GÖTEBORGS UNIVERSITET

# Imorgon: klart till växlande molnighet

## En mall för att understödja riskbedömningen vid en övergång till molntjänster

## Tomorrow: Clear to Partly Cloudy

**A model to support risk assessment in a transition to cloud services**

**ERIK MARTINSSON**

**Magisteruppsats i Informatik**

**Rapport nr. 2010:034**
**ISSN: 1651-4769**

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, Maj 2010

# ABSTRAKT

Cloud computing eller molntjänster syftar till såväl mjukvara och dess plattform som en tjänst som erbjuds via Internet samt till infrastrukturen som tillhandla håller dessa tjänster. Det finns mycket som talar för en övergång från egen drift till molntjänster men samtidigt finns det många olika risker i samband med övergången. En förstudie visar på ett antal aspekter som är sorterade efter tre övergipande områden. Här kategoriserade inom områdena teknik, ekonomi och organisation. Utifrån dessa aspekter har det gjorts en litteraturgenomgång som visar på ett antal underliggande riskområden. Dessa riskområden har resulterat i en mall. Med mallen går det att få fram varje aspekts riskvärde och mallen ska kunna användas av organisationer inför en riskbedömning vid en övergång till molntjänster. Vidare har mallen testats på fyra personer med tidigare erfarenhet av projektimplementeringar inom IT. Testet har utvecklat mallen till sin slutgiltiga form.

**Nyckelord:** Cloud computing, molntjänster, moln, riskområden, riskutvärdering, riskmall

# ABSTRACT

Cloud computing, or cloud services, refers to software and the software platform as a service provided through the Internet, as well as the infrastructure providing these services. Several arguments exist as to why a transfer from self maintained services to cloud services would be beneficial. At the same time a number of risks are associated with such a shift. A pre-study shows certain aspects sorted into three overarching areas; technology, economy and organization. Based on these aspects, a literature study has been made which reveals a number of underlying risk areas. These risk areas have resulted in a template. Using the template, it is possible to extract the risk value of each aspect, and the template could be used by organizations when assessing the risks associated with a transfer to cloud services. The template has been tested on four individuals with previous experience of project implementations within the IT sector. Based on this test, the template got its final form.

The report is written in Swedish.



**Keywords:** Cloud computing, cloud services, risk areas, risk assessment, risk template

# Innehållsförteckning

# Tabellförteckning

Globalisering och internationalisering bidrar till ett allt hårdare affärsklimat där jakten på konkurrensfördelar och fokusering på kärnverksamheter är en strävan för organisationer och företag för att inte utmanövreras och bli omkörda (Haverblad, 2006; Movin & Zandelin, 2009; Sörqvist, 2004). Att låta externa leverantörer ta hand om verksamhetens informationssystem, IS, och informationsteknik, IT, och istället koncentrera sig på den faktiska kärnverksamheten är ett sätt där man dels kan minska kostnader då man enbart betalar för den direkta användningen (Röhne, 2008), dels, med dagens teknik, möjliggör programvara som kan kommunicera med företaget oberoende var man befinner sig i världen (Etro, 2009).

Externa leverantörer inverkar ofta på hur väl ett företag eller en organisation lyckas i förändringsarbetet. Under de senaste 10-20 åren har leverantörernas betydelse ökat och detta har gjorts i mycket snabb takt. En av drivkrafterna i denna förändring är ofta kostnadsreduceringar. (Sörqvist, 2004)

Analysföretaget Gartners årliga lista över IT-trender placerar begreppet Cloud Computing, eller moln, på en förstaplats inför 2010 (Gartner, 2010a) jämfört med en sjundeplats 2008 (Gartner, 2007). Termen Cloud Computing syftar både till programvara som levereras som tjänst över Internet och till hårdvaran och systemprogramvaran som tillhandahåller dessa tjänster (Anderson et al, 2008; Armbrust et al, 2009). Enligt Lars Backhans som citeras av Radar Group (2009) är Cloud Computing en mogen teknik. Cooke (2009) menar att fyra av tio program kommer vara i molnet 2011.

Under de senaste åren har samtidigt outsourcingprojekten avseende IT visat röda siffror, 60 procent döms till misslyckande (Affärsvärlden, 2006) och trenden ser ut att hålla i sig: Två år senare skriver Röhne (2008) att nära hälften av alla outsourcingaffärer misslyckas. Ingenting tyder på att siffrorna idag skulle vara annorlunda (Nilsson & Wenell, 2009). Kritiker varnar för att företag, i detta sammanhang, låser sig till en leverantör och skapar ett beroende vilket försvårar möjligheten att byta leverantör längre fram eller att återuppta driften internt (Nilsson & Wenell, 2009; Johnson, 2008).

Samtidigt visar forskning på en ökning av antalet IS/IT-tjänster flyttar ut i molnet under den närmsta treårsperioden (Radar Group, 2009), vilket dels är en direkt effekt av dagens ekonomiska läge (Ernst & Young, 2009; Malmqvist, 2009), dels att man vill öka integreringen med organisationens samlade programvara (Summerville, 2009). En undersökning från Gartner (2009b) visar att nära 60 procent av organisationer och företag i Västeuropa kommer att lägga ut IT och affärsprocessfunktioner under 2009. Omförhandlingar av befintliga avtal kommer öka siffran ytterligare.

Trots dessa farhågorna är det alltså allt fler företag som väljer att flytta ut sin drift och i dagsläget framför allt till molnrelaterade tjänster. Anledning till detta kan vara att dels, som tidigare nämnts, satsa på kärnverksamheten och effekter av det ekonomiska läget, dels att tekniken är mogen. Andra menar dock att tekniken inte kommer vara fullvuxen förrän man enats om en standard (Beizer, 2009).

