Copenhagen Business School, 2009
Institut for Regnskab & Revision
Solbjerg Plads 3, 1. sal – blok C
2000 Frederiksberg

Revisor og IT-governance

_____

Ledelsens ansvar og revisors rådgivning vedrørende forbedring af informationssikkerhed.

_____

Udarbejdet af:

_____
Martin Jönsson

Vejleder:

_____
Dorthe Tolborg

Afleveringsdato:

21. juli 2009

Censor:

_____

Indholdsfortegnelse

1. Indledning

Den traditionelle opfattelse af IT-risiko stammer fra dengang, hvor brugen af IT-systemer var begrænset til enkelte selvstændige systemer, som kun blev anvendt i en afgrænset del af virksomhedens forretningsprocesser. Den begrænsede brug af IT, der ofte var tilfældet for 15-20 år siden, bevirkede, at mange opfattede IT-risiko som noget, der primært berørte få medarbejdere i de dengang små IT-afdelinger rundt om i virksomhederne.

De enkelte virksomheder oplever en større og større afhængighed af IT i de daglige arbejdsprocesser. Denne udvikling har betydet, at ledelsen ikke længere kan opfatte IT-risiko som noget, der begrænser sig til kun at omfatte de enkelte IT-systemer og IT-afdelinger. IT er i dag en så integreret del af de enkelte arbejdsprocesser i langt de fleste virksomheder, at IT-risikoen omfatter hele organisationen.

I Danmark har vi fulgt den internationale udvikling med udarbejdelse af rammeværktøjer. Derfor er der indført en ny Revisionsstandard - RS 315 ”Forståelse af virksomheden og dens omgivelser og vurdering af risici for væsentlig fejlinformation”[1].

Til fastlæggelse af informationssikkerhed har vi i Danmark siden år 2000 haft DS 484:2000 der senest er opdateret i 2005 til DS 484:2005 ”Standard for informationssikkerhed - Code of practice for information security management”[2]. Dette er ikke en revisionsstandard, men et rammeværktøj, der går mere detaljeret ind i, hvilke arbejdsprocesser og vurderinger virksomhedsledelsen bør foretage med henblik på at øge informationssikkerheden.

Det er essentielt, at ledelsen skal være synlig i organisationen. Ledelsen har til opgave at vise vejen for informationssikkerhedsindsatsen i virksomheden. Dette er imidlertid ikke altid tilfældet i små og mellemstore virksomheder, hvilket skyldes, at ledelsen ofte ikke til fulde har den fornødne indsigt og forståelse for sammenhængen mellem forretningsstrategien og anvendelsen af IT.

[1] Herefter benævnt RS 315
[2] Herefter benævnt DS 484

Ledelsen i de små og mellemstore virksomheder har ofte ikke forståelse af vigtigheden af informationssikkerhed, og er ikke opmærksom på, hvilke trusler og risici den nuværende anvendelse af IT har for deres virksomhed.

Jeg er som revisor jævnligt blevet opmærksom på ledelsens manglende involvering i virksomhedens informationssikkerhed, i forbindelse med revisionen af de generelle IT-kontroller og applikationskontroller. Der kan være flere forklaringer på dette, men det ses ofte, at i små og mellemstore virksomheder som har sammenfald mellem ejerkreds og ledelse, bliver informationssikkerheden nedprioriteret.

Jeg har som revisor fundet det relevant at undersøge, hvordan revisor kan rådgive ledelsen i små og mellemstore virksomheder til at vise mere interesse for informationssikkerhed.

Revisor kan optræde i en rolle som sparringspartner for ledelsen, hvor revisor vil foretage en analyse af den nuværende informationssikkerhed og komme med forslag til forbedringstiltag. Revisor skal dog nøje overveje sin uafhængighed, når han påtager sig rollen som rådgiver for virksomhedsledelsen.

2. Problemformulering

Jeg er revisor for virksomheden M-Medical A/S. I forbindelse med revisionen af virksomhedens interne kontroller er jeg stødt på en del forhold omkring, specifikt de generelle IT-kontroller, men ligeledes stødt på forhold omkring informationssikkerheden generelt, som ikke virker hensigtsmæssig.

Jeg har valgt at rådgive virksomheden om informationssikkerhed. Der skal derfor foretages en vurdering af, hvilke handlinger og holdningsændringer ledelsen bør foretage, for at forbedre informationssikkerheden.

Hvorledes kan revisors rådgivning hjælpe ledelsen i M-Medical A/S til at forbedre virksomhedens informationssikkerhed?

Ovenstående problemstilling vil jeg besvare ved at behandle nedenstående punkter:

- Hvilke frameworks kan revisor anvende ved rådgivning om informationssikkerhed?
- Hvilke handlinger og holdningsændringer bør ledelsen foretage?
- Hvilke trusler og risici er M-Medical A/S udsat for?
- Er der tilstrækkelige kontroller til at minimere trusselsniveauet fra de identificerede trusler?

3. Metodik

Nærværende afhandling er opdelt i to hovedområder:

Første hovedområde er et teoriafsnit indeholdende studier af relevant teori. Disse studier har givet en teoretisk baggrund, som i analyseprocessen har hjulpet med at identificere og løse den relevante problemstilling.

Andet hovedområde er opdelt i først en præsentation af modelvirksomheden M-Medical A/S, samt en analyse af omfanget, niveauet og betydningen af deres informationsteknologi. Dernæst følger selve analysen M-Medical A/S. Her vil der blive foretaget en vurdering af, hvilke handlinger og holdningsændringer, ledelsen bør foretage, for at forbedre virksomhedens informationssikkerhed, hvilke trusler og risici M-Medical A/S er udsat for samt om der et tilstrækkelige kontroller til at minimere trusselsniveauet.

3.1 Metode

3.1.1 Teori

For at kunne bistå ledelsen med rådgivning omkring forbedring af informationssikkerheden, har jeg fundet det relevant at studere internationale frameworks. De internationale frameworks som jeg har studeret, er COSO-rapporterne, Sarbanes-Oxley Act og CobiT udvalgt med det formål at opnå kendskab til, hvilke elementer og principper der indgår i de enkelte frameworks. Herefter vil jeg fastlægge anvendeligheden af disse, set i forhold til afhandlingens hovedproblemstilling.

Med henvisning til afhandlingens hovedproblem, er det fundet relevant også at inddrage danske frameworks. De danske frameworks, som bliver behandlet i afhandlingen, er RS 315 og DS 484. RS 315 er medtaget, da denne fortæller rådgivende revisor, hvad han skal være opmærksom i forbindelse med forståelse af virksomheden og dens omgivelser. Ydermere opnås en forståelse af vigtigheden af virksomhedens IT-strategi samt hvilke elementerne der indgår i begrebsrammen for interne kontroller.

DS 484 er medtaget, da dette framework er præsenteret som værende anvendeligt ved en praktisk gennemgang af informationssikkerhed. Dette framework beskriver i forhold til CobiT og RS 315

detaljeret, hvilke forhold, der påvirker informationssikkerhed, og hvordan en bedre informationssikkerhed opnås.

Disse studier skal give en teoretisk baggrund, som i analyseprocessen skal hjælpe med at identificere den relevante problemstilling.

3.1.2 Analyse

3.1.2.1 Modelvirksomhed

Den analytiske del af opgaven er baseret på forhold i en konstrueret modelvirksomhed. Anvendelse af en modelvirksomhed begrundes med, at det derved har været muligt at medtage en del forhold, som alle eller enkeltvis forekommer i en reel virksomhed. Det er således tiltænkt, at revisorer og virksomhedsledelser vil kunne drage en parallel mellem de i afhandlingen beskrevne forhold, og de forhold, som optræder i en faktisk virksomhed.

Samtalerne er baseret på oplevelser og situationer, som jeg igennem mit arbejde som revisor er stødt på. Disse oplevelser er brugt i sammenhæng, for at opnå så mange situationer som muligt. De enkelte tilfælde bygger således på egne observationer samt test af kontroller, herunder adgangskontroller og fysisk placering af hardware. Da der er tale om en konstrueret modelvirksomhed, har de samtaler, som fremhæves i analysen, ikke fundet sted i virkeligheden.

Præsentationen og analysen af både kompleksiteten og den forretningsmæssige betydning af informationsteknologien, har til formål at danne baggrund for analysen af, hvilke trusler og risici modelvirksomheden er udsat for.

3.1.2.2 Analyse af informationssikkerheden i M-Medical A/S

Til brug for besvarelsen af afhandlingens problemstilling vil M-Medical A/S' informationssikkerhed blive vurderet ud fra den guideline, som er i bilag A - Guideline til rådgivning omkring informationssikkerhed. Guidelinen er sammensat ud fra de områder i DS 484, som er fundet relevante set i forhold til M-Medical A/S' nuværende anvendelse af informationsteknologi.

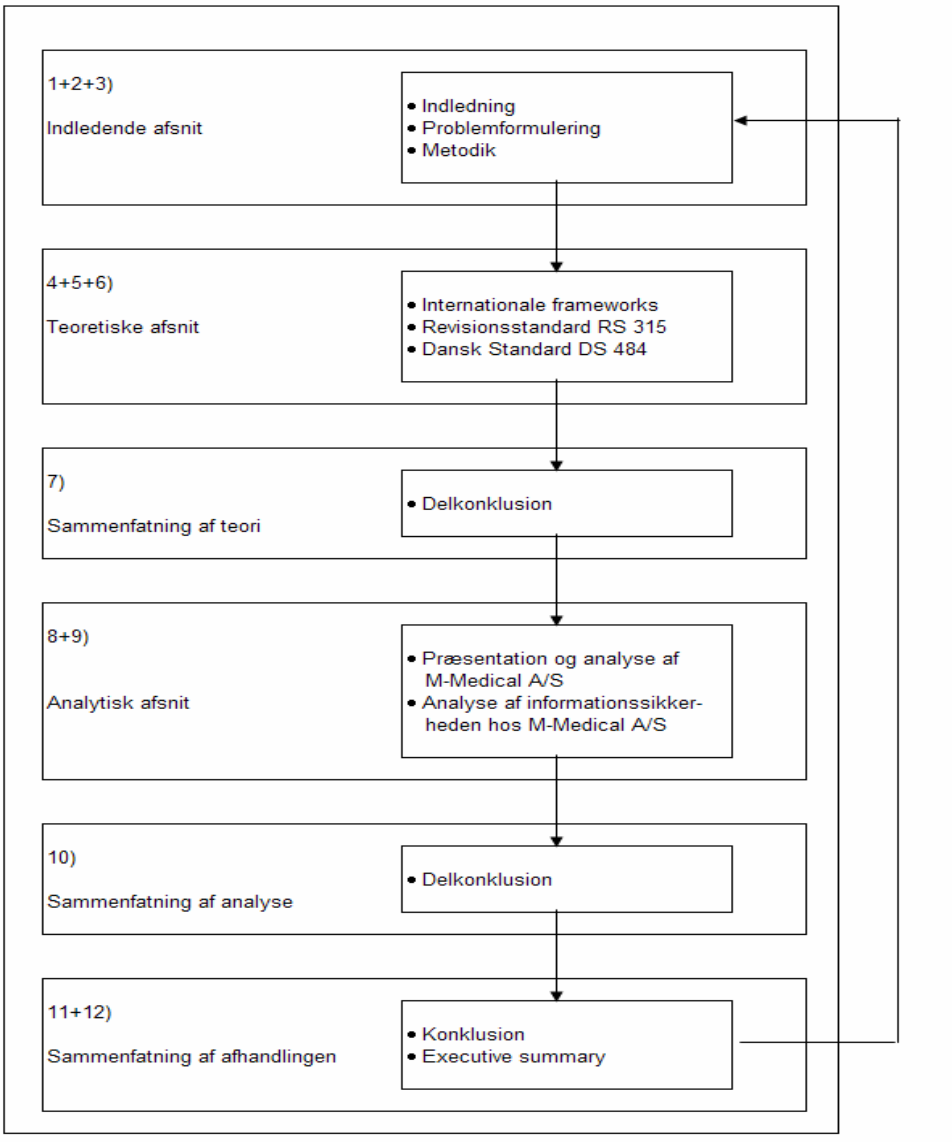
Guidelinen vil afdække ledelsens kendskab til aktuelle trusler og risici, men vil også give ledelsen en præsentation af M-Medical A/S aktuelle kontrolmiljø og nuværende kontrolaktiviteter.

Guidelinens punkter bliver igennem hele analysen gennemgået, og analysen vil til en vis grad være opdelt i områder, som henviser til et punkt i guidelinen.

Analysen vil afslutningsvis indeholde en rapportering til ledelsen i M-Medical A/S, hvor det klarlægges, hvilke handlinger og holdningsændringer, der bør foretages. Endvidere vil rapporteringen indeholde en præsentation af trusselsbillede og risikobillede for M-Medical A/S samt en handlingsplan, der beskriver, hvilke udvalgte forhold, som ledelsen først bør ændre.

Slutteligt vil konklusionen besvare afhandlingens hovedspørgsmål: ” Hvorledes kan revisors rådgivning hjælpe ledelsen i M-Medical A/S til at forbedre virksomhedens informationssikkerhed”.

3.2 Opgavens opbygning



3.3 Afgrænsninger

IT-revision indgår i både RS 315, 330, 402, 500 og 3411, men det vil kun være RS 315, der vil blive behandlet indgående i denne opgave.

Der vil i afsnittet om RS 315 ikke blive behandlet kontroller, der hører hjemme i den finansielle revision, da dette er uden for rammerne af denne opgave. I den teoretiske behandling af RS 315 vil fokus primært blive lagt på de områder af standarden, som har relevans for de generelle IT-kontroller. Derved afgrænses der fra en generel behandling af alle aspekter af RS 315.

Anvendelsen af DS 484 ligger til grund for afhandlingens analyse af M-Medical A/S´ niveau for informationssikkerhed. Der er ikke tale om en lovpligtig standard, der indeholder krav om implementering af alle områder, men den skal ses som en referenceramme, der skaber grundlag for virksomhedens informationssikkerhed både internt og eksternt.

Problemstillingen omkring anvendelse af ekstern IT-konsulent bliver berørt. Forholdet omkring aftalegrundlag, også kaldet Service Level Agreement, vil blive analyseret, men der vil ikke blive foretaget en sammenholdelse med kravene i RS 3411. Dette skyldes, at den praktiske del i denne afhandling ikke er en revisionsopgave, der vedrører anvendelse af eksterne serviceleverandører, men en rådgivning omkring de generelle IT-kontroller i modelvirksomheden.

Det vil i afhandlingen ikke blive nærmere behandlet, hvorledes revisors uafhængighed kan blive påvirket ved at påtage sig rollen som rådgiver, herunder safeguards.

Der er ved rapportering til ledelsen ikke taget stilling til rapporteringsformen eller ledelsesniveauet, det vil sige managements letter til direktionen, der indeholder praktiske guidelines til forbedringer samt protokollering til bestyrelsen vedrørende det overordnede ledelsesansvar.

3.4 Kildekritik

En overvejende del af afhandlingens kilder stammer fra organisationer, som støtter hinanden og derfor har en meget subjektiv vurdering af kilderne. Anvendelse af materiale fra ”The Committee of Sponsoring Organizations of the Tradeway”, PriceWaterhouseCoopers og ”The IT Governance Institute”, viser sig alle som varme fortalere for COSO-rapporterne samt CobiT. På trods heraf er disse kilder fundet relevante, idet de har vist sig at være de mest omfangsrige og seriøse.

Ved anvendelsen af revisionsstandarderne er det fundet relevant at bemærke, at de danske revisionsstandarder er direkte oversat fra IFAC-standarderne, og såfremt der opstår tvivl i fortolkningen af de danske revisionsstandarder, vil det være IFAC´s fortolkning, der er gældende.

Som det fremgår af afhandlingens kildefortegnelse, er der en række publikationer, som ikke er at finde som referencer i afhandlingen. Dette skyldes, at de respektive publikationer i stort omfang er brugt som inspiration, samt til forståelse af afhandlingens emne generelt.

Informationssikkerhed består af mange enkeltområder, og virksomhedens behandling i praksis vil blive belyst hovedsageligt ud fra DS 484 Standard for informationssikkerhed – Code of practice for information security management[3]. Det skal bemærkes, at DS 484 ikke er en revisionsstandard, men et værktøj, der sigter mod at gøre informationssikkerhed til en specificerbar kvalitet.

Analysen vil hovedsageligt bestå af elementer af et kvalitativt casestudie. Analysen vil vise et øjebliksbillede af, hvordan modelvirksomhedens informationssikkerhed er i skrivende stund ud fra mine observationer i virksomheden samt samtaler med ledelsen og relevante ledende medarbejdere. Samtalerne er baseret på oplevelser og situationer, som jeg igennem mit arbejde som revisor er stødt på, og har ikke fundet sted i den form, som er anvendt i afhandlingen. Disse oplevelser og situationer er præget af min egen fortolkning af forskellige scenarier.

[3] Herefter benævnt DS 484

4. Internationale frameworks

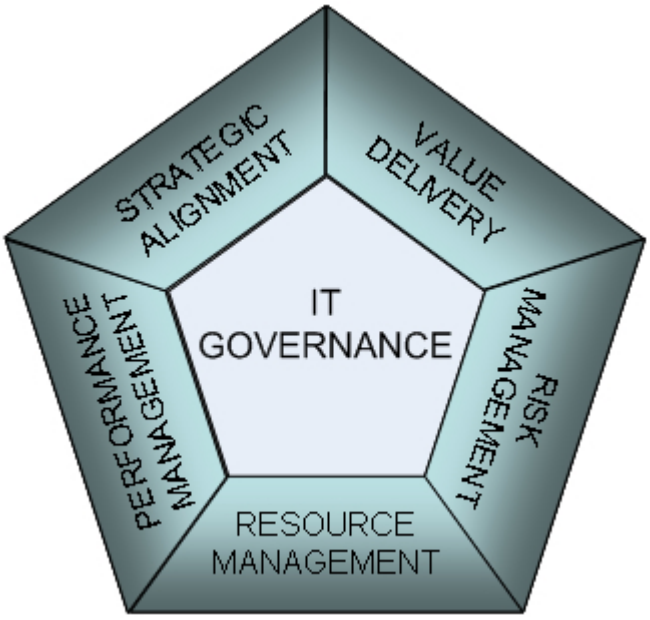
Der findes flere internationale frameworks, som behandler interne kontroller. Dette er blandt andet COSO-rapporterne, Sarbanes-Oxley Act og CobiT.

COSO-rapporterne, Sarbanes-Oxley Act og CobiT henvender sig i langt overvejende grad til store virksomheder, som allerede har et højere niveau af bevågenhed på governance, herunder IT-governance.

Til brug for rådgivningen af M-Medical A/S er COSO-rapporterne og Sarbanes-Oxley Act ikke tilpasset det nuværende niveau af ledelsen engagement. CobiT er et framework der, hjælper ledelsen med at styre de risici, der er forbundet med anvendelsen specifikt af IT[4], hvorfor denne er relevant at have kendskab til for ledelsen i M-Medical A/S.

4.1 Elementer i CobiT pentagram

I CobiT 4.1 er opstillet følgende fem fokusområder inden for IT-governance[5]:



Figur 2, kilde: www.ciber.no

[4] IT Governance Institute, CobiT 4.1 Excerpt, Executive Summery Framework, side 5
[5] itSMFInternational ”IT Governance based on CobiT 4.1, side 41

Strategisk overensstemmelse

Strategisk overensstemmelse skal sikre, at der er sammenhæng mellem forretningsstrategi og IT-strategi ved at definere, vedligeholde og vurdere værdiskabelsen ved IT-investeringer og skabe overensstemmelse mellem IT-processer og virksomhedsprocesser.

Værdiskabende

Det Værdiskabende fokusområde skal sikre, at IT-investeringer leverer de forventede fordele for det pågældende forretningsområde, for derved at sikre, at investeringen giver det forventede afkast målt op mod forretningsstrategien, og samtidig justerer omkostningerne og egenværdien af IT.

Risikostyring

Risikostyring skal sikre, at ledelsen har den fornødne opmærksomhed på risici samt en klar forståelse af virksomhedens risikovillighed, og synliggøre den signifikante forretningsrisiko, samt klarlægge ansvaret for risikostyringen i organisationen.

Ressourcestyring

Ressourcestyring har til formål at sikre optimal investering i og forsvarlig styring af kritiske IT-ressourcer, såsom personale, applikationer, informationer samt infrastruktur, dog med størst fokus på viden og infrastrukturen.

Præstationsmåling

Præstationsmåling følger og overvåger de strategiske implementeringer, og foretager løbende evalueringer ved brug af blandt andet balanced scorecards, for at sikre at IT-investeringerne leverer det forventede.

