ITIL in small and medium sized enterprises
- From a security perspective

Emelie Hedin
HT 2014
Tommy Wedlund

IT och projekt/Systemvetenskapliga programmet
Institutionen för ekonomisk och industriell utveckling
Sammanfattning

I detta arbete uppmärksammas problematiken kring SME i relation till ITIL utifrån ett säkerhetsperspektiv. Arbetet baseras på två fallstudier där en av dessa två är mer djupgående och därmed behandlas som huvudsaklig. Dessa två fallstudier analyseras sedan utifrån en teoretisk grund baserad på litterära, vetenskapliga och muntliga källor som bearbetats utifrån studiens två övergripande frågeställningar: Vilka är de avgörande faktorer som påverkar organisationen under en ITIL implementation och vilka skillnader finns det mellan större och mindre organisationer i relation till säkerhet?

Studiens huvudsakliga slutsatser är att det går att de övergripande faktorer som påverkar en implementation är relaterade till hur organisationen hanterar den organisatoriska förändring som sker i samband med implementationen samt hur de förhåller sig till ITIL innan implementationen. Vidare finner studien att det går att ifrågasätta om storleken på organisationen verkligen är en avgörande faktor i relation till arbetet med säkerhet och att det mer handlar om de kulturella skillnaderna mellan större organisationer och SME.

Abstract

This work addressed the problem of SMEs in relation to ITIL from a safety perspective. The work is based on two case studies in which one of these two is more profound and thus treated as principal. These two case studies are analyzed from a theoretical foundation based on literary, scientific and oral sources that are processed on the basis of the study's two overarching questions: What are the crucial factors affecting the organization during an ITIL implementation and what are the differences between large and small organizations in relation to security?

The study's main conclusions is that it is possible that the overall factors affecting the implementation are related to how the organization handles the organizational change that occurs in the context of implementation, and how they relate to ITIL before implementation. Further, the study finds that it is possible to question whether the size of the organization is really a critical factor in relation to the work on security and that it is more about the cultural differences between large organizations and SMEs.
Förord

Denna uppsats symboliserar slutet för mina studier på Systemvetenskapliga programmet vid Linköpings Universitet och även det arv som jag ämnar att lämna efter min tid som student.

Jag vill rikta ett stort tack till alla organisationer och respondenter som deltagit i framställningen av detta arbete och jag hoppas att detta arbete ska vara till hjälp för er och andra organisationer i ert fortsatta arbete. Ett speciellt tack vill jag även rikta till Mats Skröder vars synpunkter och kommentarer har varit till stor hjälp under framställningen av detta arbete. Din input och kunskap har varit ovärderlig för studiens utfall.

Vidare vill jag även tacka mina kollegor på Företag 1 för att jag fick möjligheten att studera er verksamhet och använda i mitt arbete.

Avslutningsvis så vill jag även tacka min handledare Tommy Wedlund för den vägledning som jag har fått under själva skrivprocessen. Jag känner att de konstruktiva kommentarer och den feedback som jag mottagit har hjälpt att höja detta arbete. Ett tack riktas även till alla som har hjälpt till att korrekturläsa och kommit med konstruktiv kritik i syfte att höja arbetets kvalité.

Linköping, Maj 2014

Emelie Hedin
## Innehåll

<table>
<thead>
<tr>
<th>Kapitel</th>
<th>Tema</th>
<th>Sidnummer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduktion ...............................................................................</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>1.1 Syfte och frågeställning ................................................</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>1.2 Målgrupp ............................................................................</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>1.3 Antagningar och avgränsningar ..........................................</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>1.4 Tidigare forskning ................................................................</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>1.5 Disposition ........................................................................</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>1.6 Språk- och referenshantering ............................................</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>Metod .......................................................................................</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>2.1 Förförståelse .....................................................................</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>2.2 Metodval ............................................................................</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>2.3 Genomförande ......................................................................</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>2.4 Intervjuer ..........................................................................</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>2.4.1 Intervjuernas genomförande ..........................................</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>2.5 Litterära källor ..................................................................</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>2.3 Trovärdighet .......................................................................</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>2.7 Metodkritik ........................................................................</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>Teoretisk referensram ................................................................</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>3.1 Small and medium sized Enterprises ...................................</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>3.1.1 IT Service Management ..................................................</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>3.2 ITIL ....................................................................................</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>3.1.2 Service Strategy ...........................................................</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>3.2.2 Service Design ..............................................................</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>3.2.3 Service Transition ..........................................................</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>3.2.4 Service Operation ...........................................................</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>3.2.5 Continual Service Improvement .......................................</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>3.2.6 Riskerna med att implementera ITIL ...................................</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>3.2.7 Organisatorisk förändring ..............................................</td>
<td>36</td>
</tr>
<tr>
<td>3.3</td>
<td>Säkerhet ...................................................................................</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>3.3.1 Hackare ..........................................................................</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>3.3.2 Social engineering ..........................................................</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>3.3.3 Hot ..................................................................................</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>3.3.4 Säkerhetsarbete i små och medelstora företag ....................</td>
<td>46</td>
</tr>
</tbody>
</table>
4 Empiri ......................................................................................................................................... 49
  4.1 Företag 1 ................................................................................................................................ 49
    4.1.1 Företagets uppbyggnad ................................................................................................. 49
    4.1.2 Implementationen av ITIL ............................................................................................. 51
  4.2 Företag 2 ................................................................................................................................ 53
5 Analys ........................................................................................................................................ 56
  5.1 Frågeställning ......................................................................................................................... 56
  5.2 ITIL ......................................................................................................................................... 56
  5.3 Säkerhet .................................................................................................................................. 59
6 Slutsatser och kunskapsbidrag .................................................................................................... 63
7.1 Reflektion ................................................................................................................................. 66
  7.2 Kritik ....................................................................................................................................... 67
  7.3 Vidare forskning ...................................................................................................................... 67
Referenser ...................................................................................................................................... 69
Bilaga 1 – Exempel på mall inför intervju .................................................................................... 74
Bilaga 2 – Exempel på transkriberat material .............................................................................. 75
Figurer:

Figur 1.1: Översiktsbild av arbetets disposition ............................................................... 7
Figur 3.2: ITIL livscykeln, Service Strategy Källa: Cartlidge et al, 2007 ................................. 24
Figur 3.3: ITIL livscykeln, Service Design Källa: Cartlidge et al, 2007 ................................. 26
Figur 3.4: ITIL livscykeln, Service Transition Källa: Cartlidge et al, 2007 ............................. 28
Figur 3.5: ITIL livscykeln, Service Operation Källa: Cartlidge et al, 2007 ............................. 30
Figur 3.7: ITIL livscykeln, Continual Service Improvement Källa: Cartlidge et al, 2007 ............ 32
Figur 3.8: Fri tolkning av Demings PDCA-cykel Källa: Tonnqvist, 2008 ................................. 33
Figur 3.9: Illustration av sambandet mellan organisation och verksamhet ............................. 37
Figur 4.1: Modell av Företag 1:s uppbyggnad. Fritt tolkad från intervjuer med Respondent 5,6 och 7. ................................................................................................................................. 50

Tabeller:

Tabell 2.1: Tabell över respondenter som använts som referenser ........................................ 13
Tabell 2.2: Tabell över respondenter relaterade till fallstudierna ............................................. 14
1. Inledning

I detta inledningskapitel så kommer utgångspunkterna för arbetet att konkretiseras i syfte att på ett tidigt stadium ge läsare insikt i bakomliggande fenomen och problemområden samt ge en förståelse för det syfte som avses med studien. Förutom detta presenteras i detta kapitel även den frågeställning som ligger till grund för arbetet och som kommer besvaras i slutsats-kapitlet.
1 Introduktion


Ett av de ramverk som är mycket populära på marknaden idag är ramverket Information Technology Infrastructure Library, ITIL, som i dagsläget har utkommit i tre olika versioner (APM Group et al, 2013). En implementation av ITIL innebär likt många andra implementationsprojekt exempel på orsaker till organisatorisk förändring, vilket likt alla andra förändringar medför både positiva och negativa aspekter. Hur stor den organisatoriska förändringen blir beror, som i de flesta andra förändringsprojekt, till väldigt stor del på i vilken omfattning man väljer att implementera ITIL (Office of Government Commerce, 2009) samt hur själva implementeringen genomförs.


När organisationen genomgår en organisatorisk förändring, till exempel i form av en ITIL implementation, så uppkommer som vid många andra förändringar en vissa säkerhetsrelaterade risker. En organisatorisk förändring kan alltså innebära en ökad risk för till exempel felhantering av information och systempenetrering i och med ovana hos användaren. Jag har sedan några år tillbaka utvecklat ett stort intresse för IT-säkerhet och behandling av information då jag läste flertalet kurser inom området och är därmed medveten om dessa risker som finns vid en organisatorisk förändring. Inom området IT-säkerhet har jag studerat både hackare, kryptering och kriminalteknik samt andra aspekter relaterade till ämnet och behandling av information.

IT-säkerhet och säker behandling av information är ett konstant aktuellt och mycket viktigt ämne inom de flesta organisationer. Anledningarna kan variera mellan allt ifrån nyutvecklade varor eller tjänster till kundinformation och företagshemligheter. IT-säkerhet är även ett ämne som trots sin stora betydelse för organisationen ofta blir ignorerad och inom många organisationer är underprioriterade, framförallt inom SME där de finansiella tillgångarna kan vara begränsade.
I detta arbete så kommer IT-säkerhetsperspektivet sättas i kontexten av de organisatoriska förändringar kopplade till en ITIL-implementation samt till det kontinuerliga ITIL arbetet som sker inom organisationen efter implementationen.

Trots den ökande efterfrågan på information inom ämnet ITIL och speciellt inom området för implementationer inom mindre verksamheter, så är utbudet av information inte i närheten av tillfredsställande. Många delar av ITIL ramverket är stora och alltför resurskrävande för att mindre organisationer till fullo ska kunna utnyttja de fördelar som finns med ITIL (Office of Government Commerce, 2009). Om implementationen blir för omfattande för organisationen så kan ramverket istället för att effektivisera organisationen tyngta ner den och ramverket blir då mer av en börda än ett verktyg (ibid).

1.1 Syfte och frågeställning

Syftet med detta arbete är bidra till ökad dokumentation och vidare utforska ITIL som ramverk utifrån ett IT-säkerhetsperspektiv gällande både själva implementationen och det fortsatta arbetet med ramverket i relation till mindre organisationer eller SME som de även kallas. Arbetet ämnar även uppmärksamma framförallt mindre organisationer på riskerna gällande felhanteringen av information. För att uppnå detta kommer arbetet cirkulerar runt följande två frågeställningar:

- Vilka är de avgörande faktorer som påverkar organisationen under en ITIL implementation?
  - Vad gör att en implementation avbryts eller att utfallet inte blir som önskat?
  - Vilka säkerhetsrisker finns under själva implementationen och är dessa iså fall relaterade till implementationen eller den organisatoriska förändringen?
- Vilka skillnader finns det mellan större och mindre organisationer i relation till säkerhet?
  - Vilka åtgärder kan vara aktuella för en mindre organisation?
  - Vem har enligt ITIL ansvaret för att ta itu med respektive hot?