Ytterligare en anledning kan vara att en organisation vill öka åtkomsten (t.ex. ge personer utanför företaget access) till dem som är berättigade (Summerville, 2009) och en önskan om att minska kostnaderna (Catteddu & Hogben, 2009).

## *Syfte och frågeställning*

Syftet med uppsatsen är utifrån ett IT-perspektiv, att undersöka vad företag och organisationer behöver fokusera på inför en övergång till molntjänster – för att vara väl förberedda och undvika misstag. Studien är även tänkt till att öka medvetandegraden inför molntjänster genom att belysa relevanta riskområden. Denna studies resultat ska utmynna i en överskådlig mall som kan understödja riskbedömningen vid en övergång till molntjänster. Frågeställningen för studien blir således:

- *Vilka områden, med underliggande aspekter bör beaktas inför ett beslut om en övergång?*

## *Disposition*

Nästföljande kapitel, (2) Metod, presenterar det tillvägagångssätt som använts i studien. Vidare presenteras informanterna som ingått i de båda undersökningarna och avslutningsvis ges en begreppsdefinition. Sedan följer kapitlet (3) Förstudie och (4) Teoretisk referensram. Förstudien presenterar de områden som ligger till grund för kapitlet Teoretisk referensram. Detta kapitel följs av (5) Modell som dels presenterar en diskussion av teorin, dels presenterar en undersökningsmall. Kapitel (6) Analys är det som följer i ordning och där analyseras svaren från bedömningen av undersökningsmallen, dessa svar diskuteras i kapitlet (7) Diskussion tillsammans med en empiri-diskussion. Slutligen presenteras studiens resultat i kapitlet (8) Slutsats.

# 2 Metod

*I detta kapitel presenteras studiens tillvägagångssätt. Vidare ges en presentation av informanterna som ingår i undersökningen. Kapitlet avslutas med en begreppsdefinition.*

## *Teoretiskt tillvägagångssätt*

Forskningsmetodik baseras på en av två olika kategorier; den kvalitativa respektive kvantitativa forskningsmetodiken. Med kvalitativt inriktad forskning avses forskning som fokuserar på mjuka data så som kvalitativa intervjuer och tolkande analyser medan kvantitativt inriktad forskning innebär mätningar vid datainsamlingen och statistiska bearbetnings- och analysmetoder. Vilken inriktning som väljs för studien baseras på vilket sätt som väljs för att generera, bearbeta och analysera den information som samlats in för studien. (Patel & Davidson, 2003).

Vid genomförandet av en studie används huvudsakligen två motsatta strategier. Antingen hypotesgenererande, vilket utgörs av en induktiv ansats, eller hypotesprövande, där ansatsen är deduktiv (Backman, 2008). Det deduktiva arbetssättet kännetecknas av att man utifrån allmänna principer och befintliga teorier drar slutsatser om enskilda företeelser medan det induktiva arbetssättet är omvänt och utgår från forskningsobjektet istället utan att först ha formulerat en teori (Patel & Davidson, 2003). Deduktion bygger på logik och induktion på empiri (Thurén, 2007). Vidare presenterar Patel och Davidson (2003) ytterligare en inriktning; abduktion. Det abduktiva arbetssättet kan sägas vara en kombination av induktion och deduktion. Arbetssättet innebär följaktligen att utifrån ett enskilt fall formulera ett hypotetiskt mönster som kan förklara fallet. I nästa steg prövas denna hypotes eller teori på nya fall. Således kännetecknas det första steget i det abduktiva arbetssättet av induktion och det andra steget präglas av deduktion. (Patel & Davidson, 2003)

### Hypotesprövning

Ejvegård (2009) redogör för tillvägagångssättet vid en hypotesprövning. Hypotesen är ett antagande som bygger på kvalificerade gissningar om vissa förhållanden. Att gissningarna är kvalificerade förklarar författaren med att de bygger på kända fakta. Hypoteserna kan vara flera och ett sätt kan vara att falsifiera eller verifiera hypoteserna. Enligt författaren har en hypotes som verifierats övergått till att bli ett faktum.

### Tillförlitlighet

Termerna för en studies tillförlitlighet brukar anges validitet och reliabilitet. Begreppen syftar till att beskriva dels om studien är gjord på ett sätt som är tillförlitligt (reliabilitet), dels att det är rätt område som undersökts (validitet). (Patel & Davidson, 2003)

### Källkritik

När bedömning av information sker måste det först avgöras vad för information det är frågan om. En grov uppdelning av information ger tre kategorier: Den första handlar om fakta som är bevisbara, om inte praktiskt så åtminstone i teorin. Andra kategorin handlar om förklaringar, vilket är betydligt svårare att bedöma. Förklaringar går att utöka genom att det görs en bedömning av trovärdigheten hos dem, vilket beror av vem som står bakom uppgifterna och om de är rimliga. Den tredje kategorin handlar om att bedöma åsikter. Genom att fråga sig om det finns en uppriktighet bakom påståendet och kunskap om vem åsikten riktas åt underlättas förhållningssättet till informationen. I fråga om åsikter är det även viktigt att titta på representativitet; om det är en person eller organisation som står bakom åsikten. (Leth & Thurén, 2000)

Thurén (2005) redogör för de källkritiska principerna. Författaren menar att det kan te sig banalt eftersom principerna är så självklara. Totalt handlar det om fyra kriterier och en distinktion. De fyra kriterierna utgörs av äkthet (källan ska vara vad den utger sig för att vara), tidssamband (ju längre tid det gått mellan en händelse och källans berättelse ju större skäl finns att tvivla på källan), oberoende (källan ska stå för sig själv och inte vara en avskrift eller referat av en annan källa) och tendens (det ska inte finnas skäl att misstänka att källan ligger ger en falsk bild på grund av egenintressen). Utöver detta nämner författaren att en skillnad måste göras på berättelser kontra teknisk bevisning. (Thurén, 2005)

Aspekterna som anges ovan handlar alltså om de grundläggande källkritiska principerna. När källorna hämtas från Internet, finns det behov att ytterligare tillägg. Författarna Leth och Thurén (2000) nämner här att tendens kan utökas med världsbild och kunskapssyn (vilken världsbild har källan) och tillägger begreppen trovärdighet (är källan trovärdig) samt förutsättningar och egenskaper för källan.