4.2 CobiT som IT-governance framework

CobiT fokuserer på forretningsgovernance og på nødvendigheden af forbedring af kontroller i organisationen. Kontrollen af IT-governance ved brug af CobiT bygger på følgende fem hovedpunkter:[6]

[6] IT Governance based on CobiT 4.1, side 36

- Have en general accept rundt i organisationen
- Skabe et skarpere forretningsfokus
- Sikre en procesorienteret indstilling
- Definere et fælles ”sprog”
- Hjælpe til at imødekomme retslige reguleringer

Generel accept

Et kontrolframework omfatter en global accepteret ”Best Practices” eller god skik, som er udviklet over tid og inkluderer input fra erfarne folk i branchen. Igennem flere implementeringsforløb bliver værdien af forskellige udgaver af god skik bevist og disse bliver, i en formel form, samlet i et framework.

CobiT er en globalt accepteret standard for forøgelse af virksomhedens organisatoriske succes gennem anvendelsen af IT. Frameworket er i en stadig proces med udvikling og forbedring, der skal sikre, at det løbende holder trit med god skik. Ved at hele organisationen har kendskab til CobiT, vil der kunne opnås en generel accept hos både ledelse og medarbejder.

Forretningsfokus

For at kunne fremskaffe de informationer, som virksomheden efterspørger for at kunne opnå de ønskede målsætninger, kræver det ledelse og kontrol med IT-ressourcerne gennem et struktureret netværk af processer, der kan levere disse informationer.

Procesorienteret indstilling

Den procesorienterede indstilling i organisationen skal sikre, at medarbejderne føler et ”ejerforhold” til en given proces på baggrund af den enkeltes ansvarsfølelse. Dette betyder, at aktiviteter er organiseret i processer, som kan henføres til den enkelte medarbejders ansvarsområde. Der vil fra den ansvarlige medarbejder blive afkrævet en godkendelse, før en proces kan gennemføres.

Når der i en organisation implementeres CobiT, vil medarbejdernes fokus automatisk blive mere procesorienteret. Uheld og problemer vil ikke længere fjerne fokus fra processen og hver proces vil definere, beskrive og tildele ansvar og gøre organisationen i stand til at opretholde kontrol, mens der tages hånd om ekstraordinære hændelser.

Fælles sprog

Set over tid vil god skik tilstræbe at opnå en særlig terminologi, som er defineret af frameworket. Den generelle terminologi er med til at etablere en generel kommunikation med et fælles sprog i organisationen, men også blandt fagfolk i andre firmaer samt eksterne konsulenter.

Med de tværfunktionelle afdelinger, som findes i erhvervslivet i dag, ledes de enkelte afdelinger ofte af personer, som ikke har det fulde overblik over implementeringen, da deres erfaring ligger i andre områder af organisationen. Koordinering indenfor og på tværs af arbejdsgrupper og organisation spiller en afgørende rolle i forhold til at opnå succes med implementering af IT-systemer.

Et framework hjælper alle i organisationen til at snakke samme sprog, ved at definere kritiske vilkår og forudsætte, at fælles fagudtryk forstås og anvendes.

Retslige reguleringer

At være i stand til at kunne imødekomme retslige reguleringer er ofte en kostbar og ressourcekrævende opgave. Det er lettere at udvise imødekommenhed overfor retslige reguleringer, hvis ens kontrolframework er baseret på godkendte standarder. Revisor vil alt andet lige også finde det lettere at foretage gennemgang af interne kontroller, når virksomheden anvender et godkendt framework.

De nuværende ledelsesskandaler har øget presset for retslige reguleringer overfor direktion og bestyrelse, for at få dem til at rapportere om deres status og derved sikre, at interne kontroller er tilstrækkelige. Dette gælder også for kontroller i IT-systemerne.

Det konstante behov for at forbedre organisationens IT-anvendelse og præstere tilstrækkelige kontroller over IT-systemerne, har fået mange IT-ledere, rådgivere og revisorer til at rette fokus mod CobiT som en afledt effekt af retlige IT-reguleringer.

4.3 Principperne i CobiT´s IT-governance

Ledelsen har ansvaret for IT-governance. IT involverer strukturer og processer, der guider organisationen hen imod at opnå sin målsætning. Ifølge IT Governance Institute [7] er IT-governance baseret på følgende fire principper:

- Styring og kontrol
- Ansvarlighed
- Målelighed
- IT-aktiviteter

Styring og kontrol

Styring og kontrol er de to nøglebegreber i IT-governance. Styring sikres ved, at den IT-ansvarlige fastsætter retningslinierne for implementeringen af en ændring i IT-systemet. For at sikre en effektiv styring, er det nødvendigt, at den IT-ansvarlige til fulde forstår den ønskede ændring. Den IT-ansvarlige kan derefter uddelegere opgaven med at foretage ændringen. Kontrol sikrer, at målsætningen nås, og at ingen uønskede handlinger optræder.

Ansvarlighed

Ledelsen har det ultimative ansvar for den interne kontrol. Afdelingslederne tildeles ansvaret for etableringen af specifikke interne kontroller og procedurer, der skal sigte mod at styrke de ansattes ansvarsfølelse for funktionerne i deres arbejdsområde. Intern kontrol er et ansvar for alle ansatte i organisationen og skal fremstå som en udtrykkelig og - på sigt - indforstået del af jobbeskrivelsen.

Målelighed

Målelighed har til opgave at sikre, at medarbejderne står til regnskab for og, rapporterer om eller forklarer deres handlinger ved arbejdet med de ressourcer, som stilles til rådighed for dem. Direktionen står til regnskab overfor bestyrelsen, hvilket sikrer governance, vejledning og tilsyn. Det er essentielt for de enkelte at vide, hvordan deres handlinger bidrager til at opnå målsætningen. Kontrolmiljøet er i vid udtrækning påvirket af, at de enkelte medarbejdere erkender, at de kan blive gjort ansvarlige for deres handlinger eller mangel på samme.

[7] IT Governance based on CobiT 4.1, side 39

IT-aktiviteter

IT-aktiviteter er først effektive når der er etableret en god IT-governance. Hvis der derimod foretages handlinger eller dispositioner i et miljø med ringe grad af IT-governance, øges risikoen for fejl og dermed tab.

5. Revisionsstandard 315

I takt med, at anvendelsen af IT bliver mere og mere udbredt, har revision af IT samtidig fået en større betydning. Dette har givet sig til udtryk ved indførslen af nye internationale revisionsstandarder, hvor IT-revisionen gøres til en integreret del af revisionen, og vil altid gøre det relevant at foretage systemgennemgang. Det forudsættes også implicit i RS 315, at virksomheden anvender IT som grundlag for regnskabsaflæggelsen.

I afsnittet "forståelse af virksomheden og dens omgivelser, herunder dens interne kontroller" i RS 315, redegøres der for specifikke aspekter ved virksomheden, som revisor skal forstå med henblik på at kunne identificere og vurdere risici for væsentlig fejlinformation. Disse består af henholdsvis branche, lovgivning, regnskabsmæssige begrebsrammer, virksomhedens art, ledelsens mål, strategier og tilknyttede forretningsrisici, måling og kontrol af virksomhedens resultater samt intern kontrol mv.

5.1 IT-strategi

I følge RS 315 skal revisor, som en del af revisionsprocessen, opnå kendskab til virksomhedens IT-strategi. Kendskabet til virksomhedens IT-strategi kan eksempelvis hjælpe revisor med at identificere nye trusler, som er opstået som følge af ændringer i informationssystemet. Endvidere er kendskabet til virksomhedens IT-strategi med til at give et overordnet billede af virksomhedens anvendelse af og fokus på informationssystemet.

På dette område består revisors overordnede arbejde i at gennemgå ledelsesstrategien og en stillingtagen til, om alle aktuelle forhold er udmøntet i politikker, som sikrer, at IT-anvendelsen understøtter virksomhedens overordnede målsætninger[8]

Ud over de krav, der stilles i forbindelse med den lovpligtige revision, vil kendskabet til virksomhedens IT-strategi kunne gøre revisor til en attraktiv sparringspartner. I kraft af sin uafhængighed og uden risiko for modstridende interesser, kan revisor påpege områder hvor IT-strategien ikke understøtter ledelsens overordnede strategi for virksomheden.

[8] Aasmund Eilifsen, Willian F. Messier m.fl., Auditing & Assurance Service – International Edition, side 73

RS 315´s krav til gennemgang af virksomhedens IT-strategi er mindre omfattende set i forhold i CobiT[9]. CobiT fokuserer på, hvorvidt virksomhedens IT-investeringer er Værdiskabende, hvorimod RS 315 kun har fokus på de områder, som har betydning for revisors påtegning af regnskabet.

Revisor skal ved RS 315 primært gennemgå de trusler, der er i forbindelsen med IT-strategien og ikke den manglende identifikation af muligheder. Revisors erfaring og kendskab til virksomheden vil ofte gøre, at revisor er en værdifuld sparringspartner, der kan hjælpe ledelsen til at se muligheder i virksomhedens IT-anvendelse.

5.2 Systemgennemgang

I RS 315 stilles der krav til dokumentationen af de vurderinger, der er foretaget. Der er kommet et væsentligt dokumentationskrav til revisors forståelse af nøgleelementer, herunder de interne kontrolelementer.

5.2.1 Interne kontroller

RS 315 har opstillet en begrebsramme for intern kontrol[10], således at det er muligt at diskutere begrebet intern kontrol ud fra en fælles referenceramme. Elementerne i begrebsrammen indgår alle i revisors forståelse og risikovurderingsproces. Revisor skal ifølge RS 315 altid gennemgå de fem elementer, og det er alene valgfrit, om revisor ved sin gennemgang også vil teste, hvorvidt kontrollerne har fungeret effektivt i hele perioden.

Begrebsrammen for intern kontrol består af følgende fem elementer, der alle vil blive beskrevet efterfølgende:

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

[9] IT Governance Institute, CobiT 4.1 Excerpt, Executive Summery Framework, side 13
[10] RS 315, artikel 43

Det er væsentligt for forståelsen af RS 315 at have in mente, at IT nu er en integreret del af revisionen. Derved vil en gennemgang af virksomhedens interne kontroller både omfatte IT-relaterede og manuelle områder.

Opdelingen af intern kontrol i de nævnte elementer giver revisor en begrebsramme til forståelse af, hvordan forskellige aspekter af intern kontrol kan påvirke revisionen. RS 315 fremhæver, at denne begrebsramme ikke nødvendigvis er et billede af, hvordan en specifik virksomhed implementerer intern kontrol. Revisor skal have fokus på, hvordan og hvorledes en kontrol forebygger eller opdager og korrigerer væsentlig fejlinformation i transaktionssystemet, balanceposter eller oplysninger og de dertil hørende revisionsmål. Fokus er ikke, hvorvidt en kontrol kan henføres til et bestemt element. Som følge heraf kan revisor anvende andre terminologier eller begrebsrammer til at beskrive de forskellige aspekter og deres indflydelse på revisionen end de fem elementer. Det forudsætter dog, at revisor forholder sig til de fem elementer, der er indeholdt i RS 315.

Kontrolmiljø

Revisor skal opnå en forståelse af kontrolmiljøet[11], herunder de elementer, som ifølge RS 315 ligger til grund for og er bestemmende for kontrolmiljøet. Der er flere artikler i RS 315, der omhandler kontrolmiljøet, samt hvilke forudsætninger der er for, at kontrolmiljøet er effektivt, og revisor kan derved basere sine handlinger på efterprøvning af den interne kontrol.

RS 315 tolker kontrolmiljøet som værende forudsætningen for intern kontrol, herunder de andre elementer i begrebsrammen. Kontrolmiljøet beskrives som værende afgørende for ”tonen” i virksomheden og kontrolbevisheden blandt de ansatte.

Kontrolmiljøet omfatter faktorer som kommunikation, integritet og etiske værdier. Disse faktorer er grundlæggende elementer, der har indflydelse på effektiviteten af udformningen, administrationen og overvågningen af kontroller. Derudover omfatter kontrolmiljøet faktorer som holdninger til kompetence hos virksomhedens ansatte, ledelsesfilosofi og lederstil, den måde, hvorpå ledelsen tildeler beføjelser og ansvar, samt organiserer og udvikler sine ansatte og endelig den opmærksomhed og vejledning, som gives af bestyrelsen. Revisor skal overveje foranstående ele-

[11] RS 315, artikel 67 ff

menter ved vurderingen af udformningen af virksomhedens kontrolmiljø, og hvordan disse er indbygget i virksomhedens processer.

Revisor har normalt kompetence til at vurdere, hvorvidt ledelsens kontroller for de ansatte i for eksempel økonomiafdelingen er tilstrækkelige. Men i virksomheder hvor IT har en betydelig rolle, er det for revisionen også væsentligt, at det vurderes, hvorledes politikken for ansættelse af IT-personale er, og om denne er tilstrækkelige.

Virksomhedens risikovurderingsproces

I forbindelse med risikovurderingsprocessen tager revisor udgangspunkt i udformningen og implementeringen af processen. Revisor skal fokusere på, hvordan ledelsen identificerer forretningsrisici, væsentligheden af risici og den dertil hørende sandsynlighed for væsentlige fejl i regnskabet. Derudover beslutter revisor, om der skal ske tiltag, for at håndtere risici. I tilfælde af, at virksomhedens risikovurderingsprocesser har været tilstrækkelige og derved har afdækket de væsentlige risici, hjælper de revisor i denne proces med at identificere risici for væsentlige fejlinformationer.

Informationssystemer, herunder tilhørende forretningsprocesser, der er relevante for regnskabsaflæggelse samt kommunikation

Det er afgørende, at der er kvalitet i den systemgenererede information[12], da den øver indflydelse på ledelsens mulighed for at træffe de rigtige beslutninger i forbindelse med styringen og kontrollen af virksomhedens aktiviteter. Derudover påvirker informationen ledelsens mulighed for at udarbejde pålidelige finansielle rapporter.

Et informationssystem består ifølge RS 315 af følgende elementer: Infrastruktur, der dækker over fysiske forhold og maskinel, software, personer, processer og data. Informationssystemet, der er centralt for regnskabsaflæggelsen, herunder regnskabssystemet, består af processer, der registrerer, bogfører, behandler og rapporterer virksomhedens transaktioner, begivenheder og forhold samt sikrer ansvar for de relaterede aktiver, forpligtigelser og egenkapital.[13]

[12] RS 315, artikel 80 ff
[13] RS 315, bilag 2, pkt. 8 og 9

Et informationssystem, skal være velfungerende og kunne identificere og registrere alle gyldige transaktioner. Transaktionerne skal afgives rettidigt og være i en detaljeringsgrad, der er tilstrækkelig og korrekt.

Kommunikation relaterer sig til det forhold at give en forståelse af de individuelle pligter og opgaver, som knytter sig til intern kontrol. Herunder det faktum, at de ansatte forstår, hvorledes deres udførte arbejde påvirker andres arbejde, samt at de ansatte rapporterer om usædvanlige hændelser. Et miljø, der styrker de ansattes tryghed ved og mulighed for at reagere og rapportere om undtagelser og afvigelser, er et godt fundament, der tilsikrer frie kommunikationskanaler. Kommunikationen kan ske elektronisk, mundtligt og via aflæsning af ledelsens handlinger.

Kontrolaktiviteter

For at kunne bedømme risici for væsentlig fejlinformation på revisionsmålsniveau, skal revisor opnå en tilstrækkelig forståelse af kontrolaktiviteterne. De vurderede risici bruges som afsæt til at udforme yderligere revisionshandlinger. Kontrolaktiviteterne beskrives i RS 315 som værende de politikker og processer, som har til formål at sikre, at den daglige ledelses direktiver bliver udført, og at der bliver reageret på risici, der konflikter med virksomhedens strategi og målsætning. Kontrolaktiviteterne forekommer både i manuelle og IT-baserede systemer og skal udføres på alle niveauer i organisationen. [14]

Kontrolaktiviteter, som vil være relevante for ledelsen i M-Medical A/S, er følgende:[15]

- Informationsbehandling
- Fysiske kontroller
- Funktionsadskillelse

Informationsbehandling

Informationssystemets kontrolaktiviteter kan opdeles i to grupper, applikationskontroller og generelle IT-kontroller.

Applikationskontrollerne vedrører behandlingen i individuelle applikationer og medvirker til at sikre, at transaktioner er sket, er godkendte og er fuldstændigt og nøjagtigt registreret og behand-

[14] RS 315, bilag 2, pkt. 14

let.[16] Et eksempel på en applikationskontrol kunne være, at det ikke er muligt at bogføre en kassekladde, såfremt balancen ikke stemmer, eller hvis der forsøges bogført på en anden dato end den aktuelle. Disse programmerede kontroller kan også omfatte en inddatavalidering, således at der sikres en højere grad af sikkerhed for, at det der indrapporteres i systemet ikke indeholder væsentlige fejl[17].

De generelle IT-kontroller er procedurer og politikker, der vedrører mange applikationer og understøtter, at applikationskontroller fungerer effektivt ved at hjælpe med at sikre en kontinuerlig og sikker drift af informationssystemer.[18] Normalt vil følgende kontroller være omfattet af de generelle IT-kontroller:

- Datacentre og drift af netværk
- Anskaffelse af systemsoftware
- Ændringer og vedligeholdelse
- Adgangssikkerhed og anskaffelse af applikationssystemer
- Udvikling og vedligeholdelse

Det er vigtigt, at ledelsen også har fokus på ovenstående og tager stilling hertil i forbindelse med outsourcing til eksterne leverandører. Virksomhedens ledelse kan aldrig stole blindt på en kontrakt med en ekstern leverandør, og det vil være nødvendigt at foretage en aktiv styring og overvågning for at sikre sig, at kontrakten overholdes[19].

Fysiske kontroller

Fysiske kontroller omfatter aktiviteter, som skal afdække aktivernes fysiske sikkerhed, herunder tilfredsstillende sikkerhedsforanstaltninger, såsom at sikre faciliteter, der giver adgang til aktiver og registreringer, godkendelse af adgang til programmer og datafiler og periodisk optælling og sammenholdelse med beløb i kontrolregistre.[20]

[15] RS 315, bilag 2, pkt. 15
[16] RS 315, bilag 2, ptk. 15, 2. bullet
[17] RS 315, pkt. 95
[18] RS 315, bilag 2, ptk. 15, 2. bullet
[19] DS 484, kapital 12, pkt. 12.5.5
[20] RS 315, bilag 2, ptk. 15, 3. bullet

De fysiske kontroller skal sikre virksomheden mod trusler, såsom brand og tyveri, ansattes svigagtige anvendelse og manipulation med data samt menneskelige fejl, som kan resultere i driftstab. Revisors kontrol af de fysiske IT-kontroller kunne bestå i at opnå sikkerhed for, at serverrum er aflåst, at der kun er adgang for autoriseret personale til sikrede områder, samt at der er godkendelsesprocedurer ved adgang til programmer.

Funktionsadskillelse

Medarbejdernes ansvarsfølelse og samarbejde er afgørende for informationssikkerheden, og medarbejderne skal gøres opmærksomme på deres ansvar, specielt vedrørende personlige adgangskoder og informationsbehandlingsudstyr.[21]

Ved at tildele flere forskellige medarbejdere ansvar for henholdsvis godkendelse af transaktioner, bogføring af transaktioner og opbevaring af aktiver, kan ledelsen reducere risikoen for, at en enkelt medarbejder er i en position, hvor det er muligt, at denne kan lave og skjule fejl eller besvigelser i forbindelse med udførelsen af sine arbejdsopgaver.[22]

Overvågning af kontroller

Den daglige ledelses overvågning af kontroller omfatter overvejelser om, hvorvidt de virker efter hensigten, og at de tilpasses ændringer alt efter omstændighederne. Udformning af rettigheder samt nødvendigheden af eksisterende og modificerede kontroller vurderes med henblik på at sikre en høj effektivitet. De løbende overvågningsaktiviteter er ofte indbygget i virksomhedens rutineaktiviteter, og er omfattet af regelmæssige ledelses- og tilsynsaktiviteter.

Revisor vil i forbindelse med afdækningen af kontrolrisikoen og eventuelle efterfølgende tests af kontrollerne vurdere effektiviteten af disse. Denne vurdering giver en indikation af værdien ved vurderingen af de overvågende kontroller, idet en dynamisk virksomhed skal have procedurer, der overvåger kontrolaktiviteterne. Hvis virksomheden har et behov for denne kontrol, men ikke udfører overvågende aktiviteter, vil revisor ikke kunne støtte sig til de interne kontroller ved gennemførelsen af sin revision.

[21] DS 484, kapitel 11, pkt. 11.3
[22] RS 315, bilag 2, ptk. 15, 4. bullet

Det understreges i RS 315, at etablering og løbende kontrol af intern kontrol er et stort ledelsesansvar[23].

[23] RS 315, bilag 2, pkt. 18

6. Dansk Standard DS 484

DS 484 er udgivet af Dansk Standard og er gældende fra 20. september 2005. Dens formål er at støtte virksomheder i at opretholde og forbedre sikkerheden omkring IT-systemer og -anlæg, herunder danne grundlag for virksomhedens målsætning for informationssikkerhed. I DS 484 defineres informationssikkerhed som:

Den samlede mængde af beskyttelsesforanstaltninger, der skal sikre virksomhedens daglige drift.[24]

Denne definition bevirker, at det ikke er indsatsen på et enkelt område, der er udtryk for den samlede informationssikkerhed. Eftersom ingen kæde som bekendt er stærkere end det svageste led, er virksomheden, herunder dens IT-medarbejdere, nødt til at anlægge en helhedsbetragtning.