Den första frågeställning avser att blotta de hinder som organisationen möter under själva implementationen och som kan resultera i att projektet avbryts eller att utfallet av projektet inte blir som önskat. Den andra frågeställningen avser att synliggöra de hot som de flesta organisationer möter under och efter en implementation i relation till säkerheten för organisationens information och tjänster samt hur de hanteras.
1.2 Målgrupp
Detta arbete riktar sig främst till mindre företag och organisationer som planerar att implementera eller redan har implementerat ITIL moduler i sin organisation. Arbetet ämnar även vara utav värde för studerande eller andra intressenter inom områdena förvaltning och utveckling av tjänster, organisatorisk förändring och IT-säkerhet inom mindre företag och organisationer. Det är även min förhoppning och ambition att detta arbete ska vara användbart för mindre organisationer både inom den offentliga och privata sektorn samt att applicerbarheten av arbetet är giltig inom fler marknader än de som studieobjekten är aktiva inom.

1.3 Antagningar och avgränsningar
Arbetet utgår ifrån ett antal antaganden i syfte att begränsa arbetets omfattning samt för att bibehålla en röd tråd genom arbetet. Jag förutsätter i detta arbete att en fullständig implementation av ITIL är omöjlig i en mindre organisation då den skulle tynga ner effektiviteten hos företaget. En fullständig implementation av samtliga ITIL-processer är även väldigt sällsynta och anses generellt som mer eller mindre ineffektiv oavsett storlek på organisationen i fråga.

Med tanke på den avsedda målgruppen så har jag även gjort antagandet att kunskapsnivån inom området kan variera noterbart och jag har därför dedikerat speciell uppmärksamhet åt att förklara svåra och branschrelaterade termer. Det är därför min förhoppning att man som läsare oavsett tidigare kunskapsnivå eller bakgrund ska finna arbetet givande och informativt.

Anledningen till att jag har valt att avgränsa arbetet till ITIL version 3 är inte bara för att det är den senaste versionen och att den i och med detta är den versionen som ett företag troligtvis skulle välja att implementera utan även för att det är det som de flesta andra forskare och utvecklare av ramverket utgår ifrån. Jag känner därför att det vore felaktigt att basera mina slutsatser på processer som andra redan förbättrat. Avgränsningarna gällande processer inom ramverket syftar till att bibehålla fokus och hålla arbetets omfattning till en begränsad volym utan att äventyra arbetets trovärdighet.

Anledningen till avgränsningarna i kapitlet om organisatorisk förändring syftar till att behålla fokus i arbetet samt att avgränsa arbetets omfattning. Det finns nämligen en mycket stor mängd metoder för organisatorisk förändring och jag har därför valt att avgränsa mig till ett fåtal av dessa.

Gällande IT-säkerhetskapiptlet så är anledningarna till avgränsningarna de samma som i de övriga kapitlens fall. Att redogöra djupgående för samtliga delar av detta väldigt stora och omfattande område skulle endast leda till otydlighet gällande den teoretiska grunden. Detta specifika kapitel inom ITI-säkerhet är även avgränsat till perspektivet av en icke auktoriserad entitet, till exempel en hackare. Detta då detta arbete syftar till att förbättra och uppmärksamma främst mindre organisationer på riskerna gällande hantering av information.

1.4 Tidigare forskning
Inom de individuella områdena ITIL, organisatorisk förändring och IT-säkerhet finns det en tillfredställande mängd information i forma av litteratur och vetenskapliga artiklar. Även inom det något begränsade området för small and medium sized enterprises så har det bedrivits en hel del forskning inom samtliga områden som publicerats i olika litterära källor och artiklar. Forskningen inom det specifika området där samtliga av dessa tre områden överlappar varandra är dock minst sagt begränsat.

Litteraturen som finns inom ämnet ITIL är mycket omfattande och stora mängder av den litteratur som finns produceras av non-profit organisationer inom ämnet IT Management (AXELOS, 2003). I detta kommer detta vidare diskuteras i den teoretiska referensramen i det avsnitt som behandlar ITIL. Forskningen inom ITIL-området gällande implementationer i mindre organisationer är däremot mer begränsad. Det är detta område som detta arbete hoppas kunna vidare utforska samt bidra till ny kunskap. IT-säkerhet är ett mycket brett område och det finns i och med detta väldigt mycket information om allt ifrån krypteringar och olika hot till människorna bakom dessa (Stallings & Brown, 2008).
1.5 Disposition

Arbetet består av sju delar: Introduktion, Metod, Teoretisk referensram, Empiri, Analys, Slutsats och Referenser. Samtliga av dessa kapitel inleds med en kortare presentation av innehållet samt i de fall där det är jag har ansett det nödvändigt så finns även en kortare förklaring av centrala begrepp. Dessa begrepp är begrepp som läsaren bör inneha en viss uppfattning om för att på ett bra sätt kunna ta till sig texten i det aktuella kapitlet. Det är inte ovanligt att dessa begrepp återkommer i efterföljande kapitel och i dessa fall förutsätts att läsaren genom i det tidigare kapitlet har givits tillräcklig information om begreppet för att ta till sig informationen även i efterföljande kapitel.

Det inledande kapitlet av arbetet, Inledningen, avser att introducera läsaren för arbetets syfte och upplägg. I detta kapitel presenteras även de antaganden, avgränsningar och bakgrund som arbetet och dess teori vilar på, detta då syftet är att ta läsaren från det breda forskningsområdet till arbetets specifika problemområde som resulterar i arbetets forskningsfrågor.

I metodkapitalet beskrivs hur arbetet med studien har genomförts samt den kritik som finns mot dessa metodiker.

![Diagram](image.png)

Figur 1.1: Översiktsbild av arbetets disposition
Efter metod kapitlet presenteras den teori som kommer att användas i arbetet. Detta kapitel syftar till att ge läsaren den teoretiska grund som behövs för att tillsammans med de empiriska data som insamlats från fallstudierna undersöka de för studien aktuella fenomen i analysekapitlet. Detta illustreras i Figur 1.1 ovan. Studien avslutas med ett slutsatskapitel där slutsatser av analysen, detta kapitel följs av en reflektion där arbetet som helhet analyseras utifrån mitt eget perspektiv. Anledningen till att detta kapitel inte är med i figuren ovan är för att den, tillika referensavsnittet, inte direkt behandlar studien.

1.6 Språk- och referenshantering

Jag har valt att i detta arbete hantera referenser med hjälp av Harvardsystemet, detta innebär att referenser till källor i texten har gjorts med parenteser i direkt anslutning till det avsnitt som källan används i (Språkrådet, 2008). När citat från källor återges i texten så görs detta i de flesta fall på originalspråket för att möjliggöra egna tolkningar av läsaren, dessa följs alltid av min egen tolkning av citatet som genomgående är på svenska. Jag har valt att ange sidnummer för avsnitt innehållande direkta citat, detta i hopp om att stärka arbetets trovärdighet genom att underlättta för en kritisk granskning av arbetet. I de fall då jag sammanhängande har använt mig av samma källa vid fler än ett tillfälle så använder ibidem (ibid) referenser efter den initiala deklarationen av källan, detta i enlighet med allmänna skrivregler.

I och med att ett flertal citat av de citat som återges på originalspråket är på engelska så förutsätts att läsaren har grundläggande kunskaper i språket. Samtliga citat efterföljs av min egen tolkning av citatet som är på svenska, vilket nämns tidigare, men bristande kunskaper i grundläggande engelska hindrar produktionen av nya tolkningar och infallsvinklar av citatets innebörd.

2. Metod

Detta kapitel avser att behandla den metodik som har använts under arbetets genomförande. I kapitlet inleds med ett kortare avsnitt gällande min förförståelse i ämnet samt en kortare motivering av metodval presenteras. Förutom arbetets metodik presenteras även de respondenter som används både som teoretiska och empiriska källor i arbetet. Detta kapitel avslutas med en kritisk analys av arbetets övergripande metodik samt insamlingen och urvalet av både teoretiskt och empiriskt material.
2 Metod

2.1 Förförståelse

Mitt val av inriktning, projektledning, påverkar även det mitt förhållningssätt till texten och den information som texten baseras på. I och med min inriktning så har jag haft chansen att arbeta både teoretiskt men även praktiskt kring de ämnen som är av intresse för arbetet. Det bör dock poängteras att merparten av den förståelse jag har i de aktuella ämnena är av teoretisk natur. Eftersom att jag har valt att arbeta ensam med detta arbete så innebär detta att jag under detta arbete inte har utgått från annan förståelse än min egen. För att förhindra att inflytandet av min personliga förståelse inom respektive ämne skall ”färga” texten i arbetet i alltför stor utsträckning så har jag tagit hjälp av extern hjälp som saknar de förkunskaper som jag har inom respektive ämne.

2.2 Metodval
En del data i arbetet stöds och tydliggörs av statistisk information insamlad från Statistiska Centralbyrån främst i syfte att poängtera viken av fenomen som är relevanta för studien och som i vissa fall utgör en bas för hypoteser och slutsatser.

2.3 Genomförande
I arbetet kommer två mindre företag som implementerat presenteras, granskas och analyseras utifrån ett IT-säkerhetsperspektiv i syfte att avslöja fakta relevant för frågeställningen. Det första företaget är ett tillverkande företag inom området för hematologi, läran om blodet samt dess uppbyggnad och relaterade sjukdomar (Hematologi, Nationalencyklopedin). Det andra företaget var ett konsultföretag specialiserade på implementationer av blandat annat ITIL. Båda av dessa företag har sin bas i Stockholm och faller inom ramarna för den europeiska definitionen av SME, som beskrivs i arbetets teoriavsnitt.


2.4 Intervjuer

Tabell 2.1: Tabell över respondenter som använts som referenser.

