virksomheden, til at være en acceptabel forsikring for ledelsen, i at opnå de mål der er opsat. Disse mål indeholder arbejdsgangene for at sikre en effektiv udnyttelse af ressourcerne i virksomheden, pålideligheden ved regnskabsaflæggelse, samt overholdelse af relevant lovgivning. Intern kontrol i COSO fra 1992 indeholder 5 emner, som er:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

Disse 5 emner bliver beskrevet enkeltvis i COSO (1992). Det er kun få steder i dette rammeværktøj, at der bliver beskrevet noget omkring IT. Dog er der flere steder, hvor ledelsen i en virksomhed bør blive opmærksom på problemstillingerne omkring IT, hvis ledelsen vælger COSO – Internal Control (1992). Eksempelvis indenfor emnet Risk Assessment, hvor det bliver beskrevet, at ledelsen i en virksomhed bør være opmærksom på de krav der bliver stillet til risikostyringen i virksomheden, når der kommer

ny teknologi. Dette kan direkte overføres til de nye teknologier der hele tiden kommer indenfor området IT. De nye teknologier, som virksomheden tager til sig, kræver opmærksomhed fra ledelsens side, da nye teknologier indeholder nye risici, som der bør tages stilling til. Ledelsen bør her finde ud af i hvilken grad, virksomheden bliver afhængig af denne nye teknologi, hvordan denne nye teknologi skal beskyttes og hvorledes virksomheden skal reagere, hvis der opstår problemer. Ligeledes under emnet Risk Assessment, stilles der krav om, at der udarbejdes en risikoanalyse. Denne risikoanalyse skal indeholde samtlige trusler for virksomheden, herunder hvilke trusler der er forbundet med IT. Men da COSO Internal Control (1992) ikke specifikt indeholder emner omkring IT-sikkerhed, bliver denne risikoanalyse meget bred, for at overholde kravene i rammeværktøjet. Dermed vil denne risikoanalyse blive meget bred og vil kræve mange ressourcer fra virksomheden, og kun en mindre del af risikoanalysen vil indeholde problemstillingerne omkring IT-sikkerheden.

Når ledelsen har udarbejdet emnerne omkring Risk Assessment i COSO Internal Control (1992), skal procedurerne for dette kontrolleres. I emnet Control Activities, er der beskrevet hvorledes IT kan hjælpe med at kontrollere emnerne i Risk Assessment. Det er i Control Activities, at der bliver beskrevet mest omkring IT i COSO Internal Control (1992). Det bliver blandt andet beskrevet vigtigheden i at kontrollere rutinerne omkring at tage back-up af data i virksomheden. Herudover beskrives vigtigheden for at der er sikkerhed omkring implementering og vedligeholdelse af systemsoftware i virksomheden, samt vigtigheden af, at der er fornuftige adgangskontroller til data og systemer i virksomheden. For at leve op til kravene i COSO Internal Control (1992), kræves det, at der løbende bliver lavet evalueringer på kontrolaktiviteterne, når der er ændrede forhold for risikostyringen.

Udover ovenstående emner i COSO Internal Control (1992), stilles der i rammeværktøjet krav om, at der er en fornuftig information og kommunikation i virksomheden. Dette kan direkte overføres til vigtigheden for at der er en åben kommunikation fra ledelsen til medarbejdere, omkring IT-sikkerheden i virksomheden. Ligesom at en god kommunikation fra ledelsen side vil være med til at forbedre forholdene for intern kontrol, vil en åben kommunikation omkring IT-sikkerhed, ligeledes skabe bedre rammer for dette. Det skyldes, at ledelsen ved en god kommunikation, viser engagement overfor emnet og dermed synliggøres emnet og vigtigheden overfor medarbejderne.

Derudover kræver COSO Internal Control (1992), at der er en fornuftig overvågning af de forskellige emner i rammeværktøjet. I den forbindelse skal, bør det være IT-afdelingen i virksomheden, der bør være daglig ansvarlig for opgaverne omkring overvågning af IT-sikkerheden, imens ledelsen skal overvåge IT-afdelingen, for at være sikker på at opgaverne bliver udført, da det er ledelsen der har ansvaret for dette.

I 2004 blev COSO Enterprise Risk Management – Integrated framework, herefter benævnt COSO ERM, udarbejdet. Her flyttede fokus sig fra intern kontrol, som i COSO Internal Control, til at omhandle risikohåndtering i virksomheden. Udgangspunktet for COSO ERM (2004) er, at virksomheder opererer i en verden af usikkerheder. COSO ERM (2004) har til formål at få ledelserne til at udarbejde en oversigt over de risici der er forbundet med at drive hver enkelt erhvervsvirksomhed. Dermed finder ledelserne ud af risiciene for virksomheden og kan efterfølgende evaluere, om disse risici stemmer overens med den ønskede risikoprofil for virksomheden. For at finde ud af, om virksomheden har den ønskede risikoprofil, er det vigtigt at ledelsen starter med at gøre sig klar, i hvilket omfang virksomheden skal påtage sig store eller små risici, i bestræbelserne på at opnå profit til ejerne.

Hvor COSO Internal Control (1992) indeholdte 5 emner, indeholder COSO ERM (2004) 8 emner, som der bliver beskrevet i rammeværktøjet. Disse 8 emner er:

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control activities
- Information & Communication
- Monitoring

I forhold til COSOs rammeværktøj fra 1992, er risikobegrebet i COSO ERM (2004) blevet uddybet, til nu at indeholde identifikation, styring og svar på de risici der er forbundet med at være virksomhed. Disse 8 emner skal sikre de 4 mål, der er udarbejdet i COSO ERM (2004), som udover målene i COSO Internal Control (1992), nu også indeholder et overordnede strategisk mål for virksomheden. Dette strategiske mål, skal sikre at ledelsen følger en overordnet strategisk målsætning for virksomheden.

Et af hovedpunkterne i COSO ERM (2004), er at ledelsen skal udarbejde en risikoprofil for virksomheden, som ledelsen er klar til at forfølge. Set i sammenhæng med IT-sikkerhed, skal ledelsen på forhånd gøre op med sig selv, hvilke risici virksomheden skal være villig til at løbe, ved udarbejdelsen af IT-sikkerheden. Ledelsen skal ligeledes udarbejde hvilke mål, der skal sikres, for at IT-sikkerheden lever op til forventningerne. Derudover er der en række generelle anbefalinger omkring risikostyring i COSO ERM (2004), som direkte kan overføres til IT-sikkerheden i virksomheder. Heriblandt at ledelsen skal sørge for at der er den nødvendige kompetence tilstede i virksomheden, for at kunne leve op til den ønskede risikoprofil, samt at ledelsen skal sørge for den rette organisatoriske opbygning.

Som tidligere nævnt, er risikobegrebet blevet uddybet i COSOs rammeværktøj fra 2004, i forhold til det tidligere fra 1992. Risikobegrebet indeholder i COSO ERM (2004) de 3 emner: Event Identification, Risk Assessment og Risk Response. I forhold til IT, er der en række områder, hvor dette bliver berørt. Det gælder blandt andet forholdene omkring identifikation af problemstillingerne ved IT, herunder risikoen for nede-tid på IT-systemerne, samt muligheden for besvigelser vedrørende transaktioner der foretages i virksomhedens IT-systemer. Håndteringen af den risiko der er, ved at være afhængig af IT, skal bygge på et estimat for sandsynligheden og konsekvensen for hvert enkelt identificeret risiko. Dette skal ske på samme vilkår, som alle andre områder i virksomheden, hvor der er samme grad af afhængighed, eksempelvis afhængigheden maskiner i produktionen. Herefter skal ledelsen finde ud af hvorledes den ønsker at imødekomme de risici der er blevet identificeret og vurderet. Dette skal blandt andet foregå via en ”cost-benefit” betragtning, hvor ledelsen skal finde ud af i hvilket omfang det er nødvendigt at sikre sig imod de konstaterede risici, i forhold til de ressourcer det koster for virksomheden.

Udover ovenstående, skal ledelsen i en virksomhed, for at leve op til kravene i COSO ERM (2004), sørge for gode kontrolaktiviteter for de foranstaltninger der blev besluttet at indføre under imødegåelsen af de identificerede risici. Set i forhold til COSO Internal Control (1992), er der i COSO ERM (2004) langt større fokus på IT. Dette indebærer en beskrivelse på hvilke kontroller der bør være omkring IT i en virksomhed, som er afhængig heraf. Beskrivelsen inkluderer kontrolaktiviteter omkring den overordnede styring med IT, IT-infrastruktur, styringen af sikkerheden for IT, samt beskrivelse af udvikling af nye programmer. Derudover beskrives flere måder til, hvorledes ledelsen kan sikre, at valideringen af data er på et højt niveau, eksempelvis ved at sammenligne data fra gang til gang.

Ligesom i COSO Internal Control (1992), stiller COSO ERM (2004) krav om, at der er en god kommunikation fra ledelsen side, samt at ledelsen sørger for at overvåge emnerne. Den gode og åbne kommunikation skal vise, at ledelsen har et stort engagement indenfor en god risikostyring, herunder en høj IT-sikkerhed. Derudover sikrer en god kommunikation, at alle i virksomheden er klar over vigtigheden af en god risikohåndtering. Ledelsen skal ligeledes sørge for, at der er en fornuftig overvågning omkring emnerne, således at ledelsen hele tiden kan leve op til deres ansvar om at sikre en god ledelse af virksomheden.

Samlet set, er der sket en meget større fokusering på IT, fra COSO Internal Control (1992), til COSO ERM (2004). I 2006 blev CobIT udgivet, og dermed blev der sat yderligere fokus på problemstillingerne omkring IT.

CobIT integrerer COSO Internal Control (1992) i deres rammeværktøj for IT-governance. CobIT - version 4,1 blev udgivet i 2007 og er den seneste udgivet version. CobIT (2007) består af 4 emner indenfor driften af IT. De 4 emner er:

- Plan & Organise
- Acquire & Implement
- Deliver & Support
- Monitor & Evaluate

De 4 emner er opdelt på i alt 34 processer. Disse processer indeholder hver en beskrivelse af hvorledes IT i en virksomhed bør organiseres og er med til at synliggøre overfor ledelsen i virksomheden, hvilke ting der skal overvejes for hver proces, samt hvilket mål der bør være for de enkelte processer.

Dermed går CobIT (2007) yderligere i dybden med hvilke forhold IT påvirker driften i virksomhederne, samt hvilke forholdsregler virksomhederne skal tage sig, når de er afhængige af IT. Derudover har CobIT (2007) for hver proces en guideline til, hvor styret processen skal være, dvs. i hvilken grad den enkelte proces overhovedet skal udføres, om den blot skal udføres når der opstår akut behov for det, eller om der skal være en formel nedskrevet forretningsgang for processen, for derved at sikre en optimal proces.

Når der samlet ses på alternative rammeværktøjer for IT-sikkerheden, kan en virksomhed, blandt andre rammeværktøjer, vælge at tage udgangspunkt i COSO Internal Control (1992), COSO ERM (2004), eller CobIT (2007). Samlet set er der sket en udvikling, hvor der er kommet et større og større fokus på IT, i disse internationale rammeværktøjer. Vælges enten COSO Internal Control (1992) eller COSO ERM (2004), er der større fokus på hhv. intern kontrol eller risikostyring, end der er på IT-sikkerhed. Dog er der flere elementer i begge rammeværktøjer, som med fordel kan overvejes i forbindelse med udarbejdelsen af IT-sikkerheden. Dette kan eksempelvis være kravene til at vise ledelsens engagement for IT-sikkerheden, eller kravet for udarbejdelse af en risikoanalyse. Dermed sikres det, at der udover flere andre områder, kommer fokus på IT-sikkerheden.

Vælges det, at tage udgangspunkt i CobIT (2007), får ledelsen et godt værktøj, til at sætte fokus på de områder der er nødvendige, for at have en god IT-governance, herunder en god IT-sikkerhed. CobIT (2007) sætter rammerne for en god IT-governance og der bliver beskrevet hvilket mål hvert enkelt proces har til formål at sikre, samt hvornår hvert enkelt mål er sikret. Dette giver ledelsen i en virksomhed en god baggrund for at arbejde med IT-sikkerhed.
I forhold til DS 484 (2005), er CobIT (2007) mere en guide til ledelsen, for at arbejde med IT-governance. DS 484 (2005) er mere operationel anvendelig, der kommer med konkrete forslag til hvert enkelt punkt, ligesom den er tilpasset danske forhold.

11. DS 484

Baggrunden for DS 484 – "Standard for informationssikkerhed", kommer fra det engelske erhvervsliv, der ønskede at lave nogle retningslinjer for virksomhederne, for hvordan disse kunne opretholde et passende sikkerhedsniveau med hensyn til IT. Efter nogle år blev denne standard mere gennemarbejdet og lavet til en britisk standard (BS 7799) i 1995[6]. Herefter blev standarden oversat til dansk, samt tilpasset danske forhold, hvorefter den første udgave af DS 484 blev udgivet i år 2000. Efterfølgende er standarden blevet opdateret i 2005 og 2005-versionen er den gældende version i dag.

DS 484 (2005) beskriver hvordan virksomheder bør agere overfor udvalgte problemstillinger, som nøje beskrives i standarden. Netop dette, at DS 484 (2005) kommer med konkrete løsningsforslag til, hvordan virksomheden kan agere, for at gøre risikoen ved IT-afhængigheden mindre, skiller DS 484 (2005) ud fra de rammeværktøjer, som beskrevet i foregående afsnit. Den er dermed mere operationel end de føromtalte rammeværktøjer, ligesom det skal holdes for øje, at DS 484 (2005) er tilpasset danske forhold, og dermed er oplagt at vælge for en dansk virksomhed, der ønsker at sætte fokus på IT-sikkerheden.

DS 484 (2005) bliver udgivet af DS Certificering A/S, som bliver ejet af Dansk Standard, der er en organisation under Økonomi- og Erhvervsministeriet. DS 484 (2005) er, ligesom andre standarder fra DS Certificering, udarbejdet af udvalg, som bl.a. kan bestå af personer fra erhvervslivet, interesseorganisationer, myndigheder og universitetsmiljøet. Når en standard skal udarbejdes, kommer initiativet ofte fra dem, som forventes at bruge den efterfølgende. Dette skyldes at standarder kun udarbejdes, hvis det forventes at de er aktuelle og forventes at blive brugt. En standard kan dog også påbegyndes, med initiativ fra myndigheder, både nationalt, men også fra EU.

Alle standarder fra DS Certificering bliver gennemgået, revideret og rettet til hvert 5. år, for at sikre at alle standarder ikke bliver forældet. Hvis det skønnes, at en standard ikke længere er relevant,

[6] http://en.wikipedia.org/wiki/BS_7799 pr. 23. maj 2008

eksempelvis på grund af teknologisk udvikling, bliver standarden fjernet. Det bør således ikke være muligt at få fat i en standard, der ikke har sin berettigelse og som ikke er anvendelig.

Grunden til at DS 484 (2005) er anvendt som målestok for hvordan BB A/S, skyldes at denne standard kommer med konkrete anbefalinger til hvordan IT-sikkerheden kan udarbejdes, på alle centrale punkter. De andre standarder, der er beskrevet i opgaven, sætter udelukkende fokus på de områder, hvor ledelsen af virksomheden bør gøre sig tanker om, hvordan IT-sikkerhedsproblematikken skal løses.

I denne afhandling, er der taget udgangspunkt i DS 484 (2005), som er opbygget af 15 kapitler, samt 2 anneks. Kapitel 1-3 er generelt om standarden og kapitel 4-15 er vejledning til hvordan IT-sikkerheden kan styres og sikres. Grunden til at afhandlingen tager udgangspunkt i DS 484 (2005) er, at denne standard kommer med konkrete forslag til, hvorledes en virksomhed kan reducere sin risiko ved at være afhængig af IT. Derudover er den udarbejdet til at opfylde behovene i en dansk sammenhæng. Dette betyder, at er denne standard den bedst egnede til at opfylde opgavens formål, som er at komme med konkrete forslag til forbedringer af IT-sikkerheden i BB A/S, idet BB A/S er en dansk virksomhed og DS 484 (2005) er den mest operationelle standard, der er blevet gennemgået i denne afhandling.
Som tidligere nævnt er BB A/S ejet af den irske koncern CC plc., hvorfor DS 484 (2005), som er en efterkommer af den engelske standard BS 7799, vil være et naturligt valg at følge, for hele koncernen. Som følge af, at der er tale om en international koncern, ville ISO 27002 dog være et godt alternativ. ISO 27002 er den internationale udgave af BS 7799, hvorfor disse på de centrale områder, ligner hinanden. Dog skal det holdes for øje, at BB A/S er en dansk virksomhed, hvorfor DS 484 (2005) vil være den mest oplagte standard, at benytte, da denne netop er udarbejdet til danske virksomheder.

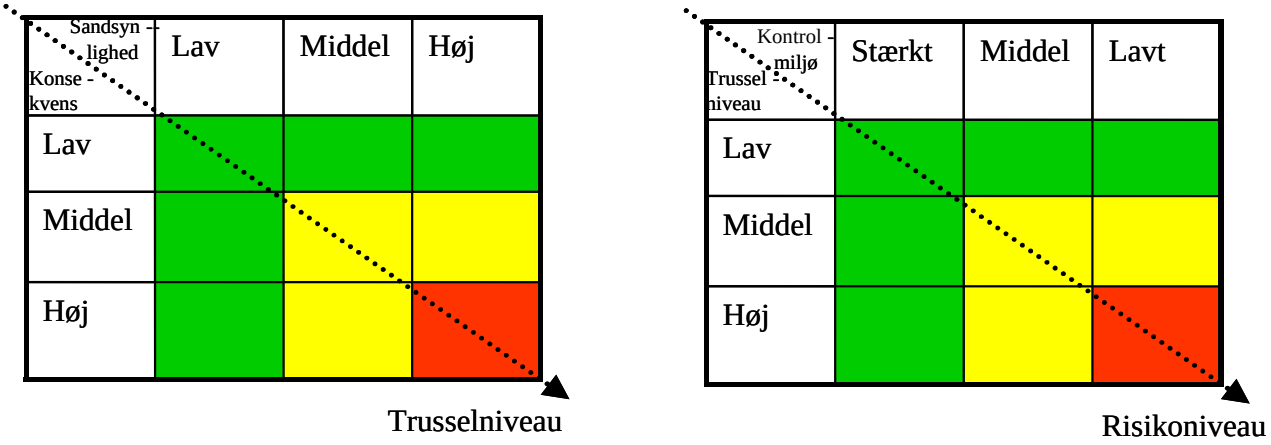
Det anbefales i DS 484 (2005) anneks B, at der udarbejdes en risikovurdering, for en virksomheds anvendelse af IT. Denne risikovurdering skal dog stilles i forhold til den enkelte virksomheds anvendelse og afhængighed af IT. Det er ikke fornuftigt, hvis eksempelvis en tømrer-virksomhed bruger mange penge på at lave en risikovurdering, hvis virksomheden ikke er afhængig af IT og blot bruger enkelte aktiver, som let kan skiftes ud. På den anden side bør en større virksomhed, der er mere/meget afhængig af IT-systemerne, være grundig, når der laves en risikovurdering.