DS 484 fastslår, på lige fod med CobiT, at det er virksomhedens ledelse, der har ansvar for at tilrettelægge styringen af informationssikkerhed. Det er altså ikke IT-afdelingens ansvar at fastlægge krav til informationssikkerhed, men ledelsens.

6.1 Elementer i informationssikkerhed

Det der er udfordringen for ledelsen, er at tilrettelægge det, der kan betegnes som et passende niveau af informationssikkerhed. Hvad det er, kan der være delte meninger om. Det kan derfor være hensigtsmæssigt at tage udgangspunkt i DS 484, der har en meget fyldig beskrivelse af, hvad der er normen inden for informationssikkerhed.

I dette afsnit er valgt 4 elementer fra DS 484. Det er min vurdering at det er disse elementer, der oftest giver anledning til anbefalinger omkring styrkelse af informationssikkerhed. Disse elementer er følgende:

- Fysisk sikkerhed
- Styring af netværk og drift
- Adgangsstyring
- Beredskabsstyring

[24] DS 484, afsnit 0.1. Indledning, side 8

Som det foreskrives i RS 315, skal der foretages en risikovurdering. Ved anvendelse af DS 484 gives en model til, hvordan en sådan kan foretages. Det vil i afsnit 6.1.5 blive beskrevet, hvorledes en sådan udføres.

6.1.1 Fysisk sikkerhed

I DS 484 fastlægges formålet med den fysiske sikkerhed at "beskytte virksomhedens lokaler og informationsaktiver mod uautoriseret fysisk adgang samt fysiske skader og forstyrrelser"[25].

Dette er et område, som de fleste virksomhedsledere kan forholde sig til. Grundlæggende handler det om at beskytte IT-systemer og anlæg mod uautoriseret adgang fra medarbejdere, men også fra uønskede personer, samt fra uheld som for eksempel brand, varme og vandskade. Når placeringen af IT-anlægget skal vælges, bør man tænke sig godt om. Som udgangspunkt bør der til centrale servere og udstyr, som for eksempel krydsfelter, findes et egnet lokale, der udelukkende er dedikeret til "serverrum". Lokalet bør vælges ud fra overvejelser om placeringen i bygningen.

Ofte er kælderrum valgt til serverrum. Fordelen er, at det er gemt lidt af vejen, og desuden er der sjældent store vinduer i lokalet. Valget af et kælderrum har desværre også en række ulemper, som ledelsen bør være opmærksom på. Vand eller fugt er typisk den største ulempe ved kælderlokaler. Typisk er bygningens rørføring ikke dækket af i kælderen, og der foreligger en potentiel risiko for, at vand- og varmerør kan springe læk. Desuden er der risiko for fugtindtrængning via kældervinduer og udluftningshuller hvor regn- og smeltevand kan trænge ind. Endvidere er der med stigningen i nedbør en øget risiko for, at kloak og afløb, kan blive stoppet og løbe over.

Såfremt ledelsen i stedet vælger at anvende et rum i stueplan eller højere op i bygningen er fordelene her, at lokalet ofte ligger bekvemt, og at man som regel er fri for de fugt- og vandproblemer, der er ved kælderrum. Valget af et lokale i stueplan er dog ikke uden ulempe. Et sådant lokale er ofte forsynet med vinduer, der til tider vender ud mod offentligt tilgængelige arealer.

Det kan derfor være svært at finde et godt lokale til IT-udstyr. Uanset hvilken placering, der vælges, er der en række grundlæggende forhold, som skal være i orden. For det første skal det valgte lokale være aflåst og kun IT-afdelingen og evt. IT-ansvarlig bør have adgang. Det kan ikke tilrådes at have fælles netværksprintere eller depot i lokalet. Den fysiske adgang kan styres af enten nøgler eller magnetkort. Desuden skal der være indbrudsalarm i lokalet og det er bedst med rumfølere, der kan sikre både dør og vinduer. IT-udstyret skal sikres ordentlige arbejdsbetingelser,

hvilket blandt andet betyder, at der skal holdes en konstant rumtemperatur ved hjælp af for eksempel et airconditionanlæg. Temperaturen bør overvåges og anlæg serviceres jævnligt. For at sikrer el-forsyningen, bør nødstrøm i en eller anden form overvejes, således at servere og lignende som minimum kan lukkes ned, uden risiko for tab af styresystemer og data. Her gælder det, som med al anden sikkerhed, at det skal overvåges og serviceres, ligesom der bør ske regelmæssig test af, at nødstrømsanlægget virker.

Sidst, men ikke mindst er der brandfaren. Under hensyntagen til virksomhedens forhold kan der vælges mellem automatisk slukning, alarmering af brandvæsen eller egnet slukningsudstyr i nærheden af lokalet. Det er dog vigtigt, at der anvendes kvælstof til slukningen, og ikke vand fra et sprinkleranlæg, da vandet vil forårsage stor skade, som det også er tilfældet med vandrør, som nævnt ovenfor.

6.1.2 Styring af netværk og drift

I DS 484 har man valgt at placere ”Beskyttelse mod skadevoldende programmer” her. Det, som i medierne bliver gjort til et meget stort emne, er i DS 484 beskrevet på cirka en side[26], i modsætning til standardens øvrige emner som fylder væsentligt mere. Det handler blandt andet om antivirusprogrammer, men også om brugernes opmærksomhed omkring virusangreb og hvad de skal gøre. Selvom der i flere år har været stor fokus på dette område, ses der desværre ofte svagheder.

Beskyttelsen mod disse programmer kan blandt andet gøres ved at udstede et generelt forbud mod at anvende uautoriserede systemer, udforme retningslinier for anvendelsen af filer fra fremmede netværk og lagermedier, gennemgang af logfiler, retningslinier for håndtering, rapportering og udbedring af skader forvoldt af ondsindede koder.

Flere ikke opdaterede virksomhedsledere er ikke klar over, at det ikke er nok bare at installere et antivirusprogram. Det skal holdes opdateret og ikke mindst skal IT-afdelingen sikre sig, at brugerne ikke bare slår det fra, fordi det ”er irriterende og gør systemet langsomt”. IT-afdelingen bør desuden sikre sig, at samtlige medier, mails med videre, kontrolleres af antivirusprogrammet. Et problem er, at flere og flere anvender USB memory-sticks, og disse er ikke altid omfattet af antivirusprogrammets scanning.

[25] DS 484, afsnit 9.1., side 40
[26] DS 484, afsnit 10.4.1., side 50

Under afsnittet ”Styring af system og drift” ligger også backup. Dette område er, ligesom området omkring beskyttelse mod skadevoldende programmer, et område, hvor de fleste virksomhedsledere føler sig godt rustet. De tager en omfattende sikkerhedskopiering, typisk en daglig fuldstændig backup. Men ledelsen bør være kritisk overfor, om det bliver kontrolleret, at medierne indeholder det forventede, og at de overhovedet kan læses.

Desværre sker det alt for ofte, at det må konstateres, at dette ikke er tilfældet. Desuden skal ledelsen sikre at der foreligger beskrivelser af indlæsning af backup og at der jævnligt udføres test af dette til for eksempel et lukket testmiljø. Når disse kontroller og tests ikke foretages betyder det, at backuppen kan være falsk sikkerhed og dermed en forbundet risiko. Her er det IT-medarbejderne, der skal forsøge at bevare overblikket og få alle forhold omkring backup med. Dette bør også omfatte ekstern opbevaring af backup.

DS 484 beskriver desuden forhold som kapacitet og planlægning af netværk. Det anbefales, at alle eksisterende og nye forretningsmæssige aktiviteter skal identificeres, og de nødvendige justeringer af systemerne skal foretages således, at stabiliteten opretholdes. Det er i den forbindelse vigtigt, at ledelsen sikrer sig, at virksomheden ikke er afhængig af få nøglepersoner.

Informationssikkerhed handler også om tilgængelighed, altså om, at brugerne kan få adgang til data og systemer, når de har brug for det, men samtidig kun har adgang til de dele af systemet, som er relevante for deres arbejde. Denne funktionsadskillelse er en organisatorisk sikkerhedsforanstaltning til minimering af risikoen for fejlagtig eller bevidst misbrug af systemerne. Ledelsen skal sikre, at der etableres funktionsadskillelse for at minimere risikoen for uautoriserede eller utilsigtede ændring eller misbrug af virksomhedens informationsaktiver.

Det er således vigtigt at den samme person ikke kan tilgå, ændre og anvende informationer, uden at dette er godkendt eller bliver opdaget. For at sikre dette, er det nødvendigt, at IT-afdelingen overvåger brug af netværk og IT-anlæg via blandt andet logning.

Efterhånden som IT-anvendelsen breder sig i virksomhederne, har flere små og mellemstore virksomheder valgt at outsource hele eller en del af styringen af netværk og drift. Dette har betydet, at flere virksomheder i de seneste år er begyndt at anvende Service Level Agreement, hvori forhold omkring sikkerhedsniveauet aftales. Ved at opstille krav og målsætning vedrørende leverandøren sikrer virksomheden, at der er et fælles udgangspunkt til forventning til den leverede ydelse.

6.1.3 Adgangsstyring

I afsnittet omkring adgangsstyring foreskriver DS 484 en lang række aspekter omkring adgangskontrol og administration. Retningslinierne for adgangsstyring skal fastlægge adgangsregler og rettigheder for brugerne. Adgangskontrollen omfatter både logisk og fysisk adgang. Både brugerne og eksterne samarbejdspartnere skal være bekendt med de forretningsmæssige krav, der ligger til grund for adgangsstyringen.

De specifikke regler for adgangsstyring skal være understøttet af formaliserede forretningsgange og en klar ansvarsplacering. Retningslinierne skal blandt andet omfatte:[27]

- De enkelte forretningssystemers sikkerhedskrav
- Identifikation af de enkelte forretningssystemers informationsaktiver
- Adgangstildeling og autorisation
- Fastlæggelse af generelle brugerprofiler for generelle arbejdsopgaver
- Styring af adgangsrettigheder i distribuerede systemer
- Sletning af adgangsrettigheder

De fleste systemer i dag, hvad enten der er tale om deciderede netværkssystemer eller forskellige dynamiske internetbaserede systemer, baserer deres sikkerhed på kombinationen af password og brugernavne. I nogle tilfælde vælges begge af brugeren, i andre tilfælde er det administratoren der vælger brugernavnet, mens brugeren selv vælger passwordet og i nogle tilfælde genereres passwordet automatisk af systemet og tilsendes brugeren.

Hvad enten det er brugeren, administratoren eller systemet, der "vælger" passwordet, så er det af afgørende betydning for sikkerheden, hvordan dette password "ser ud", hvor mange tegn det indeholder, hvilke forskellige tegn og i hvilken rækkefølge de er sat sammen.

Da et password helst skal kunne huskes, er det væsentligt, at man har en eller anden form for system, der ikke er umiddelbart gennemskueligt for andre mennesker. En god metode er at lave

[27] DS 484, afsnit 11.1.1., side 62

sine passwords ud fra en rebus, hvor specialtegnene gives navne (dem, der ikke har et navn i forvejen) og så indgår i en sætning, der er let at huske[28]. Her er nogle eksempler:

- ”Peter bor i teltet ved de 2 røde Norske havelåger” = Pbitvd2rN#
- ”Andersine, hendes 3 nevøer Rip, Rap og Rup og Fedtmule” = &h3nIAUoF
- ”hos Frederik og Frank finder du 2 hvide katte + Fido” = @FoFfd2hk+F
- ”dykkeren Svend fandt 15 gamle Russiske søminer på stranden” = dSf15gRT¤ps

Da mange brugere foretrækker et password, som er ”normalt”, er det desværre ofte meget nemme passwords, der vælges. Ledelsen skal dog gøre brugerne, klart at følgende bør undgås:

- Man må aldrig bruge brugernavnet eller dele heraf
- Man må aldrig bruge sit eget fulde navn eller dele heraf
- Man bør ikke bruge ord, der kan står i en ordbog eller ordliste
- Man bør ikke bruge navne eller numre, der kan forbindes med brugeren, for eksempel tlf.-numre, fødselsdage og børnenavne
- Man må ikke bruge logiske tastkombinationer for eksempel qwerty
- Et password må aldrig skrives ned
- Man bør ikke bruge æ, ø og å

Ledelsen bør udforme retningslinier for, hvor stort tidsinterval, der skal være mellem ændring af password. Det foreskrives, at brugernes adgangsrettigheder gennemgås hver 6. måned[29], men passwords bør ændres minimum hver anden måned, for at forhindre misbrug og uautoriseret adgang. Det bør indarbejdes i systemet, at der efter anden måned med samme password kræves nyt ved første efterfølgende log-in forsøg.

Brugerne af IT-systemerne kan opdeles i to kategorier: De ”almindelige” brugere, der typisk anvender netværk og systemer og så netværksadministratorer eller andre privilegerede brugere, der typisk passer netværk og servere.

[28] www.virk.dk – “Sådan opretter du effektive passwords”
[29] DS 484, afsnit 11.2.4., side 64

De almindelige brugere:

For de almindelige brugere handler det om at oprette bruger-ID med password og de rigtige adgange til systemer og data, så det hele er klart, når nye medarbejdere starter. Det er vigtigt at sørge for, at brugerne hele tiden kun har lige præcis den adgang, de arbejdsmæssigt har behov for. Desuden er det lige så vigtigt at få nedlagt bruger-ID, når medarbejderen forlader virksomheden.

Det er ofte indenfor de nedenstående handlinger, at der opstår uhensigtsmæssigheder.

Problemer/fejl i denne kategori vil blive rettet til hurtigt, for hvis brugeren ikke har den rigtige adgang, skal de nok tilkendegive, at der forekommer mangler i adgangen.

Omkring det med at sørge for, at brugerne har de rigtige adgange, ses det ofte, at brugerne har for vide rettigheder. Det sker for eksempel ved, at brugerne skifter funktion eller afdeling, og derfor får tilføjet flere adgange eller rettigheder i systemerne. Hvis ikke der gøres noget for at holde øje med rettighederne, kan hele adgangskontrollen meget hurtigt bliver ineffektiv. Ledelsen bør overveje, om det er muligt at definere nogle typiske brugerprofiler med ensartede adgangsbehov. Ved at klassificere den enkelte bruger med en generel brugerprofil, lettes det administrative arbejde med den periodiske opfølgning.

De privilegerede brugere:

De privilegerede brugere er en opgave for sig. Det kan komme bag på ledelsen, at reglerne for adgangskontrol også gælder netværksadministratorer. Det vil skabe et øget trusselsniveau, hvis eksempelvis brugere med særlige konti slår skift af password fra, bare fordi de kan, og ikke mener, det er ”nødvendigt” at skifte hver anden måned.

Også forholdet omkring virksomhedens brug af eksterne konsulenter samt systemleverandørers adgange bør have en særlig opmærksomhed. Det tilfælde, at disse har ubetingede rettigheder til hele virksomhedens system og data skaber et unødvendigt højt risikoniveau. Ledelsen skal sikre, at virksomheden har etableret adgangsbarrierer, således at der dels kun gives adgang for konsulenter til den del af systemet, som skal serviceres, dels at der skal foretages en godkendelse af log-in på systemet, der ønskes foretaget fra en ekstern netværksforbindelse.

Ledelsen står også her overfor udfordringer omkring adgange for de medarbejdere, der forlader virksomheden, enten for en kortere periode - ved for eksempel orlov - eller permanent.

Det er meget uhensigtsmæssigt, at der er medarbejdere, som er fratrådt eller lignende, som stadig kan få adgang til systemer og data. Ledelsen skal derfor sikre, at der bliver udarbejdet en beskrivelse af de forretningsgange, der skal følges ved brugeradministration, herunder en periodisk gennemgang af, om brugerne har de rette adgange. Beskrivelsen bør som minimum indeholde de ovenfor beskrevne forhold.

DS 484 anbefaler, at der etableres og beskrives faste forretningsgange og selvfølgelig, at det kontrolleres, at de følges. Retningslinierne skal dække, hvilke netværk og tjenester, der må gives adgang til, autorisationsprocedurerne, kontroller med og procedurer for styring af adgangen og en fortegnelse over tilladte opkoblingsområder.[30]

Før der gives tilladelse til, at eksterne brugere kan opnå adgang til netværket på en sikker måde, skal der foretages en risikovurdering, som fastlægger sikringsbehovet. På baggrund af denne vurdering skal der foretages en udvælgelse og implementering af de nødvendige sikkerhedsforanstaltninger.

6.1.4 Beredskabsstyring

Området "beredskabsstyring" i DS 484 har til formål at begrænse konsekvenserne af tab af informationsaktiver forårsaget af konsekvenserne af ulykker og fejl. Tabene skal begrænset til et acceptabelt niveau samt genoprette situationen via forebyggende og udbedrende foranstaltninger.

Det skal dog gøres klart, at en beredskabsplan ikke er "vi læser bare backuppen ind igen". DS 484 beskriver de overvejelser virksomheden eller rettere sagt ledelsen, skal gøre omkring, hvilke ulykker og fejl i IT-systemer og -anlæg, der kan have indflydelse på virksomhedens aktiviteter, herunder hvilke systemer, der er kritiske i den forbindelse, og hvor hurtigt IT-systemer og -anlæg skal kunne reetableres.

Handlingerne i beredskabsstyring er nogle, som iværksættes, når det er gået galt. Der skal udarbejdes og vedligeholdes en tværorganisatorisk beredskabsstyringsproces, som skal behandle de krav til informationssikkerhed, der er nødvendige for virksomhedens fortsatte drift.

Ledelsen har måske sikret sig, at der er etableret rigtig god sikring af tilgængelighed på det fysiske område, IT-anlæg befinder sig i godt sikrede lokaler, og at hardware og netværksforbindelser

[30] DS 484, afsnit 11.4.1., side 66

findes i rigelig mængde i forhold til det egentlige behov. At disse fysiske forhold er på plads, er dog ikke det samme som en beredskabsplan.

Beredskabsplanen skal baseres på en risikovurdering. Risikovurderingen skal omfatte identifikation af sikkerhedshændelser, der kan forårsage afbrydelse i virksomhedens forretningsprocesser. Disse årsager kan være alt fra tyveri, brand og fejl på udstyr, til naturkatastrofer og terrorisme. Desuden skal risikovurderingen omfatte en fastlæggelse af sandsynligheden for og omfanget af sådanne afbrydelser. Der skal især være fokus på skadens omfang og den tid, det vil tage at reetablere.

Disse forskellige risikoaspekter skal efterfølgende sammenholdes, således at de forskellige risici kan prioriteres i forhold til virksomhedens forretningsrelaterede mål. Der bør foreligge en beskrivelse af virksomhedens beredskabsorganisation, kontaktlister, hvilke faciliteter der skal være til rådighed på et alternativt driftssted m.v. På baggrund heraf udarbejdes og godkendes beredskabsplanen. Beredskabsplanen skal som hovedregel godkendes af ledelsen, og ansvaret for beredskabsstyringen skal placeres på et tilstrækkeligt højt ledelsesniveau. Beredskabsplanerne skal løbende afprøves og opdateres, for at sikre, at de er tidssvarende og effektive.

Afprøvningen skal sikre, at alle medlemmer af beredskabsorganisationen og andet relevant personale er bekendt med planerne, samt de pågældendes ansvar og opgaver, når planen iværksættes. Forløbet af afprøvningen for beredskabsplanen skal indeholde en beskrivelse af, hvordan og hvornår hvert element i planen skal afprøves. Som ved andre sikkerhedsøvelser anbefales det, at de enkelte elementer i planerne regelmæssigt afprøves.

6.1.5 Risikovurdering

Et redskab til udarbejdelse af en risikovurdering findes i DS 484, anneks B, som indeholder en uddybende forklaring af en fremgangsmåde, som kan anvendes i praksis. I denne risikoanalyse oplistes de potentielle trusler, et estimat af konsekvenserne ved, at en sådan trussel indtræffer, samt en vurdering af sandsynligheden for, at sådanne hændelser forekommer og derefter beregnes et trusselsniveau.