<table>
<thead>
<tr>
<th>Respondent</th>
<th>Befattning / Bakgrund</th>
<th>Studierelevant ämne</th>
<th>Kommunikationsmedel vid intervju</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jobbar som konsult på konsultföretaget Xpeedio i Stockholm.</td>
<td>ITIL</td>
<td>E-post</td>
</tr>
<tr>
<td>2</td>
<td>Forskare i ämnet informatik på Linköpings Universitet och jobbar för närvarande som konsult på PÅ AB i Stockholm.</td>
<td>Organisatorisk förändring</td>
<td>Personlig kontakt</td>
</tr>
<tr>
<td>3</td>
<td>Forskare vid Kungliga Tekniska högskolan i Stockholm och som under ett antal år varit aktiv inom området IT-säkerhet.</td>
<td>IT-säkerhet</td>
<td>Personlig kontakt / Föreläsning</td>
</tr>
<tr>
<td>4</td>
<td>Arbetar på BiTa Service Management</td>
<td>ITIL</td>
<td>Personlig kontakt</td>
</tr>
</tbody>
</table>

Samtliga uttalanden av respondenterna som använts i arbetet har kontrollerats med andra källor som till exempel litteratur och vetenskapliga artiklar för att minska risken för eventuella bakomliggande agendor hos respondenterna.

Inom de undersökta organisationerna har jag även genomfört en del intervjuer. Inom Företag 1 genomfördes ett flertal intervjuer med tre olika respondenter samt kortare informella samtal med ett antal andra anställda från olika avdelningar på företaget. De tre mer djupgående intervjuerna genomfördes med två anställda som jobbar i företagets helpdesk samt med en av IT-cheferna. Intervjuer med dessa respondenter genomfördes vid flera olika tillfällen i tre olika konstellationer, i grupp, i par och enskilt. I Företag 2 (konsultföretaget) genomfördes en intervju med företagets VD och var inte därmed inte lika djupgående som i Företag 1. Samtliga respondenters relaterade till fallstudierna redovisas i Tabell 2.2.
**Tabell 2.2: Tabell över respondenter relaterade till fallstudierna**

<table>
<thead>
<tr>
<th>Respondent</th>
<th>Företag</th>
<th>Befattning</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Företag 1</td>
<td>IT-chef</td>
</tr>
<tr>
<td>6</td>
<td>Företag 1</td>
<td>Arbetare i Helpdesk</td>
</tr>
<tr>
<td>7</td>
<td>Företag 1</td>
<td>Arbetare i Helpdesk</td>
</tr>
<tr>
<td>8</td>
<td>Företag 2</td>
<td>VD</td>
</tr>
</tbody>
</table>

2.4.1 Intervjuernas genomförande

Samtliga intervjuer som genomförts personligen med respondenter har transkriberats inom en period av 24 timmar efter intervjun. Detta då två av de teoretiskt relaterade intervjuerna samt samtliga empiriskt relaterade intervjuer, med undantag för en, blev inte inspelade utan utgår ifrån anteckningar tagna under intervjun och det var därmed kritiskt att transkriberingen skedde inom en rimlig tidsram.

Anledningen till detta var att de tekniska möjligheterna för en inspelning inte fanns att tillgå vid intervju-tillfället. Dessa två intervjuer transkriberades på grund av detta inom en accelererad tidsram av 2 timmar för att kunna på ett korrekt sätt återge information.

Samtligt färdigställt transkriberat material, oavsett inom vilken tidsram, har sammanställts efter en mall där respondentens namn och namnet på den organisation som personen representerar har använts som huvudrubrik. Vidare har de frågor som respondenten svarat på används som underrubriker, under dessa har respondentens svar skrivits ut. I marginalen på samtliga transkriberingar presenteras namnet på den som höll i intervjun, som i samtliga fall var jag, samt datum för intervjun. Ett exempel på denna mall finns i **Bilaga 1**, som innehåller det transkriberade materialet från intervjun med Respondent 1 från konsultföretaget Xpeedio.
2.5 Litterära källor

Den litteratur som har använts i arbetet har begränsats till litteratur som anes trovärdig. Användandet av källor som inte är märkta med ITIL-symbolen har i ITIL-kapitlet till exempel hållits till det minimala och i de fall som detta har inträffat så har jag använt mig av andra källor för att stödja den litterära källans påståenden. När det gäller den litteratur som innehar denna ITIL-symbol så har huvudsyftet med dessa fakta som använts legat på hur ramverket och dess processer är uppbyggt, vilket är vad jag vill kalla konkret fakta, detta genererar i sin tur en viss trovärdighet till litteraturen. När det gäller mer ”abstrakt” fakta som till exempel huruvida ramverket är effektivt eller vilken effekt det har i olika organisationer kan i ”ITIL-märkt” litteratur vara färgad. Av denna anledning så har jag funnit det nödvändigt att backa upp fakta med andra icke-märkta källor även om dessa inte alltid tagits med i arbetet. Inom de övriga två kapitlen så har jag baserat de litterära källornas trovärdighet på samma sätt som i de fall där ITIL-symbolen saknats på källan. Källorna har alltså stötts av andra oberoende källor och i samtliga fall har författaren eller författarna till den litterära källan gränsats för att avgöra källans trovärdighet. Detta har även varit en av de avgörande faktorerna då en eller flera källor presenterat motstridande fakta tillsammans med bland annat källornas ålder, ursprung och eventuellt i övrigt vinklade innehåll.

2.3 Trovärdighet


Arbetets validitet handlar om studiens slutsatser hänger ihop eller inte (Bryman, 2011). Validitet kan delas in i tre olika grupper som fokuserar på olika delar där ett av dessa är mätningsvaliditet, även kallat begreppsväiditet, där man tittar på om de begrepp som används avspeglar det som begreppet avser. Ett annat exempel på validitet är intern validitet där fokus ligger på de eventuella kausala förhållanden som presenteras i slutsatsen (Bryman, 2011). En tredje variant av validitet är extern validitet där fokus ligger på huruvida resultaten från den enskilda studien är generaliserbara och om detta ens är möjligt.

2.7 Metodkritik

Man skulle kunna argumentera att generaliserbarheten i detta arbete kan ifrågasättas då de två fallstudierna inte har varit lika djupgående. Fallstudier rymmer dock enligt Bryman (2011) i grundläggande form endast ett djupgående och detaljerat stadium av ett enstaka fall. En lika djupgående analys av ett studieobjekt vars syfte är att stärka eller förkasta generaliseringen av de slutsatser som dras av det primära studieobjektet anses därför inte nödvändigt. Organisationernas skilda uppbyggnad öppnar upp för kritik gällande om fallstudierna kan anses jämförbara eller ej. Min syn på detta är att organisationens uppbyggnad ligger utanför arbetets intresseområde då arbetet syftar till att skapa en mer generell bild av situationen för SME som grupp, oavsett om organisationen livnär sig på produktion eller tjänster.

Man kan även argumentera att de resultat som framkommit vid intervjuer med företagen inte är likvärdiga då de i den primära fallstudien var lite mer omfattande och djupgående än de i den sekundära fallstudien. Intervjuerna i den primära fallstudien genomfördes även i olika konstellationer vilket inte gjordes i fallet med den sekundära där intervjun genomfördes enskilt. Detta beror på att det primärt är det primära studieobjektet som analyseras i detta arbete.

Gällande de fyra teoretiskt relaterade respondenterna kan man argumentera, främst gällande de två första relaterade till ITIL och organisatorisk förändring, att dessa respondenter kan ha haft bakomliggande agendor med sina uttalanden.

Risken för detta har minimerats genom användandet av samma metod som använts för de litterära källorna, det vill säga att samtlig data som använts i arbetet är verifierad hos minst två andra oberoende källor för att i största möjlig utsträckning minimera att arbetet kontamineras av bakomliggande agendor. Detta gäller självlklart även de uttalanden som gjorts av studieobjekten i den mån detta har varit möjligt, kompletterande källor har då bestått av företagens egen dokumentation och liknande. När det gäller Respondent 1, så kan kritik kring valet av metodik uppkomma då denna intervjuform gör det svårt att till exempel ställa följdfrågor. Jag anser ändå att genomförandet intervjun via detta medie är rättfärdigat då situationen inte tillåt personlig kontakt som initialt var avsett på grund av schemakollisioner. Vidare klargjorde respondenten att möjligheten för vidare utfrågning via mail var möjlig vid eventuella oklarheter.
3. Teoretisk referensram

I detta avsnitt presenteras den teori som i analyskapitlet kommer appliceras på det empiriska data som samlats in under fallstudierna.

3 Teoretisk referensram

3.1 Small and medium sized Enterprises


Inom kategorin SME definieras tre olika typer av Europeiska Unionen: micro, small och medium, vilket illustreras i Tabell 3.1. För att ett företag ska kvalificera sig som ett SME av typen micro krävs det att företaget inte har mer än 10 anställda och årligen inte omsätter eller innehar en balansräkning på mer än 2 miljoner euro, motsvarande cirka 17 924 400 svenska kronor1 (Europakommissionen, 2012).

**Tabell 3.1:** Tolkad översikt av gränsvärden för typer av företag inom kategorin SME i enlighet med Europeiska Unionen. **Källa:** Europakommissionen. 2012.

<table>
<thead>
<tr>
<th>Företagskategori</th>
<th>Anställda</th>
<th>Omsättning</th>
<th>Balansräkning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro</td>
<td>≤ 10</td>
<td>€ 2 m</td>
<td>€ 2 m</td>
</tr>
<tr>
<td>Small</td>
<td>≤ 50</td>
<td>€ 10 m</td>
<td>€ 10 m</td>
</tr>
<tr>
<td>Medium</td>
<td>≤ 250</td>
<td>€ 50 m</td>
<td>€ 45 m</td>
</tr>
</tbody>
</table>

Ett företag tillhörande typen small i kategorin SME karaktäriseras av att det innehar ett maximalt antal av 50 anställda i kombination med en årlig omsättning eller balansräkning som inte överstiger 10 miljoner euro, det vill säga ca 89 622 000 svenska kronor.

---

1 Samtliga konverteringar är gjorda enligt valutakursen för 2014-04-09
Gränsvärdena för den sista SME typen medium ligger på ett maxantal av 250 anställda och en omsättning på 50 miljoner euro, ca 448 110 000 svenska kronor alternativt en balansräkning på 45 miljoner euro, ungefär motsvarande 403 299 000 svenska kronor.

Olika länder och unioner har olika kriterier och system för att definiera SME, vilket gör att ovanstående siffror endast ärapplicerbara för medlemsländerna inom Europeiska Unionen. Detta gör det möjligt för företag att definieras som SME utanför Europeiska Unionen även om företaget har över 250 anställda eller en omsättning på över 50 miljoner euro alternativt en balansräkning som överstiger 45 miljoner euro. USA är ett av de länder där gränsvärdena för SME är mer generösa än inom den Europeiska Unionen. Förutom de mer generösa gränsvärdena så skiljer sig även det amerikanska systemet sig markant från det europeiska då man i det amerikanska systemet är industribaserat och även tar hänsyn till ägarstrukturen och avkastning vid sidan av antalet anställda, som kan uppgå till 1500 personer (U.S. Small Business Administration, 2011).