Vid informationsinsamlingen i denna studie förekommer i vissa fall privata aktörer som avsändare. När en person eller organisation med vinstintressen ligger bakom en rapport går det inte att utesluta ett egenintresse eller att källan är partisk eller bådadera.

## Val av metod

Denna studie tillämpar den kvalitativa metoden eftersom empirin bygger på mjuka data och tolkande analyser. Vidare tillämpas såväl den hypotesgenererande som hypotesprövande ansatsen vilket innebär att en abduktiv inriktning tillämpas.

Patel och Davidson (2003) menar att fördelen med det abduktiva arbetssättet är att det inte låser forskaren i så hög grad vilket kan bli fallet vid ett arbete som strikt tillämpar ett deduktivt eller induktivt arbetssätt.

## *Genomförande*

Den teoriskapande undersökningen i denna studie genomgick två faser där den första fasen handlade om att ta fram intervjufrågor inom studieområdet (Appendix I). Frågorna behandlade respondenternas respektive erfarenheter inom området Cloud computing, och om medias rapportering påverkat deras syn på detta. Vidare ställdes frågor om respondenterna tidigare kommit i kontakt med molntjänster i sitt yrke. Totalt utgjordes enkäten av åtta frågor av allmän karaktär. Parallellt med att intervjuunderlaget togs fram valdes personer som kunde ingå i undersökningen. Detta gjordes genom att en första förfrågan skickades till personer med kontakter inom IT-området, för att få rekommendationer till personer som skulle passa in på studien. De personer som efterfrågades av personer med relativt bred kunskap inom IT utifrån ett organisationsperspektiv. Förstudien kan liknas vid området för induktion eftersom teorin skapas utifrån enskilda fall (Patel & Davidson, 2003).

## *Praktiskt Tillvägagångssätt*

Det praktiska tillvägagångssättet för studien baseras på två intervjuomgångar som skickats ut via e-post vid två olika tillfällen. Det första tillfället utgör förstudien och har föranlett de aspekter som senare kommit att granskas i det teoretiska ramverket.

Berg (2007) beskriver svårigheterna med att boka in intervjuer, dels ur en tidsaspekt, dels beroende på distansförhållanden mellan personerna. Författaren framhåller e-post som ett alternativ för att undvika svårigheterna. Ytterligare en fördel som Berg (2007) anger för e-postintervjun är att den på ett effektivt sätt är privat. Ingen annan än mottagaren kan ta del i, lägga till, ta bort eller avbryta ordväxlingen. Författaren pekar även på svårigheterna med e-postintervjuer. Här menar Berg (2007) att det är svårt att genomföra kvalitativa intervjuer via e-post och att respondenten måste ha tillgång till såväl dator med Internetuppkoppling och ett e-postkonto vilket får medhåll av Svenningsson et al. (2003).

Svenningsson et al. (2003) menar att e-postintervjuer utgör asynkrona arenor, vilket går att likna vid skrifter till skillnad mot synkrona arenor som syftar till tal. Således utgör e-postintervjun skillnader gentemot den mer traditionella intervjun. E-postintervjuer har både för- och nackdelar enligt författarna. Genom att väga bristerna mot fördelarna i varje enskild studie går det att se vilka egenskaper som är viktigast för den individuella intervjun.

I denna studie föll valet på e-postintervjuer vid båda intervjutillfällena. Det som talade för var bland annat det asynkrona, där respondenterna själva kunde avgöra vid vilken tid de ville svara. Att inte ta för mycket tid i anspråk av respondenterna talade också för en e-postintervju. Dessutom kunde respondenterna, efter att de tagit del av frågorna, avgöra om de kunde bidra med något svar. Det som talade emot var framför allt att svaren baserades på respondenternas möjligheter att uttrycka sig i

skrift samt minskad möjlighet att ställa följdfrågor. Eftersom det första intervjutillfället handlade om att få en mer allmän bild av branschens kunskap i ämnet var det inte aktuellt med följdfrågor och respondenternas möjligheter att uttrycka sig i skrift kunde antas vara på en acceptabel nivå då deras marknadspositioner talar för en vana vid rapportering.

Vid det andra intervjutillfället valdes återigen e-postintervjun, som tidigare nämnts som metod. Detta eftersom vissa av de personer som sa sig vara villiga att utvärdera riskområdena var verksamma på olika orter, vitt skilda i landet. Samtidigt handlade det om en bedömning och en traditionell intervju skulle i detta fall ha kunnat vägleda respondenten. Även denna gång antogs att respondenternas förmåga att uttrycka sig i skrift var på en god nivå.

## Informanter i förstudien

Personerna som ingått i förstudien är alla verksamma inom området för IT eller i dess direkta närhet och kommer från spridda verksamheter inom såväl offentlig sektor som i det privata näringslivet. Alltifrån beslutsfattare, konsulter och anställda med visst områdesansvar till yrkesverksamma förekommer i förstudien. Totalt återkom åtta respondenter som med svar på frågorna, av sammanlagt sjutton förfrågningar. Vissa av personerna som inte svarade på frågorna menade att de inte kunde någonting om ämnet och därför valde att inte svara, medan andra helt uteblev med svar när de fått se frågorna. Frågorna utgick i två omgångar. Vid första tillfällen skickades ett generellt meddelande, innehållande frågorna, till ett större antal tänkta respondenter. Vid det senare tillfället skickades frågorna ut enkom till respektive respondent.