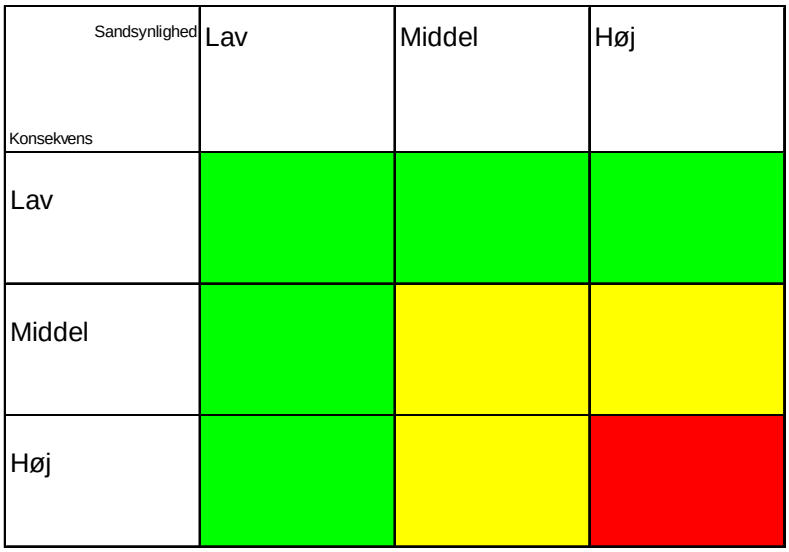
Vurdering af sandsynligheden for, at en trussel indtræffer [31]

- LAV - indtræffer meget sjældent (en teoretisk mulighed)
- MIDDEL - forekommer af og til (mindst én gang)
- HØJ - forekommer hyppigt (er observeret flere gange)

Vurdering af konsekvensen ved at, en trussel indtræffer[32]

- LAV - ingen signifikant skade
- MIDDEL - væsentlig skade
- HØJ - yderst alvorlig skade

Vurderingen har til hensigt at måle den økonomiske konsekvens ved den enkelte trussel. Når der er foretaget en vurdering af sandsynlighed og konsekvens, kan det aktuelle trusselsniveau findes ved hjælp af nedenstående figur:



Figur 3 - Kilde: DS 484, side 107

Når en trussel er identificeret, placeres den i modellen ud for det vurderede niveau af sandsynlighed og konsekvens. Trusselsniveauet er synliggjort ved farverne grøn (lavt trusselsniveau), gul (middel trusselsniveau) og rød (højt trusselsniveau). Såfremt virksomheden har en risikovurde-

[31] DS 484, side 105, oversigt ”trin 3”, uddybende kommentar

ringsproces, kan rådgiver som udgangspunkt bruge denne ved sin gennemgang af virksomheden. Dog bør rådgiver være kritisk i sin gennemgang af risikovurderingen, for at sikre, at denne er fuldkommen. I det tilfælde, at virksomheden ikke selv har en velfungerende risikovurdering, bør rådgiver forestå udarbejdelsen af en sådan. Risikovurderinger er en nødvendighed for rådgivers gennemgang af virksomheden. Desuden kan risikovurderingen være af stor værdi for virksomhedens ledelse til at få overblik over det samlede trusselsniveau.

[32] DS 484, side 105, oversigt ”trin 3”, uddybende kommentar

7. Delkonklusion

Der findes flere frameworks, som revisor kan anvende ved rådgivning om informationssikkerhed. Flere af disse frameworks henvender sig imidlertid til store virksomheder, som allerede har et højere niveau af sikkerhed, i forhold til DS 484

For at revisor kan rådgive ledelsen i M-Medical A/S omkring en forbedring af informationssikkerheden, skal ledelsen først være bekendt med, hvilke elementer, der overordnet har indflydelse på IT-governance.

For at opnå dette overordnede kendskab, er CobiT-frameworket aktuelt, eftersom dette hjælper til at styre de fokusområder, der specifikt vedrører anvendelsen af IT, herunder kontrollen med IT-governance. Overordnet foreskriver CobiT-frameworket, at ledelsen har det overordnede ansvar for IT-governance og denne skal sikre, at det værktøj, som ønskes implementeret, skal have bred accept i organisationen, hvilket opnås gennem kendskab.

Den brede accept i organisationen er vigtig, eftersom alle medarbejdere skal føle et ansvar, for at efterleve et højt niveau af sikkerhed. Derved sikres også, at medarbejderne rapporterer om forhold, som de mener vil kunne påvirke informationssikkerheden.

Revisor kan ved sin rådgivning opnå en forståelse af virksomheden og dens omgivelser ved at anvende RS 315. RS 315 foreskriver, at revisor bliver bekendt med virksomhedens IT-strategi, for derved at opnå et overordnet kendskab til virksomhedens anvendelse af informationssystemet.

Revisor kan ved anvendelse af RS 315 ligeledes blive bekendt med, hvilke elementer af interne kontroller, der skal behandles, for at opnå en tilfredsstillende forståelse af virksomheden. Disse elementer giver revisor et overordnet kendskab til systemgennemgang, herunder viden om virksomhedens anvendelse af interne kontroller og kommunikation.

Hvor CobiT og RS 315 overordnet beskriver, hvad ledelsen bør have fokus på ved IT-governance, giver DS 484 en mere praktisk tilgang til, hvordan der kan opnås forbedringer af informationssikkerheden.

DS 484 har som overordnet formål at støtte virksomheder i at opretholde og forbedre informationssikkerheden. DS 484 er væsentligt mere detaljeret omkring, hvordan forbedringer af IT-governance og informationssikkerhed opnås. Da DS 484 har en meget fyldig beskrivelse af, hvad der er normen inden for informationssikkerhed, behandler DS 484 dog områder, som ikke alle er aktuelle små og mellemstore virksomheden.

Derved giver DS 484 revisor mulighed for at rådgive om de faktiske problemstillinger i M-Medical A/S, samt give ledelsen en praktisk tilgang til forbedringer. Desuden vil anvendelsen af DS 484 hjælpe rådgiver til at foreslå ledelsen, hvilke forhold, som skal forbedres først.

Det som DS 484 ligeledes kan hjælpe med til er at opstille en risikoprofil over udvalgte fokusområder, og derved hjælpe til udarbejdelsen af en handlingsplan, som ledelsen aktivt kan anvende.

I alle tre frameworks fremhæves det, at ledelsens engagement i og forståelse for den nuværende informationssikkerhed, er essentielt for en succesfuld forbedring som følge af rådgivningen.

CobiT og RS 315 arbejder på et overordnet plan med IT-governance og informationssikkerhed. Begge frameworks fokuserer primært på, hvad der skal opnås og ikke så meget på, hvordan det opnås. For at kunne foretage en analyse af informationssikkerheden i M-Medical A/S, er det derfor nødvendigt at anvende et framework, der mere detaljeret arbejder med, hvordan den ønskede IT-governance opnås.

Det konkluderes at, DS 484 er et glimrende framework til at formidle, hvordan ledelsen i M-Medical A/S ved aktiv stillingtagen til det nuværende niveau af informationssikkerhed kan foretage forbedringer. Derfor konkluderes det, at DS 484 kan danne grundlag for en guideline, som revisor kan anvende til rådgivning omkring forbedring af informationssikkerheden i M-Medical A/S.

8. Præsentation og analyse af M-Medical A/S

8.1 Organisation og kultur i M-Medical A/S

8.1.1 Virksomhedens opbygning

M-Medical A/S er en medicinalvirksomhed, der forsker, udvikler og producerer medicin til veterinærindustrien. Virksomheden har i gennemsnit 70 fuldtidsansatte, der består af:

- En bestyrelse bestående af fire medlemmer, der alle er udpeget af hovedaktionæren, som tillige er menigt medlem af bestyrelsen
- En administrerende direktør. Det bemærkes, at direktøren er ultimativ hovedaktionær, og virksomheden derfor indirekte er ejerledet
- Fem administrationsmedarbejdere, hvoraf to modtager ordrer og fakturerer samt foretager opfølgning af debitorer - en står for lønbogholderiet og to står for den daglige bogføring af kasse- og kreditorbilag
- Fire sælgere, som står for hver sin produktgruppe
- Seks forskerchefer, der hver har tilknyttet fem til syv kemikere i teams
- Otte produktionsmedarbejdere, hvoraf der er en værkfører, fire står for at blande halvfabrikata, mens tre er i pakkeriet
- En lagerchef samt to lagermedarbejdere
- En IT-medarbejder, der står for den daglige drift, herunder indkøb, vedligeholdelse og bortskaffelse af IT. I de tilfælde, hvor IT-medarbejderen ikke kan afhjælpe problemerne, tilkaldes eksterne IT-konsulenter, som i samarbejde med IT-medarbejderen foretager de fornødne rettelser og løsninger
- Desuden har virksomheden sidste år oprettet en HR-stilling og ansat en HR-medarbejder. Denne medarbejder har i perioden efter sin ansættelse iværksat flere opgaver omkring medarbejdernes efteruddannelse

M-Medical A/S blev etableret i 1987 af direktør Mogens Berg[33], der inden da havde været ansat i en stor tysk kemikoncern. Mogens Berg er uddannet kemiker, og ved opstarten af virksomheden ansatte han en håndfuld af sine gamle kollegaer og tidligere medstuderende. Tre af disse er stadig ansat i virksomheden med titel af ”forskerchef”.

[33] Karakteren Mogens Berg er en fiktiv person som anvendes i forbindelse med modelvirksomheden ”M-Medical A/S”

Fra virksomhedens opstart har det været meget vigtigt for Mogens Berg, at der opretholdes en væsentlig grad af sikkerhed og kontrol i forskningsafdelingen. Laboratorierne ligger i en selvstændig bygning, og der skal bruges adgangskode og magnetisk ID-kort for at komme ind. De enkelte medarbejdere skal bære sterilt udstyr, når der arbejdes i laboratorierne.

M-Medical A/S' forretningsstrategi er at udvide sine eksisterende markeder inden for medicin til veterinærindustrien. Dette skal ske gennem en målrettet forsknings- og udviklingsindsats, der skal munde ud i nye produkter og nye anvendelsesområder. Derudover arbejder M-Medical A/S i stigende grad på at penetrere nye geografiske markeder med mikroorganiske løsninger. Gennem en styrkelse af organisationen vil virksomheden fortsætte denne vækst gennem lancering af en række nye produkter og anvendelser.

8.1.2 Omfang af informationsteknologianvendelsen

Kulturen i den administrative del af virksomheden karakteriseres som laissez faire fra ledelsens side med hensyn til kontrol - eller frihed under ansvar, idet holdningen er, at alle har adgang til alt, og så længe dette ikke har afstedkommet problemer med misbrug, slettede/ændrede data eller andet, er der ingen grund til at ændre på dette. Det skal dog bemærkes, at direktøren skal godkende ændringer af lønoplysninger, udbetaling af løn samt betalinger fra de likvide beholdninger.

Virksomheden benytter sig af økonomisystemet Visma, der sammen med windows- og officepakken omfatter alle centrale områder af virksomhedens IT-behandling. Derudover benytter virksomheden Dataløn til elektronisk lønhåndtering og netbank til elektroniske bankoverførsler.

Virksomheden har tre servere. En mail-server som udelukkende har til opgave at distribuerer mail, samt gemme al mailkorrespondance. Derudover findes der to netværksservere, hvor den ene er "hoved"-server og den anden en spejlserver. Alle tre servere står i samme serverrum.

Virksomhedens administration, produktion og lager ligger i hovedbygningen. Der anvendes PC'er med netværksadgang i alle tre afdelinger, og både programmer og data er gemt på netværksserveren.

Det skal dog bemærkes, at kun værkføreren i produktionsafdelingen har en PC med netværksadgang, og at denne ikke er placeret, så de øvrige produktionsmedarbejdere har direkte afgang til denne.

Medarbejderne i forskningsafdelingen anvender ligeledes PC'er med netværksadgang. Forskningsresultater registreres på PC'er, som står i et særskilt lokale i umiddelbar nærhed af laboratorierne. Alle forskningsdata bliver gemt på netværksserveren.

8.1.3 Kompleksiteten af informationsteknologianvendelsen

Virksomhedens økonomisystem Visma blev implementeret i efteråret 2008, og det er ikke fuldt afdækket, hvorvidt systemet fungerer optimalt. Der er umiddelbart ikke risiko for, at systemet genererer fejl eller mangler, men en mangelfuld instruktion i systemet med deraf menneskelige fejl ved anvendelsen af systemet har afstedkommet fejl i det vareforbrug, finanssystemet genererede på baggrund af indtastede data i lagerlogistikken. Endvidere er der mange muligheder for at generere specieltilpassede rapporter, hvor det er vigtigt, at virksomheden hele tiden følger op på, om det beslutningsgrundlag rapporterne udgøre. er korrekt.

Udover det rent økonomisystemmæssige, omfatter IT-anvendelsen ligeledes komplekse områder, såsom databaseprogrammel, netværksprogrammel med videre, men det bemærkes, at ingen systemer er selvudviklede, og at det købte standardprogrammel ikke er væsentligt tilrettet virksomhedens behov.

8.1.4 Forretningsmæssig betydning af informationsteknologi

Ved midlertidig reduktion eller bortfald af virksomhedens informationssystemer vurderes det, at der er middel risiko for væsentlige økonomiske tab, idet virksomhedens produktion i middel grad er IT-styret, og arbejdsopgaverne vil være vanskeligere at tilrettelægge manuelt.

Virksomheden vil fra tid til anden opleve forstyrrelser i selve driften og ligeledes i administration, men forstyrrelserne kan ikke karakteriseres som væsentlige, idet det i en begrænset periode er muligt at fortsætte produktionen, og manuelt kontrollere og bestille varer, skrive manuelle følgesedler mv. Dog vil driftsforstyrrelser i en periode på mere end to dage være kritisk, da de manuelle processer er langsommere, og vil resultere i en øget risiko for tab.

Eftersom forskningsafdelingens IT-system ikke er forbundet med økonomisystemet, vurderes ovenstående driftsforstyrrelser i Visma ikke at påvirke forskernes arbejde. Dog vil forskerafdelingen opleve store problemer i udførelsen af deres arbejde, såfremt der opstår driftsforstyrrelser på server og det centrale netværk. Dette skyldes, at på trods af, at en del af forskningsarbejdet foregår manuelt, vil den manglende adgang til det centrale netværk, betyde en hindring i det løbende arbejde med tidligere udviklingsresultater.

9. Analyse af informationssikkerheden hos M-Medical A/S

Med udgangspunkt i DS 484 har jeg til brug for rådgivningen af M-Medical A/S omkring forbedring af informationssikkerheden, udarbejdet en guideline. Denne guideline medtager de områder af DS 484, som jeg vurdere er relevante at analysere ud fra M-Medical A/S´ aktuelle situation.

Når punkterne i guidelinen er gennemgået for M-Medical A/S, vil resultatet af analysen af det nuværende niveau af informationssikkerhed, blive sammenholdt med ledelsens egen vurdering af trusler og risici. Hvis det er tilfældet, at ledelsen ikke selv har udarbejdet en oversigt over aktuelle problemstillinger, samt foretaget en risikovurdering, vil rådgivningen bestå af dels en analyse af forholdene ud fra punkterne i guidelinen, dels et oplæg til ledelsen, hvor hovedproblemstillinger fremhæves og sættes ind i en risikoanalysemodel.

Guidelinen er indsat som bilag A - Guideline til rådgivning omkring informationssikkerhed.

9.1 Anvendelse af guidelinen

9.1.1 IT-strategi

I forbindelse med analysen af M-Medical A/S informationssikkerhed, er Mogens Berg blevet forespurgt omkring virksomhedens IT-strategi. Mogens Berg oplyste, at IT-strategien er noget man i bestyrelsen igennem tiden har talt sig frem til, og den er præget af dels bestyrelsesmedlemmernes erfaringer fra deres bestyrelsesarbejde i andre virksomheder, dels af, hvad Mogens Berg har fundet relevant igennem tiden. Desuden oplyser Mogens Berg, at ”virksomheden da har en IT-medarbejder”, og at det er ledelsens opfattelse, at denne medarbejder styrer alt med IT.

Det lykkedes ikke at få et overblik over, hvem der er ansvarlig for IT-strategien, ligesom denne ikke findes i en nedskrevet form. Det, at IT-strategien ikke findes i nedskrevet form, gør det vanskeligt at opnå sikkerhed for, at både medarbejderne og IT-infrastrukturen lever op til Mogens Bergs forventninger, ønsker og krav. Ledelsen har dermed ikke formået at præsentere hele organisationen for, hvilke krav og ønsker, der er til anvendelsen af IT.

Denne problemstilling er blevet præsenteret og ledelsen er blevet oplyst, at det er vigtigt, at denne med udgangspunkt i virksomhedens forretningsmæssige behov og en overordnet risikovurde-

ring, formulerer en strategi, som indeholder ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan.

Ledelsen skal med strategien gøre målsætningen for informationssikkerhed klart, og skitsere de prioriteringer, som skal foretages i organisationen. Informationssikkerhedspolitikken skal fastlægge det overordnede sikkerhedsniveau og de nødvendige organisatoriske rammer, samt de overordnede retningslinier for udformningen af kontroller og sikkerhedsforanstaltninger.

Ledelsens manglende fokus på IT-strategien betyder, at der ikke er sikkerhed for overensstemmelse mellem denne og forretningsstrategien. Risikoen ved denne manglende overensstemmelse er blandt andet, at der foretages dispositioner i IT-udviklingen, som ikke understøtter den ønskede forretningsmæssige udvikling.

Desuden vil den manglende involvering fra ledelsen betyde, at der ikke vil være en overordnet identifikation af muligheder og begrænsninger i informationssystemet. Dette vil bevirke, at IT-medarbejderen vil foretage indkøb og omstruktureringer af IT-infrastrukturen ud fra egne ønsker og forventninger. Dette vil ydermere betyde, at ledelsen ikke har overblik over, om virksomheden er i en situation, hvor disse investeringer ikke harmonerer med forretningsstrategien.

Ovenstående indikerer, at ledelsen ikke har formået at udarbejde en IT-strategi for virksomheden, samt at få kommunikeret denne ud i virksomheden. Dette bevirker, at jeg i forbindelse med min rådgivning skal have øget fokus på kontrolmiljøet. Ledelsen skal informeres om, at informationssikkerhedspolitikken er den vigtigste del af strategien, og at denne som minimum bør indeholde en tydeliggørelse af, at ledelsen støtter strategien og finder den afgørende for driften, rammerne for kontroller og den risikovurdering, som skal foretages. Endvidere bør strategien indeholde en beskrivelse af ansvarsplacering og rapportering af hændelser.

9.1.2 Kontrolmiljø

For at opnå en dybere forståelse af forholdene omkring kontrolmiljøet, er virksomhedens IT-medarbejder blevet forespurgt om konkrete forhold i guidelinen.

Der er oprettet en ”medarbejderprofil” for alle ansatte med oplysninger omkring ansættelsesdato, uddannelse, gennemførte kurser og hvilke primære arbejdsopgaver, den enkelte har. Disse medarbejderprofiler er først blevet oprettet efter den nye HR-medarbejderes tiltræden, og er derfor

opdaterede. Dog kunne IT-medarbejderen oplyse, at der i profilerne ikke er anført, hvilke IT-kvalifikationer, de enkelte medarbejdere har. Disse oplysninger skal opdele medarbejderne i tre brugerniveauer sammenholdt med deres IT-anvendelse i det daglige.

På spørgsmålet omkring ledelsens bekendtgørelse og kommunikation af virksomhedens sikkerhedspolitik, blev det oplyst, at ledelsen ikke har foretaget en klar bekendtgørelse af denne. Dette kan kædes sammen med, at ledelsen, jf. afsnit 9.1.1, ikke har det fulde overblik over strategien og derfor ikke har afklaret, hvad der skal kommunikeres ud i organisationen.

Ved forespørgsel til, samt gennemgang af ansættelseskontrakter blev det konstateret, at kravet om tavshedspligt og ansvar var tydeligt. Desuden nævnes, at medarbejderen skal være ansvarlig med hensyn til sikkerheden, men der henvises efterfølgende til "Personalehåndbogen" for en uddybning. Denne personalehåndbog er af ældre dato, og indeholder ikke en uddybende forklaring omkring sikkerhed ved anvendelse af IT.

I alle ansættelseskontrakter, der er mindre end fire år gamle, er der oplyst at medarbejderen har krav på efteruddannelse og kurser, der skal vedligeholde medarbejderens kvalifikationer. Dette er desuden tilføjet et tillæg til ansættelseskontrakterne for de medarbejdere, som har mere end fire års ansættelse. Dog ses det, at der ikke er udarbejdet tillæg til ansættelseskontrakterne for de otte forskerchefer. Desuden kan det konstateres, at der ikke er udarbejdet en direktørkontrakt for Mogens Berg.

Forhold omkring ansættelsens ophør er klart defineret i en standardskrivelse, som udleveres til medarbejderen ca. en uge før sidste ansættelsesdag. I denne skrivelse fremgår det, at medarbejderen skal aflevere:

- Magnetisk ID-kort
- Nøgler
- PC (gælder også hjemme-PC)
- Mobiltelefon

Hvorledes overdragelse af ansvarsområder skal foregå, er ikke skriftligt defineret. Dette bevirker, at den fratrædende medarbejder efter egen vurdering skal videregive de oplysninger, som denne finder relevante.

IT-medarbejderen oplyser, at når en medarbejder er fratrådt, lukkes den pågældendes brugeradgang til netværket. Dog slettes brugeren ikke, da man tidligere har haft behov for at have adgang til mails og dokumenter, som tidligere medarbejdere ikke havde fået videregivet til andre i forbindelse med fratrædelsen. Dog er det således, at kun IT-medarbejderen har adgang til disse brugerprofiler, og det sikres, at brugerens password ændres til et, som kun IT-medarbejderen kender.