Respondent 4 menar att stora företag ofta är omogna och gammalmodiga när det gäller att arbeta med processer till skillnad från mindre organisationer som ofta är yngre och mer moderna inom området. OGC menar i kontrast till Respondent 4 att den största skillnaden mellan SME och större företag inte ligger i antalet anställda eller i ekonomiska faktorer utan i den interna kulturen som finns inom företaget på en organisatorisk nivå (Office of Government Commerce, 2009).

2 Intervju med Respondent 4 BiTa Service Management 2013-09-03
De påstår att kulturen inom SME ofta är mer informell än på större företag och att detta är kopplat till att anställda på företag som faller inom ramen för SME arbetar mer nära varandra på grund av det begränsade antalet anställda samt på grund av mindre komplexa strukturer.

Detta resulterar i en mer informell atmosfär som resulterar i ett minskat fokus på formella processer än inom större företag med mer komplexa strukturer där dessa tilldelas ett större fokus (ibid). Det minskade fokusen på de formella processerna medför i sin tur ett ökat fokus på personliga åsikter, fördormar och attityder hos den enskilda individen, vilket kan innebära problem för till exempel Service Management.

3.1.1 IT Service Management

För att på ett korrekt sätt kunna identifiera vad IT Service Management är så måste vi inledningsvis definiera vad IT Service, IT tjänster, är för något. Termen tjänst definieras i den svenska Nationalencyklopedin som ”en kedja av händelser eller aktiviteter i vilken en kund interagerar med ett tjänsteföretags medarbetare (eller tekniska hjälpmedel i form av t.ex. bankautomater) i syfte att tillgodose vissa behov” (Tjänst, Nationalencyklopedin). En annan definition av detta som används av OGC som menar att en tjänst är ett medel att leverera ett värde till en kund genom att utan ägandeskap av specifika kostnader och risker underlättar utfall som av kunden anses önskvärda (Office of Government Commerce, 2009). Denna definition gör det möjligt för en tjänst att existera utan att en kund för tillfället ”upplever” den vilket inte är fallet i Nationalencyklopedins definition. Även om detta arbete kommer att utgå primärt ifrån den definition som erbjuds av the Office of Government Commerce så är det viktigt att uppmärksamma att det finns olika definitioner, speciellt då det är viktigt att förstå företagets definition av tjänster kan skilja sig från uppslagsverkens. Det som de flesta av alla definitioner, inklusive de ovanstående, har gemensamt är att det är utfallet och inte tjänsten i sig som har ett värde för kunden vilket i sin tur betyder att tjänstens värde ligger i hur väl tjänsten underlättar för ett önskat utfall (Cartlidge et al, 2007).

Syftet med IT Service Management är därmed att säkerställa att tjänsterna som företaget erbjuder i största möjliga utsträckning underlättar för kundens önskade utfall och förstå vilket värde som detta har för kunden. IT Service Management kan därmed beskrivas som en uppsättning av organisatoriskt specialiserade kunskaper med fokus på att producera ett värde för kunden genom användandet av tjänster (Cartlidge et al, 2007).
De organisatoriskt specialiserade kunskaperna förkroppsligas i samtliga processer, metoder och roller som används av Service Provider, som har till uppgift att leverera tjänsten (Cartlidge et al, 2007). IT Service Management har förutom ansvaret för att leverera en tjänst även ansvaret för att konstant förbättra och aktualisera dessa. Det är i arbetet med detta som förståelsen för kundens behov blir essentiella för IT Service Managements arbete. Detta arbete kan ofta underlättas med hjälp av ett ramverk som ITIL.

3.2 ITIL

ITIL, eller Information Technology Infrastructure Library, är ett ramverk som ständigt uppdateras av flertalet organisationer världen över men som ägs av AXELOS som är ett samriskföretag skapat mellan den brittiska staten i form av OGC och Capita plc, som är det största företaget inom Business process Outsourcing och professional services in Storbritannien (AXELOS, 2013). Många befarar att denna nya ägandeform kommer påverka framtida versioner av ITIL-ramverket även om de inte är de enda som arbetar med ramverket. Det kontinuerliga arbetet med uppdateringar och förbättringar av ramverket hanteras av ett flertal olika organisationer varav en del är non-profit organisationer som till exempel The itSMF, IT Service Management Forum. Denna organisation arbetar främst med att distribuera och publicera delar av den litteratur som ofta refereras till som “the Living Library” som är ett komplement till de fem publikationerna som utgör ramverkets livscykel och är anpassad efter olika industrier, operationsmodeller och tekniska arkitekturer (ibid).

Livscyklens som ITIL utgår ifrån består av de fem faserna Service Strategy, Service Design, Service Transition, Service Operation och Continual Service Improvement, som har till syfte att vidmakthålla, vidareutveckla och nyutveckla IT-tjänsterna som företaget erbjuder (Nordström & Welander, 2010).


3.1.2 Service Strategy


Inom samtliga steg i livscykeln så finns det olika roller där en del endast är aktiva inom det aktuella steget medan andra är aktiva över flera eller ibland samtliga steg i livscykeln. En roll definieras inom ramverket ITIL som en uppsättning med plikter, aktiviteter och auktoriteter som tilldelats en person eller ett team (AXELOS, 2011). De tre mest framträdande rollerna i detta steg av livscykeln är Business Relationship Manager, IT Steering Group och Service Owner.

Huvuduppgiften för en Business Relationship Manager är att upprätthålla goda relationer med en eller ett flertal kunder (AXELOS, 2012).
Processen Business Relationship Management som rollen Business Relationship Manager är aktiv inom
har till syfte att identifiera alla kunders behov samt säkerställa att dessa tillgodoses av de tjänster som
tillhandahålls. Processen Business Relationship Manager har starka kopplingar till en annan process,
Service Level Management och det är därför vanligt att man kombinerar dessa processer och gör dem till
en process, detta leder i dessa fall ofta även till att man väger att kombinera rollen Business Relationship
Manager med Service Level Manager (ibid). Syftet med processen Service Level Management är att
förhandla fram Service Level Agreements som är utförbara samt säkerställa att dessa efterlevs (Van Bon,
2012). Ett Service Level Agreement, eller SLA, är ett avtal mellan en Service Provider och en kund och
innehåller en tydlig definition av tjänstens natur, kvalité, det vill säga vilka behov som skall tillgodoses,
och omfattning. Vidare definieras även vilka skyldigheter som Service Provider respektive kunden har
gentemot varandra, detta innebär dock inte att det är ovanligt att ett SLA kan innefatta ett flertal
tjänster samt kunder (ibid). Vidare uppgifter som åläggs processen Service Level Management är att
övervaka och rapportera den nuvarande presentationen jämfört med de satta målen, upprätthålla en
kontakt med kund genom kontinuerliga genomgångar av tjänsten samt identifiera kontinuerliga
förbättringar (ibid). Det är genom likheterna mellan dessa två processer som man ofta väljer att
kombinera dem till en, vilket även innebär att man spar på de ofta viktiga resurserna.

En IT Steering Group har till uppgift att utveckla strategier för IT-tjänster och fastställa att de är i linje
med organisationens affärmässiga ambitioner och policies (APM Group et al, 2013). Andra namn för
denna instans är IT strategy group och IT steering committee (AXELOS, 2012). Med tanke på instansens
uppdrag och syfte så är det vanligt att personer som innehar högre positioner och roller inom affärsdelen
av företaget samt den del av företaget som förväntas leverera tjänsten inkluderas i denna grupp (ibid).
Linjeringen av de båda delarna kontrolleras genom kontinuerliga utvärderingar. Det ligger även på
instansens ansvar att prioritera olika utvecklingsprojekt och program relaterade till tjänster (Cartlidge et
al, 2007).

En Service Owner har till uppgift att bära ansvaret för ett eller flera tjänster. Denna roll skiljer sig något
ifrån de övriga då denna roll inte bara är relevant för Service Strategy utan för hela tjänstens livscykel. I
och med att Service Owner rollen har en så framträdande roll i arbetet med tjänsten och innehar
ansvaret för vad tjänsten skall leverera så finns det ofta ett nära samarbete mellan Service Owners och
Business Relationship Mangern (AXELOS, 2012).
Man kan säga att Business Relationship Managern och processen Business Management fungerar som en bro mellan Service Owners samt tjänsterna de är ansvariga för och kunden. Service Strategy steget avslutas med en färdig strategi för hur tjänsten skall utvecklas i nästa steg av livscykeln, Service Design.

3.2.2 Service Design
Cartlidge et al (2007, s 18) beskriver Service Design steget som ”The design of appropriate and innovative IT services, including their architecture, processes, policies and documentation, to meet current and future agreed business requirements”. Detta betyder att det huvudsakliga målet med steget Service Design är att möta de överenskommna utfallen som definierats i det föregående steget med kund genom skapa en design som simulerar dessa. Som en del i detta arbete är det även nödvändigt att identifiera och hantera de risker som finns med tjänstens utformning och understödande processer. Detta för att kunna designa tjänsten på ett sätt som genererar i optimal funktionalitet och med minimal risk. För att detta ska vara möjligt så är det viktigt att man designar en säker och motståndskraftig IT-infrastruktur, IT-miljö och applikationer för all data och andra informationsresurser (Cartlidge et al, 2007).

![ITIL livscykeln, Service Design Källa: Cartlidge et al, 2007](image)

Likt det föregående steget så finns det även i detta steg ett antal mer framträdande roller som är länkade till olika processer. En av dessa roller är Service Catalogue Manager som har till uppgift att se till att informationen i organisationens Service Catalogue är korrekt och hålls uppdaterad samt att informationen i denna är tillgängliga för auktoriserade instanser och entiteter (APM Group et al, 2013).
En Service Catalogue kan beskrivas som en databas alternativt ett strukturerat spreadsheet eller annat dokument där all information om tjänster som är tillgängliga för kunder samt de tjänster som stödjer dessa samlats, inklusive de som är klara för distribution (AXELOS, 2012).


3.2.3 Service Transition


![ITIL livscykeln, Service Transition Källa: Cartlidge et al, 2007](image)


De flesta av dessa processer påverkar tjänsten genom flera steg av tjänstens livscykel men en process som är specifik för Service Transition är Service Validation and Testing processen som, likt namnet indikerar, ansvarar för valideringen och testandet av nya och modifierade tjänster (ibid). Det är i denna process som tjänstens egenskaper testas och valideras mot de designspecifikationer som definieras i tidigare steg samt de behov som den avses möta. Steget Service Transition avslutas med att av tjänsten som skapats, testats och validerats tillsammans med de essentiella elementen som behövs för operera och stödja den levereras till kund och vidare in i Service Operation som är det efterkommande steget i tjänstens livscykel (Van Bon, 2012).
3.2.4 Service Operation


![ITIL livscykeln, Service Operation](image)

**Figur 3.5: ITIL livscykel, Service Operation** Källa: Cartlidge et al, 2007

En Incident har likt en förändring (Change) en egen livscykel inom tjänstens livscykel som inleds med upptäckten av en incident och avslutas med en registrering av incidenten där hela livscykeln beskrivs (AXELOS, 2012). I vissa skrivas även lösningar på återkommande incidents ner för att förenkla arbetet.