I praksis kræver en sådan risikovurdering, store ressourcer fra selskabet. I anneks B i DS 484 (2005) er der en guideline for, hvorledes virksomhederne kan gribe en risikovurdering an. Denne guideline er opdelt i 7 trin, hvor der er uddybende kommentar til hvert trin. De 7 trin er:

1. Opgavestart
2. Trusselsliste
3. Sandsynlighed og konsekvens
4. Trusselsniveau
5. Sikkerhedsmiljø
6. Det samlede risikobillede
7. Risikobegrænsning

Som tidligere skrevet, skal dybden af vurderingen tilpasses den enkelte virksomhed. Når følgende 7 trin er gennemarbejdet og der er knyttet kommentarer til samtlige punkter, er det muligt at opstille det aktuelle trusselbillede for virksomheden, samt det aktuelle risikobillede for virksomheden. Dette gøres for at virksomheden kan få et overblik over hvor der eventuelt skal afsættes ekstra ressourcer og kan aflæses i nedenstående diagrammer:

Figur 1. Trusselsbillede og risikobillede[7]



[7] Figur 1, fra anneks B i DS 484:2005 version 2

Som det ses, er trussels- og risikobilledet opdelt i tre forskellige farver, grøn, gul og rød. Den grønne farve i diagrammet for trusselsniveau, indikerer at de trusler der havner i disse bokse, er acceptable for virksomheden, de gule indikerer at truslerne i disse bokse er delvis acceptable, imens de trusler der havner i det røde felt, er uacceptabelt for virksomheden.

Når trusselsniveauet er gennemarbejdet, tages hver enkelt trussel, ud fra placeringen i trusselniveauet og placeres ind i diagrammet for risikoniveau. Truslerne tilpasses efterfølgende kontrolmiljøet og havner herefter i en af de samme tre farver, som i diagrammet for trusselsniveauet. Farverne har samme betydning, i begge diagrammer, og resultatet af risikovurderingen kan til slut aflæses i diagrammet for risikoniveauet, som udover trusselsniveauet, ligeledes indeholder faktoren omkring kontrolmiljøet i virksomheden.

Når denne risikovurdering er udarbejdet, vil virksomheden have et billede af, hvor der skal afsættes flere ressourcer og hvor virksomheden allerede er godt dækket ind. Det er efterfølgende vigtigt at virksomheden løbende foretager nye vurderinger af trusler og risici, således at risikoniveauet hele tiden er aktuelt og ikke er forældet.

Udarbejdes en risikovurdering efter metoden i DS 484 (2005) anneks b, sikres det, at virksomheden opnår viden omkring hvilke forhold der er essentielle for at have et informationssikkerhedsniveau, der både er sikkerhedsmæssigt forsvarligt, samt økonomisk forsvarligt. Det er dermed op til ledelsen i enhver virksomhed at fastsætte rammen for en risikovurdering, i den enkelte virksomhed.

12. Generelle forhold for IT i BB A/S

BB A/S er ejet af CC plc. CC plc. er en stor global koncern, som har sine IT-aktiviteter centreret i Holland. I Holland sidder en stor afdeling, som udelukkende arbejder med at sikre koncernens IT-aktiver. Arbejdet med IT-aktiviteterne, bliver dog tilpasset de enkelte regioner, således også i Danmark, hvor det er den lokale IT-chef der står for at implementere de koncern-udstukne retningslinjer for IT-aktiviteterne, i videst muligt omfang. Derefter er det op til ledelsen i BB A/S at godkende og underskrive den gældende praksis på området. Dermed sikres det, at der bliver taget stilling til koncernens regler for IT-aktiver, fra ledelsens side.
Ved udarbejdelsen af denne afhandling, har det ikke været muligt at få en kopi af de retningslinjer, der bliver udstukket fra koncernens IT-afdeling, men IT-chefen i BB A/S har forklaret, at der er meget få krav i retningslinjerne. Det bliver krævet, at der er udarbejdet en nødplan, i tilfælde af, at IT-driften går ned. Derudover bliver det krævet, at de lokale ledelser af virksomhederne, godkender de til enhver tid gældende retningslinjer for den enkelte virksomhed.

IT-chefen for den danske del af CC plc. er den samme person, som er IT-chef for BB A/S. IT-chefens baggrund for at kunne bestride jobbet som IT-chef for hele den danske del af koncernen, kommer fra hans interesse for IT. IT-chefen er oprindeligt uddannet maskinmester, men har stor interesse for IT og derigennem fået færdigheder inden for området. Han har tidligere haft job indenfor IT i andre virksomheder og derigennem udviklet sine evner indenfor dette felt. IT-chefen prøver primært at holde sig selv opdateret, når han føler behov for det, ved at læse omkring nye tendenser på Internettet og snakke med kollegaer og venner. Derudover deltager han også på kurser, når han finder det nødvendigt. IT-chefen holder sig ligeledes opdateret, ved at holde sig orienteret igennem IT-leverandører til BB A/S.

BB A/S tilhører den gruppe af virksomheder, som er afhængig af sine IT-aktiviteter og det anbefales derfor at der bliver lavet en risikovurdering.

BB A/S´ ledelse har dog ikke udarbejdet en risikoanalyse, da ledelsen vurderer at dette ikke er nødvendigt. Under interviewet med IT-chefen, fortalte han, at virksomhedens revisorer de seneste år

har påpeget, at der bør udarbejdes en risikoanalyse. Ledelsen har dog afvist, med begrundelsen, at IT-anvendelsen i virksomheden, efter deres mening, ikke er så kritisk, at det behøves at udarbejde en sådan risikoanalyse. Yderligere har ledelsen af virksomheden ladet forstå, at de har fuld tiltro til It-chefens evner, til at vurdere hvilket niveau af sikkerhed virksomheden har brug for.

Selvom revisor har påpeget overfor ledelsen af BB A/S, at der bør udarbejdes en risikoanalyse, for at sikre sig, at virksomheden har det nødvendige beredskab, er dette ikke blevet gjort. Det har dog ikke givet udslag i revisionspåtegningen for virksomheden, hverken med hensyn til forbehold for going-concern, eller supplerende bemærkninger i årsrapporterne for 2005 eller 2006. Det er dog noteret, at det anbefales at udarbejde en sådan risikoanalyse i både management letter til ledelsen, samt i protokollen til bestyrelsen.

Samlet set gælder det for forholdene omkring IT-sikkerheden for BB A/S, at ledelsen har lagt ansvaret og opgaverne over på IT-afdelingen og IT-chefen. Ledelsen har ladet IT-chefen vurdere hvilke områder der skal prioriteres frem for andre. I den forbindelse har IT-chefen taget udgangspunkt i hvor lang tid de enkelte områder i virksomheden vil kunne fortsætte med at producere i tilfælde af et større IT-nedbrud, for at vurdere hvilke områder der skal have høj prioritering.
Denne fremgangsmåde finder jeg dog kritisabel, da det bør være ledelsen der udarbejder en plan over hvorledes IT-aktiverne i virksomheden skal prioriteres frem for andre IT-aktiver. Dermed sikres det, at det er et forretnings-mæssigt synspunkt, der bliver lagt til grund for prioriteringen. Derudover er det min holdning, at ledelsens ansvarsfriskrivelse ikke er gyldig, da det i bund og grund er ledelsen i virksomheden der er ansvarlig for driften. Dette understreges, som tidligere nævnt, i aktieselskabslovens § 54, stk. 3.

13. Risikoanalyse for BB A/S

I beskrivelsen af BB A/S, er der allerede listet enkelte punkter op, hvor IT spiller en stor rolle for virksomheden. Derudover, som det ligeledes er beskrevet tidligere i opgaven, har ledelsen af BB A/S ikke fundet det nødvendigt at udarbejde en risikoanalyse for IT-anvendelsen i virksomheden. Dette er ikke fundet nødvendigt, selvom revisor for virksomheden, har påpeget både i et management letter, samt i protokollen, at det anbefales at udarbejde en sådan risikoanalyse.

Som følge af BB A/S´ afhængighed af IT, er nedenstående risikoanalyse udarbejdet, for at sætte fokus på hvilke områder BB A/S bør være bedre til at sikre, herunder sikre sig imod tab af fortroligt data, samt undgå et stort IT-nedbrud.

Risikoanalysen er udarbejdet på baggrund af indholdet i DS 484 (2005). Dette skyldes, at DS 484 (2005), som tidligere nævnt, er en anerkendt standard, som indeholder anbefalinger for stort set alle tænkelige områder af IT-driften i en dansk virksomhed. Ved at tage udgangspunkt i en anerkendt standard om IT-sikkerhed, sikres det, at risikoanalysen får et passende omfang og omfatter de mest gængse problemstillinger der opstår ved afhængigheden af IT. Det skal dog holdes for øje, at risikoanalysen i DS 484 (2005), blot er et bilag og derfor er det ikke et krav, at udarbejde en risikoanalyse, for at leve op til standarden.

Ud fra de oplysninger jeg har fået fra virksomheden i forbindelse med mit besøg og interviews med både IT-chefen, samt den tidligere ansatte i BB A/S, er følgende risikoanalyse udarbejdet.

13.1 Overordnede retningslinjer

BB A/S ejes, som tidligere nævnt af en international koncern, hvorfra der bliver udarbejdet overordnede retningslinjer for driften af IT i koncernen, og dermed for BB A/S. Selvom der er fordele ved denne model, i og med at der sidder en større gruppe, med ekspertise indenfor IT-området, er der også ulemper ved denne model. Eksempelvis kræver ændringer i IT-instrukserne, at de lokale ledere af de enkelte selskaber, godkender instrukserne der udsendes fra koncernen. Disse instrukser kan være en

”sovepude” for de enkelte selskaber, som derudover kan være en måde at fraskrive sig ansvaret for IT-driften i de enkelte selskaber. Derudover kan der stilles spørgsmålstegn ved, om der er en for høj grad af bureaukratisering mht. opdateringen af IT-instruksen, i og med, at hver enkelt ledelse skal godkende den, inden den træder i kraft for den enkelte virksomhed. Den aktuelle koncern-instruks er fra 2006 og ledelsen i BB A/S har ikke lavet ændringer i den.

Sandsynligheden for at der sker et nedbrud, som følge af manglende opdatering af de overordnede retningslinjer, vurderes til lav. Dette skyldes at instrukserne er overordnede og dermed ikke er detaljeret retningslinjer for driften af IT i virksomheden, hvilket betyder at den daglige drift løbende varetager akutte problemstillinger.
Konsekvensen af et nedbrud, som skyldes manglende opdatering af de overordnede retningslinjer, vurderes til høj. Vurderingen sættes som baggrund for, at en manglende opdatering af de overordnede retningslinjer, kan medføre at der ikke er taget højde for eventuelle store områder, såsom anvendelse af ny teknologi. Dermed kan driften påvirkes i stor grad, hvis denne allerede er begyndt at tage den nye teknologi i brug.

13.2 Organisering af informationssikkerhed

13.2.1 Interne organisatoriske forhold

Ledelsens rolle omkring IT-sikkerheden i BB A/S, er i teorien central. Ledelsen skal godkende de koncern-instrukser der kommer fra Holland, for at sikre sig, at disse instrukser er relevante og tilstrækkelige for lige netop BB A/S. I praksis er det dog udelukkende IT-chefen, der forholder sig til koncern-instrukserne, samt hvilket behov for sikkerhed, BB A/S har brug for. Risikoen ved at det udelukkende er en person der har til opgave at vurdere sikkerhedsniveauet for virksomheden, er at der ikke er tilstrækkeligt modspil, til denne person. Derudover er IT-chefen, som mange andre IT-medarbejdere i andre virksomheder, udelukkende fokuseret på IT. Det vil sige, at IT-medarbejdere umiddelbart ikke er i stand til at vurdere konsekvensen af et eventuelt nedbrud, for virksomheden. IT-medarbejdere kan ikke umiddelbart lave en opgørelse over tab, hvis et enkelt IT-aktiv har et nedbrud,

eller hvilke økonomiske konsekvenser det vil have, hvis der er et større eller totalt nedbrud på virksomhedens IT.

Selvom der er flere medarbejdere i IT-afdelingen, er der ingen tvivl om, at IT-chefen er den ansvarlige for IT-driften og IT-sikkerheden i BB A/S. Når der stort set kun er en person til at styre IT-forholdene i virksomheden, bliver virksomheden i høj grad afhængig af denne medarbejder. Dette er en naturlig konsekvens ved at overlade alt ansvaret på et område, til en enkelt medarbejder. IT-chefen beskriver selv forholdet til ledelsen, som et tillidsforhold, hvor ledelsen har givet ham ansvaret for at IT-driften fungerer efter hensigten.

Sandsynligheden for at der bliver prioriteret uhensigtsmæssig, når det udelukkende er en IT-medarbejder, der bedømmer hvilke områder der skal fokuseres på, vurderes høj. Vurderingen herfor begrundes af den manglende forretningsmæssige indsigt i virksomheden, som IT-chefen besidder.
Konsekvensen ved et eventuelt nedbrud, hvor det rammer forretningskritiske informationer og data, vurderes høj. Dette skyldes, at eventuelle nedbrud på forretningsmæssige kritiske aktiver, vil have stor betydning for driften i virksomheden.

Ledelsen har, på foranledning af koncern-instrukser, udarbejdet en nødplan, for et eventuelt større nedbrud på virksomhedens IT.. Nødplanen skal som minimum indeholde en række områder, som er beskrevet i den koncern-instruks, der er godkendt af ledelsen i BB A/S. Nødplan bliver ligesom den generelle IT-sikkerhed udelukkende justeret af IT-chefen, hvis han mener at der er brug for små justeringer.
Heri kan der være en potentiel risiko, idet nødplanen ikke regelmæssigt bliver opdateret og godkendt af ledelsen. Dette kan eksempelvis være med hensyn til den eksterne konsulent, hvor det ikke er sikkert at denne person stadig er medarbejder i det konkrete firma. Derudover vil der i praksis kunne opstå nye behov, som den aktuelle nødplan ikke tager højde for. Dette bliver ikke regelmæssig vurderet, idet der ikke er noget krav til en fast procedure for opdateringen af denne nødplan.

Sandsynligheden for at nødplanen ikke bliver opdateret, når der udelukkende sidder en enkelt person, som skal tage stilling til hvornår denne skal opdateres, vurderes til at være høj. Denne vurdering skyldes, at den enkelte person ikke nødvendigvis stiller sig kritisk nok overfor sit eget arbejde.
Konsekvensen ved at nødplanen ikke er opdateret, er fastsat til høj, selvom der som udgangspunkt er lavet en plan for beredskabet. Der er derfor tidligere tænkt over, hvorledes en gendannelse af IT-systemerne i BB A/S skal foregå. Dog kan en forældet nødplan ikke tage højde for nye aktiver og dermed vil denne ikke tilstrækkelig ved et eventuelt nedbrud.

I sammenhæng med ovenstående punkter, er følgende vurderet til at være en risiko. Der er ingen nedskrevet regler omkring periodisk opfølgning. Som et eksempel på manglende krav til periodisk opfølgning, er kravene til backup af data. Nedenstående er taget fra "IT-sikkerhedspolitik" for BB A/S:

"*Læsbarhed og genikraftsættelse af alle backup skal testes med jævne mellemrum.*

Backup af data på PC er brugernes ansvar og virksomheden skal gøre dette klart for alle medarbejdere. Ideelt bør vigtige data opbevares på de centrale servere."

Der er ikke nedskrevet en konkret tidslinje for, hvornår der senest skal laves et simuleret nedbrud, for at efterprøve de data der er taget backup af. Der står udelukkende at dette skal gøres "med jævne mellemrum". Derved er det op til IT-afdelingen at vurdere, hvornår de mener, at det er tid til at efterprøve procedurerne omkring genindlæsning af data.
I de tilfælde, hvor genindlæsning har været foretaget som en del af en prøve, har det udelukkende været efter en vurdering af IT-afdelingen, hvorfor det ligeledes kun var med deltagelse af personer fra IT-afdelingen.

Sandsynligheden for at der sker fejl, når backup-procedurer ikke efterprøves regelmæssigt, vurderes til høj, idet der over en længere periode, kan være kommet nye applikationer i virksomheden, som ikke er prøvet genindlæst. Derudover kan der opstå diverse fejl, som først opdages, når data i praksis forsøges genindlæst.

Konsekvensen ved at det ikke er muligt at genindlæse data vurderes til høj. Dette skyldes at hvis virksomheden ikke er i stand til at genindlæse data omkring indgående og udgående ordrer, samt alle andre data, kan det koste et betydeligt beløb. Da der skal følges op på arkitekttegninger, varelager med mere, kræver dette et kæmpe arbejde. I værste fald kan det betyde at BB A/S mister så betydelige data, at skaden er uoprettelig og dermed kan lide store tab.

13.2.2 Eksterne samarbejdspartnere

BB A/S samarbejder i høj grad med eksterne samarbejdspartnere. I denne forbindelse har de eksterne samarbejdspartnere adgang til BB A/S´ netværk. Dette betyder at eksterne samarbejdspartnere har mulighed for at opdatere programmer, som bruges af BB A/S, ligesom vare-leverandører har mulighed for at se den aktuelle lagerstatus. Det er dog blevet foruddefineret, hvilke områder hver enkelt samarbejdspartner har adgang til på netværket. Der er dog ingen krav til de eksterne leverandører, om eksempelvis virus-beskyttelse. Derved risikerer BB A/S at få uønsket software ind på virksomhedens netværk.

Sandsynligheden for at der kommer uønsket software ind på netværket hos BB A/S vurderes som lav, da dette kun vil ske, hvis den eksterne leverandør har denne software i deres systemer. Da virus generelt er uønsket, formodes det, at hver enkelt virksomhed arbejder for at holde sig fri for virus.
Konsekvensen ved at der kommer virus ind på netværket, vurderes til at være middel. Dette skyldes at virus kan skade virksomhedens data i stort omfang. Dog kan der forholdsvis hurtigt indlæses en backup af samtlige data, hvorefter systemet vil være frit for vira, under forudsætning af, at denne backup virker.