Generelt lider kontrolmiljøet under, at ledelsen ikke har fastlagt virksomhedens IT-strategi og derfor heller ikke har kunnet kommunikere denne ud i organisationen. Derved opstår der en risiko for, at medarbejderne ikke er bekendt med og ordentlig informeret om sikkerhedsroller og ansvar i de tilfælde, hvor der gives adgang til fortrolige informationer. Desuden vil der være en risiko ved, at medarbejderne ikke har adgang til relevante og opdaterede retningslinier. Denne manglende uddannelse i virksomhedens sikkerhedspolitikker og -procedurer gør, at medarbejderne ikke kan vide, hvornår retningslinierne for sikkerhedsprocedurerne bliver brudt, hvilket medfører, at virksomheden ikke er sikker på at få anvendt de rette sanktioner mod medarbejderne.

I relation til inddragelse af rettigheder har virksomheden klare politikker, som sikrer, i den fysiske adgang lukkes i forbindelse med en medarbejders fratræden. Dog er det problematisk, at der ikke foreligger faste retningslinier for, hvorledes dokumentationen sikres fra medarbejdere, der ligger inde med særlig information. Derved kan virksomheden risikere at miste oplysninger, som ikke kan erstattes.

9.1.3 Risikovurderingsproces

For at sikre en effektiv risikovurdering, er det essentielt, at risici kan identificeres. Dette gøres ved først at identificere de aktiver, virksomheden er i besiddelse af. I den forbindelse skal aktivernes ejere identificeres, for derved at klarlægge, hvilke kontraktlige og lovgivningsmæssige krav, der er knyttet til aktivet. Dernæst skal det klarlægges, hvilke trusler, de pågældende aktiver er udsat for.

Modellen for risikovurderingen er beskrevet i afsnit 6.1.5, og modellen vil blive brugt som udgangspunkt for, hvordan man i praksis foretager en risikovurdering.

En ting, som skal gøres klart overfor virksomhedsledelsen er, at man ikke kan sikre sig mod alt, og at der er begrænsninger for, hvad der kan betale sig at bruge ressourcer på at sikre sig imod. Før ledelsen kan foretage denne vurdering – cost/bennefit – er det nødvendigt at foretage en risikovurdering.

Som det følger af DS 484, skal informationsejeren identificere de aktiver, den pågældende er ansvarlig for. Derefter fastslås opgavens omfang, og de relevante personer, som skal deltage i analysen, udvælges. Det er vigtigt, at der er kompetencer, som dels har erfaringer med aktiver og derved kan vurdere de forretningsmæssige konsekvenser af en sikkerhedsbrist, og dels personer, som har erfaring fra IT og risikovurdering.

Ledelsens manglende fokus på IT-strategien gør, at der ved udarbejdelse af risikovurderingen ikke er etableret de nødvendige processer, som effektivt identificerer og klassificerer trusler. Ledelsen har den indstilling, at IT-medarbejderen i forbindelse med sin daglige virke i organisationen, forestår den nødvendige identifikation af trusler.

Desuden er der ikke udarbejdet en oversigt over, hvilke informationsejere, der er knyttet til de enkelte aktiver. Dette bevirker, at der let kan opstå usikkerhed omkring, hvilket ansvar den enkelte medarbejder har. Dette skyldes, at der i en virksomhed ofte er en naturlig forventning til, hvem der ”ejer” et system og dets informationer og de rettigheder, som deraf følger.[34] Som udgangspunkt ”ejer” bogholderne de finansielle informationer og lagerchefen ”ejer” de beholdningsmæssige informationer.

IT-medarbejderen foretager i et vist omfang rapportering til ledelsen, når der identificeres en mulig trussel. Det er dog langt fra i alle tilfælde dette sker, da IT-medarbejderen ofte oplever, at ledelsen ikke har den fornødne indsigt og tekniske forståelse for, hvorfor den pågældende trussel udgør en risiko for virksomheden. IT-medarbejderen foretager i langt størsteparten af tilfældene sin egen vurdering med baggrund i sin erfaring, og foretager de tilpasninger i IT-infrastrukturen som han finder nødvendig.

[34] DS 484 side 14

I de tilfælde, hvor IT-medarbejderen finder at en trussel er af så væsentlig karakter at den ud fra hans vurdering udgør en forøget risiko for virksomheden, henvender han sig til ledelsen og forelægger situationen. Direktør Mogens Berg foretager en vurdering, men da han ikke besidder den tekniske ekspertise, sker vurderingen i samråd med IT-medarbejderen. Historisk set er bestyrelsen kun blevet involveret i de tilfælde, hvor en trussel reelt har været årsag til økonomisk tab.

Et eksempel på dette er en tidligere medarbejder, der stadig havde adgang til sin mail og som en efterrationalisering af sin fyring loggede på og påvirkede M-Medical A/S´ kunder negativ. Årsagen til tabet er blevet fremlagt og bestyrelse, og direktionen bad IT-medarbejderen rette op på problemet.

I forbindelse med min rådgivning om de generelle IT-kontroller skal der udarbejdes en vurdering af, hvorvidt virksomhedens samlede risikovurderingsproces er effektiv. Ud fra ovenstående kan det vurderes, at den samlede risikovurderingsproces er meget mangelfuld. Som rådgiver skal jeg gøre ledelsen klart, at kendskabet til, hvilke risici virksomheden har og sandsynligheden for, at en trussel indtræffer, er essentielt for styringen af virksomhedens kontrolaktiviteter.

Det anbefales at stifte en IT-styregruppe med deltagelse af ledelsen, ”ejere” af væsentlige brugerområder samt IT-medarbejdere. Det er væsentligt at ledelsen engagerer sig i sikkerhedsproblematikken, og at sikkerhedsarbejder koordineres. IT-styregruppen skal introduceres til ”Risikomatrix”, som er omtalt i afsnit 6.1.5. Denne kombinerer sandsynligheden og konsekvensen i form af tab, for at en trussel bliver til en hændelse. Hvis der ikke er tale om et acceptabelt niveau, skal de risici, der kræver en indsats, identificeres. Endvidere skal disse uacceptable risici prioriteres, således at man tager hånd om de værste risici først.

Herefter skal styregruppen overveje sine muligheder for at behandle risici, hvilket inkluderer en identifikation af allerede eksisterende kontroller, og efterfølgende sætte ind gennem etablering af relevante ekstra kontroller. Derved minimeres risici, og slutteligt vil virksomheden opnå sikkerhed mod visse hændelser eller disses indvirkning.

Det vil ikke være muligt i praksis at foretage en fuld risikoafdækning, da dette ikke vil kunne svare sig ud fra en cost-/benefit-analyse. Den udækkede del af det oprindelige risikobillede betegnes som ”den resterende risiko” og vil være et udtryk for virksomhedens ”risikoappetit”. Sty-

regruppen skal opstille mål for, hvad man finder behov for at kontrollere og efterfølgende vurdere. Når ledelsen skal foretage denne vurdering med udgangspunkt i DS 484, er det ikke er krav, at samtlige kontrolpunkter implementeres[35]. Ledelsen skal prioritere indførslen af kontroller, da det ikke vil være hensigtsmæssigt at indføre alle kontroller på en gang.

Den manglende risikovurdering, sammenholdt med den manglende IT-strategi gør, at punkterne omkring kontrolaktiviteter i guidelinen skal analyseres mere indgående. Ledelsen vil derfor i forbindelse med gennemgang af guidelinens punkter omkring kontrolaktiviteter blive bedt om en vurdering af sandsynlighed for og konsekvens af, at en trussel bliver reel. Denne vurdering vil blive indarbejdet i risikomatrixen, og forelagt ledelsen som konklusion på rådgivningen.

9.1.4 Kontrolaktiviteter

Direktør Mogens Berg har siden virksomhedens stiftelse været optaget af, at der i organisationen er kontrolaktiviteter. Disse kontrolaktiviteter har fra opstarten været koncentreret om at sikre de forskningsmæssige aktiviteter i virksomheden. Efterhånden som driftsaktiviteterne og organisationen er vokset, er behovet for kontrolaktiviteter blevet tilsvarende større. Mogens Berg har blandt andet haft kontakt til et sikkerhedsfirma, som efterfølgende installerede elektronisk låsesystem og magnetkort.

De følgende afsnit vil derfor indeholde en gennemgang af de faktiske forhold i organisationen inden for guidelinens arbejdsområder, men vil også omtale andre forhold, som er væsentlige for virksomheden, men som ikke er direkte kan henføres til punkterne i guidelinen.

9.1.4.1 Fysisk sikkerhed

Formålet med, at en virksomhed forholder sig til dens fysiske sikkerhed er, jf. DS 484[36], at sikre, at virksomhedens informationsaktiver er beskyttede mod uautoriseret adgang, skader, tyveri og lignende, der kan forvoldes fysisk. Denne sikring skal den enkelte virksomhed vurdere og foranstalte i forhold til den risikoprofil virksomheden har, herunder væsentlighed og forretningsmæssige risici.

[35] Såfremt virksomhedens ønsker at blive certificeret efter DS 484:2005, skal alle punkter følges, med mindre der foretages en saglig begrundelse for at fravige.
[36] DS 484 side 40

En liste over, hvilke eksterne trusler M-Medical A/S skal beskytte sig imod, vil generelt indeholde punkter som skadepåvirkning fra naturfænomener, ulykker, brand og andre natur- eller menneskeskabte trusler, der kan ødelægge væsentlige informationsaktiver, herunder et brud på strømforsyningen, der vil påvirke driften negativt. M-Medical A/S har aktivt vurderet, at de skal forholde sig til truslen fra brand, idet sandsynligheden er uforudselig og konsekvensen kan være høj og have going-concern-indvirkning.

Ydre adgangskontrol

Hos M-Medical A/S er proceduren for den fysiske sikkerhed begrænset til anvendelsen af magnetisk nøglekort og kode. Dette er efter ledelsens vurdering den mest effektive adgangskontrol til virksomheden. Der er desuden installeret videoovervågning af virksomhedens udenomsarealer samt af indgangsdøre, som dog kun anvendes i forbindelse med forsikringserstatning ved tyveri.

Ledelsen oplyser desuden, at låsesystemet med de elektroniske magnetkort indeholder en logningsfunktion, som sammen med den personlige kode kan identificere, hvem der ønsker adgang til virksomheden. Logningen anvendes dog ikke præventivt, hvilket ellers ville give ledelsen et indtryk af, hvem der opnår/forsøger af opnå adgang til bestemte områder.

Ekstern fysisk sikkerhed hos M-Medical A/S består i, at virksomheden sikrer sig overfor uautoriseret adgang til bygningen samt til de enkelte lokaler i virksomhedens bygning, der indeholder kritiske informationsaktiver. Den fysiske afgrænsning af bygningen er sikret igennem en politik om, at yderdøre altid er låst, at de områder, hvor der sker af- eller pålæsning er overvåget, at vinduer i stueetagen altid er lukket, at vinduer i lokaler med værdifuldt IT-udstyr altid er afskærmet med persienner, at der er installeret alarm på døre og vinduer og at arealet foran virksomhedens indgang er videoovervåget.

Ud fra ovenstående kan det konstateres, at DS 484´s anbefalinger vedrørende fysisk afgrænsning af bygningen er sikret i forhold til trusselsbilledet. Ledelsen har ikke vurderet, at der er behov for, at visse områder er underlagt særlige sikkerhedsforanstaltninger udover videoovervågning som en beskyttelsesforanstaltning, hvilket jeg ikke er uenig i, i forhold til den foretagne risikovurdering.

Indre adgangskontrol

En liste over trusler, der har relevans for M-Medical A/S vedrørende den lokalemæssige fysiske afgrænsning og adgangskontrol, vil indeholde punkter som uautoriseret adgang udefra, særligt adgangsbegrænsninger til enkelte områder, når en person allerede har fået adgang til bygningen, hvor konsekvensen kan være, at der fjernes eller ødelægges væsentlige informationsaktiver i form af PC´ere, servere eller informationsmateriale i hardcopy. M-Medical A/S' vurdering er, at sandsynligheden er lav, men at konsekvenserne kan være meget høje, alt efter, hvad der mistes af data.

Ud fra ovenstående skal det fremhæves, at der ikke bliver foretaget yderligere adgangskontrol til serverrummet, når der først er givet adgang til virksomhedens lokaler. Den eneste "fysiske" barriere er et skilt med "INGEN ADGANG" på døren, men i praksis har alle adgang, så snart kontrollen ved de ydre indgange er godkendt.

Den fysiske adgangskontrol, når først en person har fået adgang til bygningerne, er ikke fastlagt nærmere af virksomheden. Ingen områder i bygningen er direkte defineret som sikre områder, hvor der er begrænset adgang, og alt personale har i princippet mulighed for at bevæge sig frit på virksomhedens område. Ledelsen i M-Medical A/S bør diskutere, hvorvidt for eksempel serverrummet, forskningsafdelingen eller varelageret bør defineres som et sikkert område med fokus på begrænset adgang.

Industrispionage

Ledelsen har vurderet, at risikoen for industrispionage er lille, og at risikoen for indbrud er større, hvorfor det er de ydre adgangsbarrierer, der er sikret. Endvidere er serverrummet sikret igennem sin fysiske placering, der kun er tilgængeligt via administrationslokalet, og ikke direkte kan identificeres som værende serverrum.

Forskningsafdelingen er ikke placeret utilgængeligt, men er etableret i en selvstændig bygning. Der er i denne bygning en del sikringsforanstaltninger, såsom overvågning, indgangssluse med to døre, hvor der kræves ekstra kontrol samt kode og aflåsning, når sidste mand forlader bygningen. Adgangskontrollen har både til formål at sikre mod uautoriseret adgang, men i væsentlig grad skal den sikre, at udefrakommende ikke kan "forurene" laboratorierne.

Optageudstyr

Der er ikke formuleret en politik om optageudstyr med videre, dette gælder ligeledes for produktionshallen og lageret, der er fysisk placeret tæt på hovedindgangen. For lager- og produktionshallen er der kun adgangskontrol i form af magnetkort og kode. Af- og pålæsningsområdet er afgrænset fra den øvrige del af virksomheden, og når der flyttes varer fra pakkeriet til færdigvarelageret, kræves der ligeledes kort og kode, før en skydeport åbnes mellem de to virksomhedsområder. Dette er i overensstemmelse med ledelsens vurdering af, at risikoen for industrispionage er lille, men vurderingen af risikoen for simpelt tyveri eller uheld, hvis uautoriseret personale får adgang, mangler.

Brandforanstaltninger

Sikringsforanstaltningerne mod brand består i, at backupbånd opbevares i brandskab og ikke på virksomhedens adresse, mens sikringsforanstaltninger mod for eksempel oversvømmelser består i, at serverrummet er placeret på første sal. Rummet er endvidere sikret mod brand, da der er installeret både iondetektorer, som aktiveres ved røg, samt termiske følere, som aktiveres ved temperaturstigninger. Det oplyses, at hvis en eller begge af disse udløses, aktiveres brandbekæmpelsesudstyr i form af kvælstof og et alarmselskab kontaktes, hvilket er i overensstemmelse med anbefalingerne i DS 484. Et tilsvarende brændslukningssystem er ligeledes installeret i forskningsafdelingen, da et almindeligt sprinkleranlæg vil kunne ødelægge laboratorieudstyret mv. I de resterende bygninger er et almindeligt sprinkleranlæg installeret.

Genstart af system

Der er ikke etableret faste procedurer for genstart af server samt rapportering af sikkerhedshændelser i forbindelse med nedbrud, jf. nedenstående behandling i afsnit 9.1.4.2. Et forbedringstiltag som skriftlige retningslinier og procedurer, såfremt systemerne ikke kan genstartes, vil være en opgradering af sikkerhedsmiljøet, der ikke er omkostningstungt.

Strømafbrydelser

Virksomheden har ikke etableret et sikkerhedsmiljø vedrørende afværgelse af mulige konsekvenser ved strømafbrydelser. De har konstateret, at strømafbrydelser forefindes, men at konsekvenserne er lave, idet strømafbrydelserne endnu ikke har forårsaget andet end kortvarigt afbrud i tilgængeligheden af IT-systemerne. Etablering af nødstrømsanlæg er ligeledes et forbedringstiltag, men virksomheden har vurderet, at sandsynligheden for, at IT-systemets tilgængelighed helt bortfalder og ikke kan reetableres, er lille.

9.1.4.2 Drift af netværk

Eksterne konsulenter

Som omtalt i afsnit 8.1.1, anvender M-Medical A/S til tider eksterne IT-konsulenter i de tilfælde, hvor virksomhedens egen IT-medarbejder ikke har kompetencerne til at løse et aktuelt problem. Ved anvendelsen af eksterne IT-konsulenter kan ledelse ikke fraskrive sig ansvaret for de generelle IT-kontroller. Ledelsen skal derfor være opmærksom på, at der i forbindelsen med udarbejdelse af kontrakten ligeledes udarbejdes en Service Level Agreement, hvori forhold omkring sikkerhedsniveauet aftales.

Kravet til udarbejdelsen af et Service Level Agreement, vurderes i M-Medical A/S' tilfælde lavere, end hvad der anbefales ifølge RS 315 samt DS 484. Dette skyldes, at der ikke er tale om en fuldstændig udlicitering af IT-leverancen til en ekstern leverandør, men at der er tale om et forhold, hvor en "In-house" IT-funktion løbende køber ydelser hos en leverandør. I praksis vil IT-medarbejdere og den eksterne konsulent arbejde i et team om løsningen af den pågældende opgave. Derved er det IT-medarbejderen, som er ansvarlig for, at IT-sikkerheden bibeholdes i de tilfælde, hvor den eksterne konsulent tildeles afgang til netværket. Dette er IT-medarbejderen klart opmærksom på, og derfor sikres det, at der, inden en tilpasning eller opdatering sættes i drift, først foretages test i en kopi af det pågældende system. Derved sikres det, at der en funktionsadskillelse mellem test og drift af systemerne. Ledelsen skal gøres opmærksomme på risikoen ved at IT-medarbejderen alene både designer, tester, godkender og implementerer i systemet.

Der har dog været tilfælde, hvor IT-medarbejderen har givet den eksterne konsulent adgang til virksomhedens netværk via den ADSL-forbindelse, som anvendes til kommunikation med omverdenen. Dette forhold udgør en høj risiko for virksomheden, eftersom en åben ADSL-forbindelse tillader alle at opnå uhindret afgang til netværket. Ligeledes er konsekvensen høj, hvis nogle opnår adgang, da der efterfølgende ikke er nogle adgangskontroller, som forhindrer fuld råderet i systemerne.

Backup

Formålet med, at en virksomhed forholder sig til backup er at sikre virksomhedens adgang til elektronisk lagrede informationsaktiver. Virksomheden skal vurdere risiko og væsentlighed og opbygge et sikkerhedsmiljø i overensstemmelse hermed.[37]

Truslen er, at serveren ikke er funktionsdygtig, og at data på serveren ikke er tilgængeligt, og konsekvenserne af dette kan være en overvejelse af virksomhedens going-concern. Et servernedbrud vil ikke umiddelbart standse produktionen, idet ordrer printes i forbindelse med planlægning af produktionen, og der findes printede versioner af de enkelte produkters sammensætning af halvfabrikata. De elektroniske produktbeskrivelser opdateres løbende, i takt med, at forskerafdelingen videreudvikler på de enkelte produkter.

Disse manualer opbevares, af hensyn til industrispionage, ikke på virksomhedens adresse, men i en bankboks. Dog har det vist sig, at disse ikke er opdaterede til samme niveau som de elektroniske.

Såfremt det ikke er muligt at få adgang til data på serveren, eventuelt fordi data er ødelagt, vil det afskære virksomheden fra kundeinformationer, økonomidata, visse former for kommunikation, lageroplysninger, udvikling med videre, det vil sige information, der er væsentlig for virksomheden, for at kunne operere udover de næste par dage.

Der foreligger skriftlige retningslinier for, hvem der har ansvaret for, at der foretages backup af serveren og behovet er vurderet til en gang ugentligt. Det er IT-medarbejderen, som i samråd med ledelsen, har fastlagt dette. Direktionen har fokus på, at det er væsentligt for virksomheden, at der foretages backup, og IT-medarbejderen foretager den ugentlige backup, uden at procedurerne er nærmere beskrevet. Det er fastlagt, at backuppen tages fredag eftermiddag og direktør Mogens Berg tager denne med hjem weekenden over. Det konstateres, at det ikke er fastlagt, om den enkelte har ansvaret for at tage backup af c-drevet på den enkeltes arbejdsstation.

I tilfælde af ferie hos IT-medarbejdere, viser det sig, at der ikke tages den ugentlige backup. Endvidere oplyser IT-medarbejderen, at når direktør Mogens Berg har ferie, er det ham selv, som tager backuppen med hjem. I disse tilfælde bliver backuppen ikke beskyttet.