Processerna hänger inte helt oväntat ihop då arbetet i denna process implementerar de policens som definierats i Information Security Management-processen (ibid).

3.2.5 Continual Service Improvement

![ITIL livscykel, Continual Service Improvement Källa: Cartlidge et al, 2007](image)

Trots att denna process i första hand associeras med Continuous Service Improvement så utförs ett antal av processens aktiviteter i andra steg av livscykeln och grundtanken bakom processen kommer ifrån den fyra steg långa cykeln Plan-Do-Check-Act, som ofta förkortas PDCA, se Figur 3.8.

Figur 3.8: Fri tolkning av Demings PDCA-cykel Källa: Tonnqvist, 2008

3.2.6 Riskerna med att implementera ITIL

En av de risker som finns vid en ITIL implementation är att organisationen inte ser ITIL som ett verktyg utan som en färdig lösning. Respondent 4 beskriver detta som att organisationen försöker realisera den ”rosa värld” som ramverket hoppas uppbringa och att den faktiska nyttan bakom processerna glöms bort.³

ITIL, likt alla andra ramverk är designade för att anpassas till den individuella organisationens behov och är därmed med inte en universell lösning på alla organisatoriska problem. Respondent 4 påpekar även vikten av att man från organisationens håll har ett tydligt mål med implementationen och inte att det genomförs för att man ska ha något att visa upp för sina intressenter, så som kunder, investerare eller myndigheter (ibid).


En annan risk som finns med ramverket som Respondent 1 påpekar är att det kan vara svårt att på ett korrekt sätt besätta alla nödvändiga roller. Detta kan leda till att en person i slutändan kan inneha flera roller vilket leder till att rollerna inom processerna blir ofokuserade.⁴ Detta problem kan bli extra påtagligt inom processerna Incident, Problem och Change. Att besätta rollerna Incident Manager, Problem Manager och Change Manager då dessa roller är så nära kopplade med varandra och om dessa roller ligger på samma person så kan det vara svårt att upptäcka problem vid överlämningsprocesser och rutiner (ibid). Detta missgynnar verksamheten då processer och rutiner som missgynnar företaget inte kan omarbetas och förbättras då de inte upptäcks.

³ Intervju med Respondent 4 BiTa Service Management 2013-09-03
⁴ Intervju med Respondent 1 på Xpeedio 2013-10-17

Respondent 4 påpekar att det under ett ITIL-implementationsprojekt är viktigt att under förstudien fokusera på att utvärdera den nuvarande situationen och fastslå organisationens ”sjukdomstillstånd”. Genom att man fastslår organisationens ”sjukdomstillstånd” så synliggörs de brister som finns.

Respondent 4 menar även att insikten av detta ”sjukdomstillstånd” kan bli överväldigande för organisationen vilket i vissa fall kan leda till att projektet avbryts. Respondent 1 menar även han att det är viktigt för organisationen att fastslå vad som finns och hur de arbetar i sina nuvarande processer. En annan sak som Respondent 1 poängterar är att det är viktigt i en förstudie är att lokalisera eventuella ambassadörer för förändringsarbetet.

Respondent 1 menar i motsats till Respondent 4 att den mindre processen inte är tillräcklig för att utgöra den bas som projektet behöver och anser därmed att en förstudie är nödvändig för en lyckad implementation.

En annan risk som Pamela Erskine (2013) tar upp i sin bok ”ITIL and organizational change” är att många av de initiativ som tas i relation till ITIL inte hanterar aspekterna relaterade till den organisatoriska förändring som sker i samband med implementationen av ITIL-komponenter. Detta kan leda till att ramverket och dessa processer kan upplevas som effektlösa eller som om de påverkat organisationen negativt. I denna situation så kan det vara bra att gå tillbaka och undersöka hur aspekterna kring den organisatoriska förändringen behandlades under implementationen (Erskine, 2013). Ett exempel på en organisatorisk aspekt kan vara den ”rosa värld” som Respondent 4 beskriver. I detta fall har man inte anpassat ramverket efter organisationen och dess interna kultur vilket leder till att man måste ifrågasätta om förändringen i det arbetsrelaterade beteendet är försvarbart.

3.2.7 Organisatorisk förändring

Figur 3.9: Illustration av sambandet mellan organisation och verksamhet.

Citatet "It is not necessary to change. Survival is not mandatory" av William E. Deming förkroppsligar kärnan av organisatorisk förändring.


Respondent 2 menar även att det är viktigt att man förankrar beslut relaterade till organisatorisk förändring hos samtliga personal och inte endast hos de närmast berörda då en organisatorisk förändring på något sätt påverkar alla anställda. Hurst (1995) menar vidare att det är viktigt att identifiera den personer inom organisationen som är mest drivande i förändringsarbetet, både för och emot, samt att dessa personer i största möjliga mån bör involveras i förändringsarbetet, speciellt om den tidigare inställningen till initiativet har varit av en negativ natur. Anledningen till att det är viktigt att denna gemensamma vision av förändringen finns är inte endast för att minska riskerna för en misslyckad implementering utan även utifrån ett säkerhetsperspektiv.

3.3 Säkerhet

Det finns många definitioner av vad ett hot är och förståelsen för detta är essentiell i arbetet att skydda sig mot dessa. William Stallings och Lawrie Brown definierar term ett hot som en potentiell överträdelse av säkerheten som existerar under vissa förhållanden, förmågor, aktioner eller tillfällen då överträdelser av säkerheten kan inträffa och skada verksamheten (Stallings & Brown, 2008).

3.3.1 Hackare
Ordet hackare har enligt Nationalencyklopedin tre väldigt olika innebördar där den första syftar till en dataintresserad person som är hängiven och skicklig inom området datateknik (Hackare, Nationalencyklopedin). Den andra definitionen, som är den mer allmänt erkända, syftar på en person som använder sina kunskaper inom framförallt datateknik för att tillskaffa sig information som denne inte är auktoriserad till (ibid). Den tredje definitionen av hackare som återfinns i Nationalencyklopedin är syftar på en programmerare som har ett osymmetriskt och ostrukturerat arbetssätt (ibid). Hackarkulturen grundades under 1960-talet på Massachusetts Institute of Technology (MIT), där definitionen av en hackare var en person som inte bara var en skicklig programmerare utan även en visionär som tillskrev datatekniken samhällsinverkande potential (ibid).

---

5 Intervju med Respondent 2 2013-09-17

Hackarkulturen kan likt andra kulturer delas in i olika subgrupper, som i detta fall är tre till antalet. Dessa tre kallas White hats, Grey hats och Black hats.


Denna grupp av hackare har under den senare tiden uppmärksammats i och med de hot som under de senaste åren genomförts av hacktavistgruppen Anonymous. Denna grupp är ett typexempel på Grey hat hackers och den etiska problematik som finns runt dessa. Det råder nämligen delade meningar angående om Grey hat hackare då vissa anser att de inte är annorlunda ifrån Black hat hackare utan att de bara gömmer sig bakom ytliga argument.


3.3.2 Social engineering


---

6 Föreläsning med Respondent 3
Många kända hackare världen över använder sig av metoden för att få tillgång till information som de sedan använder för att hacka databaserade. Uttrycket myntades av datahackers som insåg att metoden var mer effektiv och mindre tidskrävande än att försöka ta sig in genom att hacka systemen (Britz, 2012).

Problemet med social engineering är att det inte finns något riktigt bra sätt för organisationer att skydda sig emot det. Det enda som en organisation kan göra för att minska riskerna för social engineering är att uppmärksamma de anställda på problemet och i och med detta skapa så kallad "Security Awareness".


---
7 Intervju med Respondent 3
3.3.3 Hot

De flesta hot kan kategoriseras som antingen ett passivt eller aktivt hot samt som ett internt eller externt hot, vilket illustreras i **Figur 3.10**.

![Figur 3.10](image-url): En illustration av de kategorier av hot som behandlas i avsnittet. Fritt tolkade utifrån beskrivningar av Stallings & Brown (2008).


Ett internt hot är, liksom namnet antyder, ett hot där hotet kommer från auktoriserad källa som inte använder informationen i avsett syfte (ibid). Vi kan till exempel ån en gång applicera fallet med den anställda som är nyfiken på sin kollegas lön om denne, i och med sin position, har tillgång till exempelvis lönelistor och använder dessa för att ta reda på sin kollegas lön. I ett mer allvarligt fall så kan det röra sig om att en auktoriserad anställd använder sin access för att exempelvis extrahera information från systemet som sedan vidarebefordras till konkurrenter eller brottslingar som önskar använda den i egna syften. Detta är den vanligaste typen av hot, även om det oftast rör sig om harmlösa gärningar som är ett resultat av en nyfiken anställd eller dåligt utbildad personal (ibid).


Man kan på en översiktlig nivå dela in alla hot i övergripande grupperingar baserat på var hotet kommer ifrån (intern eller extern) samt i vilket syfte som hoten utförs (passiv och aktiv). Det finns många olika metoder för att ta sig in i eller påverka ett system och de flesta av dessa kan delas in i en av fyra grupper: Icke-auktoriserat avslöjande (unauthorized disclosure), Bedrägeri (deception), avbrott (disruption) och usurpation (usurpation) (Stallings & Brown, 2008).

Dessa fyra grupper kan sedan delas in ytterligare i tolv olika grupperingar: Avslöjande hot, uppsnappning, slutledning, intrång, maskerat hot, förfalskning, nekande, funktionsduglighet, korruption, obstruktion, förskingring och missbruk (ibid).

Ett exempel på detta fenomen är att en anställd tjuvlyssnar på en konversation som denne inte är auktoriserad att delta i (Stallings & Brown, 2008).

Slutledning, eller inference som det kallas på engelska, är ett hot som på ett sätt kan beskrivas som en variant av uppsnappning då det definieras som när en icke-auktoriserad källa på ett indirekt sätt införskaffarkänslig data eller information genom att utifrån resonemang baserade på kännetecknande eller kommunikativa förbindelser.


Återigen kan denna mängd information känns något överväldigande för den vanliga användaren speciellt då många av dessa definitioner är väldigt lika men likt gällande i det föregående avsnittet så handlar det om att skapa sig en översikt. För mer avancerade användare inom området, som till exempel IT-organisationen, så kan de olika varianterna av hot vara av ett större intresse då nyanserna i hotens karaktär påverkar de efterföljande konsekvenserna på olika sätt. Man kan generellt säga att informationen är relevant i förebyggande syfte både för den vanliga och för den mer avancerade användaren även om det för den mer avancerade användaren ligger på ett högre plan. Detta innebär att den mer avancerade användaren har användning av mer detaljerad information om olika hot än den vanliga användaren vars intresse är av mer generell karaktär.
3.3.4 Säkerhetsarbete i små och medelstora företag


Fördelarna med den nya trenden är många, det är bland annat enkelt för den anställde då denne kan använda ett operativsystem som denne föredrar samt att kostnaderna för utrustning minskar (ibid).