13.3 Styring af informationsrelaterede aktiver

Der er en samlet oversigt over informationsrelateret aktiver i BB A/S. Denne oversigt indeholder informationer om hvor aktivet er og hvem der har ansvaret for det. Denne oversigt skal ajourføres, hver gang der bliver anskaffet nye aktiver, samt når nuværende aktiver bliver frasolgt eller skrottet. I praksis

bliver denne oversigt dog ikke altid ajourført, da IT-afdelingen i nogle perioder "har andet at se til"[8]. Dette bevirker, at der ikke er en komplet liste over hvilke aktiver der forefindes hos BB A/S. De mest kostbare aktiver, bliver dog altid registreret.
Det skal dog holdes for øje, at de mest kostbare aktiver, ikke er det samme som de mest værdifulde aktiver. På eksempelvis eksterne harddiske, hvor medarbejdere kan gemme data, kan der være meget forretningskritisk materiale, som kan være til skade for virksomheden, hvis det slipper ud. Hvis ikke der forefindes ajourførte oversigter, så udviser medarbejdere ikke nødvendigvis den rette omtanke for aktivet, da medarbejderen ikke kan gøres ansvarlig for at aktivet bortkommer. Dette kan eksempelvis ske på de enkelte byggepladser, hvor medarbejdere ikke passer nok på eksempelvis en ekstern harddisk, med forretningskritisk materiale. Dette kan ske ved byggemøder med mere, hvor der er flere personer tilstede.

Sandsynligheden for at miste aktiver, som følge af at der ikke er en ajourført oversigt over informationsrelaterede aktiver, vurderes til middel, idet de enkelte medarbejdere ikke har samme ansvarsfølelse overfor aktiver, som ikke er registreret i deres navn.
Konsekvensen ved at miste data, vurderes til middel, da forretningskritisk materiale, såsom arkitekttegnede skabeloner og forslag til et konkret byggeri kan skade virksomhedens muligheder for eksempelvis, at få ordrer til nye byggerier.

13.4 Medarbejdersikkerhed

13.4.1 Sikkerhedsprocedure før ansættelse

Før ansættelsen af en medarbejder, er det vigtigt at lave en vurdering af, hvor stor erfaring personen har med at håndtere forretningskritiske data, hvis personen via jobbet har adgang til dette. Derudover skal det vurderes, om kandidaten til et job med stor berøring af forretningskritiske data, forventes at leve op til ansvaret omkring hemmeligholdelse af disse data. I BB A/S bliver der umiddelbart ikke spurgt ind til dette, når en kandidat vurderes til et job, medmindre det er et job i IT-afdelingen. Der bliver dog

[8] Fra interview med IT-chefen

foretaget en general vurdering af nye medarbejdere til jobsamtalen, hvor personerne der skal ansætte kandidater, laver en vurdering af integriteten hos kandidaten.

Sandsynligheden for at en uerfaren bruger af IT laver fejl, samt at den generelle vurdering af kandidaten, ikke er god nok, vurderes til lav/middel. Der kan ske fejl for uerfarne brugere af IT, som kommer til at omgås forretningskritisk materiale på en uhensigtsmæssig måde. Derudover kan vurderingen af en kandidats integritet være utilstrækkelig, da denne vurdering er generel og ikke møntet på kandidatens integritet overfor IT.
Konsekvensen vurderes til høj, da en medarbejder der, enten tilsigtet eller utilsigtet, omgås forretningskritiske data uden den påkrævet fortrolighed, kan være skyld i tab af ordrer med mere. Dette kan eksempelvis være scenariet, hvis konkurrenter får mulighed for at se hvilke projekter BB A/S arbejder med eller hvilke nye elementer der forskes i at forbedre.

13.4.2 Ansættelsens ophør

Der er flere medarbejdere der får udleveret blandt andet bærbare computere. Når en medarbejder stopper skal det udleverede udstyr returneres og brugerrettighederne skal inddrages af IT-afdelingen, for derved at undgå misbrug af data og adgang til BB A/S´ netværk. Dette overholdes dog ikke i praksis, da det er de lokale ledere på BB A/S´ fabrikker rundt om i landet, som skal stå for at få aktiverne tilbage og meddele ansættelses ophør til IT-afdelingen. Når listerne for medarbejderne på virksomhedens fabrikker i rundt om i landet ikke ajourføres, er det ikke muligt for IT-afdelingen i Esbjerg, at holde styr på hvor de enkelte aktiver befinder sig, ligesom det ikke er muligt for IT-afdelingen at spærre for adgangen til netværket i BB A/S. Derved er der mulighed for at kritisk materiale bliver offentligt tilgængeligt, ligesom der kan være fare for, at den tidligere medarbejder tilsigtet forårsager skade på netværket, ved eksempelvis at installere programmer på netværket, som kan være skadelige.

Sandsynligheden for at der er problemer med tidligere medarbejdere, vurderes til at være lav, idet det ikke forventes at tidligere medarbejdere er illoyale, samt at det generelt er fornuftige personer der befinder sig i virksomheden..

Konsekvensen vurderes til at være høj, da det er yderst problematisk, hvis forretningskritisk materiale bliver offentliggjort af tidligere medarbejdere, ligesom uønsket programmer kan skade virksomhedens data. Derudover har en tidligere medarbejder også mulighed for manuelt at slette data, således at disse går tabt.

13.4.3 Ansættelsesforholdet

Under ansættelsesforholdet skal ledelsen sørge for, at medarbejdere med daglig brug af IT, løbende bliver uddannet. Uddannelsen skal sikre, at medarbejderne hele tiden har viden om, hvorledes data skal behandles, så virksomheden undgår tab af data. Denne løbende uddannelse bliver ikke gennemført i BB A/S, der udelukkende giver en kort præsentation til relevante IT-systemer, for nyansatte.
Derudover er ansatte ikke forpligtigede, og bliver heller ikke gjort opmærksomme på, at følge op på ændringer i IT-håndbogen for virksomheden. IT-chefen forklarede under interviewet, at ændringer bliver lagt på virksomhedens intranet, hvorefter det er op til den enkelte medarbejder, at holde sig ajour med de gældende regler.
IT-chefen fortæller at der ikke er nedskrevet sanktioner, hvis en medarbejder, tilsigtet eller utilsigtet, laver fejl. Han forestille sig dog at det bliver løst ”*på fornuftig vis, med en passende sanktion*”, som kan være alt fra påtale, advarsel eller fyring, alt efter grovheden og hensigten.

Sandsynligheden for at der sker fejl, når uddannelse i IT under ansættelsesforholdet nedprioriteres, vurderes til middel. Der kan med tiden komme nye programmer, ny hardware eller andet, som medarbejderne skal undervises i, for at undgå problematiske situationer.
Konsekvensen ved at medarbejdere i virksomheden ikke er opdateret med hensyn til IT, vurderes til middel/høj. Hvis medarbejderne ikke behandler følsomt materiale med den fornødne påpasselighed, kan konsekvensen være at fortroligt materiale ender steder hvor det ikke er meningen, og dermed skader virksomheden.

13.5 Fysisk sikkerhed

Den fysiske sikkerhed er afgørende for, at der ikke mistes data ved et eventuelt indbrud, eller ved brand osv.
Den fysiske sikkerhed for IT i BB A/S opdeles i henholdsvis computere og servere. Dette skyldes at der er stor forskel på de forretningsmæssige risici, der knytter sig til de to typer af aktiver.

13.5.1 Sikre områder

For computere gælder det, at den fysiske sikkerhed består af den generelle fysiske sikkerhed der er på BB A/S. På kontoret i Esbjerg, hvor mit besøg fandt sted, består den fysiske sikkerhed af computere af selve kontorbygningen, med dertil hørende sikkerhedsforanstaltninger. Dette inkluderer et hegn rundt om virksomheden, således at personer ikke bare kan gå ind på virksomhedens grund, i det tidsrum, hvor der ikke er nogle til stede. Det er kun ledere i BB A/S der har nøgle til virksomheden, og dermed mulighed for at komme ind, uden for almindelig åbningstid. Der er ligeledes tilknyttet en vagtordning, som betyder at der bliver tilkaldt en vagt, hvis alarmen går på virksomheden.
På BB A/S i Esbjerg, bærer samtlige medarbejdere id-kort, således at det er muligt for de ansatte at se, om personerne på kontoret er ansatte, eller ej. Dermed er det svært for personer udefra, at få adgang til computere, i dagtimerne på virksomheden.
Computere på virksomheden, er udelukkende beskyttet ligesom alle andre aktiver. Da det hovedsageligt er stationære computere der bliver brugt, bliver de ikke lagt væk efter de ikke bliver brugt mere. Dermed er computerne sikret på samme måde, som resten af inventaret, hvis virksomheden kommer ud for, at der opstår brand, oversvømmelse mm., hvilket blandt andet indebærer brandalarmer og varsling ved oversvømmelse.

Sandsynligheden for at BB A/S mister betydningsfulde data, som følge af sikkerheds-niveauet for at sikre området omkring virksomheden og dennes computere vurderes til lav. Vurderingen bygger på virksomhedens sikring, som må betegnes som passende for computerne, der er sikret på lige fod med andre aktiver. Der er taget højde for indbrud, uautoriseret adgang og varsling ved brand og oversvømmelse.

Konsekvensen for skader opstået ved ovenstående hændelser, vurderes til middel/høj. Denne vurdering skyldes, at der ikke er noget regelsæt for, hvorledes data skal gemmes i BB A/S. Dermed kan det risikeres, at der befinder sig værdifulde data på de fritstående stationære computere. Konsekvensen ved dette kan være, at virksomheden mister data, eksempelvis arkitekttegnede skabeloner til betonelementer der benyttes i driften, ved en eventuel brand eller tyverisag.

For servere gælder stort set det samme, som for computere, i BB A/S. Serverne er placeret i kontorbygningen i Esbjerg, hvor ovenstående beskriver sikkerheden. Derudover er serverrummet låst, og det er udelukkende IT-afdelingen der har nøgle til rummet. Døren er en almindelig dør, hvorved den ikke er brandsikret og den udelukkende bliver åbnet med en almindelig nøgle.
I serverrummet er der, udover brandalarm, også installeret specialudstyr, som bliver aktiveret ved brand. Dette sikrer serverne endnu mere imod skader ved brand, da serverne er længere tid om at tage skade.

Sandsynligheden for et større nedbrud vil forekomme, som følge af forholdene for at sikre området omkring serverne i BB A/S, vurderes til lav. Som nævnt er der taget yderligere sikringsforanstaltninger i forhold til serverrummet, som indebærer at en ekstra sikkerhed i forhold til andre aktiver i virksomheden.
Konsekvensen ved situationer, som opstår på grund af manglende sikkerhedsniveau for området omkring serverne, vurderes til høj. Hvis serverne i BB A/S ikke fungerer, er det ikke muligt for virksomhedens ansatte at kommunikere via programmerne i BB A/S. Derudover kan teknikere og andre ansatte ikke få adgang til de skabeloner, der tidligere er tegnet af arkitekterne, ligesom der er flere andre data, som ikke er tilgængelige, hvis serverne ikke kører.

13.5.2 Beskyttelse af udstyr

For arbejdscomputere, der som tidligere nævnt er stationære i BB A/S, er der ikke taget nogle sikkerhedsmæssige hensyn til placeringen. Det er udelukkende et spørgsmål om hvor det passer ind med hensyn til placeringen af arbejdspladser.

Hvis strømmen afbrydes i virksomheden, har BB A/S en nødgenerator, der slår til og som kan levere strøm i tilstrækkelig tid, indtil samtlige computere lukkes ned korrekt. Derved undgås det, at brugerne mister deres data, da de kan nå at gemme disse data og derefter slukke deres computere.
Vedligeholdelse af computere foretages af IT-afdelingen, når brugerne kommer og fortæller, at der er noget galt, eller når IT-afdelingen selv vurderer, at det er hensigtsmæssigt at foretage vedligeholdelse af virksomhedens IT.
Når virksomheden skal skille sig af med IT-udstyr, er det IT-afdelingen der skal foretage de nødvendige handlinger, for at det er sikkert at bortskaffe udstyret. Denne procedure er fast i virksomheden, således at intet udstyr bliver smidt ud, uden en IT-medarbejder har sagt god for at der ikke befinder sig materiale fra virksomheden, på computeren.

Sandsynligheden for at der sker et kritisk brud på sikkerhedsniveauet, som følge af uregelmæssigheder i forholdene omkring beskyttelse af computere i BB A/S, vurderes til lav. Vurderingen bygger på ovenstående forhold, som bør være tilstrækkelig for at oprette en fornuftig driftssikkerhed.
Konsekvensen ved et nedbrud for forhold omkring beskyttelsen af computere, vurderes til middel. Denne vurdering bygger hovedsageligt på bekymringer omkring placeringen af computerne. Computere er generelt attraktive at stjæle fra virksomheder og sker dette, kan BB A/S miste kritisk data. Derudover er det bekymrende, at der ikke er en fast procedure ved vedligeholdelse af computere, da der kan være computere i virksomheden, som ikke har fået foretaget et service-eftersyn i lang tid, og dermed har større risiko for at gå i stykker.

For serverne i BB A/S er placeringen foretaget efter overvejelser omkring forskellige risici. Dette indebærer tilgængeligheden ved brand, tilgængeligheden ved indbrud, samt sikring mod oversvømmelse. Med hensyn til brand, er serverrummet placeret så langt væk fra rum, som indeholder brandbart materiale. Det vil sige, at den anden side af samtlige vægge i serverrummet er ud til en gang eller en trappe. Derved har ilden sværere ved at brede sig fra et rum, til serverrummet, da der umiddelbart ikke er noget brandbart i nærheden af rummet. Serverrummet er ligeledes placeret så langt væk som muligt fra vinduer og døre, ligesom der ikke er aktiver af værdi, der står omkring serverrummet. Ved at placere serverrummet så langt væk fra andre værdier og aflåse rummet, mindskes risikoen for nedbrud, ved indbrud. Inde i serverrummet er samtlige maskiner placeret ca. 30 cm. over

gulvet, således at der ikke trækker vand ind i dem, hvis der sker oversvømmelse. Det skal dog nævnes, at der løber vandrør oppe under loftet i serverrummet. Dermed er det ekstra fornuftigt, at serverne er placeret over gulvhøjde, da et eventuelt brud på vandrørene vil medføre vand i lokalet.
Serverne er sikret imod strømafbrydelse, på samme måde, som computerne i virksomheden. Dermed er det muligt at lukke serverne ned i på forsvarlig vis, hvis der skulle opstå problemer med strømmen. Der er flere kabler der forbinder virksomhedens servere. Serverne kan godt fungere, selvom enkelte kabler er gået i stykker. Hvis et kabel går i stykker, advares IT-afdelingen ved hjælp af indikatorer på serverne.
Ligesom med computerne, er der ikke nogen fast procedure med hensyn til vedligeholdelse af serverne i BB A/S. IT-chefen forklarede i interviewet, at han eller en anden medarbejder fra IT-afdelingen "kigger" til serverne en gang i mellem, for at se om alt er, som det skal være. Derudover er det også IT-afdelingen der er ansvarlig for en eventuel sikker bortskaffelse af servere, således at det sikres at der ikke fortroligt materiale på maskinerne, når de ikke længere er i virksomheden.

Sandsynligheden for at der sker forretningskritiske nedbrud, som følge af beskyttelsen omkring IT i virksomheden, vurderes til lav. Dette gøres selvom der er nogle umiddelbare risici omkring dette emne. Eksempelvis er der en øget risiko for at serverne tager skade, da disse er placeret i et rum med vandrør. Ydermere kan den manglende vedligeholdelsesprocedure for serverne, ligeledes spille en rolle for sandsynligheden for at serverne går ned, og BB A/S dermed mister kritiske data.
Konsekvensen for nedbrud på serverne, vurderes til høj. Generelt når serverne bliver udsat for nedbrud, er det kritisk for virksomheden, da dette som regel indebærer tab af data. Mængden og vigtigheden af data kan variere, alt efter hvilke projekter der arbejdes på i virksomheden og alt efter hvor lang tid siden der sidst er taget backup.

13.6 Styring af netværk og drift

13.6.1 Operationelle procedurer og ansvarsområder

Som altoverskyggende hovedansvarlig for IT-driften i BB A/S er IT-chefen. Det er ham som der skal stå til ansvar overfor den øverste ledelse, hvis der er problemer med IT i virksomheden.

Ledelsen i BB A/S har ikke udstedt specielle retningslinjer til IT-afdelingen, for hvordan IT i virksomheden skal afvikles og styres. Ledelsen har lavet nogle retningslinjer, på opfordring af koncern-ledelsen, som omhandler IT-retningslinjer for samtlige medarbejdere i virksomheden. Disse retningslinjer arbejder IT-afdelingen ligeledes efter, men der er ikke udstukket specifikke retningslinjer til hvilke procedure der skal op- eller nedprioriteres, i forhold til forskellige grupper af informationsaktiver eller procedurer.
Personalet i IT-afdelingen har adgang til samtlige computere og applikationer i BB A/S, hvorfor der ikke er tale om nogen form for funktionsadskillelse. Derved kan en enkelt person i IT-afdelingen ændre i opsætningen på programmerne i virksomheden. IT-chefen fortæller dog, at det er meget sjældent at de selv retter i programmer, der bliver brugt af BB A/S. Programmerne bliver for det meste vedligeholdt af leverandørerne af programmerne. Dermed bliver faserne udvikling, drift og test holdt adskilt fra hinanden i virksomheden.
IT-afdelingen kan, uden foregående aftale eller accept, overtage styringen af medarbejdernes computere, hvis computerne er tilsluttet BB A/S´ netværk, og dermed har personalet i IT-afdelingen adgang til samtlige data der er i virksomheden. Den eneste begrænsning IT-afdelingen har, som skyldes funktionsadskillelse, er at IT-medarbejderne ikke kan godkende betalinger fra virksomhedens konti, da disse godkendelser går via netbank. Men med muligheden for at overtage styringen af samtlige personers computer i virksomheden, er der mulighed for at installere en key-logger på computerne og derved aflure samtlige koder, i virksomheden.