[37] DS 484 side 51

Det er endvidere ikke fastlagt, hvilke data, der er kritiske og hvilke systemer, der er væsentlige, om alt skal køre på samme server, om der er nok sikkerhed i, at en server spejler sig i en anden server, når de står i samme lokale, om der skal tages backup af kun den ene server eller dem begge med videre.

Den ugentlige backup opbevares i en måned, for derefter at blive overskrevet. Ved udløbet af et regnskabsår foretages desuden en årsbackup, som gemmes i fem år. Virksomheden har vurderet, at sikker opbevaring er væsentlig, hvorfor den sker på direktørens private adresse i et aflåst, brandsikret pengeskab.

Udover at der ikke forefindes skriftlige retningslinier for backup, er der ligeledes ingen skriftlige procedurer for gendannelse af data, og det testes ikke, hvorvidt backuppen kan indlæses og anvendes. Derved opnås en falsk form for sikkerhed, hvilket er værre end ingen sikkerhed.

Derved er sikkerhedsmiljøet kun tilstrækkeligt, såfremt data kan gendannes, og konsekvensen, hvis det ikke kan benyttes til at gendanne virksomhedens elektronisk lagrede informationer, er høj.

Antivirus

M-Medical A/S anvender Symantec AntiVirus. Antivirussoftware holdes løbende opdateret, da IT-medarbejderen har en fast procedurer for at foretage opdatering en gang om ugen. Desuden holder han sig orienteret om eventuelle advarsler om angreb via hjemmesider og nyheder, og foretager en ekstra opdatering, hvis dette findes nødvendigt. Opdateringen foregår som udgangspunkt automatisk ved, at der på serveren er installeret software, som ugentligt foretager opkald til Symantec-serveren og henter den seneste opdatering. Når de enkelte medarbejdere så logger på netværket, kontrollerer Symantec-softwaren, om der er installeret seneste version på PC'en. Hvis dette ikke er tilfældet, vil serveren foretage opdatering, og der er knyttet en log til denne proces, som viser historikken for de enkelte PC'er.

Da Symantec AntiVirus er et anerkendt software, som holdes rimeligt opdateret, vurderes risikoen for, at et virusangreb får konsekvenser for M-Medical A/S som middel. Dog vurderes konsekvensen for tab, såfremt virus skulle inficere virksomheden som middel til høj, alt efter hvilket

virus, der er tale om. Desuden er der etableret firewall, for at forhindre uautoriseret ekstern adgang. Mere herom i afsnit 9.1.4.3.

Destruktion af gammelt udstyr

Gammelt IT-udstyr samles på IT-medarbejderens kontor, hvor denne forestår en formatering af harddisken på alle gamle PC'er. Når der er en større mængde gammelt udstyr, kontaktes et transportfirma, som kører udstyret til destruktion. IT-medarbejderen oplyser, at der ikke er procedurer, som sikrer, at medarbejdere fra transportfirmaet ikke tager noget af udstyret til eget brug. Som udgangspunkt registrerer IT-medarbejdere, hvilket udstyr, der sendes til destruktion, men der er flere tilfælde, hvor der ikke er kommet bekræftelse retur fra modtageren af udstyret. Derved kan kontrolsporet ikke følges.

Sikkerheden omkring bortskaffelse af udstyr er ikke tilstrækkelig og risikoen for, at udstyr genanvendes er middel. Ligeledes er risikoen for, at der kan frembringes følsomme data fra formaterede harddiske tilstede, hvilken dog betegnes som lav.

Det forhold, at virksomheden ikke har kendskab til, hvad der sker med det gamle udstyr, er et forhold, som ledelsen skal være opmærksom på. Det vurderes imidlertid, at det ikke for nuværende er et område, som skal have høj prioritet. Dette skyldes, at meget gammelt udstyr består af printere, tastaturer mv. og sjældent harddiske.

Logning

Formålet med logning er at afsløre uautoriserede handlinger. IT-systemerne skal overvåges og hændelser, der udgør en trussel mod sikkerheden, skal registreres. Anvendelsen af logning er i særdeleshed relevant for M-Medical A/S, da alle medarbejdere har adgang til alt. Ledelsen oplyser, at der er logning visse steder i systemet. Disse logninger, som er standard i de pågældende systemer, omfatter følgende:

- Sletning af bogføringslinier fra lagermodulet, som ikke er bogført i finansmodulet
- Log på opdatering på varelaget til korrekt kostpris
- Ændring af stamdata på debitorer og kreditorer
- Ændring i standardopsætning af Visma
- Log på opdatering af antivirusprogrammel

Det kan dog tilrådes, at der som forbedringstiltag etableres en administrator- og operatørlog, der har til formål at logge handlinger udført af medarbejdere med særlige rettigheder. Dette er dog næppe relevant for M-Medical A/S, da der ikke er etableret adgangsbegrænsninger i systemerne. For at overvågningen skal være effektiv, er det derfor vigtigt, at brugerne kun har mulighed for at gøre det, de har autorisation til.

Formålet med, at M-Medical A/S aktivt styrer håndteringen af sikkerhedshændelser og svagheder, er at sikre rettidig omhu, således at en hændelse eller svaghed ikke får negativ indflydelse på virksomhedens informationssystemer samt behandlingen af informationer.

Det er alene IT-medarbejderen i M-Medical A/S, der varetager drift, vedligeholdelse og sikkerhedscheck af IT-systemet. Selvom der ikke forefindes skriftlige procedurer på dette område, er den enkelte medarbejder i virksomheden vidende om, at eventuelle driftsforstyrrelser eller nedbrud rapporteres til ham. At der ikke er en fastlagt procedure for, hvad der skal rapporteres, hvad er væsentligt, hvad den enkelte medarbejder skal være opmærksom på, og hvornår der forekommer sikkerhedshændelser, giver risiko for at nogle hændelser ikke rapporteres. Dette sker, idet den enkelte medarbejder ikke er opmærksom på, at det er noget, der kan karakteriseres som en sikkerhedshændelse.

Der er generelt ikke formuleret ansvarsområder og ansvarsfordeling samt dertilhørende forretningsgangsbeskrivelser for rapportering af de enkelte sikkerhedshændelser indenfor de fastlagte ansvarsområder. Ledelsen har ikke sikret, at sikkerhedshændelser rapporteres, således at væsentlige sikkerhedsbrud håndteres korrekt.

Sikkerhedshændelser, som ulovlig fysisk indtrængen, uautoriseret systemændring og tab af tilgængelighed på IT-systemet er områder, hvor der forefindes en vis sandsynlighed for, at hændelsen vil indtræffe og konsekvenserne kan være høje. Det er samtidig områder, hvor sikkerhedsmiljøet er svingende og forbedringstiltag er mulige i forhold til konsekvenserne. Et forbedringstiltag, som ikke har anden omkostning end tid er, jf. behandlingen i afsnit 9.1.4.3, at oprette adgangsbegrænsninger til økonomisystemet.

9.1.4.3 Adgangsstyring

Adgangen til serveren og dermed de harddiske, der indeholder programmer og følsomme data er åbne for alle, der er registreret som brugere af systemet. Disse brugere får adgang til systemet

ved opkoblingen på netværket. Denne opkobling kan ske på samtlige arbejdsstationer tilsluttet LAN- netværket, og kræver indtastning af brugernavn og password.

Når der først er logget på netværket, har brugeren adgang til samtlige systemer med undtagelse af økonomistyringssystemet Visma. For at få adgang hertil, kræves yderligere indtastning af brugernavn og password. Virksomheden anvender på ingen måde de muligheder, der er, for begrænsninger af den enkelte brugers rettigheder i økonomisystemet. Det eneste, som en netværkslogin ikke giver adgang til, er lønadministrationssystem (Dataløn), der kun findes på lønbogholderens PC og direktørens PC samt netbank, som kun findes på chefbogholderens og direktørens PC.

Med de undtagelser er virksomhedens retningslinier langt fra kravene i DS 484 og god IT-skik. Der er teoretisk retningslinier for ændring af passwords – de skal være hemmelige og skal ændres med jævne mellemrum - men faktisk har medarbejderne aldrig skiftet disse. Holdningen hos IT-medarbejderen er ”at det er bedre at have det samme password, som man kan huske, end at skrive et nyt hver 14. dag, som ligger i skuffen”. Holdningen hos IT-medarbejderen har naturligvis smittet af på de øvrige medarbejdere og risikoen for, at den enkelte medarbejders password er kendt af andre, er derfor overhængende. Desuden logger ingen medarbejdere af netværket, når de forlader deres arbejdsplads for en kortere eller længere periode (for eksempel, når de går til frokost), og den står derfor ubeskyttet hen.

Såfremt M-Medical A/S ønsker en sikker beskyttelse af sine data, bør der som minimum kræves, at passwords skiftes hver anden måned og består af en kombination af tal og bogstaver[38]. Herudover bør den enkelte PC automatisk logge af netværket efter en given periode. Herved sikres, at en medarbejder ikke kan udnytte en andens brugeridentitet. Endeligt skal det sikres, at forhenværende medarbejdere slettes som brugere af systemet.

Eftersom alle medarbejdere kan opnå adgang til samtlige programmer og moduler i økonomisystemet, er der en overvejende risiko for, at der, bevist eller ubevist, foretages ændringer i data, som den pågældende måske ikke er klar over. Dette vil naturligvis kunne opdages ved gennemgang af logs, men den nuværende systemopsætning kan imidlertid ikke vise logs på andre end de i afsnit 9.1.4.2 omtalte handlinger.

[38] www.virk.dk – “Sådan opretter du effektive passwords”

Der bør dog i forbindelse med etablering af begrænsninger i brugeradgangene oprettes særlige adgange for eksempelvis virksomhedens sælgere, som bør kunne anvende oplysninger i lager-modulet. Det vil dog være essentielt, at en sådan adgang er begrænset til en læseadgang, som udelukkende gør det muligt for sælgeren at se, om varen er på lager, inden de sælger den.

Forholdet omkring håndtering af nye, ændrede og slettede brugere er et område, som virksomheden har fokus på. Dette skyldes, at man for nylig blev opmærksom på, at en tidligere medarbejder ikke var blevet slettet som bruger, og stadig anvendte sin tidligere arbejdsmail ved at logge på virksomhedens netværk fra sin private PC. Denne opdagelse bekræfter, at der er en potentiel risiko for uautoriseret, ikke-opdaget adgang til virksomhedens netværk, såfremt tidligere medarbejdere ikke slettes fra systemet. Disse vil teoretisk set også kunne bryde ind i M-Medical A/S' netværk, og således have ubegrænset adgang til data.

Efterfølgende har virksomheden indført procedurer, som sikre, at brugerkontoen for en fratrådt medarbejder lukkes dagen efter pågældendes sidste arbejdsdag. Brugerkontoen slettes dog først efter noget tid, da der kan være mailkorrespondance til medarbejderens brugerkonto, som har betydning for virksomhedens drift.

Til brug ved afsendelse af mails og kommunikation med den eksterne systemadministrator er M-Medical A/S´ system via en ADSL-forbindelse åbent overfor omverdenen.

Denne eksterne forbindelse gør det også muligt for andre end virksomhedens samarbejdspartnere at skaffe sig adgang til systemet. For at undgå uautoriseret adgang, har virksomheden etableret firewalls. Skulle det på trods af de etablerede firewalls alligevel lykkes en uautoriseret person at skaffe sig adgang til virksomhedens netværk, vil denne sandsynligvis hurtigt kunne bryde de indlagte passwords, da det ikke er etableret spærring for antal forkerte forsøg.

Det skal bemærkes, at ledelsen ikke har udarbejdet et notat eller lignende om, hvorvidt den etablerede firewall er tilstrækkelig. Det bør anbefales, at virksomhedens ledelse og IT-ansvarlige etablerer logs og jævnligt gennemgår disse for forsøg på ulovlig indtrængen i systemet og/eller forsøg på opkoblinger til netværket, hvor der har været anvendt forkert password.

Et andet forhold, som der skal gøres opmærksom på er, at IT-medarbejderen ikke har nogle begrænsninger i sine brugerrettigheder. Reelt set kan han derfor foretage rettelser og tilpasninger i samtlige af virksomhedens systemer. Det anbefales derfor, at der oprettes en log for aktiviteter udført af systemadministration som har særlige rettigheder. En sådan logning vil sikre, at oplysninger om filhåndtering, ændring i setup mv. registreres. Når der foretages handlinger vedrørende fejlhåndtering er det vigtigt, at loggen viser, hvilke korrektioner, der er foretaget, samt om der er udført eventuelt kompenserende foranstaltninger.

Udover de uautoriserede forsøg på adgang er der også de eksterne parter, som M-Medical A/S selv giver adgang til systemet. Her tænkes specielt på virksomhedens eksterne IT-konsulent, som har adgang til alle dele af systemet. Da konsulenten har fjernadgang, har virksomheden ikke umiddelbart nogen kontrol over dennes adgang, dog har konsulenten ingen konstant brugerrettighed til systemet, men skal tildeles en af virksomheden. Dette ændrer dog ikke på, at virksomheden bør sikre sig, at konsulenten har egne interne velfungerende kontroller og sikkerhedsprocedurer. I modsat fald er der en teoretisk risiko for, at andre end konsulenten kan komme i besiddelse af følsomme data.

I forbindelse med rådgivningen anbefales ledelsen, at ADSL-forbindelsen udskiftes med en krypteret adgang, for at begrænse uautoriseret adgang.

9.1.4.4. Anskaffelse af software

Ønsket om at foretage en gennemgang af procedurer omkring anskaffelse af software, er at sikre, at sikkerhedsaspektet tænkes ind i alt udstyr og det forhold, at udstyret over tid vedbliver med at være sikkert. Som ved alle andre dele af IT-infrastrukturen, skal sikkerhed indgå som en integreret del af virksomhedens informationsbehandlingsudstyr.

Ved anskaffelse af software sker der en løbende vurdering af behovet hos de enkelte medarbejdere. Denne vurdering foretages af den IT-ansvarlige sammen med brugeren, og når ønsker og behov er afstemt, forelægger den IT-ansvarlige det for ledelsen, som godkender anskaffelsen.

Denne procedure indebærer en risiko for, at der anskaffes programmer og hardware, som ikke er afstemt til virksomhedens forretningsstrategi. Ledelsens manglende viden om, hvorledes denne del af IT-strategien påvirker forretningsstrategien, indebærer ligeledes en risiko. Dette skyldes

især det forhold, at der ikke foretages test og evalueringer af nye systemer, inden de implementeres.

Et eksempel på dette er, at en medarbejder i forskningsafdelingen har ønsket modul til Visma der kunne vise salgsstatistik. Der er ikke fra ledelsens side foretaget en vurdering af trusselsniveauet ved anskaffelse af software, hvilket er uheldigt. En løbende vurdering ville i større grad sikre, at der ikke anskaffes nyt software, blot fordi man fra medarbejdernes side ønsker det, med deraf følgende risiko for at åbne op for uautoriseret adgang og lignende.

Sandsynligheden for, at en hændelse med nyt software vil true sikkerheden, vurderes som lav, eftersom langt størstedelen af M-Medical A/S' softwareanskaffelser er standardprogrammer, som er udviklet til at fungere på en Windows-platform.

Konsekvensen af, at et program ikke opfylder sikkerhedskravet vurderes som middel, men sandsynligheden for, at der anskaffes sådanne programmer, vurderes som lav.

9.1.4.5 Ændring, udvikling og vedligeholdelse af systemsoftware

Procedurer og standarder i forbindelse med systemudvikling og vedligeholdelse skal sikre, at der udvikles pålidelige og effektive systemer, samt at disse systemer vedligeholdes forsvarligt. Såfremt systemerne i ændrings- og udviklingsfasen er testet, dokumenteret og godkendt af brugerne, vil det alt andet lige give en styrket antagelse af, at systemerne er velfungerende og velkontrollerede.

Derimod vil systemer, der er udviklet i et miljø med svag systemsikkerhed indeholde en øget risiko for dårligt fungerende og utilstrækkeligt dokumenterede systemer.

Anskaffelsen af IT-systemer hos M-Medical A/S foregår efter fælles aftale mellem ledelsen og den IT-ansvarlige. Samtlige af virksomhedens IT-systemer er tilkøbte standardsystemer, der i forbindelse med driftsperioden løbende er blevet tilpasset efter brugernes ønsker. Tilpasningerne bliver foretaget af systemleverandøren, som sammen med brugeren finder frem til, hvor og hvordan ændringen skal være.

IT-medarbejderen har godkendt disse tilpasninger, men har efterfølgende ikke foretaget test på, om en given ændring har påvirket andre systemer eller opsætninger. IT-medarbejderen oplyser at

der findes logninger i blandt andet finanssystemet Visma, som viser, hvilke ændringer og tilpasninger, der har været foretaget i forhold til standardopsætningen. Disse logninger anvendes sjældent, da man ikke har fundet uhensigtsmæssig påvirkning af andre systemer.

Der sker ikke en løbende kontrol af systemerne, som sikrer at det altid er seneste version, som anvendes. Denne verifikation foretages som oftest i forbindelse med, at en konsulent fra systemleverandøren bliver tilkaldt, for at løse et problem og derved kan konstatere at systemet mangler en opdatering.

Der foretages en overordnet gennemgang af, om en rettelse har haft konsekvenser for den interne kontrol. Denne har dog en relativ lille effekt, eftersom alle brugere, jf. afsnit 8.1.2, har adgang til alle data og systemer efter succesfuld netværks- eller finanssystem login.

Med henvisning til den manglende risikovurdering fra ledelsens side, som er omtalt i afsnit 8.2.3, foretages der ingen vurdering af, om ændringer i systemsoftware vil påvirke det eksisterende trusselsbillede for M-Medical A/S.

Den manglende overvågning ved ændringer i systemerne, vil øge sandsynligheden for trusler mod virksomheden. Vurderingen af konsekvensen for virksomheden kan ikke umiddelbart gradueres, da den kan være alt fra lav til høj, afhængig af, hvilken trussel ændringen har skabt. Dette må bero på en dybere undersøgelse af de enkelte tilpasninger.

Et eksempel på tilpasninger er en opdatering af lagermodulet, som ændrede værdiansættelsen fra gennemsnitlig kostpris til FIFO. Dette viste sig at have konsekvens for sælgerne af de fik forkerte dækningsbidrag på de enkelte salg.

9.1.5 Beredskabsplan

Både ledelsen og IT-medarbejderen er blevet forespurgt med hensyn til, om der er udarbejdet en beredskabsplan for M-Medical A/S. Ledelsen mente, at det var der, eftersom man jo tager back-up og i øvrigt har flere PC'er, som kan bruges, hvis en medarbejders PC skulle gå i stykker.

IT-medarbejdere oplyste, at man har en aftale med den eksterne konsulent om, at man altid kan ringe efter ham i tilfælde af nedbrud. Hverken ledelsen eller IT-medarbejderen var bekendt med, at der skulle foreligge en beredskabsplan i udskrevet form.

Eftersom der ikke eksisterer en egentlig beredskabsplan for M-Medical A/S må konsekvensen siges at være omend meget høj i tilfælde af større nedbrud. Trusselsniveauet vurderes til at være middel og sikkerhedsmiljøet er lavt.

9.2 Rapportering til ledelsen

Som rådgiver for ledelsen i M-Medical A/S er det, grundet den manglende risikovurdering, fundet nødvendigt at foretage en sådan i samråd med ledelsen. Desuden er det funder relevant, at udarbejde en handlingsplan, der indeholder forslag til forbedringer. Det er vigtigt at understrege, at rådgivningen alene vil være forbedringsforslag, som ville kunne forbedre sikkerhedsmiljøet. Disse forslag kan ledelsen vælge enten at indføre eller forkaste, da det i sidste ende alene er ledelsen, der skal træffe valget.

Derved forbliver revisor selv som rådgiver en uafhængig part, og kan derfor på et senere tidspunkt udføre revision af virksomheden, herunder de IT-kontroller, som virksomheden efterfølgende har etableret, uden at komme i problemer med inhabilitet.

9.2.1 Trusler

Nedenstående skema er udarbejdet med henblik på en opsummering af de væsentligste trusler, som M-Medical A/S er eksponeret for. Oversigten er en del af rådgivningen, og vil blive forelagt ledelsen med henblik på, at direktion og bestyrelse bliver bekendt med forholdene omkring M-Medical A/S' IT-sikkerhed. Det skal gøres ledelsen klart at, uden en præcis IT-strategi er det sandsynligt, at de forslag, som er fremsat i forbindelse med rådgivningen, ikke er i fuld harmoni med den strategi, som ledelsen har tiltænkt for M-Medical A/S.

I skemaet er ikke alle punkter medtaget, da det dels kun er de punkter, som vurderes at have størst påvirkning af M-Medical A/S, dels de områder, som umiddelbart lettest kan forbedres. Dette skal ses ud fra det faktum, at ikke alle forhold kan eller skal ændres med det samme. Forbedringstiltagene i skemaet er ikke at betragte som endelige løsningsforslag, men skal betragtes som en handlingsplan, der giver ledelsen en indsigt i de faktiske forhold, og som ledelsen løbende skal genoverveje og vurdere.