Detta kan verka som något bra speciellt för mindre företag och organisationer där de ekonomiska tillgångarna kan vara något begränsade men det är viktigt att man tar hänsyn till den säkerhetsrisk som trenden innebär. Problemet är att IT-avdelningen inte har någon kontroll över vad som ”kommer in” på det slutna nätverket när användaren kopplar upp sig. Ett virus kan alltså ligga på den anställdes privata enhet och sedan spridas till andra delar av systemet. Detta kan orsaka att konfidentiell information läcker ut till icke-auktoriserade personer. BYOD har skapat en hel del debatt inom säkerhetsområdet och man har kommit fram till att man kan tvinga problemet genom att vidta olika säkerhetsåtgärder i stil med de som Secret Service vidtog. Frågan är om mindre företag och organisationer har de ekonomiska och administrativa tillgångarna att hantera de åtgärder som i en ideal värld borde vidtas.

I den undersökning som FBI genomförde 2005 deltog 2066 individer ifrån olika organisationer och av dessa organisationer var de flesta, enligt amerikansk standard, så kallade SME. En av de huvudsakliga upptäckter som studien avslöjade var bland annat att en stor del av respondenterna uttryckte en önskan att bli bättre informerad gällande hur man bättre skyddar sig mot olika datarelaterade brott och relation till detta var hela 75 procent av respondenterna intresserade av att närvara vid informationsseminarium inom ämnet (FBI, 2005). Detta innebär att det finns ett intresse i mindre organisationer för bra hantering av system och känslig information. En förklaring till detta relativt höga intresse indikerar att det inte finns tillräckligt med tillgänglig information inom ämnet som är anpassat för just denna grupp av organisationer i nuläget.
4. Empiri

Detta kapitel avser att beskriva de två företag som undersökts i detta arbete. Det är på denna data som den teoretiska delen av arbetet kommer appliceras på i det nästkommande analyskapitlet.

De data som detta kapitel vilar på har sitt primära ursprung i intervjuer och observationer men även till viss del i företagsdokumentation och företagen hemsidor. Om källor som företagsdokumentation eller information från hemsidor ligger till grund för påståenden framgår detta i texten, detta då denna information kan innehålla försköningar av verkligheten.
4 Empiri

4.1 Företag 1

Företag 1 är en mindre organisation med cirka 185 anställda och som är aktiva inom hematologibranschen. De beskriver sig på sin hemsida som ”ett diagnostikbolag som utvecklar, tillverkar och marknadsför system och konsumentprodukt för komplett blodcellsanalys till icke-institutionell vård”. Deras huvudprodukt är utvecklandet av blodcellsräknare även om de tillverkar förbrukningsvaran reagens. Reagens är en kemisk sammansättning som resulterar i en specifik kemisk reaktion eller förändring under vissa omständigheter (reagens, Nationalencyklopedin). Sammansättningen av reagensen kan variera för olika maskiner och system. Detta innebär att sammansättningen av reagensen är specifik för företagets egna produkter.


4.1.1 Företagets uppbyggnad

Företaget består av två dotterbolag som tillsammans bildar ett större företag, se Fig. 4.1. Företaget är uppbyggt utifrån en horisontell företagsstruktur (Beynon-Davies, 2009), där en Steering Board och en IT Manager, utgör de två komponenterna som är gemensamma för de två dotterbolagen. Steering Board, är en styrelse bestående av fyra medlemmar däribland Verkställande Direktörerna för moderbolaget samt de två dotterbolagen. Uppgiften som denna instans har är att fastställa de övergripande och generella riktlinjerna för verksamheten samt besluta i frågor som involverar större investeringar. IT Managerns uppgift är att se till att den IT strategi som fastslagits överensstämmer med de generella riktlinjerna för företagets policy.

---

8 Presentation under studiebesök i reagensfabriken.
Under IT Managern så tar dotterbolagens individuella hierarkier vid i forma av ett IT Counsel som har till uppgift att hantera frågor som rör mellanstora investeringar eller problem. Denna instans är den högsta inom de enskilda dotterbolagen. Under dem opererar ytterligare en IT Manager men som till skillnad från den tidigare endast har inflytande över det dotterbolag för vilket denne arbetar.

Uppgifterna för IT Managern på denna nivå är primärt att styra och kontrollera implementationer samt koordinera IT relaterade problem. Till sin hjälp har IT Managern två team: IT Operations och IT Development. Uppgiften för IT Operations är primärt att sköta den dagliga verksamheten och underhåll av system, detta involverar bland annat att göra backups och agera som stöd för slutanvändare. IT Development teamet har som primär uppgift att skydda och utveckla företagets system och applikationer.

![Figur 4.1: Modell av Företag 1:s uppbyggnad. Fritt tolkad från intervjuer med Respondent 5,6 och 7.](image-url)
4.1.2 Implementationen av ITIL

I och med att företaget börsnoterades 2011 så ställdes nya krav på dokumentering och informationshantering i enlighet med svensk lagstiftning. Detta ledde till en inledande implementation av komponenter av ITIL ramverket, till exempel skapades en helpdesk\(^9\). I det underlag som finns för granskning av IT-kontroller beskrivs bland annat krav på dokumentation över personer med behörigheter, programändringar och drift. Dessa kontroller styrs inte av företaget utan kontrolleras av externa entiteter som företaget inte kan påverka. Under hösten gjorde företaget en satsning på en vidare implementation av ITIL-ramverket där fokus låg på processerna Change, Incident och Problem Management.

De problem som uppdagades under de initiala intervjuerna med Respondent 6 och 7 var främst att det fanns stora frågetecken kring graderingar och definitioner gällande framförallt incident och problem. Det fanns ingen tydlig definition av hur prioriteringarna inom de olika områdena skulle ske, även om de olika graderingarna fanns med i företagsdokumentationen. En tydlig definition på vad skillnaden mellan en kritisk och medium klassad incident fanns till exempel inte. Konsekvenserna av detta blev att man ofta väntade med att åtgärda incidenter och problem tills de blev kritiska då detta var det enda som var tydligt definierat i företagsdokumentationen. Att det inte fanns tydliga definitioner medförde även i att de verktyg som tillhandahölls inte användes i den utsträckning som de borde. Utifrån detta beslutades fastslogs att de processer som skulle beröras av implementationen i första hand var change, incident och problem.

Det var under projektets tidiga stadium inte helt säkert att det var ramverket ITIL som skulle implementeras, även om detta var den initiala planen, då det under projektets gång fanns tankar kring ramverket CoBit, som kan beskrivas som en amerikansk variant av ITIL. Företag 1 valde sedan att fortfarande som planerat med ITIL trots att det fanns drivande personer bakom båda alternativen.

Initiativet till implementationen av ITIL låg inte endast i det faktum att företaget börsnoterats utan hade även viss grund i Respondent 5: s tidigare erfarenheter av organisatoriska problem i relation till tekniska problem.

\(^9\) Intervju med Respondent 5
De erfarenheter som Respondent 5 ofta refererade till var när ett större tekniskt problem innebar att större delen av styrelsen stod i företagets serverrum och skulle ta beslut om hur man ska lösa problemet. Detta innebar att det uppstod, vad han beskrev som ”en hönsgård”, vilket inte är givande i situationen\(^\text{10}\).

Några månader efter implementationen genomfördes ytterligare en gruppintervju med de inblandade i implementationen. Vid denna intervju så visade det sig att de anställda nu lite smått börjat arbeta med verktyget när tydliga definitioner fanns.

4.1.3 Observationer i relation till ITIL-projektet och säkerhet.


\(^{10}\) Intervju med Respondent 1
Redan första dagen observerade jag några av de problem som denna kultur orsakade då jag stod ute i solen och väntade på min handledare. En av personalen släppte då in mig i byggnaden utan att ens ifrågasätta mitt ärende. Vidare, samma dag, så glömde jag koden till dörren på min våning som en annan i personalen gladeligen knappade in utan att ifrågasätta vilket ärende jag hade till avdelningen. När jag senare fick insikt gällande den mer tekniskt relaterade säkerheten så var den överväldigande bra i relation till den fysiska säkerheten. I relation till detta ansågs det nödvändigt att integrera delar av Information Security Management och Access Management processerna under implementationen. En annan anledning till att säkerhet blev en del av implementationen är att företaget i sin egen dokumentation klargör den vikt som de lägger på ämnet och att de tar detta på allvar. I företagsdokumentationen framhålls det hur företaget skall arbeta på ett kontrollerat sätt i relation till säkerhetsfrågor samt att ansvaret för dessa frågor ligger på en välägt hög organisatorisk nivå. I verkligheten så har jag utifrån mina observationer dragit slutsatsen att ansvaret för säkerheten till stor del ligger på en lägre organisatorisk nivå. Som jag beskrivit tidigare så är det en del av de arbetsuppgifter som utförs av IT Operations och IT Development. Detta kan tolkas som att det organisatoriska ansvaret för säkerheten ligger längre upp i organisationen medan det faktiska utförandet ligger på en lägre organisatorisk nivå. När det gäller den fysiska säkerheten på företaget så uppfattade jag inte tillståndet acceptabelt i och med lokalernas geografiska position men eftersom att den fysiska säkerheten specifikt tas upp i företagsdokumentationen så fick jag uppfattningen att resurser till säkerhet generellt inte avsätts särskilt frikostigt. 4.2 Företag 2

Företag 2 är ett mindre konsultföretag baserat i Stockholm som både jobbar med att implementera ITIL och erbjuder olika ITIL-certifieringskurser på olika nivåer. Företaget har cirka 25 anställda, vilket enligt Europakommissionens standarder klassificerar företaget som small sized SME.

Under intervjun framkom att företaget delvis implementerat ITIL i den egna verksamheten men att de var dåliga på att arbeta med processer. Vidare kom det fram att de processer som organisationen implementerat främst var Change och Incident Management.

Den interna kulturen på Företag 2 skiljer sig markant från den definition som Office of Government Commerce använder sig av. Jag uppfattade den interna kulturen som mer formell än informell i jämförelse med Företag 1 vilket kan bero på den geografiska skillnaden men även på den marknadsrelaterade skillnaden.