Sandsynligheden for at der sker forretningskritiske skader, som følge af forholdene omkring operationelle procedurer og ansvarsområder vurderes til lav. Dette skyldes hovedsageligt, at det er tydeligt, at IT-afdelingen ikke har til hensigt, at udnytte de muligheder de har. Hvis det var tilfældet, at de ville udnytte dem, ville de allerede have gjort det. Mit indtryk ved interviewet har været, at IT-afdelingen besidder en høj integritet, ligesom de har en professionel stolthed, som de sætter højt. De vil ikke have, at deres arbejde skal kunne kritiseres. Denne stolthed og integritet gør nødvendigheden af procedurer for den generelle drift mindre, selvom det aldrig kan garanteres, at integriteten kan holde personer i IT-afdelingen fra, at lave ting, som ikke er acceptable.
Denne vurdering af integriteten for IT-afdelingen er dog meget subjektiv og kan ikke underbygges af fakta.

Konsekvensen af forretningsmæssige skader, som følge af især IT-afdelingens tilsigtede fejl, vurderes til høj. Hvis en medarbejder i IT-afdelingen bliver meget utilfreds med situationen i virksomheden, vil denne medarbejder være i stand til at afbryde al IT i BB A/S og dermed udgøre en reel risiko for virksomhedens overlevelse. Derudover er der mange andre scenarier, hvor en IT-medarbejder har mulighed for at udnytte sine muligheder, til skade for BB A/S.

13.6.2 Ekstern serviceleverandør

BB A/S benytter sig i stort omfang af eksterne serviceleverandører, eksempelvis i produktionen af betonelementer og i administrationen. BB A/S benytter flere eksterne serviceleverandører, til at holde virksomhedens programmer ved lige og for at få tilføjet de nyeste funktioner i programmerne. Programmerne vedligeholdes, og tilføjelser bliver installeret, ved at leverandørerne får fjern-adgang til BB A/S´ netværk og derigennem har mulighed for at konfigurere programmerne. IT-chefen fortæller at hver enkelt leverandør udelukkende har adgang til den del af netværket, som der er behov for, for lige netop at kunne opdatere leverandørens program. Dermed har den eksterne serviceleverandør ikke adgang til andre dele af netværket, hvor der er andre programmer og data, og hvorfor leverandøren heller ikke kan skade øvrige programmer eller data.
Der er ingen formelle krav til at den eksterne serviceleverandør har nogen form for virusbeskyttelse mm., da dette anses for en selvfølgelighed, for en leverandør af software.

Sandsynligheden for at der opstår et nedbrud, som følge af en hændelse i forbindelse med opdateringer fra en ekstern serviceleverandør, vurderes til lav. De eksterne serviceleverandører er eksperter i at foretage sådanne opdateringer og deres forretningers succes afhænger i stor grad af, at deres kunder ikke oplever gener ved at give dem adgang til deres netværk. Sandsynligheden for at der sker fejl, er dog forøget af, at der ikke stilles formelle krav til serviceleverandørernes IT-sikkerhed.
Konsekvensen ved et nedbrud, der forårsages af eksterne serviceleverandører, vurderes til middel. Hvis eksempelvis leverandøren af det program der styrer blandingen af beton i betonelementerne, kommer til at efterlade blandingsprogrammet i en tilstand, hvor det ikke virker efter hensigten, er konsekvensen, at produktionen må stoppe. Dette koster naturligvis mange penge for BB A/S, som dermed er udsat for

en forretningsmæssig risiko ved at have givet den eksterne serviceleverandør adgang til virksomhedens netværk.

13.6.3 Logning og overvågning

IT-afdelingen i BB A/S overvåger og logger samtlige hændelser på virksomhedens netværk. Dette indbefatter alt fra hvornår hver enkelt computer opretter forbindelse til netværket, hvornår der kobles op til virksomhedens netværk via fjern-adgang, til hvornår eksterne serviceleverandører logger sig på netværket. Derudover bliver samtlige ændringer i virksomhedens programmer logget og gemt.
Logning i virksomheden registrerer også hvad hver enkelt bruger foretager sig på netværket. Dette gælder både almindelige brugere, samt administratorerne i IT-afdelingen. Det er dermed muligt at for IT-afdelingen at se hvem og hvornår der eventuelt er blevet ændret i virksomhedens programmer.
Dette gælder dog kun computere i administrationen, da computere i selve produktionsafdelingen for betonelementer, altid er tændte og der kræves ikke log-in, for at betjene disse computere, som er forbundet til virksomhedens netværk.
IT-administratorerne i BB A/S har ikke nogle faste procedurer for behandling af logningerne, men bliver dog alarmeret ved uregelmæssigheder. Det bør dog også nævnes, at logningerne ikke er låste for IT-administratorerne, som dermed har mulighed for at ændre i dem.

Sandsynligheden for at der sker nedbrud, som følge af virksomhedens brug af logning, vurderes til lav/middel. Da virksomhedens logningsovervågning er meget omfattende, for computerne i administrationen, bør det ikke være muligt for ansatte at lave uautoriseret ændringer i programmer eller installere programmer på virksomhedens computere, uden dette bliver opdaget og rapporteres til IT-afdelingen. For computerne i produktionen, er der ikke nogen faste medarbejdere, der er knyttet til den enkelte computer. Dermed er der større sandsynlighed for at der bliver installeret uautoriseret programmer på BB A/S´ netværk, uden at det kan spores hvem der har gjort det.
Konsekvensen ved at der er mulighed for at foretage sig uautoriseret handlinger, uden at det kan bevises hvem der står bag, vurderes til middel/høj. Det vil være en alvorlig trussel, hvis der bliver installeret fjendtligsindede programmer på virksomhedens netværk. Det vurderes dog, at der skal en vis

teknisk forståelse, og ondsindede hensigt, til at konsekvenserne ved en sådan handling, får kritiske konsekvenser for BB A/S.

13.7 Adgangsstyring

13.7.1 Administration af brugerrettigheder

Der er flere forskellige grupper ad brugerrettigheder, som BB A/S benytter sig af, for at give medarbejderne adgang til lige netop det der er relevant for de enkelte grupper. Adgangen til de forskellige områder på virksomhedens netværk bruges, således at det ikke er muligt for eksempelvis bogholdere, at få adgang til hemmelige dokumenter, som kun er tiltænkt ledelsen.
Styringen af adgang til netværket, for de forskellige grupper, er lavet af IT-afdelingen, som sammen med ledelsen har defineret hvilke adgange den enkelte gruppe skal have. Definitionen bliver ikke revurderet efter nogen forud aftalt periode. Hvis der opstår nye behov for den enkelte medarbejder, skal denne søge om at få adgang til de nødvendige dele, hvorefter IT-afdelingen drøfter forespørgslen med den ansattes daglige leder, og giver derefter tilladelse, hvis det skønnes fornuftigt.
Når der bliver ansat nye medarbejdere, bliver de placeret i en gruppe og proceduren er den samme, når disse nye medarbejdere skal have adgang til nye områder på netværket, som når andre medarbejdere skal have adgang til mere. Når en medarbejder først har fået adgang til et område, bliver denne tilladelse ikke revurderet på noget tidspunkt. Når tilladelsen er givet, er der ikke nogle procedurer eller retningslinjer for, at brugerrettighederne skal revurderes, hverken af IT-afdelingen eller en mellemleder.

Sandsynligheden for at der sker kritiske nedbrud på BB A/S´ IT-aktiver, eller at fortrolige dokumenter kommer til kendskab for uvedkommende personer, som følge af virksomhedens procedure omkring adgangsstyring, vurderes til middel. Når der ikke er nogle faste procedure for gennemgang af brugerrettigheder, kan nogle medarbejdere få informationer, som er kritiske for virksomheden, da der ikke er styr på hvilke personer der har udvidet adgang.

Konsekvensen ved at uvedkommende personer får adgang til fortroligt materiale, eller at der sker et IT-nedbrud, som følge af BB A/S´ administration af brugerrettigheder, vurderes til middel. Denne vurdering bygger på, at fortrolige dokumenter, der er tilgængelig for mange medarbejdere, har større mulighed for at blive lækket til konkurrenter, enten tilsigtet eller utilsigtet. Dette vil have stor indflydelse på BB A/S´ konkurrenceevne, da konkurrenterne får indsigt i hvordan BB A/S prisfastsætter projekter med mere

13.7.2 Brugernes ansvar

Brugerne skal holde sig opdateret med hensyn til nye retningslinjer, som bliver udstukket af BB A/S. Det er brugernes eget ansvar, at holde sig opdateret og sørge for at holde sig inde for gældende retningslinjer. De til enhver tid gældende retningslinjer for IT i BB A/S, er placeret på selskabets intranet, som samtlige computere har som startside, når brugerne åbner browseren til Internettet. Der bliver dog ikke sendt nyhed rundt i virksomheden, hvis retningslinjerne bliver ændret, og dermed bliver disse ændringer kun set, hvis den enkelte medarbejder tilfældigvis læser dem igennem, på det rette tidspunkt.
I ansættelseskontrakten for medarbejderne i BB A/S, er det indskrevet at samtlige personlige koder til computere og netværk, skal holdes hemmelige og derfor ikke må deles med hverken kollegaer eller familiemedlemmer. De personlige koder, som medarbejderne har, skal ændres efter en forud defineret periode, som IT-systemet selv sørger for bliver overholdt. IT-systemet sørger ligeledes for, at retningslinjerne omkring et sikkert kodeord bliver overholdt, og dermed kommer til at indeholde både tal, samt store og små bogstaver.

Sandsynligheden for at BB A/S mister forretningsmæssigt kritisk materiale, samt at kritiske IT-nedbrud forekommer, er vurderet til middel. Denne vurdering bygger på, at der ikke er nogle faste procedure for hvorledes ændringer i retningslinjerne for brug af IT, bliver meldt ud til medarbejderne. Da brugerne selv skal være opmærksomme på opdateringer af detaljer i retningslinjerne, er der stor sandsynlighed for at dette ikke bliver læst. Dermed kan brugerne utilsigtet få installeret programmer, eller videregive fortroligt materiale på offentlige tilgængelige steder, som IT-afdelingen allerede har beskrevet, men som ikke er kommunikeret videre til brugerne.

Konsekvensen ved ovenstående er vurderet høj. Vurderingen bygger på den manglende procedure der er omkring opdateringen af retningslinjer for brugen af IT, i BB A/S. Den manglende procedure for opdatering af medarbejdere, kan få konsekvens for medarbejdernes omgang med nye programmer, hjemmesider og opdateringer. Hvis en medarbejder installerer et program på en computer, uden at kende til dette program, kan dette forårsage et IT-nedbrud, som kan være kritisk for virksomheden.

13.8 Anskaffelser, udvikling og vedligeholdelse af informationsbehandlingssystemer

Overordnede set, for anskaffelser, udvikling og vedligeholdelse af informationsbehandlings-systemer, gælder det at IT-afdelingen, står med ansvaret for at virksomhedens programmer fungerer efter hensigten.
IT-afdelingen i BB A/S har mulighed for at opdatere samtlige programmer og mulighed for at ændre i opsætningen af programmerne. Det kræver dog en indgående teknisk indsigt i virksomhedens programmer, for at kunne opdatere dem, og derfor benytter IT-afdelingen heller ikke muligheden for at opdatere programmerne. I praksis er det derfor udelukkende den eksterne serviceleverandør der opdaterer programmerne i den daglige drift og sørger for at programmerne har de muligheder, som BB A/S efterspørger. Når ændringerne er gennemført, bliver IT-afdelingen opdateret med de nye kildekoder, således at IT-afdelingen, formelt, stadig kan lave ændringer i programmerne og gennemgå ændringerne.
Når den eksterne serviceleverandør har opdateringer til de programmer, som BB A/S anvender, sender de en forespørgsel til IT-afdelingen, for at få adgang til netværket, hos BB A/S. Opdateringerne foregår udelukkende når programmerne ikke bruges i driften, gerne om natten og op til en weekend, således at den daglige drift ikke forstyrres og der ikke sker tekniske fejl, som følge af opdateringerne. Når opdateringerne er gennemført, er det den eksterne serviceleverandør der sørger for, at programmet fungerer efter hensigten og at programmerne stadig lever op til BB A/S´ krav indenfor sikkerhed og anvendelighed. Hvis medarbejderne, der dagligt bruger programmerne i driften hos BB A/S, finder uregelmæssigheder, rapporteres dette til IT-afdelingen, som derefter enten retter fejlene eller rapporterer det videre til serviceleverandøren.

Sandsynligheden for at der sker et nedbrud på IT-driften hos BB A/S, som følge af procedurerne omkring anskaffelse, udvikling og vedligeholdelse af informationssystemer, vurderes til lav. Dette begrundes med det faktum, at de eksterne serviceleverandører lever af at sælge holdbare løsninger til deres kunder og dermed ikke kan eksistere, hvis der er mange og kritiske problemer med den måde de driver forretning. Dog øges sandsynligheden for et nedbrud på programmerne, da der ikke er en IT-medarbejder fra BB A/S, der godkender opdateringerne, inden de sættes i drift i virksomheden.
Konsekvensen ved at et af BB A/S´ programmer går ned, som følge af en fejl i en opdatering, vurderes til høj. Da BB A/S er afhængig af, at deres programmer i både administrationen og produktionen virker, vil et nedbrud være omkostningsfuldt for virksomheden. Det vil eksempelvis ikke være muligt at blande beton til elementerne, hvis programmerne i produktionen ikke virker.

13.9 Beredskabsstyring

BB A/S har udarbejdet en nødplan for et større IT-nedbrud, som koncerninstruksen foreskriver. Denne nødplan indeholder en personoversigt over hvilke personer der skal kontaktes ved et eventuelt større nedbrud. Disse personer er IT-chefen og en navngivet person fra et eksternt selskab, indenfor IT-branchen.
Denne nødplan beskriver hvorledes IT-driften i BB A/S skal reetableres, med hensyn til fremgangsmåde og i hvilken rækkefølge de enkelte punkter skal reetableres. Nødplanen stiller som krav, at de personer der er i oversigten, skal have den fornødne viden, for at gennemføre en reetablering af IT, og at der altid skal være minimum to personer, som står i oversigten. I nødplanen er det blot beskrevet, at der skal indlæses en brugbar backup, men der stilles ikke krav til hvornår denne backup senest må have været foretaget.
Ved et eventuelt nedbrud, er det IT-chefen der står for at skulle forklare de enkelte mellemledere, hvilke problemer der er og hvornår det forventes at IT-driften er reetableret. Der er ikke nogle nedskrevet procedure for, hvem der tager sig af den eksterne kommunikation til kunder og leverandører.

Da det kræver en stor teknisk indsigt til, for at vurdere hvor stor sandsynligheden er, for at nødplanen ikke virker efter hensigten, vil der ikke blive kommenteret på denne sandsynlighed.

Konsekvensen ved, at nødplanen ikke virker efter hensigten, vurderes til høj. Denne vurdering bygger på BB A/S´ afhængighed af IT, som er stor og derfor er det vigtigt, at virksomheden har et beredskab klar, ved et eventuelt IT-nedbrud. Som tidligere nævnt, er BB A/S afhængige af, at deres IT-systemer er pålidelige, da både produktion af betonelementer, arkitekt-tegninger og størstedelen af administrationen vil være ude af drift, hvis alt IT bliver ramt af et nedbrud.

13.10 Opsummering af risikoanalyse for BB A/S

Ovenstående risikoanalyse er udarbejdet med et formål, at sætte fokus på de mest relevante problemstillinger indenfor IT-sikkerhed i BB A/S. Risikoanalysen har beskrevet forhold der er betænkelige ved anvendelse af IT i virksomheden.

For hvert emne er der beskrevet forholdene i BB A/S og der er lavet en vurdering af sandsynlighed for, og konsekvens af, et større nedbrud eller tab af fortroligt materiale.
Nedenstående tabel viser hvordan hvert enkelt område blev vurderet i risikoanalysen med hensyn til sandsynligheden for tab af materiale og/eller større IT-nedbrud, samt konsekvensen heraf.:

Tabel 1: Oversigt over trusselsbilledet i BB A/S

Område:	**Sandsynlighed:**	**Konsekvens:**	**Trusselsnummer:**
Overordnede retningslinjer	Lav	Høj	Nr. 1
Organisering af informationssikkerhed			
- *Interne organisatoriske forhold*	Høj	Høj	Nr. 2
- *Eksterne samarbejdspartnere*	Lav	Middel	Nr. 3
Styring af informationsrelaterede aktiver	Middel	Middel	Nr.4
Medarbejdersikkerhed			
- *Sikkerhedsprocedure før ansættelsen*	Lav/Middel	Høj	Nr. 5
- *Ansættelsens ophør*	Lav	Høj	Nr. 6
- *Ansættelsesforholdet*	Middel	Middel/Høj	Nr. 7
Fysisk sikkerhed			

- *Sikre områder, computere*	Lav	Middel/Høj	Nr. 8
- *Sikre områder, servere*	Lav	Høj	Nr. 9
- *Beskyttelse af udstyr, computere*	Lav	Middel	Nr. 10
- *Beskyttelse af udstyr, servere*	Lav	Høj	Nr. 11
Styring af netværk og drift			
- *Operationelle procedurer og ansvarsområder*	Lav	Høj	Nr. 12
- *Eksterne serviceleverandør*	Lav	Middel	Nr. 13
- *Logning og overvågning*	Lav/Middel	Middel/Høj	Nr. 14
Adgangsstyring			
- *Administration af brugerrettigheder*	Middel	Middel	Nr. 15
- *Brugernes ansvar*	Middel	Høj	Nr. 16
Anskaffelser, udvikling og vedligeholdelse af informationsbehandlingssystemer	Lav	Høj	Nr. 17
Beredskabsstyring	-	Høj	Nr. 18

Efter risikoanalysen er gennemgået, og det er muligt at danne sig et overblik over hvilke områder BB A/S bør fokusere på. Det er i første omgang de områder, som er forbundet med de største risici, altså der hvor der både er høj sandsynlighed for et IT-nedbrud/tab af fortroligt materiale og høj konsekvens ved dette. Herefter tages de områder med næststørst risici, altså der hvor sandsynligheden og konsekvensen er henholdsvis "Middel/Høj og "Høj/Middel". Dernæst kommer områder hvor sandsynligheden og konsekvensen er: "Høj/Lav", "Middel/Middel" og "Lav/Høj". Til sidst kommer de områder med både lav sandsynlighed og lav konsekvens, hvis det vurderes relevant.

For at skabe det bedste overblik over det aktuelle trusselsbillede, er samtlige punkter fra oversigtet indsat i nedenstående figur, fra DS 484 (2005). Denne figur viser hvor hvert enkelt punkt er placeret i forhold til sandsynlighed og konsekvens.