## Informanter i undersökningen

De personer som ingick i undersökningens andra fas, det vill säga de som kom att kommentera mallen, valdes utifrån sin erfarenhet och förkunskap. Målet var att hitta respondenter som hade erfarenhet av liknande bedömningsåtaganden i sin yrkesroll. I ett första skede kontaktades sju personer inom offentlig sektor. En av kontakterna förmedlades via en informationsansvarig, två kontakter togs direkt med aktuella personer och de resterande kontakterna förmedlades via en av de direkt tillfrågade ovan. Av de personer som kontaktats inom offentlig verksamhet svarade sex personer att de kunde ställa upp.

För att öka studiens reliabilitet kontaktades även totalt fyra personer verksamma inom det privata näringslivet. Av dessa återkom en person. Kontakten med personerna i det privata näringslivet togs i tre av fyra fall via en informationsansvarig som ombads vidarebefordra förfrågan till annan lämplig person. Ingen av dessa återkom med svar.

Utskicket innehöll dels en kort presentation av ämnesområdet, och två frågor, där den första frågan hade följdfrågor (Appendix II), dels bifogades undersökningsmallen och en sammanfattning som

förklarade respektive riskområde. En av personerna återkom inom kort och sa sig vara osäker på vad som avsågs med frågorna. Således gjordes en tydligare förfrågan som distribuerades till alla som sagt sig kunna svara. Totalt återkom fyra personer med svar efter att de fått ta del av modellen.

## *Definitioner*

Begrepp som förekommer i studien och inte kan anses vara av generell karaktär presenteras nedan. Först definieras vad som i studien avses med Cloud computing vilket följs av en definition av andra förekommande begrepp.

### Cloud computing

Termen cloud, eller svenskans moln, har historiskt använts som en metafor för Internet. Denna användning av begreppet härstammar ursprungligen från en gemensam skildring av nätverksdiagram som ett moln som använts för att representera transporten av data över ett nät till en slutpunkt på andra sidan molnet. Illustrationer av detta som ett moln har gjorts sedan början av 1960-talet (Rittinghouse & Ransome, 2009).

Enligt Google Trends (2010), som sammanställer information om sökord och söktermer och presenterar detta i en trendgraf, har Cloud computing använts som begrepp sedan slutet av 2007. Begreppet är vida omtvistat och betydelsen är inte helt självklar. Armbrust et al. (2009) förklarar att Cloud computing både avser tillämpningar som levereras som tjänster över Internet och den maskin och programvara i datacenter som tillhandahåller dessa tjänster. Catteddu och Hogben (2009) menar att det inte alls handlar om en teknik, utan att Cloud computing är ett nytt sätt att leverera dataresurser. En teknik eller inte – flera menar att idéerna är gamla, men att det först nu finns möjlighet till ett genomförande (Armbrust et al., 2009; Dikaiakos et al., 2009). Ett exempel på definition är den som Foster et al. (2008) presenterar:

> *”A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the internet”* (Foster et al., 2008:1)

Den mer vedertagna definitionen av begreppet Cloud computing är den som presenterats av NIST, National Institute of Standards and Technology. Författarna Mell och Grance (2009) är de som står bakom rapporten och författarna menar att Cloud computing är ett såpass ungt begrepp att det antagligen kommen ändra betydelse över tiden, och att deras definition beskriver en övergripande bild som ska omfatta hela området.

Modellen som Mell och Grance (2009) ger bygger på fem väsentliga egenskaper, tre tjänstemodeller och fyra molntyper. De fem egenskaperna utgörs av On-demand self-service, Broad network access, Resource pooling, Rapid elasticity samt Measured Service. Tjänstemodellerna utgörs av Infrastructure-as-a-Service, IaaS, Platform-as-a-Service, PaaS, och Software-as-a-Service, SaaS. De fyra olika molntyper som presenteras av Mell och Grance (2009) är Publika, Privata, Gemensamma och Hybrida moln.

## Egenskaper

Enligt Mell och Grance (2009) rapport går det att urskilja fem väsentliga egenskaper för molntjänster:

**Självbetjäning on-demand** (On-demand self-service), handlar om att det är beställaren som bestämmer omfattning av den datorkapacitet som ska användas. Detta kan handla om servertid, lagring via nätverk som styrs automatiskt efter beställarens behov av att inte ha mänsklig inblandning.

**Bred nätverksaccess** (Broad network access), utgörs av att funktioner är tillgängliga via nätet och nås via standardmekanismer. Dessa främjar i sin tur användningen av olika klienter, vilket kan utgöras av olika plattformar så som mobiltelefoner, bärbara datorer et cetera.

**Sammanslagning av resurser** (Resource pooling), handlar om att leverantörens samtliga datorresurser slås samman för att på så sätt kunna tjäna flera användargrupper som använder sig av samma leverantör men med olika fysiska, såväl som virtuella resurser. Resurserna tilldelas dynamiskt till respektive användargrupp och omfördelas beroende på efterfrågan. Resurserna handlar i detta fall om lagring, exekvering, trafikmängd, minne et cetera.

**Snabb elasticitet** (Rapid elasticity), utgörs av möjligheten av tänjbarhet. Genom att snabbt kunna ändra omfång, i vissa fall automatiskt för att kunna ge användaren möjlighet till – i stort sett – obegränsade resurser, oavsett mängd, när som helst.

**Uppmätt service** (Measured service), i molntjänster erbjuds möjligheten att automatiskt mäta och kontrollera nyttjandet av tjänsterna på olika nivåer. Vilket kan handla om lagring, exekvering och bandbredd et cetera och hur dessa övervakas, kontrolleras och anges av både leverantör och användare.