Det som är intressant i denna organisation var att deras syn på säkerhet. Respondenten för företaget menade nämligen att mindre organisationer har större problem med säkerhetsrelaterade frågor än de
större organisationerna då större verksamheter som till exempel SAAB genom åren har lärt sig att hantera den sortens problem. Han valde att exemplifiera detta med att de inom företaget använde sig av sina privata telefoner i arbetet och att hans egen telefon som han hade med sig vid intervjuutställfallet inte ens var låst med pinkod. Detta innebär att epost och annan information relaterad till företaget är exponerad och oskyddad.
5. Analys

I detta kapitel kommer den information som presenterades i den teoretiska referensramen appliceras på det data som presenterades i det föregående empirikapitlet. Syftet är i detta kapitel att genom en analys baserad på teorier från den teoretiska referensramen söka svaren på de frågor som definierades i frågeställningen.
5 Analys

5.1 Frågeställning

Eftersom att analysen utgår ifrån den frågeställning som presenterades i det indelande kapitalet så avser detta avsitt att återkoppla till denna. Den frågeställning som detta arbete utgår ifrån är följande:

- Vilka är de avgörande faktorer som påverkar organisationen under en ITIL implementation?
  - Vad gör att en implementation avbryts eller att utfallet inte blir som önskat?
- Vilka skillnader finns det mellan större och mindre organisationer i relation till säkerhet?
  - Vilka åtgärder kan vara aktuella för en mindre organisation?
  - Vem har enligt ITIL ansvaret för att ta itu med respektive hot?

5.2 ITIL

När det gäller problematiken kring implementationer av till exempel ITIL, som innebär organisatoriska förändringar så är det viktigt att man har en öppen dialog inte bara med de närmast inblandade utan även med de övriga anställda liksom Respondent 2 argumenterar. Man skulle kunna argumentera att de bristfälliga definitioner som återfanns i företagsdokumentationen kan vara ett tecken på bristfällig förankring hos berörd personal vid implementeringen, vilket var anledningen till att personalen i Företag 1 använde verktyget i begränsad utsträckning, vilket jag inte tror vad Företag 1 hade i tankarna när denna implementation genomfördes. Under den andra implementeringen i Företag 1 så fanns det en dialog med verksamheten, även om den var på en mindre skala och genomfördes utifrån ett mer vardagligt förhållningssätt. Fokus under implementeringen låg liksom det empiriska kapitlet reflekterar på de närmast påverkade inom IT-organisationen. Genom att skapa denna sociala vision som Hurst (1995) argumenterar för så förebygger man som organisation att hamna i den fälla där man försöker realisera den ”rosa värld” som Respondent 4 tar upp som en av de stora riskerna vid en implementering. Inom Företag 1 så uppkom en diskussion innan implementeringen angående om en vidare implementering av ITIL var vad som var önskvärt eller om man istället skulle satsa på COBIT.

Även om det fanns drivande parter för båda alternativa så blev det till slut ITIL, och även här involverades den påverkade delen av personalen i arbetet. Detta för att de skulle känna sig involverade samt att deras åsikter räknades och var viktiga. Detta byggde så småningom upp till vad man skulle kunna kalla en social vision vilket kan vara en de faktorer som påverkat personalen till att faktiskt använda verktyget efter den andra implementeringen.

De avgörande faktorerna för en ITIL-implementation framtåg ligger även i den acceptans som organisationen måste, liksom Respondent 4 poängterar, ha för sitt egna ”sjukdomstillstånd” samt den förankring som måste ske hos all personal inom främst organisationen men även inom verksamheten för att man ska uppnå de mål som man satt med implementeringen. Om organisationen inte kan acceptera sitt ”sjukdomstillstånd” så finns det en överhängande risk att projektet läggs ner eller att resultatet inte blir som önskat. Respondent 1 menar vidare att en förstudie är nödvändig för att säkerställa att projektet är genomförbart och att en positiv förändring kommer att ske vilket Respondent 4 menar inte är fallet och vidare hänvisar till de ekonomiska aspekternas av en implementering. Under den andra implementeringen på Företag 1 genomfördes ingen större förstudie i relation till detta handlade denna implementering om vidareutveckling och inte en initial implementering av avgörande processer. Med tanke på implementeringens natur så ansågs en förstudie överflödig och resursmässigt onödigt kostsam.

Detta är något som både Respondent 1 och Respondent 4 argumenterar för, det måste finnas en vilja och en drivkraft bakom förändringen och projektet för att maximera chansen för ett lyckat resultat.

5.3 Säkerhet

Gällande säkerhet inom SME så ligger, likt rapporten som FBI presenterade 2005, inte problemet i de tekniska säkerhetsåtgärderna som till exempel anti-virus och antispyware som finns till för att hålla externa hot ute utan det är istället de interna hoten som skapar problem, vilket reflekteras i främst Företag 2. Det kan vara svårt för mindre organisationer och företag att adressera dessa säkerhetsrelaterade problem på grund av de begränsade ekonomiska resurser denna grupp har och det är därmed viktigt att man vidtar de icke-resurskrävande stegen. Ett exempel på detta är det som observerades i Företag 2 där mobilen var olåst.

I detta fall kan det vara en bra idé att till exempel införa ett krav på pinkod på samtliga enheter som innehåller företagsrelaterad information speciellt om dessa även används privat. Trenden ”Bring Your Own Device”, BYOD, har skapat stora problem inom så väl SME som större organisationer och det är viktigt att IT-avdelningar, framförallt inom mindre organisationer där resursbrister kan bidra till en ökning av tenden, är medvetna och informerar om faran med denna trend. Denna information borde främst riktas till ledningar som kan ha svårt att se nackdelarna med trenden.

När det gäller hot som social engineering kan man anta att SME har en fördel gentemot större organisationer då man ofta vet vilka som jobbar i till exempel Helpdesken, förutsatt att detta inte är outsourcat till ett annat företag. På Företag 1 visste man till exempel vilka som jobbade i Helpdesken vilket innebar att man troligtvis inte skulle ge ut information om lösenord och liknade till en hackare som använde sig av Social engineering.


Jag har svårt att tro att kostnaderna för att skicka ett fåtal personer från IT-avdelningen på kurs varannat år överstiger de av att förlora företagets känsliga information speciellt och om detta är fallet kan man, om man arbetar med till exempel ITIL, avgränsa sig till de personer som berörs av processerna Information Security Management och Access Management eller motsvarande.

6. Slutsatser och kunskapsbidrag

Detta kapitel avser att i relation till den problembild och de mål som definierades i inledningskapitlet sammanfatta de slutsatser som genererats i analysen. Det är vidare detta kapitels syfte att definiera det bidrag som dessa slutsatser genererat i forma av kunskapsbidrag.
6 Slutsatser och kunskapsbidrag

En av de avgörande riskerna under en implementation att man inom organisationen inte arbetar kontinuerligt med att ”få med alla på samma båt” och förankrar beslut om nuvarande och kommande förändringar hos personalen. Det gäller även att denna förankring sker inom verksamheten även om förändringen i sig endast påverkar organisationen. Anledningen till detta är att förändringar i organisationen indirekt kan påverka verksamheten och om inte annat så kan det vara viktigt att all personal får chansen att känna sig delaktiga i viktiga beslut. En annan risk som påverkar en implementation av till exempel ITIL är organisationen inte vågar acceptera sitt eget ”sjukdomstillstånd” vilket kan innebära att implementationen avbryts eller att utfallet påverkas negativt. Meningarna angående huruvida en förstudie är nödvändig för att fastslå detta ”sjukdomstillstånd” går likt arbetet visat isär inom konsultvärlden.

En risk som inte är lika framträdande är den med de ”drivande” människor inom organisationen vid en implementering som lätt kan snöa in organisationen på ett alternativ och vilket leder till att man inte överväger alla alternativ utan tar det som är mest modernt eller det ”som man vet fungerar”. Detta innebär att det finns risk för att man missar att överväga något som kunde ha varit ett bättre alternativ just den verksamheten. En annan risk som kan finnas i relation till alltför drivande parter inom ett implementationsprojekt kan vara att man försöker att realisera en ”rosa värld” och glömmer bort att anpassa verktyget efter verksamheten. Det är trots detta viktigt att man utnyttjar intresserade parter till lika negativt inställda parter vid en implementation för att få ett så bra resultat som möjligt och om inte annat motivera parter som eventuellt motsätter sig projektet. Det är trots bieffekterna av ökad börda för delar av organisationen ändå viktigt att man arbetar processorienterat för att undvika vad Respondent 5 beskrev som ”en hönsgård”. I och med att man arbetar processorienterat så blir det ”färre hönor i hönsgården” vilket underlättar arbetet för alla parter.

Gällande hotbilden mot mindre företags information så är betydligt mindre än den mot större företag men bör ändå inte anses som mindre allvarlig. Som detta arbete påvisar så är det stor skillnader mellan SME och större organisationer gällande tillgången till både kunskapsrelaterade och ekonomiska resurser inom ämnet där de större organisationerna har ett tydligt försprång. Anledningen till att kunskapsmässiga resurser saknas beror inte på en avsaknad av intresse ifrån mindre organisationer utan är direkt kopplade till de ekonomiska begränsningar som denna grupp har. SME utgör en stor del av många länder ekonomi och det är därför viktigt att det finns resurser tillgängliga för denna grupp.
Även om hotbildens utifrån ett hackarperspektiv borde vara mindre i SME baserat på att hackarkulturen är en meritokrati och att en hack av ett mindre företag inte är lika meriterande som en hack av ett större företag med bättre säkerhet så rättafärbar det inte det ofta underråliga säkerhetsarbetet inom SME. I kontrast till detta är även mindre organisationers arbete med säkerhet mindre utvecklat än de större företagen som genom åren har utarbetat olika strategier för att hantera problemet. Detta insinuerar att skillnaderna inte ligger i storleken av företaget utan är relaterade till dess resurser och erfarenheter inom området säkerhet.


Som företag kan mindre resurssatsningar som informationsseminarier gällande säkerhet löna sig rent ekonomiskt då man kan påvisa att man kontinuerligt arbetar med problemet. I och med detta ses man inte av potentiella kunder som ”den svagaste länken” viket i sin tur innebär att man inte förlorar lika många viktiga avtal. Att officiellt skylta med att man har ett bra säkerhetsarbete kan däremot ge motsatt effekt då man lätt kan bli ett onödigt mål för meritsökande hackare.