Figur 2 – trusselsbilledet i BB A/S

Sandsynlighed

Konse-kvens	Lav	Middel	Høj
Lav			
Middel	**3 – 8 – 10 – 13**	**4 – 14 – 15**	
Høj	**1 – 6 – 9 – 11** **12 – 17**	**5 – 7 – 16**	**2**

I ovenstående figur, er trusselsnummer 18 – "beredskabsstyring", ikke indplaceret, da der ikke er foretaget en vurdering af sandsynligheden for, at dette punkt ikke virker efter hensigten.

Figuren illustrerer i hvilket omfang, BB A/S er udsat for risici, ved at være afhængige af IT. Det mest kritiske, er hvis der er forhold der bliver kategoriseret i det røde felt. Derefter kommer forhold i de gule felter og til sidst, forhold i de grønne felter.

14. Kontrolmiljøet i BB A/S

Ledelsen i BB A/S, har valgt at lægge opgaverne omkring IT i IT-afdelingen. Dette indebærer opgaver indenfor den daglige drift, men også overordnede beslutninger omkring hvorledes IT-sikkerheden skal gribes an i virksomheden.

Fra koncernledelsen er der udstukket retningslinjer, som foreskriver hvilke formalia der skal overholdes for IT-driften i dattervirksomhederne. Dette inkluderer, at der bl.a. skal udarbejdes en nødplan. Derudover foreskriver koncern-retningslinjerne også, at den lokale ledelse i dattervirksomhederne skal forholde sig aktivt til de gældende IT-retningslinjer i de lokale virksomheder. Som tidligere beskrevet, er der i BB A/S tale om, at det er IT-chefen der har udarbejdet de gældende IT-retningslinjer, som efterfølgende er godkendt af ledelsen. Selvom dette ikke er helt efter hensigten, tvinger det dog ledelsen i BB A/S, til at sikre sig, at retningslinjerne som minimum overholder koncern-retningslinjerne.

Selvom ledelsen godkender IT-retningslinjerne, beskriver IT-chefen dog dette, som formalia. Ledelsen stoler på at IT-chefen har sørget for, at retningslinjerne for IT sikrer, at der er et fornuftigt sikkerhedsniveau. Udover godkendelse af IT-retningslinjerne, har ledelsen af BB A/S ikke været nævneværdigt engageret i problemstillingerne omkring IT i virksomheden. I realiteten fralægger ledelsen sig ansvaret for IT-sikkerheden i BB A/S.
Dermed er der ikke gjort særligt meget omkring kontrolmiljøet for IT i BB A/S, som må betegnes som generelt svagt. Illustreret ved nedenstående figur, vises hvilke trusler, der som følge af det pågældende kontrolmiljø, bør arbejdes med, for at forbedre sikkerheden:

Figur 3 – risikobilledet i BB A/S

Kontrolmiljø

Trussel-niveau	Stærk	Middel	Svagt
Lav			**1 – 3 – 6 – 8 – 9 – 10 – 11 –12 – 13 – 17**
Middel			**4 – 5 – 7 – 14 – 15 – 16**
Høj			**2**

Trusselsnumrene refererer til de oplistede trusler i tabel 1 "Oversigt over trusselsbilledet i BB A/S"

Det anbefales at ledelsen i BB A/S starter med at overveje, hvorledes virksomheden bør forholde sig til de interne organisatoriske forhold, herunder ledelsens rolle og ansvarsplacering. Dette begrundes med, at det er dette punkt der er placeret i det røde felt, i oversigten over risikobilledet og dermed udgør den største risiko i virksomheden.

Efterfølgende bør ledelsen i BB A/S tage sig af den resterende del af områderne i risikoanalysen, hvor ledelsen især bør være opmærksom på følgende emner, som alle er placeret i det gule felt i oversigten over risikobilledet i virksomheden:

- Medarbejdersikkerhed, herunder ansættelsesforholdet.
- Styring af netværk, herunder logning og overvågning.
- Adgangsstyring, herunder brugernes ansvar.

15. Anbefalinger til BB A/S

Efter udarbejdelsen af risikoanalysen for BB A/S, er følgende gennemgang bygget på anbefalingerne fra DS 484 (2005). Standarden kommer på hvert område kommer med konkrete løsningsforslag, samt hvilke overvejelser, virksomheder bør gøre sig, i forbindelse med gennemgangen af informationssikkerheden. De punkter der er beskrevet i følgende afsnit, er de punkter, som det er vurderet, at BB A/S bør efterleve. Dette skal sikre et acceptabelt sikkerhedsniveau, for informationssikkerheden i virksomheden.

15.1 Overordnede retningslinjer

I risikoanalysen blev de overordnede retningslinjer vurderet til at have en lav sandsynlighed, men høj konsekvens, for at forårsage et kritisk nedbrud, eller tab af kritisk materiale, i BB A/S. Det beskrives ligeledes at de overordnede retningslinjer ikke regelmæssigt bliver gennemgået, for at vurdere, om der kræves nye formuleringer, beskrives nye forhold eller nye retningslinjer for allerede beskrevet emner.

DS 484 (2005) anbefaler, at en virksomheds overordnede retningslinjer for informationssikkerhed, opfylder en række punkter, heriblandt "en understregning af ledelsens støtte og engagement"[9]. Når man læser de overordnede retningslinjer for BB A/S, er den eneste formulering fra ledelsen side, at retningslinjerne er udarbejdet i samarbejde med IT-chefen og ledelsens vurdering er at:

"*BB A/S er stærkt afhængigt af at IT systemerne virker 100 % optimalt hver eneste dag og det er derfor yderst vigtigt, at IT-sikkerhedspolitikken respekteres*.[10]".

Denne beskrivelse, er eneste sted, hvor ledelsen kommer med sit synspunkt på IT i virksomheden og det anbefales, at ledelsen viser et større engagement for informationssikkerheden i virksomheden.

[9] DS 484, side 23
[10] BB A/S – IT-sikkerhedpolitik, side 3

DS 484 (2005) anbefaler ligeledes at de overordnede retningslinjer løbende vedligeholdes og revurderes. Denne vedligeholdelse og revurdering, bør efter anbefalingerne i DS 484 (2005), bygges på blandt andet:

- Tilbagemelding fra interessenter
- Resultatet af tidligere ledelsesvurderinger
- Ændringer i trusler og sårbarheder

Derudover bemærkes det i DS 484 (2005), at der skal ske en opfølgning på de overordnede retningslinjer mindst en gang om året.

Disse punkter, samt bemærkningen, bliver ikke fuldt i BB A/S. IT-chefen, samt den tidligere ansat, fortæller at der ikke er nogen løbende undersøgelser i virksomheden, som går på at få tilbagemeldinger fra brugerne af virksomhedens IT. Derudover bliver der ikke foretaget ledelsesvurderinger af de overordnede retningslinjer i virksomheden, hvorfor det ikke er muligt at få et resultat fra tidligere ledelsesvurderinger. Ledelsen laver ikke løbende vurderinger af ændringer i trusler og sårbarheder, og får heller ikke IT-afdelingen til at følge op på dette punkt. IT-afdelingen laver dog løbende sine egne vurderinger, men der er ikke nogle fastsatte tidspunkter, hvor ledelsen beder om en vurdering, eller beder IT-afdelingen fokusere på dette område. Hvis ikke IT-afdelingen, i en periode, udelukkende koncentrerer sig om denne problemstilling, kan arbejdet blive forstyrret af de daglige opgaver og problemer, som der opstår i en virksomhed der er afhængig af IT.

15.2 Organisering af informationssikkerhed

15.2.1 Internt i virksomheden

I risikoanalysen bliver det vurderet, at der er en høj sandsynlighed for at IT-chefen i BB A/S kan lave nogle uhensigtsmæssige prioriteringer, som følge af ledelsens manglende engagement i organiseringen af informationssikkerheden. Det vurderes ligeledes, at have en høj konsekvens, hvis der sker nedbrud

på forretningsmæssige vigtige IT-aktiver, ligesom læg af forretningskritisk materiale er yderst kritisk for virksomheden.

I DS 484 (2005) anbefales det, at ledelsen i virksomheden laver en præcis ansvarsplacering for IT. Dette gøres i retningslinjerne for IT i BB A/S, hvor ansvaret for den samlet drift af IT, bliver placeret hos ISO (IT-chefen). Denne ansvarsplacering sker på første side af IT-sikkerhedspolitikken i virksomheden.

Udover placering af ansvaret for IT i virksomheden, anbefales det i DS 484 (2005) blandt andet, at ledelsen skal påse følgende:

- At sikkerhedsstrategien bliver løbende revurderet og godkendt
- At der foreligger handlingsplaner for den løbende sikkerhedsbevidstgørelse
- At implementeringen af sikringsforanstaltninger er tværorganisatorisk koordineret

Disse anbefalinger er ikke praksis i BB A/S, hvor ledelsen ikke udfører nogle af ovenstående punkter. Sikkerhedsstrategien bliver udelukkende opdateret, når der udarbejdes nye krav fra koncernens IT-afdeling i Holland. Som nævnt i risikoanalysen, er den sidste sikkerhedsstrategi fra 2006. Det har ikke været muligt at finde ud af, om ledelsen har handlingsplaner for hvordan den løbende sikkerhedsbevidstgørelse skal foregå. Det er dog konstateret, ved interview med IT-chefen og den tidligere ansatte i BB A/S, at der ikke løbende bliver holdt kurser for IT-sikkerheden i BB A/S. Sikringsforanstaltninger i BB A/S varetages stort set kun af IT-afdelingen, som sørger for at implementeringen bliver udført og kommunikeret ud i de enkelte afdelinger, hvis der skønnes et behov herfor.

Som bemærkning i DS 484 (2005), anbefales det, at ledelsen skal vurdere behovet for ekstern rådgivning, i forhold til de kompetencer, som virksomheden selv besidder og erfaringer, som virksomheden selv har gjort sig.
I praksis, er der tilknyttet en enkelt konsulent, som skal være behjælpelig med proceduren omkring genstart af IT-systemet og dataindlæsning af backup, hvis der sker et større nedbrud på serverne i

virksomheden. Denne konsulent er udpeget i en fælles beslutning af IT-chefen og ledelsen i virksomheden.
Derudover er der ingen tilknyttede konsulenter, da ledelsen i BB A/S har tillid til at IT-chefen de fornødne kompetencer på alle områder indenfor IT, eller at IT-chefen selv melder ud, hvornår han har brug for assistance ved konkrete problemstillinger.

For nødplanen i BB A/S, er det vurderet i risikoanalysen, at procedurerne herfor giver en høj sandsynlighed for, at nødplanen ikke bliver opdateret i det omfang det bør gøres. Begrundelsen er, at der ikke er nogle faste procedure for periodisk opfølgning, hverken for formuleringen eller for at afprøve læsbarheden af backup data. Konsekvensen ved at nødplanen ikke bliver løbende revurderet er vurderet til høj.

DS 484 (2005) anbefaler, at der skal udarbejdes planer med konkrete intervaller for gennemgang af praksis i virksomheden. Dette indebærer både gennemgang af eksempelvis nødplanen, samt gennemgang af praksis for indlæsning af backup. Det anbefales at gennemgangen af eksempelvis procedure for genindlæsning af backupdata, bliver ledet af en uafhængig rådgiver, så det er muligt at få et reelt billede af virksomhedens procedurer. Denne gennemgang kan eksempelvis ledes af virksomhedens revisor, hvis denne har de nødvendige kvalifikationer, til at lede en sådan gennemgang. Når gennemgangen er udført, skal det dokumenteres hvilke områder der er gået godt og hvilke områder der er plads til forbedringer. Derudover skal det dokumenteres hvordan procedurerne overholder retningslinjerne i virksomheden. Hvis den samlede dokumentation viser, at virksomhedens retningslinjer ikke overholdes, skal ledelsen foretage de nødvendige beslutninger, således at sikkerhedsniveauet er på højde med det forventede. Derudover kan den samlede dokumentation også indeholde konkrete forbedringsforslag, hvis den uafhængige rådgiver, mener der er væsentlige forbedringer.

Samtlige af ovenstående anbefalinger foreslår, at ledelsen i virksomheden skal have, og vise, et stort engagement for IT-sikkerheden i BB A/S. Det er ikke nok med at give ansvaret til IT-chefen, da denne person ikke nødvendigvis har den rette forretningsmæssige forståelse for, hvad der er skal prioriteres frem for andet. Dette kan eksempelvis give udslag i, at der bliver prioriteret forkert med hensyn til de

sikkerhedsniveauer der skal gælde for de forskellige områder. Ledelsen af BB A/S bør tage det overordnede ansvar for IT-sikkerheden og IT-driften og kommunikere ud i virksomheden, at IT er et centralt område for BB A/S. Derefter kan ledelsen overlade opgaverne for den daglige drift til IT-afdelingen. Dette vil sikre, at der arbejdes i den retning, som ledelsen ønsker, samtidig med at ressourceforbruget i ledelsen ikke ændres fra at have fokus på at udvikle de kompetencer, der er nødvendige, for at BB A/S kan klare sig på markedet for betonelementer.
Ved at tage det overordnede ansvar for IT i virksomheden og engagere sig i IT-driften, får ledelsen en bedre indsigt i hvordan der bør arbejdes med IT i virksomheden. Dermed undgår virksomheden at være afhængig af en enkelt person, som kan være et problem, hvis denne person ikke ønsker at være i virksomheden mere.

15.2.2 Eksterne samarbejdspartnere

Sandsynligheden for nedbrud, som følge af BB A/S´ samarbejde med eksterne samarbejdspartnere, er i risikoanalysen vurderet til lav. Konsekvensen er vurderet til middel.

DS 484 (2005) anbefaler, at der laves en risikovurdering for, hvordan eksterne samarbejdspartners adgang til virksomhedens eget netværk kan påvirke driften i virksomheden. Denne risikovurdering, skal blandt andet udarbejdes under overvejelse af følgende punkter:

- De informationsbehandlingsfaciliteter samarbejdspartneren skal have adgang til
- Den forretningsmæssige værdi af de involverede informationsaktiver
- Beskyttelsesforanstaltninger for informationsaktiver, der ikke er omfattet af samarbejdet
- Samarbejdspartnerens informationslagrings-, behandlings- og kommunikationsudstyr og de hertil knyttede sikringsforanstaltninger

IT-chefen fortalte under interviewet, at de eksterne samarbejdspartnere, udelukkende har adgang til den del af netværket, som behøves for at kunne opdatere de programmer, som BB A/S benytter sig af og har brug for at få opdateret. De programmer der opdateres af eksterne samarbejdspartnere, bruges blandt andet i produktionen af betonelementer og har dermed en høj forretningsmæssig værdi.

For samarbejdet med eksterne samarbejdspartnere, er det IT-chefen, der har defineret hvilke adgange samarbejdspartnerne skal have. De forretningsmæssige betingelser har ledelsen af BB A/S været med til at udforme. Dermed følger ledelsen til dels anbefalingerne fra DS 484 (2005), hvor de skal spille en aktiv rolle omkring engagementet med eksterne samarbejdspartnere, dog uden at sætte betingelserne for adgang til BB A/S´ netværk, samt hvilke sikkerhedskrav de skal leve op til.

15.3 Styring af informationsrelaterede aktiver

I risikoanalysen blev det vurderet, at sandsynligheden for at miste forretningskritisk materiale, er middel. Konsekvensen blev også vurderet til middel, ved at miste materiale, som eventuelt befinder sig på transportable medier.

I DS 484 (2005) bliver det anbefalet, at der føres en fortegnelse over alle væsentlige aktiver i virksomheden og at denne fortegnelse løbende bliver ajourført. Fortegnelsen over IT-aktiver bør ligeledes indeholde en vurdering over aktivets sikkerhedsklassifikation, for på den måde at fortælle den ansvarlige for aktivet, hvilket niveau det skal beskyttes.
Fortegnelsen med IT-aktiver, bør løbende udarbejdes, når nye aktiver bliver købt i virksomheden. Det bør fremgå af fortegnelsen, hvem der er ansvarlig for hvert enkelt aktiv og det skal fremhæves, at den enkelte ansvarshaver skal beskytte og står til ansvar for aktiverne. For IT-aktiver, hvor der ikke er en enkelt bruger, eksempelvis printer og fax, skal der anføres, hvilket sted aktivet står, således at det er muligt at finde hvert enkelt aktiv. IT-aktiverne skal mærkes, så det er muligt for IT-afdelingen at tage et hvilket som helst aktiv, og se hvem der har ansvaret for aktivet, eller hvor aktivet bør være placeret.

15.4 Medarbejdersikkerhed

15.4.1 Sikkerhedsprocedure før ansættelsen

I risikoanalysen blev det vurderet, at der er lav/middel sandsynlighed for at BB A/S mister forretningsmæssigt kritisk materiale, eller at der sker et IT-nedbrud, som følge af virksomhedens

procedure for ansættelse af nye medarbejdere. Konsekvensen ved dette, er i risikoanalysen vurderet til høj.

Det anbefales i DS 484 (2005), at virksomhederne inden ansættelse af nye medarbejdere, vurderer kandidaternes egnethed til et job, hvor der er adgang til forretningsmæssige kritiske oplysninger. Det anbefales ligeledes, at virksomheden gør kandidaten opmærksom på, at det er et ansvarsfuldt område, og at manglende integritet og forsigtighed, vil kunne pådrage virksomheden tab, ved eksempelvis tyveri og menneskelige fejl.

Ved ansættelse, anbefales det at den nye medarbejder blandt andet underskriver en tavsheds-erklæring, hvis medarbejderen har adgang til fortrolige/følsomme oplysninger. Denne anbefaling følges ikke i BB A/S, hvor nye medarbejdere udelukkende underskriver en erklæring om, at de er bekendte med de gældende retningslinjer for brugen af IT i virksomheden. Herunder står der dog, at det ikke er tilladt at dele fortroligt/følsomt materiale med andre.

15.4.2 Ansættelsens ophør

I risikoanalysen blev det vurderet at der er lav sandsynlighed for, at der sker et kritisk IT-nedbrud, eller at virksomheden mister forretningskritisk materiale, som følge af virksomhedens procedure for tidligere medarbejdere. Konsekvensen ved at tidligere medarbejdere, offentliggøre forretningsmæssigt kritisk materiale, eller tilsigtet laver et større IT-nedbrud, er vurderet til høj.

Når en medarbejder forlader virksomheden, hvad enten det er virksomheden, eller den ansatte der ønsker at ophæve samarbejdet, anbefaler DS 484 (2005), at der er en fast procedure, som den HR-ansvarlige i virksomheden gennemgår med den tidligere ansat. Dette skal gøres for at understrege den tidligere ansattes forpligtigelser, hvis denne har sådanne, efter ansættelsesforholdet. Derudover skal den tidligere ansat aflevere samtlige aktiver fra virksomheden, herunder IT-relateret aktiver. Det skal sikres at der bliver tilbageleveret eksempelvis virksomhedsdokumenter, bærbart udstyr, adgangskort og manualer.