For at sikre, at ledelsen har et fornuftigt overblik over, hvor der skal sættes ind med forbedringer, er der i forbindelse med rådgivningen udarbejdet en risikoanalyse for de udvalgte områder. Ri-

sikoanalysen præsenterer først en matrix, der placerer de konstaterede trusler ud fra deres sandsynlighed og konsekvensen af deres forekomst. Denne indplacering af de udvalgte trusler skal gøre ledelsen i M-Medical A/S bekendt med, hvilket trusselsbillede, virksomheden er eksponeret for.

Sandsynlighed / Konsekvens	Lav	Middel	Høj
Lav		4	
Middel	2	1	11 7
Høj	5 3 6	8 9	10

Figur 4 - Sandsynlighed/konsekvens - kilde: Egen tilvirkning

9.2.2 Handlingsplan

Nedenstående handlingsplan er udarbejdet, for at ledelsen skal have overblik over, hvor der bør sættes ind med forbedringer først. Det er vigtigt, at forbedringstiltagene er afstemt med forretningsstrategien, for at øge ledelsens informationsniveau i forhold til, hvor de foreslåede forbedringstiltag bør indarbejdes. Der er som resultat af trusselsbilledet udarbejdet en matrix for indplacering af sikkerhedsniveauet. Derved opnås overblik over det overordnede risikobillede, som virksomheden står overfor.

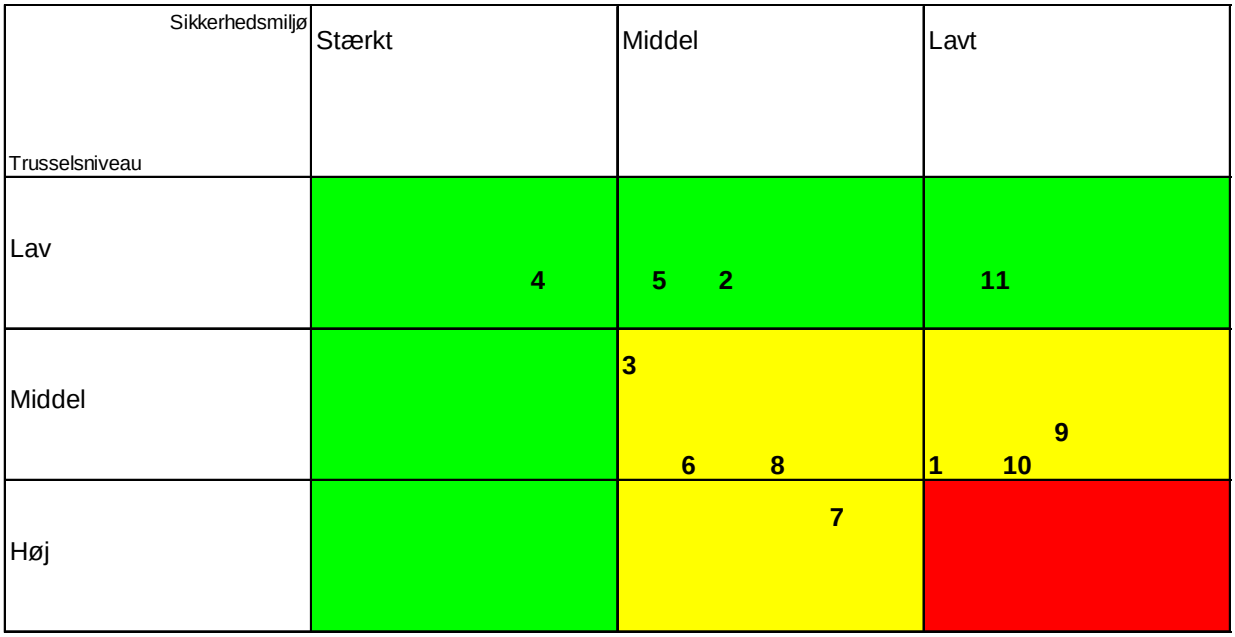
	Trusler samt mulige konsekvenser	Sikkerhedsmiljø	Forbedringstiltag
1.	Langtidssygemelding hos IT-medarbejderen, med driftproblemer til følge.	Da der anvendes standardiserede systemer, der ikke kræver konstant vedligeholdelse. Sikkerhedsniveauet vurderes mellem.	Etablering af dokumentation af arbejdsgange, systemer samt rutiner omkring fejlrettelser. Tilknytning af anden intern medarbejder og til den eksterne konsulent.
2.	Ingen forbindelse til internettet i 3-4 dage som følge af overgravet kabel. Ingen elektronisk kommunikation med risiko for svigt i bestilling af råvarer, ordremodtagelse mv.	Ingen sikkerhed. Sikkerhedsniveauet vurderes lavt.	Etablering af alternativ internetforbindelse til anden udbyder, eventuelt gennem modem. Automatisk registrering af mails til ekstern mailserver, således at ingen mails går tabt.
3.	Tyveri af server med finans- og produktionsstyringssystem med totalt datatab til følge. Serveren er placeret i et serverrum uden ekstra aflåsning i administrationslokalet.	Aflåst bygning og serverskab. Installerede alarmer med direkte kontakt til vagtselskab. Sikkerhedsniveauet vurderes som mellem.	Placering af server i normalt serverrum med ekstra sikring.
4.	Softwarefejl i applikation gør, at ordrer ikke registreres, selvom kunden modtager bekræftelse. Fejlen opdages efter et par dage.	Overvågning fra IT-afdeling. Mangeårige fejlrettelser er foretaget. Sikkerniveauet vurderes lavt.	Etablering af manuelle kontroller til sikring af ordreoprettelse. Tilretning af applikationslogik, således at risikoen for, at sådanne fejl ikke sker.
5.	En betroet medarbejders misbrug af bankapplikation. Uautoriserede personer, som opnår adgang til banken og virksomheden, oplever tab af likviditet.	Passwordbeskyttelse af applikationen. Begrænsning i personkredsen, som har kendskab til password. Sikkerhedsniveauet vurderes mellem.	Opretholdelse af begrænsningen af personer med kendskab til password. Indføre procedurer, som sikrer et jævnligt skift i password. Gennemgang og tilpasning af fuldmagtsforhold.
6.	Brand i serverrummet. Vitale data mistes, og det vil i reetableringesperioden ikke være muligt at arbejde normalt	Brandbekæmpelsesud-styr i form af kvælstof, og et alarmselskab kontaktes. Sikkerhedsniveauet vurderes mellem.	Etablering af en branddør mellem serverrummet og den øvrige administration. Dette sikrer, at en brand i kontorlokalerne ikke så nemt spreder sig til serverrummet.

7.	Tab af historiske data som følge af et virusangreb.	Antivirus software er installeret på samtlige PC'er. Sikkerhedsniveauet er lavt til mellem	Udarbejdelse og implementering af forskellige politikker, herunder mailpolitik samt politik for anvendelse af internet. Etablering af procedurer til sikring af opdateret software.
8.	Tab af væsentlige data som følge af utilstrækkelig backup. Sammenholdt med tab af data ved virusangreb har dette væsentlig konsekvens for reetablering af historiske data.	Ugentlig backup med bånd placeret i aflåst brandsikret pengeskab i direktørens privatbolig. Sikkerhedsniveau vurderes mellem.	Etablering af faste testprocedurer til sikring af funktionsdygtighed. Periodisk overførsel til bankboks af måneds- og årsbackup.
9.	IT-medarbejderen tillader den eksterne konsulent adgang, men glemmer at lukke adgangen igen. Uautoriseret adgang opnås, data stjæles og der plantes en virus i systemet.	Adgang er begrænset til en bestemt konsulent, men ellers ingen sikkerhed. Sikkerhedsniveauet vurderes som lavt.	Det anbefales, at der oprettes en krypteret forbindelse, så det sikres, at udefrakommende ikke får adgang.
10.	Der foreligger ikke en dokumenteret beredskabsplan. Afhængigheden af IT-medarbejderen giver risiko for længerevarende stop i IT-anvendelsen. Dette kan resultere i en truende going concern i tilfælde af f.eks. brandskade, tekniske problemer eller sabotage.	IT-medarbejderen har alt ansvar og kendskab til virksomhedens IT. Der er tilknyttet en ekstern konsulent, men denne virker kun til afhjælpning af specifikke problemer og ikke den daglige drift. Sikkerhedsniveauet vurderes som lavt.	Personafhængigheden kan afhjælpes ved at forbedre dokumentationen samt at sikre, at der er en grad af overlap af ansvarsområder. Desuden bør der udarbejdes skriftlige beredskabsplaner, der sikrer, at andre end IT-medarbejderen vil være i stand til at reetablere driften i tilfælde af problemer.
11.	Det er alene IT-medarbejderen, som både designer, tester, godkender og implementerer i systemet. Dette kan resultere i, at det udviklede ikke i opfylder brugerens behov.	Der er ikke noget sikkerhedsmiljø, som godkender, de af IT-medarbejderen foretagne ændringer. Sikkerhedsniveauet vurderes som lavt.	Der skal oprettes en fast procedure, som sikrer, at igangsætning af ændringer godkendes af ledelsen, og at ændringer lever op til brugerens behov.

Figur 5 - Handlingsplan - kilde: Egen tilvirkning

9.2.3 Risikoanalyse

Risikoanalysen giver et overblik over risikoniveauet ved at betragte, hvor nummermarkeringerne synligt ophober sig. Ledelsen vil måske, som resultat af rådgivningen, sætte sig som mål at få fjernet alle markeringer i det gule område. Der vil i forbindelse med ledelsens målsætning imidlertid komme økonomiske overvejelser ind i processen, da en generel cost-/bennefit-betragtning vil knytte sig til introduktion af mere sikkerhed op mod de risici, virksomheden er udsat for.



Figur 6 - Risikomatrix - kilde: Egen tilvirkning

Truslerne ved ikke at have fastlagte procedurer vedrørende håndtering af sikkerhedshændelser er, at der intet effektivt bliver gjort, for at modvirke hændelsen og sikre, at den ikke sker igen.

En trussel for M-Medical A/S kan være fejltastninger i Visma som følge af manglende adgangsbegrænsning til de enkelte moduler i systemet, hvor konsekvensen alt efter væsentligheden af fejlindtastningen kan være lav, middel eller høj.

En anden trussel kan være midlertidige eller længerevarende begrænsninger af tilgængeligheden af IT-systemer grundet strømafbrydelser, hvor konsekvensen kan være et kortvarigt nedbrud, der giver en ikke væsentlig begrænsningen i tilgængelighed, eller et nedbrud, der kan afstedkomme en væsentlig begrænsning i adgangen til systemer, og permanente begrænsninger i adgangen, indtil der reetableres nye systemer og genetableres data.

Det kan ses af ovenstående, at en alvorlig konsekvens at en trussel kan afstedkomme at en anden trussel indtræffer og sandsynligheden og konsekvensen ved, at en trussel indtræffer derfor skal vurderes nøje.

Ved at indarbejde de forbedringstiltag, der i forbindelse med rådgivninger er forelagt ledelsen, vil M-Medical A/S' risikobillede blive forrykket, således at punkt 1, 9 og 10 ikke mere er at finde tæt på det røde felt, men er flyttet "til venstre" mod midten. Desuden er det ønsket, at ledelsen via denne proces er blevet bekendt med behovet for engagement i styringen af informationssikkerheden, samt at få synliggjort sig i og fremstå som et godt eksempel i henhold til IT-strategien.

Først og fremmest skal ledelsen informeres om det signal den sender til organisationen ved ikke at være en aktiv del af IT-sikkerhedspolitikken. Dette gælder også den manglende IT-strategi og den ansvarsfralæggelse, der er foretaget, ved at overdrage så mange vurderinger og beslutninger til IT-medarbejderen.

Endvidere er formålet med præsentationen af ovenstående risikobillede at præsentere den risiko, som den begrænsede bemanding i IT-afdelingen (kun en medarbejder) udgør for virksomheden. IT-medarbejderen har i gennemgangen ikke lagt skjul på, at der anvendes eksterne konsulenter til at assistere ham ved manglende ekspertise. Ledelsen skal være opmærksomme på den forhøjede risiko ved, at det er IT-medarbejderen alene, der både designer, tester, godkender og implementerer i systemet.

Forholdet omkring den ikke-krypterede forbindelse til den eksterne konsulent er et område, som både ledelsen og IT-medarbejderen skal være meget opmærksomme på. Ledelsen bør kende risikoen ved ikke at anvende denne type forbindelse, mens IT-medarbejderen har det direkte ansvar for at sikre, at den anvendte forbindelse ikke kan misbruges.

Ledelsen skal ved anvendelsen af eksterne konsulenter desuden vise sit engagement, og opfordres til at være en aktiv del af processen ved valg af leverandør. Her tænkes især på den dobbeltrolle, som den eksterne leverandør har, dels som en del af rådgivningen omkring IT, dels at optræde som sælger for sin arbejdsgiver. Ledelsen skal derfor vælge en leverandør, som kan håndtere denne dobbeltrolle, og derved ikke stiller M-Medical A/S i en situation, hvor den eksterne konsulent har oversolgt egne produkter eller løsninger.

Placeringen af serveren er ligeledes et fokusområde, som ledelsen bør prioritere højt. En forbedring i form af en rigtig branddør samt lås og adgangskontrol af lokalet, hvor serveren er placeret, vil umiddelbart styrke sikkerhedsmiljøet. Endvidere bør ledelsen få etableret procedurer, som sikrer at der foretages reetableringstest af backuppen samt udarbejdelse af en effektiv beredskabsplan.

Desuden skal det fremhæves, at den manglende beredskabsplan er et kritisk punkt for virksomheden, da dette i værste fald kan påvirke going-concern. Ledelsen skal igen gøres opmærksom på sit ansvar. Der skal findes en plan for at afprøve og vedligeholde virksomhedens beredskab, samt en fastlæggelse af de retningslinjer, som træder i kraft, når skaden er sket. Et beredskab, der ikke er vedligeholdt, er ikke noget beredskab.

Da beredskabsplanen beskriver sårbarheder i organisationen og derfor kan indeholde fortrolige informationer, bør denne ikke ligge frit tilgængelig i virksomheden. Kopier af beredskabsplanen skal altid opbevares således, at kopierne ikke berøres af en katastrofe i selve virksomheden. Ledelsen skal sikre, at disse kopier altid er opdaterede og beskyttet på samme niveau som i organisationen.

10. Delkonklusion

Det konkluderes at, ledelsen i M-Medical A/S kun i begrænset omfang har kendskab til niveauet og vigtigheden af informationssikkerhed. Ledelsens manglende kendskab betyder et lavt engagement i vurderingen af virksomhedens aktuelle situation inden for den nuværende anvendelse af IT. Medarbejderne påvirkes af ledelsens laissez faire holdning til informationssikkerheden, og de føler ikke et ansvar for at sikre sig yderligere, end hvad IT-medarbejderen har foreskrevet.

Det konkluderes at, ledelsens manglende engagement gør, at det generelle krav til governance - at vise lederskab - ikke opfyldes. Først når ledelsen begynder at vise lederskab, vil dette sprede sig til organisationen. Selvom ledelsen på nuværende tidspunkt ikke har den fornødne indsigt i IT-anvendelsen, skal denne dog aktivt involvere sig i alle dele af virksomheden. Dette gælder også informationssikkerhed.

Når ledelsen først er blevet bekendt med sit ansvar og tager dette alvorligt, vil det med al tydelighed være klart for ledelsen, at den manglende IT-strategi er årsag til medarbejdernes generelle adfærd. Ledelsen skal ændre sin holdning til, at det er IT-medarbejderen, som via sin stilling er ansvarlig for alt vedrørende informationssikkerheden. Det er derimod ledelsen, som med IT-strategien opstiller, hvilke krav og ønsker, der er til anvendelse af IT i organisationen.

Det kan derfor konkluderes, at ledelsen skal træde i karakter og begynde at lede M-Medical A/S, for derigennem at vise organisationen, at informationssikkerhed vægtes højt.

Ledelsens holdning til informationssikkerheden bevirker, at M-Medical A/S er udsat for en række trusler og risici. Disse trusler og risici har resulteret i udarbejdelsen af en handlingsplan, hvori elleve trusler er beskrevet samt de konsekvensen af disse. Endvidere er M-Medical A/S' nuværende sikkerhedsmiljø beskrevet. Endelig vil der blive præsenteret et forslag til forbedringstiltag, for hver enkelt trussel, som vurderes at kunne styrke informationssikkerheden. Af disse elleve trusler vurderes især fem at have en væsentlighed, der gør, at ledelsen med det samme bør foretage forbedringer.

Den første væsentlige trussel er tab af data ved backup som følge af den manglende kontrol af backup. Dette er en trussel, som ledelsen skal være klar over forekommer, når der ikke foretages

test af backup. Dette giver en falsk tryghed for ledelsen, hvilket er værre end at ledelsen er vidende om mangler, men har valgt at acceptere den.

Den anden væsentlige trussel er tyveri af serveren. Denne trussel er lavere en truslen fra den manglende kontrol af backup, eftersom der er fysiske låse på yderdørene. Ledelsen skal dog være opmærksom på, at hvis en person først har fået uautoriseret adgang til administrationen, eksisterer der ikke andre adgangskontroller. Det vil dermed være muligt at fjerne server og andet udstyr.

Den tredje væsentlige trussel er afhængigheden af IT-medarbejderen. I tilfælde af længerevarende sygdom hos IT-medarbejderen står virksomheden reelt i den situation, at det ikke er muligt at opretholde en fornuftig drift af netværket. Ligeledes vil adgangsstyringen over tid blive svækket.

Den fjerde væsentlige trussel, som vejer tungt i risikovurderingen, er det forhold, at der ikke anvendes en krypteret forbindelse mellem virksomheden og den eksterne konsulent. Ved at anvende en almindelige åben ADSL-forbindelse, åbner virksomheden op for direkte angreb. Det forhold, at IT-medarbejderen endvidere skal foretage manuel lukning af adgangen, øger risikoen for uautoriseret adgang, såfremt lukning ikke foretages.

Den femte væsentlige trussel er den manglende beredskabsplan. Da denne først bliver aktuel i det tilfælde, at skaden er sket, vil det således være for sent at skulle foretage vurderinger omkring indholdet af en sådan. Især omkring udarbejdelsen af beredskabsplanen skal ledelsen vise sit ansvar og aktivt udforme en plan, som nedbringer virksomhedens afhængighed af IT-medarbejderen.

Desuden skal det fremhæves, at den manglende beredskabsplan er et så kritisk punkt for virksomheden, at denne i værste fald kan påvirke going-concern.

Ledelsen skal ligeledes vise sit engagement ved at inddrage IT-medarbejderen aktivt i udformningen af beredskabsplanen og sikre, at han løbende holder beredskabsplanen opdateret. Ledelsen skal kommunikere ud i organisationen, at et beredskab, der ikke er vedligeholdt, ikke er noget beredskab.

Det kan konkluderes, at virksomhedens nuværende kontroller ikke er tilstrækkelige til at minimere trusselsniveauet. Størstedelen af de kontroller, som er implementeret i virksomheden, er ydre fysiske adgangskontroller. De indre adgangskontroller begrænser sig til log-in med brugernavn og password på PC'erne, og der er ikke etableret brugerdefinerede rettigheder eller afgrænsninger i IT-systemet. Analysen af M-Medical A/S har vist, at IT-medarbejdere alene kan disponere over adgangsrettigheder til systemer, uden at der foretages en kontrol.

Ledelsen skal i forbindelse med den fremadrettede forbedring af informationssikkerheden have en mente, at forslagene i handlingsplanen ikke er udtømmende. Derfor skal ledelsen løbende holde sig orienteret om nye trusler og mulige risici.

11. Konklusion

Det konkluderes at, ledelsen i M-Medical A/S kan forbedre virksomhedens informationssikkerhed ved at fokusere på sit ansvar som ledelse, og derved vise lederskab, governance.

Revisor kan, til brug for rådgivning af ledelsen i M-Medical A/S omkring forbedring af informationssikkerheden, anvende flere forskellige frameworks. Revisor skal i forbindelse med sin rådgivning sikre sig, at ledelsen er bekendt med begrebet IT-governance.

Til brug for opnåelse af dette kendskab er CobiT-frameworket aktuel, eftersom dette hjælper til at styre de fokusområder, der vedrører IT-governance. Her fremhæves det, at ledelsen har det overordnede ansvar for IT-governance, og at ledelsen skal sikre, at det værktøj, som ønskes implementeret, skal have bred accept i organisationen, hvilket opnås gennem kendskab.

I forbindelse med sin rådgivning kan revisor opnå en forståelse af virksomheden og dens omgivelser ved at anvende RS 315. Derved bliver revisor bekendt med M-Medical A/S´ IT-strategi og derigennem opnås et overordnet kendskab til virksomhedens anvendelse af informationssystemet.