## Tjänstemodeller

Inom ramen för Cloud computing presenteras vanlig tre olika tjänstemodeller (bl.a. Briscoe & Marinos, 2009; Mell & Grance, 2009). Vissa utökar modellerna för att ge en tydligare bild av något enskilt fenomen (bl.a. Rittinghouse & Ransome, 2009; Stanoevska-Slabeva et al., 2009), men i stort ingår redan dessa enskilda områden i de mer övergripande modellerna.

**Software-as-a-Service**, SaaS eller mjukvara som tjänst, ger konsumenten (beställaren) möjlighet att använda leverantörers program som erbjuds via molninfrastruktur. Applikationerna ges åtkomst från olika enheter via ett mindre program, t.ex. en webbläsare. Beställaren ansvarar inte för den underliggande infrastrukturen med nätverk, servrar, operativsystem och lagring eller individuella applikationer med undantag för vissa användarspecifika program och konfigurationsinställningar. (Mell & Grance, 2009)

**Platform-as-a-Service**, PaaS eller tjänsteplattform tillåter beställaren att skapa egna applikationer för molninfrastrukturen, via programmeringsspråk och verktyg som tillhandahålls utav leverantören. Kunden har inte möjlighet att administrera den underliggande infrastrukturen men har kontroll över sina egenutvecklade applikationer och möjlighet till vissa konfigurationsinställningar. (Mell & Grance, 2009)

**Infrastructure-as-a-Service**, IaaS eller Infrastruktur som tjänst, beskriver ett område där användaren kontrollerar bearbetning, lagringsutrymme, nätverk och andra grundläggande dataresurser. Användaren har möjlighet att utveckla och köra egen mjukvara vilket kan utgöra både operationssystem och applikationer. Möjlighet att administrera den underliggande infrastrukturen ges dock inte till användaren, däremot har de kontroll över operationssystem, lagringsutrymme, utvecklade applikationer, och möjlighet att välja vissa nätverkskomponenter som brandväggar och liknande. (Mell & Grance, 2009)

## Molntyper

I litteraturen förekommer olika typer av moln. Framför allt handlar det om publika och privata moln, där det publika karakteriseras av att det ägs och drivs av tredje part eller leverantörer via Internet och tjänster erbjuds genom att användaren (externa kunder) betalar för det som används. Det privatägs och drivs istället av den egna organisationen (interna kunder) och är då inte publikt nåbart. (bl.a. Armbrust et al., 2009; Smith et al., 2010; Srinivasa et al., 2009)

Det bör noteras att det finns leverantörer som erbjuder sina privata moln till externa användare vilket gör att dessa privata moln, beroende på synsätt, kan anta ett privat alternativ med en publik skepnad. Samtidigt finns det andra leverantörer som enbart utvecklar och erbjuder molntjänster för ett publikt moln. Vanligtvis är det större organisationer och storföretag som oftast väljer att använda privata moln, medan mindre företag och konsumenter väljer de publika. (Motahari-Nezhad et al., 2009)

Gemenskapsmoln, community cloud, avser en molninfrastruktur som delas av flera olika organisationer och baseras på speciella krav (Mell & Grance, 2009; Sriram & Khajeh-Hosseini,

2010). Förvaltningen sker antingen av organisationerna själva eller av tredje part och infrastrukturen finns tillgänglig antingen lokalt eller publikt. (Mell & Grance, 2009)

Hybrida moln, vilka syftar till en kombination av publika tjänser och privata IT-tjänster som antingen utgörs av lokala molnapplikationer eller mer klassiska IT-tjänster (Smith et al., 2009). Moln-infrastrukturen bygger på sammansättningen av två eller flera moln, där varje moln kan vara publikt, privat eller ett gemenskapsmoln, har den egenskapen att alla enheter förblir unika men är sammanfogade med standardiserad eller patenterad teknik som ger en portabel möjlighet för data och tillämpningar. (Mell & Grance, 2009)

## Övriga begrepp

Nedan redogörs för mer allmängiltiga begrepp. Begreppen används inte exklusivt för molntjänster, men i litteraturen för området har de en stor betydelse, vilket motiverar en djupare definition för studiens kontext.

### Application Programming Interface

Application Programming Interface, eller API, utgör en regeluppsättning som möjliggör funktioner som används vid applikationsutveckling. Det kan handla om proxytjänster, innehåll och filtrering av skräppost, webbläsarens cacheminne, registrering av användare, godkännande, lösenordshantering för säkrare inloggning et cetera. (Sloan, 2009)

### Cross Site Scripting

Cross site scripting, XSS, handlar om att en angripare hittar felaktigheter i en webbplats kommunikation via webbservern och utnyttja detta. XSS kan inträffa när dynamiskt genererade webb-sidor visas och en angripare kan således utnyttja denna svaghet och kan via genereringen exekvera ett injicerat skript i webbläsaren via serverns privilegier. (Wassermann & Su, 2008)

### Malware

Malware står för malicious software, vilket kan översättas som illasinnad mjukvara och är samlingsnamnet på sabotageprogram som utgörs av trojaner, virus och liknande. Malware utnyttjar brister i andra datorprogram och kan via dessa bädda in dolda funktioner. (Christodorescu et al., 2005)

### Service Level Agreement

Service Level Agreement, SLA, är ett avtal eller en överenskommelse om servicenivå. Detta avtal används för att reglera en avtalad servicenivå och utgör en överrenskommelse mellan beställare och leverantör med gemensamma ansvarsområden. Avtalet garanterar att tjänstens kvalitet uppfyller överrenskomna krav. (van Bon et al., 2008)

# 3 Förstudie

*Förstudien utgjorde grunden för den fortsatta studien och det är informationen från denna som varit vägledande under studiens utveckling.*

## Studieområde

De aspekter som studien beaktar utgår från de svar som inkom på frågorna (Appendix I) vid förstudien. Av dessa svar gick det framför allt att utläsa tre områden, vilka även fått utgöra huvuddragen för studien. Vid en närmare granskning av svaren visade det sig att varje område kunde delas upp i ytterligare undergrupperingar – här kallat aspekter. Uppdelningen i matrisen bygger således på tolkningar av det empiriska undersökningsmaterialet (Tabell I).