For at en tidligere ansat bliver påkrævet at tilbagelevere førnævnte udstyr, kræves det, at der er ajourførte fortegnelser over hvilke medarbejdere der har fået udleveret aktiverne. I BB A/S, er disse lister ikke ajourførte, og det anbefales derfor, at dette får højere prioritering.

IT-afdelingen i virksomheden skal derudover sørge for, at samtlige brugerrettigheder for en tidligere ansat bliver slettet og derved ikke længere kan få adgang til virksomhedens netværk. Dette skal gøres ved at der bliver oprettet en fast procedure for ophør af ansættelsesforhold, således at IT-afdelingen bliver meddelt, at en pågældende medarbejder ikke længere er i virksomheden.

15.4.3 Ansættelsesforholdet

For nuværende medarbejdere, blev det i risikoanalysen vurderet at sandsynligheden for et kritisk nedbrud, eller tab af data til middel, er middel. Konsekvensen ved førnævnte, vurderes til middel/høj.

Det anbefales i DS 484 (2005), at ledelsen sørger for at medarbejderne, igennem hele ansættelsesforholdet, fastholder virksomhedens sikkerhedsniveau, med hensyn til sikkerhedspolitik, retningslinjer og procedurer. Dette gøres blandt andet ved, at ledelsen i BB A/S, har fokus på følgende punkter fra DS 484 (2005), for medarbejderne:

- At de er blevet tilstrækkeligt informeret om deres roller og ansvar i forbindelse med sikkerhed, før de tildeles adgang til virksomhedens systemer og data.
- At de er blevet gjort bekendt med de nødvendige retningslinjer, således at de kan leve op til virksomhedens informationspolitik.

Under ansættelsesforholdet er medarbejderne i BB A/S, ikke forpligtet til løbende at holde sig opdateret med retningslinjerne i virksomheden[11]. Medarbejdere i BB A/S underskriver ved ansættelsens start, at de er bekendt med indholdet af IT-sikkerhedspolitikken, men bliver ikke løbende orienteret om ændringer.

[11] Oplyst af tidligere medarbejder under interview

Som bemærkning, beskriver DS 484 (2005), at hvis virksomheden har en uengageret ledelse, i forhold til IT-sikkerheden, skaber dette et forringet sikkerhedsniveau.

Det anbefales også i DS 484 (2005), at der er en fast procedure for sanktioner, overfor medarbejdere, der forbryder sig mod IT-sikkerhedspolitikken. Denne anbefaling er ikke praksis i BB A/S, hvor det er op til IT-chefen, sammen med medarbejderens afdelingsleder, at fastsætte en konkret straf. Hvis medarbejderen har forbrudt sig i grov grad, overfor sikkerhedspolitikken, bliver HR-chefen dog kontaktet, og er med til at bestemme den konkrete sanktion.

15.5 Fysisk sikkerhed

Ligesom i risikoanalysen, bliver afsnittet for anbefalinger i DS 484 (2005), opdelt i computere og servere. Dette skyldes, ligesom i risikoanalysen, at der er stor forskel på de forretningsmæssige risici. Fokus for computerne, er at undgå at miste data, imens fokus for servere, er at undgå nedbrud.

15.5.1 Sikre områder

I risikoanalysen var vurderingen for computere, at sandsynligheden for at miste forretningsmæssigt kritisk data, er lav. Konsekvensen for BB A/S, ved tab af kritisk materiale, blev i risikoanalysen vurderet til middel/høj.

Risikoanalysen beskriver hvordan den generelle fysiske sikkerhed er i BB A/S, som følge af, at denne er afgørende for computernes sikkerhed.
I forhold til de anbefalinger DS 484 (2005) har, er BB A/S godt sikret, når det handler om den fysiske sikkerhed for computere i virksomheden. Dog bør virksomheden overveje følgende anbefalinger fra DS 484 (2005):

- Der skal være etableret fysisk adgangskontrol, så kun autoriseret personale kan få adgang.
- Fysiske barrierer skal være udformet, så de forhindrer uautoriseret adgang og skader fra det fysiske miljø.

Disse punkter bør ledelsen i BB A/S overveje, om de bliver fulgt i tilstrækkelig grad i virksomheden. Dette begrundes med muligheden for at gå ind på virksomhedens område, uden autorisation, eksempelvis i produktionshallerne, hvor der ikke er nogen fysisk adgangskontrol. Derudover er der heller ingen fysiske adgangskontroller for adgang til administrationen. Begge mangler opvejes dog af, at det er påbudt for medarbejdere, at bære id-kort, således at ansatte kan se, om en given person hører til virksomheden, eller ej.

For servere i BB A/S gælder stort set samme vurdering, indenfor sikre områder, som for computere i risikoanalysen. Sandsynligheden for et nedbrud på serverne, som følge af sikkerheden i virksomheden, blev vurderet til lav, imens konsekvensen blev vurderet til høj.

For serverne gælder det, som beskrevet i risikoanalysen, at der er større sikkerhed, i forhold til indbrud eller uautoriseret adgang. Serverrummet er beskyttet af en dør, hvor det udelukkende er personalet i IT-afdelingen, der har adgang, i form af en nøgle. Som følge af den høje konsekvens ved et IT-nedbrud, anbefales det dog, at der bliver sat en branddør i serverrummet, som samtidig er svær at bryde ind i. Derudover bør adgangen til rummet være mere sikkert, end en nøgle. Denne sikkerhed kunne eksempelvis designes således, at der kræves både nøgle samt kode, for at kunne komme ind i serverrummet.

15.5.2 Beskyttelse af udstyr

I risikoanalysen var vurderingen for computere, at der er en lav sandsynlighed for kritiske nedbrud, som følge af forholdene omkring beskyttelse af udstyr i virksomheden. Konsekvensen for et nedbrud, blev vurderet til middel. Konsekvensen ved et nedbrud er rangeret højere end en umiddelbar vurdering, på grund af den manglende procedure for vedligeholdelse af virksomhedens computere.

Det anbefales i DS 484 (2005), at der tages hensyn til hvorledes IT-aktiverne er placeret i virksomheden, således at risikoen for skader og uautoriseret adgang minimeres. Dette kan gøres ved at følge anbefalingerne i DS 484 (2005), som bland andet indeholder følgende:

- Udstyr skal placeres, så behovet for uvedkommendes adgang til arbejdsområdet minimeres.
- Udstyr, hvorpå der behandles kritiske/følsomme informationer, skal placeres, så informationerne ikke kan læses af uvedkommende.

Disse anbefalinger følges til dels i BB A/S. Det blev dog konstateret under besøget hos virksomheden, at i nogle afdelinger, var det muligt at se hvilke arkitekt-projekter, tegnerne var i gang med at lave.

Derudover anbefales det, at der bliver nedskrevet faste procedure for vedligeholdelsen af computere i BB A/S, således at der løbende kan føres kontrol med vedligeholdelsen.

I risikoanalysen blev det vurderet, at sandsynligheden for et nedbrud på serverne i BB A/S, som følge af procedurerne for beskyttelse af udstyr, er lav. Konsekvensen for et nedbrud er vurderet til at være høj.

Det anbefales blandt andet i DS 484 (2005), at der er en nødgenerator i virksomheden, således at det er muligt at lukke systemerne ned, på sædvanligvis. Dette lever BB A/S op til, da de har en nødgenerator stående, som slår til, i tilfælde af strømafbrydelser. Derudover anbefales følgende i DS 484 (2005):

- Udstyr skal placeres eller beskyttes, så risikoen for mulige fysiske trusler som tyveri, brand, varme, eksplosioner, røg, vand, støv, rystelser, kemiske påvirkninger, strømforstyrrelser, kommunikations-forstyrrelser, elektromagnetisk stråling, hærværk osv. minimeres.

Denne anbefaling lever BB A/S i stor grad op til. Men som det er beskrevet i risikoanalysen, så løber der et vandrør igennem serverrummet, som ved lækage, kan kortslutte og ødelægge serverne. Denne risiko har IT-afdelingen prøvet at minimere, ved ikke at placere serverne på gulvet, men de er derimod blevet hævet, så de ikke får vand ind i sig, hvis der blot ligger lidt vand på gulvet. Der er dog ikke lagt noget oven på serverne, så hvis et vandrør sprænger lige over serverne, vil de blive våde.
Det anbefales at der i højere grad tages højde for denne risiko, således at vandrøret enten ledes udenom serverrummet, eller at serverrummet bliver flyttet til et bedre lokale. Derudover anbefales det, ligesom

med computerne i virksomheden, at der udarbejdes en fast procedure for vedligeholdelse af serverne, således at der løbende bliver fulgt op på servernes tilstand.

15.6 Styring af netværk og drift

15.6.1 Operationelle procedurer og ansvarsområder

I risikoanalysen blev det vurderet, at sandsynligheden for IT-nedbrud og tab af forretningsmæssige kritiske oplysninger, er lav, som følge af forretningsgangene for operationelle procedure og ansvarsområder i BB A/S. Konsekvensen blev vurderet til høj, ved eksempelvis tilsigtede fejl.

Som beskrevet i risikoanalysen, er det overordnede ansvar for IT i BB A/S, IT-afdelingens, med IT-chefen i spidsen. Foruden ansvaret, har IT-afdelingen også ubegrænset adgang til samtlige informationer, der findes i virksomheden. Der findes ingen funktionsadskillelse for IT-medarbejderne, som det ellers anbefales i DS 484 (2005), således at en enkelt medarbejder ikke kan ændre en handling, samtidig med at denne selv godkender handlingen.
Der kan ligeledes ske tilsigtede fejl, ved at en IT-medarbejder overtager en af de andre ansattes computer og derefter godkender svigagtige handlinger, i den anden medarbejders navn. Det anbefales, at en IT-medarbejder ikke kan overtage kontrollen med en anden computer på netværket, uden accept fra den bruger, der er logget ind på computeren. Hvis dette var tilfældet, vidste brugeren, at en IT-medarbejder havde taget kontrollen med computeren og kan dermed sikre sig, at der ikke foregår uhensigtsmæssige handlinger.

15.6.2 Ekstern serviceleverandør

I risikoanalysen blev det vurderet, at der er lav sandsynlighed for, at der sker et kritisk IT-nedbrud, som følge af procedurerne for eksterne serviceleverandører. Konsekvensen blev vurderet til middel.

DS 484 (2005) anbefaler, at der laves en overvågning af de eksterne serviceleverandører. Dette skal sikre, at der er opmærksomhed på de hændelser der opstår, når den eksterne serviceleverandør logger sig på BB A/S´ netværk. Nedenstående punkter er fra anbefalingerne i DS 484 (2005):

- Gennemgang af og opfølgning på sikkerhedshændelser, driftsproblemer, fejl og nedbrud
- Gennemgang af sikkerheds- og driftsrelateret logninger

Derudover påpeger DS 484 (2005), at det er virksomheden selv, der har det endelige ansvar for sikkerhedsniveauet i virksomheden.
Ved at gennemgå ovenstående punkter, har BB A/S mulighed for at sikre sig et godt fundament, for at lave en opsummering af risici og konsekvenser, ved at benytte en ekstern serviceleverandør. DS 484 (2005) lægger også op til dialog imellem parterne, hvorved det er muligt at årsagsforklare handlingerne, der er opstået som følge af de eksterne serviceleverandørers log-in på netværket i BB A/S. IT-chefen forklarede i interviewet, at de eksterne serviceleverandører i BB A/S, ikke bliver overvåget, da der ikke tidligere har været problemer. Der føres dog altid log, hvorved det er muligt at gå tilbage og se hvem og hvad der er ændret i programmer mm.

Derudover anbefaler DS 484 (2005), at der laves revision på den eksterne serviceleverandør, for derved at sikre sig, at leverandøren lever op til de sikkerhedsmæssige krav, der stilles i virksomheden. Denne revision kan eksempelvis udføres af leverandørens egen revisor, som derefter erklærer sig om, hvorvidt klienten overholder de retningslinjer, der er opstillet. Hvis revisor bliver opmærksom på afvigelser, skal denne omgående rette henvendelse til både leverandør og kunde, for at gøre opmærksom på problemstillingen.

15.6.3 Logning og overvågning

Det blev i risikoanalysen vurderet, at sandsynligheden for et større IT-nedbrud i BB A/S, er lav/middel, som følge af procedurerne for logning og overvågning. Konsekvensen blev vurderet til middel/høj.

Det anbefales i DS 484 (2005), at opfølgningsloggen blandt andet skal indeholde:

- Brugeridentifikation
- Arbejdsstationens identitet
- Aktivering og deaktivering af beskyttelsesprogrammer, fx antivirus og indbrudsalarmer.

Som beskrevet i risikoanalysen, så er det ikke muligt at se hvem der bruger computerne i produktionen, da disse computere ikke kræver at brugerens personlige log-in. Så selvom logningerne i BB A/S både viser arbejdsstationens identitet og aktivering og deaktivering af beskyttelsesprogrammer, så er det altså ikke muligt at se, hvem der foretager sig disse handlinger. Det må derfor anbefales, at det indføres, at der skal bruges log-in, på samtlige computere i virksomheden, for på den måde at kunne se, hvilke brugere der benytter computerne. Derved undgås sager, hvor det ikke er muligt at opspore, hvilken medarbejder der er ansvarlig for uhensigtsmæssige handlinger.

DS 484 (2005) anbefaler ligeledes, at det ikke er muligt at ændre i log-oplysningerne, som skal beskyttes imod følgende:

- Enhver form for ændringer i indholdet
- Sletning og ændringer af logfiler
- Tekniske fejl, eksempelvis overskrivninger, fordi der ikke er tilstrækkelig plads på lagringsmediet.

IT-chefen fortalte, at hvis der opstod en situation, hvor det var nødvendigt, så ville medarbejderne i IT-afdelingen kunne ændre i log-oplysningerne i virksomheden. Det er ledelsens ansvar, at designe effektive kontroller, som efterfølgende kan kontrolleres af en ekstern rådgiver. I dette tilfælde er der ikke tale om nogen effektiv kontrol, da IT-medarbejderne, hvis de ønsker det, kan ændre og slette de spor, som de finder nødvendige, for eventuelt at skjule en uhensigtsmæssig handling.

15.7 Adgangsstyring

15.7.1 Administration af brugerrettigheder

I risikoanalysen blev det vurderet, at der er middel sandsynlighed for tab af forretningsmæssige kritiske oplysninger, samt et IT-nedbrud, som følge af virksomhedens procedurer omkring adgangsstyring og brugernes ansvar. Konsekvensen heraf, vurderes til middel.

Når der bliver ansat nye medarbejdere i BB A/S, for de brugerrettigheder indenfor den gruppe, som den nye medarbejder skal arbejde sammen med. Derved sikres en ensartet rettighedsstyring. Hvis en medarbejder har brug for yderligere rettigheder, som følge af arbejdsmæssige opgaver, bliver disse rettigheder tildelt af IT-afdelingen, hvis dette er godkendt, af medarbejderens nærmeste leder. Disse to punkter lever op til DS 484´s (2005) anbefalinger, om at tildeling af brugerrettigheder sker systematisk og yderligere brugerrettigheder udelukkende bliver givet, som følge af et arbejdsrelateret behov.

DS 484 (2005) anbefaler ligeledes, at der skal være en periodisk gennemgang af brugerrettigheder, for at undgå uautoriseret adgang til følsomme data i virksomheden. Dette bliver ikke praktiseret i BB A/S, hvorfor der er risiko for, at medarbejdere har fået adgang til data, som ikke længere er relevant for deres arbejde. Det anbefales derfor, at der bliver oprettet konkrete retningslinjer for, hvorledes gennemgang af brugerrettigheder skal foregå. Denne gennemgang bør følge anbefalingerne fra DS 484(2005), som blandt andet indeholder følgende punkter:

- Brugernes rettigheder skal gennemgås regelmæssigt, fx hver 6. måned, og i forbindelse med ændringer i brugerens arbejdsmæssige forhold.
- Udvide adgangsrettigheder skal gennemgås regelmæssigt for at sikre, at ingen har fået uautoriserede rettigheder.

Dette vil sikre, at der ikke opnås uautoriseret adgang til virksomhedens data, som følge af fejlagtige brugerrettigheder.

15.7.2 Brugernes ansvar

Det blev i risikoanalysen vurderet, at der er middel sandsynlighed for at BB A/S mister kritisk materiale, eller der opstår et kritisk IT-nedbrud, som følge af procedurerne omkring brugernes ansvar. Konsekvensen heraf blev vurderet til høj.

Når IT-retningslinjerne for brugerne i BB A/S bliver opdateret eller justeret, bliver der, som omtalt i risikoanalysen, ikke udsendt nogen informationer til brugerne. Det forventes derimod, at medarbejderne selv holder sig opdateret med IT-retningslinjerne i virksomheden. Disse retningslinjer er placeret på virksomhedens intranet. Det anses dog ikke for tilstrækkeligt, at retningslinjerne blot placeres på første side af intranettet, da det ikke kan forventes, at brugerne læser disse retningslinjer løbende.
Derfor anbefales det, at medarbejderne skal informeres, når der kommer opdateringer og justeringer til IT-retningslinjerne, således at medarbejderne ved hvornår det er aktuelt at læse retningslinjerne.

15.8 Anskaffelser, udvikling og vedligeholdelse af informationsbehandlingssystemer

Sandsynligheden for et IT-nedbrud, som følge af procedurerne for anskaffelser, udvikling og vedligeholdelse af informationsbehandlingssystemer, er vurderet til lav i risikoanalysen. Konsekvensen ved et IT-nedbrud, vurderes til høj.

For at sikre virksomheden mod IT-nedbrud, som følge af vedligeholdelse fra eksterne serviceleverandører, anbefaler DS 484 (2005) at virksomheden blandt andet overvejer følgende:

- Licenser, ejerskab af kildekoder, andre intellektuelle rettigheder
- Test af nye versioner og rettelser før implementering for at sikre mod skadevoldende kode og trojansk kode.

Ovenstående punkter har BB A/S afdækket, ved at sørge for at have ejerskab og adgang til kildekoderne for programmerne der anvendes i virksomheden. Derudover har de eksterne

serviceleverandører forpligtet sig til at adskille testmiljøet fra driftsmiljøet og laver kun færdigprøvet opdateringer på programmerne i virksomheden.
Det anbefales dog, at der er en IT-medarbejder, der godkender samtlige opdateringer, inden disse tages i brug i BB A/S. Dette vil give en ekstra sikkerhed for, at der ikke opstår fejl ved implementeringen af nye opdateringer, og sikrer dermed imod IT-nedbrud.