Igennem det overordnede kendskab til anvendelsen af informationssystemet, opnås ligeledes en forståelse for M-Medical A/S´ anvendelse af interne kontroller og strømmen af kommunikation i organisationen.

Det kan konkluderes, at både CobiT og RS 315 er gode frameworks, som kan hjælpe rådgiver til at forklare ledelsen, hvilke elementer, som indgår i en god IT-governance, og hvad der har indflydelse på niveauet af informationssikkerhed.

DS 484 er et framework, der er væsentligt mere detaljeret omkring, hvordan forbedringer af IT-governance og informationssikkerhed opnås. DS 484 behandler dog de samme forhold, som indgår i RS 315, men via sin detaljeringsgrad giver anvendelsen af DS 484 i rådgivningen, ledelsen en praktisk tilgang til forbedringer.

Det kan dermed konkluderes, at både CobiT, RS 315 og DS 484 er gode frameworks, som kan hjælpe revisor ved rådgivning om forbedring af informationssikkerhed. Det konkluderes, at DS 484 findes mest egnet til at danne grundlag for en guideline, som revisor kan anvende til rådgivning omkring forbedring af informationssikkerheden i M-Medical A/S.

Det må ligeledes konkluderes, at i den aktuelle situation, er DS 484 det mest anvendelige framework til at rådgive om, hvordan ledelsen i M-Medical A/S ved aktiv stillingtagen til det nuværende niveau af informationssikkerhed, kan foretage forbedringer.

Igennem analysen af M-Medical A/S er jeg blevet bekendt med, at virksomhedens ledelse kun i begrænset omfang har kendskab til niveauet og vigtigheden af informationssikkerhed. Ledelsens manglende kendskab har betydet et lavt engagement, hvilket igen gør, at ledelsen derfor ikke opfylder det generelle krav til governance - at vise lederskab. Først når ledelsen begynder at vise lederskab, vil dette sprede sig til organisationen.

Det manglende engagement hos ledelsen kommer til udtryk ved, at ledelsen ikke har opstillet en IT-strategi, der beskriver ønsker og krav. Ledelsen har derimod overladt ansvaret for informationssikkerheden til IT-medarbejderen.

Ud fra analysen af M-Medical A/S kan det konkluderes, at ledelsen skal træde i karakter og begynde at tage ansvar i den nuværende situation, for derigennem af vise organisationen, at informationssikkerhed vægtes højt.

Endvidere konkluderes det, at M-Medical A/S er eksponeret for en del trusler og risici i forbindelse med det nuværende niveau af informationssikkerhed. Disse trusler og risici er præsenteret i en handlingsplan, som indeholder i alt elleve forhold. For hvert af disse forhold er det nuværende sikkerhedsmiljø præsenteret, tillige med et forbedringsforslag som ledelsen kan vælge om den vil gøre brug af.

En væsentlig trussel er afhængigheden af IT-medarbejderen. Denne afhængighed betyder, at virksomheden reelt står i en situation, hvor det ikke er muligt at opretholde en fornuftig drift af netværket, hvis IT-medarbejderen i en længere periode ikke er disponibel for M-Medical A/S.

En anden væsentlig trussel er virksomhedens manglende beredskabsplan. Ledelsen skal sikre sig, at der etableres en beredskabsplan, som bevirker, at M-Medical A/S ikke oplever problemer med going-concern. Ledelsen skal endvidere sikre sig, at beredskabsplanen holdes opdateret og være vidende om, at et beredskab, der ikke er vedligeholdt, ikke er noget beredskab.

Ud fra analysen af M-Medical A/S kan det konkluderes, at virksomhedens nuværende kontroller ikke er tilstrækkelige til at minimere det aktuelle trusselsniveau. Der mangler både en effektiv adgangsstyring til netværket, og der er ikke etableret brugerdefinerede rettigheder eller afgrænsninger. Endvidere er der ikke etableret tilstrækkelige applikationskontroller, der sikrer at IT-medarbejderens eventuelle systemtilretninger ikke påvirker for eksempel fuldstændigheden af en transaktion.

Ved anvendelsen af DS 484, som grundlag for den udarbejdede guideline, har revisor fået et praktisk redskab som i høj grad kan anvendes til rådgivning omkring forbedringer af informationssikkerhed. Rådgivningen har givet ledelsen i M-Medical A/S et overblik over, hvilke trusler, der blandt andet eksisterer ved det nuværende niveau. Revisor har i egenskab af rådgiver ligeledes givet ledelsen et værktøj til at foretage vurderinger af informationssikkerheden.

Ledelsen skal i forbindelse med den fremadrettede forbedring af informationssikkerheden have in mente, at de forslag til forbedringer, som er præsenteret i handlingsplanen, ikke er udtømmende. Derfor skal ledelsen løbende holde sig orienteret om nye trusler og mulige risici.

12. Executive Summary

The management of small and medium-sized companies often does not realise the importance of information security and is not aware of the threats and risks that their current use of IT pose to their business. As an auditor you can be a sparring partner to the management by analysing the current level of information security and making suggestions for improvements.

In my capacity as auditor for the company M-Medical A/S, I have used RS 315 in my advice to the company in order to learn about the company and its surroundings. During my audit, I became aware of matters concerning information security in general, which do not seem appropriate.

In order to be able to advise the company about the different aspects of information security, I have used DS 484 as the basis for a guideline I have prepared. This has provided me with a practical tool, which is highly suitable for advising companies on how to improve information security.

In connection with my analysis of information security at M-Medical A/S, I talked to the management and relevant key members of staff. During my analysis, I found that the management of M-Medical A/S has only limited knowledge of the level and importance of information security and is therefore unaware of the threats and risks facing the company.

My advice has helped the management of M-Medical A/S to understand the threats posed by the current level of security. My advice has also provided the management with a tool to assess information security.

When making future improvements in information security, the management should remember that my suggestions for improvements, which are presented in the action plan, are not exhaustive. The management therefore needs to keep itself up-to-date on new threats and potential risks.

13. Begreber og terminologier

Afhængighed	Er udtryk for virksomhedens afhængighed af hardware, programmer, data, leverandører og medarbejdere.
Applikationskontroller	Applikationskontroller er manuelle eller programmerede procedurer, der skal være med til at sikre, at transaktioner har fundet sted, er godkendte og er fuldstændigt og nøjagtigt bogført og behandlet
Corporate Governance	De mål, et selskab styres efter, og de overordnede principper og strukturer, som regulerer samspillet mellem ledelsesorganerne i virksomheden, ejerne samt andre, der direkte berøres af virksomhedens dispositioner.
Ejeren af et aktiv	Med aktivets ejer menes en person, som er placeret på ledelses- eller mellemlederniveau, og for hvis funktion eller ansvarsområde aktivet har en stor indflydelse. For de IT-baserede aktiver vil der ofte være flere ejere – en for funktion/processiden og en for driftssiden.
Ekstern sikkerhed	Den eksterne sikkerhed omfatter en afdækning af risici, der opstår på baggrund af udefrakommende faktorer, som virksomheden i første omgang ikke har mulighed for at kontrollere.
Forebyggende foranstaltninger	Er udtryk for en fysisk foranstaltning eller en kontrol, som forventes at forhindre eller begrænse hændelser eller begivenheder, som kan medføre tab.
Generelle IT-kontroller	Generelle IT-kontroller er de kontroller og sikkerhedsforanstaltninger, som virksomheden har indført for at vurdere, om data, systemer og drift efter virksomhedens forhold er tilstrækkeligt sikret. De generelle IT-kontroller dækker både over kontroller i forbindelse med drift af netværk, anskaffelse, ændring og vedligeholdelse af systemsoftware, adgangssikkerhed mv.
Informationssikkerhed	Begrebet informationssikkerhed dækker over alle IT-forbundne informationer, men også ikke-IT-forbundne, såsom oversigter over organisationens og medarbejdernes kompetencer, fysiske rammer, fysiske dokumenter, for eksempel aftaler, ansættelseskontrakter mv.
Informationssystem	I afhandlingen anvendes begrebet ”informationssystem” om systemer, der består af to eller flere relaterede komponenter, som interagerer for at opnå et mål, og hvis primære formål er at generere informationer til organisationen.

Interne kontroller	En proces iværksat af virksomhedens ledelse, designet til at give en rimelig sikkerhed for målopfyldelsen.
Intern sikkerhed	Den interne sikkerhed omfatter en afdækning af risici ved interne forhold, såsom personale, infrastruktur, adgange mv.
IT-governance	De overordnede IT-mæssige mål, som virksomheden styres efter og de overordnede principper og strukturer, der regulerer samspillet mellem IT og forretningsmål.
IT-infrastruktur	IT-infrastrukturen dækker over PC'er, servere, kabler, krydsfelter. Desuden er netoperativsystemer, software, databaser, intranet og internet systemer omfattet.
IT-sikkerhed	Begrebet IT-sikkerhed dækker over de IT-forbundne informationer, som er indeholdt i systemer og anlæg.
IT-sikkerhedspolitikken	IT-sikkerhedspolitikken har til formål at tilkendegive overfor alle, som har en relation til M-Medical A/S, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinier.
IT-strategi	IT-strategien er en overordnet præsentation af, hvilke krav og ønsker, ledelsen har for anvendelse af IT i virksomheden.
Konsekvens	Udtrykker den fysiske konsekvens af, at et givet risikomål udsættes for en given risiko.
Ledelsen	Betegnelsen virksomhedens "ledelse" skal opfattes som en samlet betegnelse for bestyrelse og direktion i det tostrengede ledelsessystem. Hvor der i afhandlingen refereres til "ledelsen", menes den daglige ledelse.
M-Medical A/S	M-Medical A/S er den modelvirksomhed, som anvendes i afhandlingens analysedel.
QWERTY	QWERTY betegner det mest udbredte tastaturudlægning af bogstaverne på tastaturer til computere og skrivemaskiner. Navnet QWERTY kommer fra de seks første bogstaver i den øverste række af bogstaver på tastaturet.
Referenceramme/Framework	Referenceramme eller framework anvendes som betegnelse for et sæt retningslinier uden juridiske aktionsmuligheder for håndtering af processer og virksomhedsstyring.
Revisor	Anvendelse af revisor i afhandlingen, er synonym med statsautoriseret eller registreret revisor.
Risikofaktor	Hændelse eller begivenhed, der kan medføre fejl, tab af data, etc.

Risikohyppighed	Den hyppighed, hvormed den enkelte risikofaktor skønnes at forekomme. Hyppigheden beskrives som en faktor, der udtrykker forekomst pr. år.
Risikostyring	Betegnelse for en samlet styring af kendte og ukendte hændelser, som indtræffer, når virksomheden forsøger at opnå sin målsætning, og som kan have en negativ eller positiv påvirkning på målopfyldelsen.
Små og mellemstore virksomheder	Små og mellemstore virksomheder defineres som virksomheder, der er omfattet af Årsregnskabslovens klasse A til B.
Sårbarheder	Er udtryk for den følsomhed, de enkelte risikomål har overfor forskellige risici.
Virksomhed	Betegnelsen ”virksomhed” anvendes som en samlet betegnelse for mindre og mellemstore virksomheder – virksomheder, der er omfattet af Årsregnskabslovens klasse A til B.

14. Litteraturliste

Revisionsstandarder

Revisionsstandard RS 315 - Forståelse af virksomheden og dens omgivelser og vurdering af risici for væsentlig fejlinformation, Foreningen af Statsautoriseret Revisorer.

Revisionsstandard RS 402 - Revisionsmæssige overvejelser vedrørende virksomheder, der anvender serviceleverandører, Foreningen af Statsautoriseret Revisorer.

Revisionsstandard RS 3411 - Erklæringsopgaver om generelle IT-kontroller og applikationskontroller mv. , Foreningen af Statsautoriseret Revisorer.

Bøger og artikler:

Accounting Information Systems, Marshall B. Romney og Paul John Steinbart, 9. udgave, Pearson Education, 2003. ISBN 0-13-049541-7.

Accounting Information Systems, Ulric J. Gelinas og Richard B. Dull, 7. udgave, Forlaget Thomsen 2008. ISBN 03-243-7883-1

BS ISO/IEC 17799:2005 / BS 7799-1:2005 – Information technology – Security techniques – Code of practice for information security management, British Standard, 2005

CobiT 4.1 “Executive Summary and Framework”, The IT Governance Institute, 2007

CobiT 4.1 “Framework, Control Objectivies, Management Guidelines, Maturity Models”, The IT Governance Institute, 2007

COSO ”Internal Control – Integrated Framework”, The Committee of Sponsoring Organizations of the Treadway Commission 1992

COSO “Enterprise Risk Management” – Integrated Framework, Application Techniques” The Committee of Sponsoring Organizations of the Treadway Commission 2004

COSO “Enterprise Risk Management” – Integrated Framework, Executive Summaty Framework” The Committee of Sponsoring Organizations of the Treadway Commission 2004

Den skinbarlige virkelighed – om valg af samfundsvidenskabelige metoder, Ib Andersen, 1. udgave, Samfundslitteratur. ISBN 87-593-0915-6

DS 27005 – Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for risikostyring, Dansk Standard, 1. udgave, 2008

DS 484 - Standard for informationssikkerhed - Code of practice for information security management, Dansk Standard, 1. udgave, 2005

Effektivisering af risikostyring og interne kontroller i forbindelse med implementering af informationssystemer, Thomas Greve Houmølle, Cand.merc.aud. kandidatafhandling, 2005.

God IT-skik, Arbejdsudvalget for god IT-skik. Forlaget FSR 1999, ISBN 87-7747-266-7

Information Systems Auditing and Assurance, James A. Hall, 2000, South-Western College Publishing. ISBN 0-324-01653-0

IT Governance – How Top Performers Manage IT Decision Richts for Superior Results, Peter Wiell and Jeanne W. Ross, 2004, Harvard Business School Press. ISBN 1-59139-253-5.

IT Governance based om CobiT® 4.1 – A Management Guide, Koen Brand og Herry Boonen, 3. udgave, 2007, Van Haren Publishing. ISBN 978-90-8753-116-4

IT revision, Carsten W. Heilbuth og Carsten Tjagved, 1. udgave, Forlaget Thomsen 2000. ISBN 87-619-0137-7

IT-sikkerhed – I små og mellemstore virksomheder, Morten Klitgaard Friis, Carsten W. Heilburt og Henrik Lei, KPMG IT Risk Management, 1. udgave, 2003, DANSK IT. ISBN 89-88972-31-3

Ledelse af IT-sikkerhed – for forretningens skyld, ITEK og Dansk Industri, 2002. ISBN 87-7353-427-7

Mistede data koster kroner og kunder, Thomas Breinstrup, business.dk, 2. februar 2009.

Pressemeddelse Deloitte & Touche – "Hver fjerde virksomhed har ikke styr på IT-sikkerheden", Per-Henrik Goosmann, Deloitte & Touche, 2002

Revisor og IT-Governance, Jens Bjargum, Cand.merc.aud. kandidatafhandling, 2008.

Revisionsstandarden RS 3411 – Erklæringsopgaver som generelle it-kontroller og applikations-kontroller mv., Dorthe Tolborg, Revision og Regnskabsvæsen nr. 11, 2005

Summary of the Provisions of the Sarbanes-Oxley Act of 2002, The Center for Audit Quality, 2002

TDC sendte Danske Bank i sort, Rune Pedersen, Computerworld, 13. marts 2009.

Hjemmesider

www.ciber.no

www.coso.org

www.isaca.org

www.itek.di.dk

www.itgi.org

www.thecaq.aicpa.org

www.virk.dk

Bilag A - Guideline til rådgivning omkring informationssikkerhed

IT-strategi[39]

Det skal undersøges, om

- Der er udarbejdet en strategisk IT-plan, som omfatter relevante IT-initiativer
- Der er overensstemmelse mellem IT-strategi og forretningsstrategi
- Ledelsen er involveret i udarbejdelsen af virksomhedens IT-strategi
- Der er identificeret muligheder og begrænsninger i informationssystemet
- Der er planlagt væsentlige ændringer i informationssystemet
- Virksomhedens anvendelsesniveau af IT er vurderet

Kontrolmiljø[40]

Ved forespørgsel til den ansvarlige for IT-funktionerne afdækkes følgende:

- Udarbejdelse og vedligeholdelse af stillings- og funktionsbeskrivelser
- Efterprøvning af ansøgers kvalifikationer, såsom identitet, eksamensbevis, CV, straffeattest
- Ledelsens bekendtgørelse og kommunikation af virksomhedens sikkerhedspolitik
- Udformningen af ansættelseskontrakt med fokus på tavshedspligt, ansvar, krav til sikkerhed, mv.
- Uddannelse og opretholdelse af medarbejdernes kompetencer
- Procedurer ved ansættelsesophør såsom blokering for adgangsrettigheder, tilbagelevering af udstyr, overdragelse af ansvarsområder, information om tavshedspligt, mv.

Virksomhedens risikovurderingsproces[41]

Det undersøges, om

- Der findes en strategi der effektivt identificerer og klassificerer trusler
- Hvem har ansvaret for at identificere trusler
- Hvorvidt informeres ledelsen om identificerede trusler

Der udarbejdes en vurdering af, hvorvidt virksomhedens samlede risikovurderingsproces er effektiv.

Kontrolaktiviteter

Fysisk sikkerhed[42]

- Er der udarbejdet procedurer for den fysiske sikkerhed?
- Hvem har adgang til serverrummet?

[39] CobiT afsnit PO samt DS 484, kapitel 5
[40] DS 484, kapitel 8
[41] DS 484, anneks B
[42] DS 484 kapitel 9

- Hvorledes er adgangskontrollen til serverrummet – skal der anvendes nøgle, adgangskort og kode?
- Foretages der en adgangslogning med dato og tidspunkt?
- Hvilken beskyttelse med eksterne trusler findes der – er der den fornødne temperaturstyring, brandsikring, mv.?

Drift af netværk[43]

- Er der udarbejdet en Service Level Agreement[44], såfremt der benyttes eksterne leverandører og er der sammenhæng mellem denne og virksomhedens forretningsstrategi?
- Findes der kontroller, som løbende overvåger og evaluerer ydelse og kapacitet i systemet, der derved sikrer, at kravene i Service Level Agreement overholdes?
- Forefindes der backupprocedurer, herunder plan for backuphyppighed, opbevaring af backup (internt og/eller eksternt), reetablering af backup mv.?
- Kontrol af retningslinier for netværkssikkerhed, samt sikkerhedsforanstaltninger mod uautoriseret adgang
- Er der etableret funktionsadskillelse mellem udvikling, test og drift?
- Procedurer for destruktion og bortskaffelse af datamedier, som ikke længere anvendes
- Kontrol af antivirusprogrammer, herunder at der løbende foretages opdateringer
- Hvilke procedurer er der for sikkerhedslogning – krav om indhold, hyppighed, adgangskontrol af loggen?
- Er der etableret procedurer for rapportering og håndtering af sikkerhedshændelser og brud?

Adgangsstyring

- Kontrollerede, dokumenterede og opdaterede retningslinier for adgangsstyring
- Sikrer dokumentation for alle brugere og deres tilknyttede rettigheder
- Gennemgå procedurer for håndtering af nye, ændrede og ophørte brugere
- Er administratorer kun tildelt de fornødne rettigheder?
- Identificere eksterne netværksadgange og vurdere de firewalls, der sikrer dem
- Dokumentere procedurer for adgangskoder, herunder krav til udformning og længde, ændringskrav, praksis vedrørende nedskrivning af koder, auto log-off, begrænsning i antal forkerte forsøg, kode skjules ved log-in.

Anskaffelse af software

- Kontrollere, om der forefindes procedurer for anskaffelse af systemsoftware
- Hvilke medarbejdere er involveret i anskaffelsen af systemsoftware?
- Hvilke strategier er der for test og evaluering af nyt software?
- Foreligger der en vurdering af trusler mod det nye software
- Er der anskaffet nye systemer i forbindelse med rådgivningen?

[43] CobiT afsnit DS samt DS 484, kapitel 10
[44] CobiT 4.1, side 102, pkt. DS 1.3 samt IT-revision, kapitel 16, side 285

Ændring, udvikling og vedligeholdelse [45]

- Gennemgå procedurer for ændring, udvikling og vedligeholdelse af systemsoftware
- Hvilke medarbejdere er involveret i ændring, udvikling og vedligeholdelse af systemsoftware?
- Hvilke retningslinier er der for test og evaluering af ændrede eller nye systemer?
- Findes der et kontrolspor for alle ændringer?
- Føres der en log med beskrivelse af alle ændringer af driftsmiljøet?
- Foretages der verificering af, at systemet anvender senest opdaterede tilgængelige version?
- Foreligger der en vurdering af trusler mod det udviklede/ændrede software?

Beredskabsplan[46]

- Foreligger der en beredskabsplan?
- Er der sikret en fysisk udgave af beredskabsplanen?
- Bliver beredskabsplanen løbende vedligeholdt?

[45] DS 484, kapitel 12
[46] DS 484, kapitel 14