| | TEKNISKA | | | EKONOMISKA | | ORGANISATORISKA | | |
|---|---|---|---|---|---|---|---|---|
| | Säkerhet | Sociotekniska | Tekniska | Verksamhet | Teknik | Juridiska | Politiska | Sociala |
| 1 | x | | x | x | x | x | | |
| 2 | x | x | | x | x | x | | x |
| 3 | x | | x | x | x | | | x |
| 4 | | | x | | | x | | |
| 5 | x | | | x | x | x | x | |
| 6 | x | | x | x | x | | | x |
| 7 | x | | x | | | x | x | |
| 8 | x | | | | | x | | x |

**Tabell I:** Översikt av studieområde

Siffrorna i vänsterkolumnen beskriver respondenterna. Översta raden innehåller de tre huvudområdena medan aspekterna presenteras i raden under. Kryssen visar vilken aspekt som respondentens svar har bedömts motsvara.

Det går dock inte att utesluta att medias rapportering kan ha färgat svaren i enkäten. Begreppet Cloud computing har som tidigare visats använts mer eller mindre sedan sista kvartalet av 2007 (Google Trends, 2010). I media började begreppet få sitt riktigt stora genomslag under 2008 och då även i Sverige. Sveriges största dagstidning med fokus på IT, Computer Sweden, ger vid en sökning på begreppet ”cloud computing” inom tidsspannet första oktober 2007 till femte maj 2010 totalt 133 träffar inom alla kategorier och ”cloud” totalt 223 under samma period. Begreppet ”moln” genererar totalt 165 träffar och i bestämd form, ”molnet”, totalt 385 träffar. Eftersom alla fyra begreppen förekommer såväl var för sig som tillsammans är det svårt att utesluta att vissa av träffarna vid respektive sökning inte avser samma artikel. Det som sökningen däremot visar är att begreppet har förekommit relativt ofta under denna tid och personer som någon gång läser denna tidning, i pappersformat eller på Internet bör därför ha stött på artiklar i ämnet vid flera tillfällen.

Enligt IDG Media (2010), det företag som har hand om annonsförsäljningen för Computer Sweden, är detta i särklass Sveriges största tidning för IT-nyheter. De läsargrupper som är typiska för tidningen är IT-chefer, CIO:er, IT-strateger, affärsområdeschefer, utvecklare, IT-projektledare och konsulter. (IDG Media, 2010)

Mycket av rapporteringen från media i ämnet går att dela upp i framför allt två huvudspår. Dels handlar det om kritikerna, där fokus utgörs av säkerhetsaspekter och inlåsning (bl.a. Catteddu & Hogben, 2009), dels förespråkarna som i första hand framför de ekonomiska fördelarna (bl.a. Khajeh-Hosseini et al., 2010; Summerville, 2009). Svaren från enkäten visar även de att näst intill alla nämnde säkerhet, teknik och juridik (inlåsning kan ske både i teknik och i juridisk mening). Vidare handlar många av svaren om ekonomi.

# 4 Teoretisk referensram

*I detta kapitel presenteras den teori som ligger till grund för studien. Teorin behandlar de områden med underliggande aspekter som framkommit i förstudien.*

## *Området för teknik*

Ett av de huvudområden som framkom vid förstudien är området teknik. Inom detta område samlas samtliga aspekter av direkt teknisk karaktär samt aspekter med stark koppling till teknik.

### Säkerhet

Säkerhet är en av de aspekter inom området teknik som är flitigast diskuterade inom ämnet. Detta beror dels på att säkerheten är avgörande för att molntjänster ska fungera, dels på att detta är ett område som är allmänt bekant och lätt att ta till sig. Det senare kan anta ha betydelse när kritiker väljer områden att anmärka på. Att säkerheten är en avgörande faktor vid lagring, kommunikation och liknande är elementärt. Inom molntjänstområdet finns det de som pekar på att säkerheten inte alls är något problem (Miller, 2009) utan att säkerheten där har en annan struktur (Miller, 2009; Walsh & Hayes, 2010). Armbrust et al. (2009) menar att det inte finns några direkta hinder för att säkerheten inte skulle kunna vara lika bra som den är för lokala IT-miljöer. Dessa hinder skulle gå att klara av med välkända lösningar där Armbrust et al. (2009) nämner kryptering som en möjlighet. Vidare redogör författarna för att om informationen är krypterad innan den läggs ut i molnet blir resultatet faktiskt säkrare än vid normal lagring. Catteddu och Hogben (2009) menar att säkerhetslösningar i molntjänster både blir billigare och effektivare i och med storskaligheten. Khajeh-Hosseini et al. (2010a) menar att flera säkerhetsrisker har funnits länge och inte alls är unika för molnet. Författarna redogör för att attacker som sker i molnet faktiskt kan vara mindre allvarliga än liknande attacker som sker direkt mot företagets interna system. Vidare menar författarna att en annan säkerhetsrisk kan finnas vid organisatorisk kontroll (se socioteknik) när ett företag tillämpar hybrida moln. Khajeh-Hosseini et al. (2010a) framhåller ett exempel med en länk i ett dokument till en webbplats som är blockerad i det lokala molnet, men som är nåbar via dokument placerade i det publika. Innehåller webbplatsen som länken pekar mot malware är detta en uppenbar säkerhetsrisk.