15.9 Beredskabsstyring

I risikoanalysen, blev der ikke vurderet på hvor stor sandsynlighed der er for, at nødplanen i BB A/S ikke virker efter hensigten. Dette gøres ikke, da det kræver et stort teknisk indblik i hvordan processerne skal være, hvis en nødplan skal fungere efter hensigten. Konsekvensen for at nødplanen ikke virker, er vurderet til høj.

Som beskrevet er nødplanen udarbejdet på foranledning af kravet i koncern-instrukserne. Denne nødplan beskriver i hvilken rækkefølge, IT-aktiverne skal genstartes og hvem der er ansvarlig herfor. Derudover beskriver den, hvilken person der skal kontaktes uden for virksomheden, for at hjælpe med at genstarte IT-systemerne i BB A/S.

Nødplanen beskriver dog intet om hvem der skal stå for den eksterne kommunikation. Det anbefales, at der laves en Business Recovering Plan, som sætter fokus på hvordan hele virksomheden skal agere, i stedet for kun at have fokus på en IT Recovering Plan. Business Recovering Planen skal foreskrive hvilke procedure der skal foretages i tilfælde af et større IT-nedbrud, for hele virksomheden. Dette indebærer hvilke eksterne personer og selskaber der skal kontaktes uden for virksomheden, som eksempelvis leverandører og kunder. Kunder og leverandører bør få fortalt hvorledes et større IT-nedbrud påvirker lige netop dem, i form af eventuel forsinkelse på leverancer til kunderne eller forsinkelse i forfaldne beløb til kreditorerne. Derudover bør Business Recovery Planen også indeholde procedurer for hvordan produktionen af betonelementer skal berøres. Dette indebærer hvem der skal kontaktes og hvem der tager beslutninger om hvilke betonelementer der skal produceres færdigt, hvis det kan lade sig gøre, og hvilke betonelementer produktionen skal stoppe. For arkitekterne bør der også beskrives procedurer for, hvorledes produktionen af tegninger bliver prioriteret og hvem der tager

beslutninger omkring forhold i tegnestuen og der skal ligeledes være en ansvarlig for at informere medarbejderne i virksomheden.

15.10 Opsummering af anbefalinger til BB A/S

Samtlige områder i risikoanalysen for BB A/S er blevet belyst i afsnittet om anbefalinger til BB A/S og der er konkrete løsningsforslag til hvert punkt.

Tidligere i opgaven blev det anbefalet, at ledelsen skal starte med at kigge på forholdene med de største risici, som er omkring interne organisatoriske forhold, herunder ledelsens rolle og ansvarsplacering. For at efterleve anbefalingerne i DS 484 (2005), bør ledelsens rolle blandt andet være, at påse følgende:

- At sikkerhedsstrategien løbende bliver revurderet og godkendt
- At der foreligger handlingsplaner for den løbende sikkerhedsbevidstgørelse
- At implementeringen af sikringsforanstaltninger er tværorganisatorisk koordineret

Som nævnt i afsnittet for interne organisatoriske forhold, bliver disse punkter ikke efterlevet i BB A/S. Når dette ikke sker, bliver ledelsens rolle indenfor IT i virksomheden ikke synlig for medarbejderne i BB A/S. Hvis ledelsen derimod er synlig og viser engagement i forhold til IT, vil medarbejderne få øjnene op for, at dette er et vigtigt område for virksomheden og dermed vil medarbejderne også være engageret i at opretholde et fornuftigt IT-sikkerhedsniveau.

Ledelsen i BB A/S har lagt alt ansvaret for driften af IT, i hænderne på IT-chefen i virksomheden. Når alt ansvar på et område lægges i hænderne på en person, er denne person stort set umulig at erstatte for virksomheden, da personen er den eneste i virksomheden der kender til samtlige arbejdsgange på området.
Hvis ledelsen derimod udstikker retningslinjerne for IT-driften og dermed tager ansvaret, vil afhængigheden af IT-chefen også blive mindre, til gavn for BB A/S.

Udover ovenstående anbefalinger, bør ledelsen i BB A/S følge anbefalingerne for de andre områder. Prioriteringen af områderne bør ske ud fra risikobilledet i virksomheden, der er illustreret i figur 3 – "risikobilledet i BB A/S". Dermed bør de næste områder i prioriteringen fra ledelsen bl.a. være:

- Medarbejdersikkerhed, herunder ansættelsesforholdet.
- Styring af netværk, herunder logning og overvågning.
- Adgangsstyring, herunder brugernes ansvar.

Ovenstående er emner, der blev vurderet til at have henholdsvis "Høj/Middel" eller "Middel/Høj" for sandsynlighed og konsekvens i risikoanalysen, og sammen med det generelt svage kontrolmiljø i BB A/S, giver dette anledning til, at ledelsen bør henlede deres opmærksomhed på disse emner, som følge af risikobilledet i virksomheden.

Til sidst blev det anbefalet, at ledelsen laver en "Business Recovery Plan" for BB A/S, i stedet for blot at have en nødplan for IT. Business Recovery Planen skal, udover at opstille procedurer for genoprettelse af IT, ved et IT-nedbrud i virksomheden, ligeledes indeholde faste procedurer hvad der skal ske i de andre afdelinger. Dermed sikres det at alle i virksomheden er med til at sikre den forsatte drift optimalt og det sikres ligeledes at samtlige interessenter informeres omkring situationen i BB A/S.

Hvis ledelsen følger anbefalingerne i dette afsnit, vil dette medføre, at de samlede risici for virksomheden, ved at være afhængig af IT, reduceres. Anbefalingerne omkring ledelsens rolle i virksomheden omkring IT, vil påvirke kontrolmiljøet i virksomheden, som dermed vil blive bedre og ændret fra svagt imod stærkt. De øvrige punkter vil påvirke sandsynligheden for det enkelte område positivt, hvilket vil sige at sandsynligheden for, at et IT-nedbrud vil forekomme, eller tab af forretningsmæssigt kritisk materiale, vil blive reduceret.

Nedenstående figur illustrerer hvor hvert enkelt punkt vil blive indplaceret, hvis ledelsen i BB A/S følger anbefalingerne til virksomheden:

Figur 4 – Trusselsbilledet i BB A/S, efter implementering af anbefalinger

Sandsynlighed

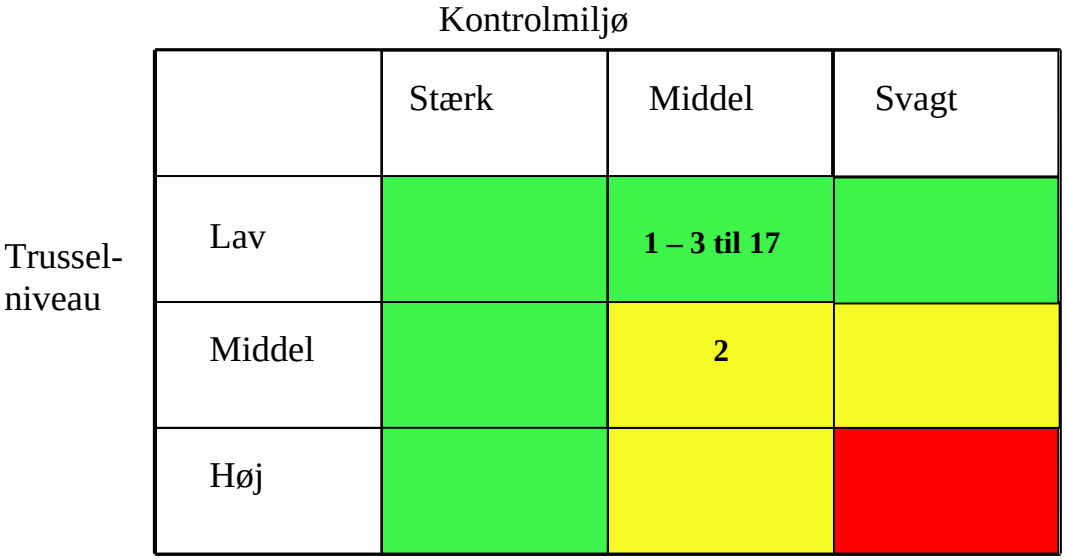
Konse-kvens	Lav	Middel	Høj
Lav			
Middel	1 – 3 – 4 – 8 – 10 – 13 14 – 15	2	
Høj	5 – 6 – 7 – 9 – 11 – 12 – 16 – 17		

De angivne trusselsnumre, refererer til de anvendte numre i tabel 1 " Oversigt over trusselsbilledet i BB A/S"

Da anbefalingerne ligeledes lægger op til, at ledelsen i BB A/S skal være mere aktive i forhold til problemstillingerne for IT, samt vise deres engagement for området, vil dette sammenlagt medvirke til, at kontrolmiljøet bliver forbedret. Dermed går det samlede kontrolmiljø fra at være svagt, imod at være stærkt.

At indarbejde et godt kontrolmiljø i en virksomhed, er ikke noget der kan indarbejdes i virksomhedskulturen over en kort periode. Selvom ledelsen i første omgang sætter fokus på problemstillingerne omkring IT, vil processen for at opnå et stærkt kontrolmiljø i virksomheden, tage tid. Nedenstående figur viser derfor, hvorledes det samlede risikobillede vil komme til at se ud i BB A/S, indenfor den nærmeste fremtid, hvis ledelsen implementerer anbefalingerne fra afhandlingen. Der tages dermed udgangspunkt i, at det samlede kontrolmiljø bliver løftet fra "svagt" til "middel":

Figur 5 – Risikobilledet i BB A/S, efter implementering af anbefalinger



Ovenstående figur viser hvorledes risikobilledet for BB A/S vil se ud, hvis ledelsen følger anbefalingerne der er givet i denne afhandling. Det er dog i første omgang op til ledelsen at overveje hvordan virksomheden er rustet til at stå i en situation, hvor IT-driften er gået ned, og hvordan virksomheden er rustet, i forhold til at miste forretningsmæssig kritisk materiale. Anbefalingerne til hvordan IT-sikkerheden kan forbedres, kræver store ressourcer i virksomheden at gennemføre. Det koster både tid og penge at have et godt sikkerhedsniveau for IT-sikkerheden i en virksomhed som BB A/S, da der er mange punkter der skal håndteres af ledelsen, samt medarbejderne i virksomheden.

Ledelsen bør derfor lave en konkret økonomisk vurdering af, om den finder det nødvendigt at gennemføre de anbefalinger der er i denne afhandling. For at lave denne vurdering, er første krav, at ledelsen er opmærksom på hvilke problemstillinger der er for IT-sikkerheden i virksomheden.

Hvis ledelsens vurdering er, at de risici, der er påpeget i denne afhandling, er acceptable for virksomheden, så er det et valg som ledelsen har truffet. Ledelsen bør, alt andet lige, være de bedste til at vurdere, i hvilket omfang virksomheden er i stand til at undgå for store økonomiske tab, trods et større IT-nedbrud, eller tab af forretningsmæssig kritisk materiale. Dette valg bør dog ske, efter det er anskueliggjort overfor ledelsen, hvilke områder der har de største risici for, at være skyld i et økonomisk tab. Beslutningen bør derefter tages i fællesskab mellem bestyrelse og direktion i virksomheden.

16. Perspektivering

16.1 Revisors rolle

Dette afsnit søger at perspektivere revisors rolle i forhold til IT-sikkerheden i virksomheden. Der er dermed ikke tale om en udtømmende liste af overvejelser, som revisor skal gøre sig, i forhold til at revidere en virksomhed. Der nævnes dog forhold, som revisor bør overveje, ved revision af en virksomhed, der er afhængig af IT.

16.1.1 DS 484

I DS 484 (2005), afsnit 6.1.8, anbefales det, at en uafhængig person bør lave periodisk opfølgning af virksomhedens procedure for eksempelvis genindlæsning af backup-data. I afsnittet nævnes konkret, at denne gennemgang kan foretages af en ekstern revisor og senere i afsnittet nævnes det, at den eksterne revisor kan komme med konkrete løsningsforslag til forbedringer af procedure. I den forbindelse skal revisor dog være opmærksom på, at hvis revisor også reviderer virksomhedens årsrapport, må det ikke være sådan, at revisor reviderer egne løsninger. Dermed kommer revisor i interessekonflikt med sig selv, hvor der kan stilles spørgsmålstegn ved uafhængigheden og objektiviteten hos revisor. Da der ikke må kunne stilles spørgsmålstegn ved den eksterne revisors uafhængighed og objektivitet, er det vigtigt at revisor ikke udøver selvrevision.

16.1.2 RS 315

Revisionsstandard 315 – "Forståelse af virksomheden og dens omgivelser og vurdering af risici for væsentlig fejlinformation" foreskriver hvilke handlinger revisor bør gøre sig, for at opnå viden omkring virksomheden og dens omgivelser. Herigennem skal revisor ligeledes opnå viden omkring interne kontroller i virksomheden.

I RS 315, afsnit 43 beskrives hvilke elementer intern kontrol bygger på i en virksomhed, ved følgende punkter:

- Kontrolmiljøet
- Virksomhedens risikovurderingsproces
- Informationssystemet, herunder de tilknyttede forretningsprocesser, der er relevante for regnskabsaflæggelse, samt kommunikation
- Kontrolaktiviteter
- Overvågning af kontroller

Disse punkter udgør tilsammen definitionen på intern kontrol. Især det første punkt, der omhandler kontrolmiljøet i virksomheden, bør have ekstra opmærksomhed i revisionen af BB A/S. Det manglende engagement fra ledelsen side, for at forhindre tilsigtede og utilsigtede fejl, udgør en risiko for fejlinformation og/eller besvigelser i virksomheden. Dette uddybes blandt andet fra afsnit 67, samt afsnit 69, litra C, i RS 315.

Når der skal afgives en revisionspåtegning på et selskabs årsrapport, skal revisor forholde sig til spørgsmålet om virksomheden er i stand til at drive forretningen videre, indenfor det næste regnskabsår. Dermed skal revisor, med høj grad af sikkerhed, opnå overbevisning om, at virksomheden er going-concern, selvom IT i virksomheden bliver ramt af et længerevarende nedbrud. Dette er dog kun nødvendigt, hvis virksomheden er meget afhængig af IT i driften af selskabet.
Måden hvorpå revisor kan sikre sig dette, er ved at tage en dialog med ledelsen i virksomheden og se om der er udarbejdet risikovurderinger og om der er et fornødent beredskab, til at håndtere eventuelle IT-mæssige nedbrud.

16.1.3 RS 240

RS 240 – "Revisors ansvar for at overveje besvigelser ved revisionen af regnskaber" beskriver hvilke overvejelser revisor skal gøre sig, for at sikre sig, at der ikke foregår besvigelser i virksomheden. Besvigelser defineres som "en bevidst handling udført af en eller flere personer blandt den daglige

ledelse, den øverste ledelse, medarbejdere eller tredjeparter, hvor vildledning for at opnå en uberettiget eller ulovlig fordel er indvolveret."[12]

Revisor har svært ved at finde besvigelser i en virksomhed, som følge af, at der er personer i organisationen, der ønsker at skjule dem, og i den forbindelse kan give revisor ukorrekte oplysninger. I afsnit 24 understreges det dog, at "revisor skal opretholde en professionel skeptisk holdning gennem hele revisionen".

Set i forhold til denne RS, er især forholdene omkring medarbejderne i IT-afdelingen kritisable, da disse medarbejdere har ubegrænset adgang til data og handlinger. Der bør derfor sættes ekstra fokus på dette område og der skal laves en vurdering af, hvor stor risikoen er for, at medarbejderne i IT-afdelingen benytter deres brugerrettigheder til at tilgodese dem selv, på bekostning af virksomheden.

16.2 Fremtiden for IT-sikkerhed i produktionsvirksomheder

Fremtiden for IT-sikkerheden i danske produktionsvirksomheder, ser ud til at blive mere og mere afgørende for, om virksomhederne kan klare konkurrencen på i globale markeder. Denne afhandling tager udgangspunkt i en konkret virksomhed, hvor IT-sikkerheden ikke har høj prioritet fra ledelsens side.
Som nævnt tidligere, har budskabet fra undervisningen på cand.merc.aud-studiet været, at der generelt er manglende fokus på IT-sikkerheden i danske virksomheder. Derfor er der ingen grund til at tro, at valget af virksomhed i forbindelse med denne afhandling, er noget sjældent tilfælde.

I forbindelse med globaliseringen, oplever samtlige brancher større konkurrence på markederne. Denne konkurrence betyder, at kun yderst konkurrence-effektive virksomheder kan klare sig på markederne, uanset om der er tale om den ene eller anden branche. Når virksomhederne tvinges til at være effektive, inkluderer dette også, at være effektive på IT-driften i virksomheden.
Som følge af den øgede globalisering, stilles der større og større krav til de danske virksomheder, som ikke kan klare sig i den internationale konkurrence, hvis ikke virksomhederne overbeviser markederne

[12] RS 240, afsnit 6

om, at det er en fordel at vælge lige netop deres virksomhed. Der er flere konkurrenceparametre, der spiller ind, når en virksomhed skal promovere sig selv. Dette kan eksempelvis være markedsføring, design, pris, kvalitet og stabilitet.
Især parametrene pris og stabilitet hænger sammen med en fornuftig IT-drift i virksomhederne. IT-driften kan hjælpe virksomhederne med at være effektive, således at planlægningen af produktionen, logistikken i virksomheden, samt administrationen foregår optimalt. Dermed sikres det, at der ikke bruges unødige ressourcer i virksomheden, hvorfor det er muligt at fastholde et konkurrencedygtigt prisleje, for produkterne. Derudover kan en effektiv IT-drift være med til at skabe stabilitet for virksomhederne. Det er på baggrund af udnyttelsen af IT, at større danske virksomheder, kan planlægge produktionstider mm. for de produkter, som virksomheden lever af at kunne levere.