Avslutningsvis så är det min åsikt att arbetet bidragit till en vidare dokumentation inom området för hur mindre organisationer hanterar en ITIL implementation samt hur arbetet med ITIL kan analyseras utifrån ett säkerhetsperspektiv, vilket var arbetets syfte. Det var även arbetets syfte att undersöka hur mindre organisationer förhåller sig rent generellt till säkerhetsarbete i kontrast till större organisationer vilket, enligt mig, denna studie tydligt påvisat.
7. Reflektion, Kritik och Fortsatta studier

I detta kapitel presenteras mina egna reflektioner kring arbetet. Vidare anser detta kapitel även att ta upp den kritik gällande de brister som jag i egenskap av arbetets författare anser att arbetet har. Anledningen till att detta adresseras är för att stärka arbetets reabilitet och validitet, vilket förklarades i inledningskapitlet. Avslutningsvis presenteras även förslag på vidare forskning inom de områden som arbetet tar upp, det vill säga ITIL, säkerhet och SME.
7. Reflektion, Kritik och Fortsatta studier

7.1 Reflektion

De största utmaningarna i detta arbete har varit att riktigt sätta sig in i ITIL och alla processer och roller som är kopplade till ramverket. Detta då jag genom min utbildning inte har kommit kontakt med detta så mycket innan genomförandet av fallstudien hos Företag 1. Det svåraste med just ITIL är den överväldigande mängden information som gör det svårt att hitta en bra startpunkt för undersökningar och informationssökande. I och med att jag redan hade ett företag med ett specifikt problem så var det något lättare för mig att hitta en bra utgångspunkt för arbetet.

I och med att mitt arbete innehöll ett antal praktiska komponenter, det vill säga fallstudien och den etnografiska undersökningen av den valda organisationen, så innebar det ytterligare en dimension för mig då jag fick applicera mina kunskaper i praktiken. Vidare fick jag användning för kunskaper som jag samlad på mig utanför mitt ordinarie programval inom systemvetenskap på Linköpings Universitet då jag valde att avgränsa mig till säkerhetsaspekten av ITIL. I och med denna praktiska del av arbetet har jag även insett vilka styrkor och brister som finns i min kunskap. Arbetet med denna rapport har alltså på ett tydligt sätt konkretiserat vilken vetenskaplig kunskapsgrund som jag har att stå och dess brister.

I relation till min inriktning, IT-projekt, så har detta arbete inneburit en unik insikt i den verklighet som till skillnad från de teoretiska skildringar som ges inom den akademiska världen ofta är mycket komplexa. Denna komplexitet är dock inte helt av ondo utan är även det som gör organisationer, verksamheter och andra entiteter till de individuellt samverkande och unika delar av vårt samhälle som de är.

Den upptäckt som jag under detta arbete blev mest förvånad över var att man i praktiken inte alltid utnyttjar det intresse som finns inom varken organisationen eller verksamheten. Det kan visserligen finnas olika anledningar till detta som på något sätt är avgörande även om min personliga åsikt är att intresse sällan är av ondo.

Arbetet som helhet har inneburit en hel del processande av material både teoretiskt och empiriskt. Det har även gått åt en hel del tid till att bearbeta information som inte har använts i arbetet men som har varit nödvändig för mig som författare för att jag ska kunna sätta mig in i de olika ämnena och förstå dem.
7.2 Kritik
En av de aspekter som man kan kritisera i detta arbete är generaliserbarheten, vilket även är fallet i många andra kvalitativa studier. Arbetet är huvudsakligen baserat på ett enskilt fall vilket innebär att de resultat som arbetet genererat kan uppfattas som "färgade" av den individuella organisationens interna problem och kultur. Jag kan till viss del förstå detta i viss utsträckning samtidigt som jag känner att de resultat som arbetet har producerat ändå upp till en viss nivå är generaliserbara. 

Den teori som använts i arbetet anser jag på ett bra sätt stödjer de slutsatser som dragits på en generell nivå även om arbetet isig har utgått från studien av en enskild organisation.

Jag har under arbetets gång även haft mer eller mindre fri tillgång till de roller som jag ansett viktiga för studien i huvudorganisationen. I den mindre studien av Företag 2 så kände jag att jag fick svar på de frågor som jag ställde och därigenom fick de svar jag behövde. Samma sak gällde de teoretiskt relaterade respondenterna och en stor bidragande faktor till detta var den tid som jag hade att arbeta med rapporten i anslutning till den etnografiska studie som jag genomförde i Företag 1. Det finns dock inga garantier eller vetenskapliga belägg för att de resultat som presenterats i arbetet skall vara applicerbara eller avgörande i alla organisationer som tillhör gruppen SME.

7.3 Vidare forskning
Det område som jag har valt att studera är trots sin avgränsade karaktär ändå väldigt brett och vidare forskning inom området är i min mening absolut nödvändig. Exempel eller förslag på delar av problemområdet som behandlats i arbetet där jag anser att ytterligare kunskap kan vara nyttig eller till och med nödvändig gäller framförallt SME:s förhållande till ny teknik, resurshantering samt staten relation till SME.

Detta med anledning av den överväldigande andel som SME utgör av ett flertal länders ekonomi och samhällsstruktur. Det kan i relation till detta även vara intressant att ifrågasätta vilka konsekvenser som de säkerhetsrelaterade problem inom SME kan få på en nationell och global nivå.
Ett annat område som kan vara intressant att forska vidare inom och ligger närmare min egen utbildning inom systemvetenskap kan vara undersökningar gällande hur man på bästa sätt skall alloker resurser för säkerhetsarbete inom SME utifrån perspektivet av Human Relations.
Referenser

**Publicerade Källor:**


AXELOS (2012). *Best Management Practice portfolio: common glossary of terms and definitions*, version 1, AXELOS Limited


Erskine, Pamela (2013). *ITIL and Organizational Change*. UK.ITGP


Ey. (2013). *Bring your own device: Security and risk considerations for your mobile device program*.


Mitnick, Kevin D. (2012). *Ghost in the wires: My adventures as the world’s most wanted hacker*. Little Brown


Elektroniska källor:


Bilaga 1 – Exempel på mall inför intervju

Vilka risker finns det med att implementera ITIL?

Vad bör man fokusera på under en förstudie?

Det är ofta som företag skippar förstudien hur ser du på det?

Varför väljer man ITIL?

Använder ni ITIL själva?

- Vilka moduler har ni implementerat?
- Har ni upplevt några problem?
- Varför valde ni den lösningen?
- Vad gjorde ni för förstudie?

Hur mycket skall organisationen anpassa sig efter ramverket (ITIL)?

Berätta mer om:

- Change Management
- Incident Management

Hur viktigt är det att man förankrar implementationen av ITIL hos personalen?

IT-avdelningarna är kända för att arbeta runt problem. Vad brukar hända när man implementerar strukturerade ITIL processer?

Vi hade i en tidigare en kurs i IT-förvaltning, där vi i vår grupp kom fram till att det var bra för mindre till medelstora företag att satsa på en ITIL och Pm3 blandad lösning. Vad tror du om det?
Bilaga 2 – Exempel på transkriberat material

Intervju med Företag 2

Intervju med Respondent 4 på Företag 2, på deras kontor i centrala Stockholm.

*Vilka risker finns det med att implementera ITIL?*

Det finns en risk att man försöker realisera den ”rosa världen ” som utlovas av ramverket och att den faktiska nytta med processerna inom ITIL glöms bort. Det är även så att det är svårt att påvisa nytta som ITIL gör. Om man tar ett Helpdesk som exempel så är det svårt att förklara för en VD för ett företag vad företaget tjänar på att man i Helpdesken lyckas hjälpa användarna på fyra minuter istället för sju.

Man måste anpassa ramverket efter verksamheten och komma ihåg att det är ett verktyg. Det är även viktigt att man har ett tydligt mål med implementationen och inte gör det bara för att man ska kunna ha något att visa upp för sina kunder.

*Vad bör man fokusera på under en förstudie?*

Det är ofta som företag skippar förstudien hur ser du på det?

Jag ser det inte som något negativt då den ofta kostar en massa pengar och man har förståelse för företag som lägger ner en massa pengar på att göra en förstudie som sedan inte leder någon vart. Gör man detta tre gånger med samma resultat så kommer man vill man ju inte göra det igen utan då vill man komma igång och få något för pengarna. När man kommer in som konsult så genomför man ju en mindre förstudie i alla fall, förtäckt under ett annat namn då man intervjuar anställda och samlar in relevant data. Nyttan med en förstudie kan visserligen bero på vad det är man ska göra och hur det påverkar verksamheten i det dagliga arbetet. En ITIL-implementation påverkar ju inte i så stor utsträckning den dagliga verksamheten så drastiskt och brukar inte leda till några större problem även om det händer. En ITIL implementation är lite annorlunda jämfört med en implementation av t ex ett ERP system och har därmed inte samma effekt på verksamheten.

Varför väljer man ITIL?

I växande företag så kan det var bra att börja implementera ITIL och sätta fokus på nyttan. Den tidiga implementationen kan företaget sedan dra fördel av när det blivit större då personalen redan ”kommit in rullarna” i avseendet att arbeta med ITIL. Det är ofta enskilda individer med tidigare erfarenheter som är drivande i implementationer av det här slaget inom mindre till medelstora företag. Annars handlar det även ofta om konkurrensmässiga skäl till att man väljer att implementera ITIL och att man pratar samma språk.

Använder ni ITIL själva?


Hur mycket ska organisationen anpassa sig efter ITIL?

Man ska i första hand anpassa ITIL efter verksamheten och inte tvärtom men visst får man göra en viss anpassning i och med att man kan behöva arbeta lite annorlunda. Det kan även vara så att personal som normalt sett har fullt upp hela dagarna får ännu mer att göra i och med att de ska jobba med ITIL också. Det är därför viktigt att man förklarar nyttan med att arbeta efter ITIL för användarna.
**Mer om applikationerna Change Management/Incident Management?**


**Hur viktigt är det att man förankrar implementenationen av ITIL hos personalen?**

Livsviktigt. Det är viktigt att man skapar ett engagemang hos personalen för att det ska fungera och att man förklarar varför det är viktigt med IT. Sedan krävs det så klart att man har en bra support vid implementenationen.

**IT-avdelningarna är kända för att arbeta runt problem. Vad brukar hända när man implementerar strukturerade ITIL processer?**

Vi hade i en tidigare en kurs i IT-förvaltning, där vi i vår grupp kom fram till att det var bra för mindre till medelstora företag att satsa på en ITIL och Pm3 blandad lösning. Vad tror du om det?

Jag tror att Pm3 är mer lämpat för större företag än medelstora och mindre företag speciellt med tanke på ursprunget av Pm3. Pm3 känns även lite gammalmodigt då det är väldigt objektfokuserat till skillnad från ITIL som är mer tjänstefokuserat. Det hade varit bättre om de i de senaste releaserna hade lagt mer fokus på tjänster speciellt eftersom att den senaste versionen av ITIL (Version 3) anses ha ett mer affärsmässigt fokus.

Är det många som certifierar sig inom ITIL? Är det nödvändigt? Eller är det bäst att ha så kallade superanvändare inom mindre till medelstora företag?

Ur ett säkerhetsperspektiv, hur ser ITIL på den nya trenden BYOD (Bring Your Own Device)?


Ge en kortfattad summering.