Walsh och Hayes (2010) menar att traditionellt skyddas information med flera lager av brandväggar. Svagheten med detta system är att om malware eller någon obehörig lyckas komma igenom ges det full access till informationen. Författarna använder i ett exempel företaget Amazons moln och förklarar att där används inte brandväggar, utan informationen är istället utspridd på flera olika servrar i Amazons moln. Detta gör att ett eventuellt angrepp bara når en del av systemet eftersom trafiken mellan servrarna i Amazons moln är osynlig, så finns det enligt författarna inte heller någon risk till spionage. Khajeh-Hosseini et al. (2010a) menar att säkerhetsriskerna till största del handlar om användares brist i kontroll över den fysiska infrastrukturen.

Heiser (2010) menar att de absolut största riskerna, inom tjänstemodellerna SaaS, PaaS och IaaS utgörs av Extensibility (utökning), Accessibility (tillgänglighet) och Complexity (komplexitet). Det författaren menar handlar om utökning beskriver till vilken grad ny kod kan kopplas till ett system och menar att alla moderna datamiljöer har någon form av utbyggbarhet. Heiser (2010) drar en parallell till operativsystem och menar att dessa lätt accepterar ny kod som exempelvis drivrutiner eller liknande. Det samma menar författaren gäller flera olika webbläsare som idag accepterar nästan ett oändligt antal med insticksprogram. Dock är flera av dessa insticksprogram osäkra och kan ses som ett inträde till datorns skrivbord.

Vidare menar Heiser (2010) att tillgängligheten skapar problem med attacker. Författaren menar att en fristående arbetsstation i ett låst rum är relativt otillgänglig för attacker medan tjänster som erbjuds via Internet, speciellt de som riktas till konsumenter, har helt andra krav och måste kunna motstå alla typer av angripningsförsök. Tillgängligheten på Internet baseras på lyssnande portar, typer av tjänster som lyssnar på dessa portar och antalet IP-adresser som betjänar de portar som blir avlyssnade. Internettillgängligheten avser således graden av exponering för vanliga såväl som privilegierade användare. Heiser (2010) menar att ju större tillgång en systemadministratör har ju lättare kan denna stjäla data eller sabotera system.  Så ju större graden är av administrativ tillgång, ju mer arbete behövs för att granska och övervaka administratörer och att följa deras verksamhet.

Komplexiteten enligt Heiser (2010) beskriver mängden kod och krångligheten i datormiljöer. Författaren menar att det finns ett beroende mellan antalet rader kod och sårbarhetseffekten. Komplexitet kan även leda till framväxande sårbarheter som i sig beror på ett resultat av oförutsedda interaktioner mellan funktioner som ensamma kan anses vara fullgott säkra. Författaren nämner SQL-injektioner som en form av sårbarhet som via en tjänst eller webbserver kan leda till en attack mot en närstående tjänst eller databas som annars är skyddad mot angrepp. En annan form av utsatthet är Cross site scripting, (XSS) som har möjliggjorts på grund av oförutsedda interaktioner mellan fristående funktioner som i stort fungerar som ett komplext system. Elasticitet och skalbarhet tillhandahålls av distribuerade och virtuella plattformar som sammanfattas av komplexiteten vilket bara ökar effekterna och komplexiteten av molntjänster enligt Heiser (2010).

## Teknisk inlåsning

Hanseth och Lyytinen (2004) förklarar att begreppet teknisk inlåsning används för att beskriva den situation en organisation befinner sig i när infrastrukturen eller befintliga system inte längre är kompatibelt med aktuella standarder och den senaste tekniken. Möjligheten att anpassa sig blir då både komplicerad och kostnadskrävande. Vidare menar författarna att teknisk inlåsning även kan utvecklas av att en organisation väljer att använda system som bygger på en speciell standard vilket leder till att mer och mer av organisationens system anpassas efter den valda standarden. Om det

längre fram visar sig att valet var misslyckat är utsikterna varken ekonomiskt hållbara och i värsta fall inte ens praktiskt möjligt att senare övergå till en annan standard.

Inlåsningen kan te sig olika beroende på vilken tjänstemodell som används. För SaaS handlar inlåsningen om kundernas anpassning till leverantören. Inlåsningen är inte specifik för molnet och kan ske antingen genom att leverantören skapar applikationer som passar målgruppen eller om att kunden skapar applikationer och skräddarsyr dessa för att fungera till det API som leverantören erbjuder. Detta kan dels skapa problem om kunden har en väldigt stor användarbas, dels att applikationerna, vid ett eventuellt byte av leverantör, måste göras om. (Catteddu & Hogben, 2009)

Inlåsningar för PaaS sker både via API-anrop och på komponentnivå. Leverantören kan erbjuda lagringsmöjligheter back-end och beställaren måste således utveckla programvara för att kunna kommunicera med lagringen. Denna programvara behöver nödvändigtvis inte vara flyttbar mellan olika leverantörer. Inlåsningseffekterna ligger helt och hållet på beställaren. (Catteddu & Hogben, 2009)

Inlåsning för IaaS utgörs av en än mer komplex struktur och varierar beroende på vilken specifik infrastrukturtjänst som avses. Bristen på öppna standarder gör migrering till andra leverantörer komplicerad (Catteddu & Hogben, 2009). Detta får medhålla av Nilsson och Wenell (2009) som menar att standarder minskar risken för inlåsning, men att kunden annars måste motivera en viss inlåsning med att de låga löpande kostnaderna uppväger inlåsningseffekterna. Enligt författarna är det också viktigt för beställaren att fritt kunna välja leverantör när leverantörsavtalet löper ut.

Stanoevska-Slabeva och Wozniak (2010) nämner problemet med inlåsning och standarder och menar att eftersom det i dagsläget inte finns några standarder för varken för IaaS, Paas eller SaaS-gränssnitt blir valet av såväl leverantörer som investeringar i molnintegration riskabelt. Detta kan enligt författarna i sin tur leda till en stark inlåsningseffekt, till fördel för leverantören men som kan vara förödande för användaren. Resonemanget får medhåll av bl.a. Dikaiakos et al. (2009) som menar att en av de stora utmaningarna med molnet blir att bygga nya standarder för att öka såväl flexibiliteten som virtualiseringsgraden. Författarna nämner att det pågår diskussioner om att skapa öppna standarder för detta.