IT-driften, som kan være med til at sikre de danske produktionsvirksomheders konkurrenceevne, er et kritisk punkt i mange virksomheder og alt tyder på, at afhængigheden af IT, bliver større i fremtiden. Under IT-driften, som dækker over mange ting, hører IT-sikkerhed til. IT-sikkerheden sørger for, at IT-driften er pålidelig, og dermed også, at virksomhederne kan være en pålidelig og stabil samarbejds-partner for kunderne.
Når alt tyder på, at IT-driften i danske virksomheder får en mere og mere kritisk position i danske virksomheder, så indebærer dette også, at IT-sikkerheden får en yderligere kritisk position, end vi ser i dag. Derfor bør der i fremtiden fokuseres mere på IT-sikkerheden i danske virksomheder, da IT-sikkerheden er et af fundamenterne for, at en virksomhed kan være en effektiv aktør på de globale markeder.
Når tendensen tidligere, og til dels også i nutiden, er at ledelserne i danske virksomheder overlader ansvaret for IT-driften i virksomhederne, til de enkelte IT-afdelinger, skaber dette et unødvendigt afhængighedsforhold til IT-afdelingen, samtidig med, at prioriteringerne omkring IT-sikkerheden ikke nødvendigvis er optimal, set fra et forretningsmæssigt synspunkt. I fremtiden bliver ledelserne i danske virksomheder dog nødt til at være aktive, for at sikre optimale vilkår for den enkelte virksomhed, da globaliseringen vil presse konkurrencen på markederne op. Dette indebærer også, at ledelserne bliver nødt til at sikre, at IT-sikkerheden før den fornødne opmærksomhed i virksomhederne.

17. Konklusion

For at besvare opgavens overordnede problemstilling, "Hvorledes forholder BB A/S sig til at være afhængige af IT, og hvilke handlinger vil kunne reducere risiciene ved at være afhængige af IT?" vil der i første omgang blive konkluderet på arbejdsspørgsmålene i problemformuleringen.

Hvordan er BB A/S afhængig af IT?

BB A/S er i høj grad afhængig af, at deres IT-systemer fungerer efter hensigten. Virksomheden producerer og leverer betonelementer til byggebranchen i Danmark og det nordlige tyskland, hvor markederne er præget af høj konkurrence. For at sikre konkurrenceevnen, skal BB A/S være en pålidelig leverandør. Dette skal blandt andet sikres igennem en pålidelig IT-drift, som har indflydelse på produktionen af betonelementer, arkitekttegnede skabeloner til ønskede projekter, samt den daglige drift af ind- og udbetalinger.

Hvordan opgøres afhængigheden af IT i BB A/S og risiciene ved at være afhængig af IT?

I BB A/S er det IT-chefen der er blevet pålagt ansvaret og opgaverne omkring vurderingen af afhængigheden, og de dertilhørende risici, for IT. Det er således ikke en repræsentant fra ledelsen, der foretager de konkrete vurderinger for hvilke områder indenfor IT-sikkerhed, der skal have høj prioritet i virksomheden. Dermed bliver det en person, der ikke nødvendigvis har den rette forretningsmæssige forståelse, der er blevet sat til at vurdere hvilke områder der har størst betydning for driften i virksomheden.
Risiciene ved at være afhængig af IT er ikke tidligere blevet belyst i BB A/S. Trods anbefalinger fra virksomhedens revisor, om at der bliver lavet en risikoanalyse af IT-driften, har ledelsen valgt at dette ikke er nødvendigt, da ledelsen har stor tiltro til at IT-chefen foretager de nødvendige dispositioner.

Hvilke risici for IT-sikkerheden er der konstateret i BB A/S?

I risikoanalysen er følgende konstateret som værende de punkter, hvor der er størst risici for, at BB A/S kan lide størst økonomisk tab:

- Interne organisatoriske forhold, herunder:
  - Ledelsens rolle
  - Ansvarsplacering

Ovenstående punkter, er de punkter i BB A/S, hvor der er konstateret de største risici, omkring IT-sikkerheden i virksomheden. Dette skyldes, at ledelsen i BB A/S ikke har vist det fornødne engagement.

Hvilke IT-sikkerhedsforanstaltninger gør BB A/S brug af, for at reducere de konstaterede risici?

Ledelsen i BB A/S har som svar på de risici der er ved at være afhængig af IT i driften, lagt ansvaret for en tilfredsstillende IT-drift, over på IT-chefen. Det forventes herefter at IT-chefen kontrollerer og sørger for, at IT-driften foregår på betryggende vis og hvis der er områder han mangler viden om, selv videreuddanner sig, eksempelvis via kurser eller rådgivning fra leverandører. Dermed mener ledelsen af BB A/S, at der er taget sig betrykkende af de risici der er forbundet med, at være afhængig af IT.

Hvad burde der gøres, for at reducere de konstaterede risici, i IT-sikkerheden?

Som nævnt i "anbefalinger til BB A/S", anbefales det, at ledelsen engagerer sig i højere grad, i IT-driften. Hvis ledelsen engageret sig fuldt ud omkring IT i virksomheden, vil dette understrege vigtigheden i, at virksomhedens IT-systemer fungerer efter hensigten. Dette vil påvirke medarbejderne i BB A/S, til at opretholde et højt niveau for IT-sikkerheden.
Derudover vil et højere engagement fra ledelsens side, betyde at virksomheden ikke vil være afhængig af enkeltpersoner, herunder især IT-chefen, da ledelsen vil være i stand til at udstikke retningslinjer for

IT til nye medarbejdere, hvis ansættelsesforholdet for nuværende medarbejdere i IT-afdelingen ophører.

Efter konklusionerne på arbejdsspørgsmålene, kan der nu konkluderes på den overordnede problemstilling " Hvorledes forholder BB A/S sig til at være afhængige af IT, og hvilke handlinger vil kunne reducere risiciene ved at være afhængige af IT?"

Ledelsen i BB A/S har valgt at ansvar og opgaver omkring IT i virksomheden, skal være placeret hos IT-chefen. Denne måde at håndtere afhængigheden af IT, finder ledelsen i BB A/S tilstrækkelig, da de har tiltro til, at IT-chefen har de rette forudsætninger til at foretage de fornødne prioriteringer. Dette mener jeg ikke er i overensstemmelse med aktieselskabslovens § 54, stk.3, som foreskriver, at det er ledelsen der skal sørge for, at formueforvaltningen i virksomheden, sker på betryggende vis.

Som tidligere nævnt, er der en række punkter, som med fordel vil kunne implementeres i BB A/S, for at reducere risiciene ved at være afhængig af IT. Den største anbefaling går på, at ledelsen i BB A/S påtager sig ansvaret for IT-driften, herunder IT-sikkerheden i virksomheden. Ved at tage ansvaret og kommunikere ud til virksomhedens ansatte, at ledelsen aktivt forholder sig til dette område, synliggøres vigtigheden af at opretholde et acceptabelt niveau for IT-sikkerheden. Selvom ledelsen tager ansvaret for IT i virksomheden, betyder det ikke at ledelsen skal bruge samtlige af deres ressourcer på IT og dermed ikke har mulighed for at fokusere på videreudvikling af de kompetencer der er i virksomheden. For selvom ledelsen tager ansvaret for IT, vil det være naturligt, at opgaverne stadig placeres i IT-afdelingen, blot med den forskel, at ledelsen aktivt går ind i de overordnede beslutninger og fastlægger retningslinjerne for IT-afdelingen.

18. Litteraturliste

Bøger:

Titel: Revisionsstandarder, Revisionsvejledninger, Revisionsudtagelser
Forfatter: Foreningen af statsautoriseret revisorer (FSR)
Udgivelsesår: 2007
Forlag: Nordbook A/S.

Titel: Strategies for Information Technology Governance
Forfatter: Wim Van Grembergen
Udgivelsesår: 2004
Forlag: Idea Group Publishing.

Titel: Den skindbarlige virkelighed, 3. udgave
Forfatter: Ib Andersen
Udgivelsesår: 2006
Forlag: Forlaget Samfundslitteratur.

Andre publikationer:

Foreningen af statsautoriseret revisorer (2005): Risk Management – Risikostyring og intern kontrol set fra bestyrelsens bord.

Internetsider:

www.retsinfo.dk, pr. 2. maj 2008
www.wikipedia.org pr. 7. august 2008
www.ds.dk pr. 1. august 2008

Standarder:

Titel: Standard for informationssikkerhed, 1. udgave

Udgiver: Standard for informationssikkerhed

Udgivelsesår: 2005

Titel: COSO Internal control – Integrated framework

Udgiver: Committe of Sponsoring Organizations of the Treadway Commission

Udgivelsesår: 1992

Titel: COSO Entreprise Risk Management – Integrated framework

Udgiver: The Committe of Sponsoring Organizations of the Treadway Commission

Udgivelsesår: 2004

Titel: CobIT – Version 4,1

Udgiver: IT-Governance institute

Udgivelsesår: 2007

19. Bilag 1 – Interviews i forbindelse med afhandling

Spørgsmål og svar i forbindelse med interview med IT-chefen for BB A/S d. 16. april 2008.

I hvilket omfang anvendes IT i BB A/S?

- Bruges IT i produktionen, i salg og igangværende arbejde?

Svar: Der bruges både IT i administrationen, eks. bogføring, opfølgning på kunder og HR-området. I produktionen bruges IT, når der skal fremstilles betonelementer, herunder blandingsforhold mm. Derudover beskæftiger BB A/S ca. 50 tegnere, som bruger IT, når de designer elementer til kunderne.

Hvilke risici er der for BB A/S ved at være afhængig af IT?

- Hvilke overvejelser er der blevet lavet i den forbindelse, af hhv. IT-afdelingen og ledelsen?

Svar: Risiciene for BB A/S, ved at være afhængig af IT, er at systemerne går ned og det dermed ikke er muligt at arbejde. Især produktionen og tegnerne bliver hårdt ramt. Produktionen kan fortsætte ca. 1 døgn, hvorefter de bliver ramt af, at det ikke er muligt at starte på nye elementer. Tegnerne bliver ramt med det samme, da de ikke har adgang til data samt programmer.

Der er ikke udarbejdet en risikoanalyse.

Hvem udstikker retningslinjerne for brugen af IT i BB A/S?

- Er der udstukket koncern-interne retningslinjer?
- Hvor stor en del spiller ledelsens rolle i disse retningslinjer?
- Er der formuleret en informationssikkerhedspolitik? Hvem opdaterer evt. denne?

Svar: Der er udstukket meget overordnede koncern-retningslinjer fra koncern-IT i Holland. Disse retningslinjer beskriver, at der skal udarbejdes retningslinjer der er tilpasset lokale forhold og at disse retningslinjer skal godkendes af den lokale ledelse. Disse godkendelser er dog kun formaliteter. IT-afdelingen har udarbejdet retningslinjerne, så de overholde de krav der er i koncern-instrukserne og det er også IT-afdelingen der løbende holder retningslinjerne opdateret. De seneste retningslinjer er godkendt i slutningen ag 2006.

Hvorledes forholder BB A/S sig til risikovurdering og håndtering?

- Hvem står for dette område?

Svar: Der er ikke udarbejdet en risikoanalyse i BB A/S. Revisor har påpeget, både overfor IT-afdelingen, den daglige ledelse og bestyrelsen, at der bør udarbejdes en risikoanalyse. Dette afvises af ledelsen, da de mener at IT-afdelingen udfører jobbet tilfredsstillende og at de har fuld tillid til IT-chefen, som er ansvarlig for IT i virksomheden. Denne anbefaling bruger It-chefen overfor ledelsen, når han mener, at der er områder der skal forbedres, eks. nye programmer eller ny hardware. Derudover har IT-chefen i sine overvejelser for risikovurderingen, fundet ud af hvor lang tid produktionen ca. kan fortsætte, indenfor eksempelvis produktion og design, ved et nedbrud. For

produktionen af betonelementer, er hans vurdering, at produktionen kan fortsætte ca. 1-2 dage, imens design af elementer vil gå i stå med det samme, ved et større nedbrud.

Der er udstukket overordnede retningslinjer fra koncernen, som har en større IT-afdeling i Holland. Dette inkluderer bl.a. en nødplan.

Hvem er ansvarlig for organisering af informationssikkerhed?

- Er der en ansvarsfordeling på de forskellige områder? Eksempelvis ved nyanskaffelser mm.

Svar: Det er udelukkende IT-afdelingen der står for al IT i virksomheden. Afdelingen står for den løbende vedligeholdelse og det er IT-afdelingen der er ansvarlig for samtlige IT-relateret aktiver.

Har BB A/S eksterne samarbejdspartnere omkring driften af IT?

- Hvem har ansvaret for dette?
- Er der nogle risici ved at have eksterne samarbejdspartnere?
- Er der aftaler med serviceleverandører, som kan hjælpe ved evt. nedbrud mm?

BB A/S benytter sig i høj grad af eksterne serviceleverandører. Der er nedskrevet aftaler med leverandørerne omkring hvilke programmer der skal serviceres. Dette foregår via ekstern opkobling. Ikke nedskrevet aftaler omkring IT-sikkerhedsforhold, eks. virus-beskyttelse. Leverandørerne lever af at levere gode og stabile produkter, derfor anses dette for en selvfølgelighed. Leverandørerne har kun adgang til de dele af BB A/S´ netværk, som de har brug for. Dermed har de ikke adgang til andre data.

Det er nedskrevet, at det er BB A/S der har rettighederne til de programmer der anvendes og opdateres.

Hvordan sikres alle IT-aktiver(bærbar- og stationære computere og servere mm)?

- Hvorledes sikres det at alle IT-aktiver er opdateret?
- Hvorledes sikres det at alle IT-aktiver stadig forefindes i virksomheden og ikke forsvinder/er forsvundet?

Svar: Der findes en oversigt i IT-afdelingen, hvor der står hvor hvert aktiv befinder sig. Det er brugernes ansvar at meddele, hvornår aktiver fysisk bliver flyttet. Der er dog problemer omkring fratrædelser på andre fabrikker, end den i Esbjerg, da idet at den lokale leder skal rapportere til IT-chefen, når en medarbejder skal lukkes ude af systemerne i virksomheden. Dette sker sjældent tilfredsstillende.

Er der klare regler for medarbejdernes brug af IT?

- Er der formuleret regler herfor? Både mht. brug af IT i virksomheden, men også evt. hjemmearbejdspladser og opkobling på netværk hos kunder?
- Er der særskilte afsnit i ansættelseskontrakten, for relevante medarbejdere?
- Adgangsstyring, hvem har adgang til hvad? Har IT-medarbejdere adgang til alt?

Svar: Medarbejdere i IT-afdelingen har adgang til alt. De kan logge sig på samtlige computere, uden forudgående tilladelse fra computerens bruger. De har adgang til alle systemer og alle data. Der er

oprettet brugergrupper, som har adgang til relevante data. Hvis der er brug for yderligere rettigheder for brugerne, tildeles dette via godkendelse af mellemleder.

I ansættelseskontrakten, skriver medarbejderen under på, at denne har kendskab til virksomhedens IT-sikkerhedskrav. Disse krav ligger på forsiden af Intra-nettet.

Hvorledes sikres den fysiske sikkerhed for IT-aktiver?

- Hvem har ansvaret for at der følges op på sikkerheden?

Rundvisning på virksomheden. Det er IT-afdelingen der skal vurdere, om IT-aktiverne har et tilfredsstillende sikkerhedsniveau.

Hvorledes styres selve driften af IT og netværk?

- Hvem har ansvaret for dette?
- Har ledelsen udstukket retningslinjer?
- Er det muligt at se hvem der har lavet hvilke ændringer og hvornår? (log-styring)

Svar: Der foretages log-overvågning. IT-afdelingen kan dog ændre i dem, hvis de vil. Ledelsen har fuld tillid til IT-chefen, som har det overordnede ansvar for en tilfredsstillende drift.

Hvem har ansvaret for at opdatere IT-driften?

- Har ledelsen udstukket retningslinjer herfor?

Svar: Det er IT-afdelingen der har det overordnede ansvar.

Er der et beredskab for håndteringen af evt. nedbrud?

- Er der lavet vurderinger af hvor lang tid IT-driften i BB A/S kan være nede, uden betydelige omkostninger for virksomheden?
    - Har IT-afdelingen lavet sådanne beregninger/konsekvensanalyser?
    - Har ledelsen lavet sådanne beregninger/konsekvensanalyser?

Svar: Koncernretningslinjerne foreskriver, at der skal være udarbejdet en nødplan for genetablering af IT-systemerne. Denne er udarbejdet og der er beskrevet hvorledes der skal handles i tilfælde af et nedbrud, i forhold til genetableringen. Denne er udleveret.

Derudover blev der ved interviewet talt om andre forhold, som der ikke tidligere havde været berørt og der blev foretaget en opsummering af interviewet.

Eksempel på mail-korrespondance

-----Oprindelig meddelelse-----
Fra: Jesper Gravlund Nielsen
Sendt: 17. maj 2008 17:28
Til: xx xx
Emne: Kandidatafhandling

Hej xx

Jeg håber du har tid til at svare på et par efterfølgende spørgsmål omkring min opgave.

Jeg har faktisk kun et i denne omgang, men det kan jo være der kommer flere senere hen.

Hvad er din baggrund inden for IT? Hvad har du lavet tidligere, inden du er blevet IT-chef? Har du haft tidligere jobs indenfor samme felt og derved uddannet løbende eller har du taget en uddannelse for at kunne varetage jobbet som IT-chef? Eller begge dele???

Ingen af delene :-). Jeg er uddannet Maskinmester, er selvlært i IT og holder mig selv opdateret. Tager nogen gange kurser for at booste min viden inden for et felt.

Mvh xx

Jeg håber du har tid til at besvare mit spørgsmål.

MVH
Jesper

-- Anden mail --

Et par enkelte uddybende spørgsmål. Hvor længe har du været IT-chef i BB A/S, og hvor lang tids erfaring har du med IT, hvor det har været dit job?

Jeg har været IT chef i BB A/S fra 2000-2005 afbrudt af et konsulentjob 2005-2006, hvorefter jeg blev ansat i CC DK A/S som bl.a. står for BB A/S´ IT. Tidlige fra 1996-2000 arbejdede jeg som IT konsulent/sælger i et IT firma i Esbjerg.

Så det bliver vist 12 års erfaring.

Mvh

xx

Spørgsmål til PP, d. 1. maj 2008

Er du bekendt med IT-retningslinjerne for virksomheden?

Svar: Ja, de ligger på intra-nettet. De er læst. Der kommer ikke meddelelser omkring opdateringer. Er der generelt nogle spørgsmål, bliver der taget kontakt til IT-chefen, som er meget behjælpelig med at afklare spørgsmål osv.

Det er tidligere oplevet, at der er en medarbejder fra IT-afdelingen, der har taget kontrol med computeren, og det blev kun opdaget, fordi PP så på computeren og kunne ikke forstå at der foregik ting på den, så han ringede til IT-afdelingen og det viste sig, at IT-chefen var i gang med at lave nogle opdateringer.

Derudover blev der talt om diverse forhold for IT i koncernen, set fra en medarbejders perspektiv.