## Standarder

Stango (2004) redogör för vad som avses med standarder och menar att standarder framför allt bygger på två egenskaper; sponsrade eller icke-sponsrade standarder. Standarderna kan samtidigt förekomma som bland annat de facto- eller de jure-standarder. Sponsrade standarder har en ägare som således också är den som har möjlighet att påverka standarden. De facto-standarder karakteriseras av en standardtyp med ett brett stöd på marknaden, samtidigt som standarden inte bygger på några

överenskommelser eller annan rättsgrund (Hanseth & Monteiro, 1997). Liebowitz och Margolis (1996) visar som exempel på De facto-standarden de båda tangentbordsmodellerna QWERTY (namnet kommer från översta raden på ett vanligt tangentbord) och Dvorak (Namngivet efter upphovsmannen). I sin linda förekom det ofta att tangenterna på skrivmaskinerna fastnade när det skrevs för snabbt. För att undvika detta placerades tecknen i en ordning så att de som vid skrivning oftast hamnade bredvid varandra placerades så lång isär som möjligt. Under mitten av 1930-talet presenterades en ny utformning av tangentbordet, Dvorak, som sägs vara 20 % effektivare än dess föregångare QWERTY. Trots Dvoraks överlägsenhet är det enbart ett fåtal som använder denna uppsättning i dagsläget och QWERTY-modellen, som är den absolut vanligaste idag, är den som blivit standard (Allen & Sriram, 2000). QWERTY-tangentbordet är ett exempel på hur de facto-standarden kan bidra till att motverka innovation. Vidare framhåller Liebowitz och Margolis (1996) att Dvorak var en patenterad teknik vilket kan ha bidragit till minskat genomslag.

Motsatsen till en De facto-standard, är det som brukar kallas enbart standard, industristandard eller de jure-standard. Alltså en standar som bygger på överrenskommelser eller liknande. Blatt (1999) menar att de jure-standarder skapar en miljö som gynnar alla involverade, från tillverkare till slutanvändare. Standardisering bidrar även till en slags gemenskap där utvecklingsfrihet råder vilket skapar nya innovationer och förbättringar. (Blatt, 1999; Allen & Sriram, 2000)

Enligt SIS (2010) väcker nya begrepp behov av standardisering. Att ett begrepp är nytt medför ofta att det saknas en överenskommen terminologi och det är viktigt att beställare förstår leverantörer och vice versa. Vidare nämns att gemensamma standarder underlättar vid upphandling och användning av molntjänster, och minskar risken för problem med säkerhet, juridik och interoperabilitet. Inom IT-infrastrukturen framhäver Sirkemaa (2002) vikten av standarder och menar att standarder gör det möjligt att få en flexibel infrastruktur.

Rönnbäck et al. (2006) problematiserar kring standarder. Visserligen menar författarna att standardisering i samband med infrastruktur är den enda hållbara alternativet, och menar att motsatsen som bygger på ömsesidiga avtal snabbt blir både tidskrävande, kostsam och ohanterlig för större nätverk att samordna. Samtidigt menar författarna att standardisering inte är en rättfram process. Detta då universella standarder bara är så i abstrakt mening, avlägsnade från användning i praktiken. När standarder implementeras och vävs in i lokala miljöer blir standarderna istället unika och icke-universella. Författarna förklarar att standarder därför inte kan användas för att skapa ordning på det sätt som vanligtvis anses. Istället kan ordning bara skapas lokalt, från ett unikt perspektiv, vilket leder till att ordning ur ett perspektiv utgör oordning i ett annat.

Vidare menar Rönnbäck et al. (2006) att den lokala anpassningen till trots finns vissa universella aspekter kvar. Författarna skriver att standarderna kan vara lokala och universella på samma gång.

Standarder minskar således oordningen men kan inte användas för att förhindra inkompatibilitet och redundans. Detta menar författarna måste göras på annat sätt; genom gateways, ad hoc-patchar, överlappning eller liknande får accepteras. Fokus bör istället läggas på att hitta nya sätt att hantera oordning.

Dikaiakos et al. (2009) nämner att det finns intressen för att ta fram öppna standarder för cloud computing. En sådan intressegrupp är, Open Cloud Manifesto (2009), som har tagit fram sex principer för detta ändamål, vilka är: (1) Leverantörer av molntjänster måste samarbeta. (2) Leverantörerna ska inte använda sin marknadsposition för att skapa inlåsningar. (3) Leverantörerna måste använda befintliga standarder där det är möjligt och framhåller att IT-industrin redan satsat enorma summor på att arbeta fram standarder och därför finns det ingen anledning att göra om samma jobb. (4) I de fall när det handlar om att arbeta fram nya standarder, eller vid en modifiering av befintliga måste detta ske med förnuft och vara pragmatisk för att undvika allt för många standarder. Eftersom standarder ska främja innovation, inte stjälpa densamma. (5) Det är kundernas behov som ska styra arbetet med öppna moln, inte bara leverantörernas tekniska behov av att testas eller verifieras mot verkliga kundbehov. Som sista punkt står att (6) standardiseringsorganisationer, intressegrupper och sammanslutningar ska verka tillsammans och vara samordnade så att insatserna inte står i konflikt med eller överlappar varandra.

Beizer (2009) förklarar att det är standarder som möjliggör spridningen av teknik och genom användningen av vedertagna standarder blir effekten en leverantörskonkurrens som kan leda till lägre priser och minskad inlåsning.

## Socioteknik

Den sociotekniska aspekten utgör ett område som är mindre diskuterat i litteraturen men inte mindre relevant. Summerville (2009) problematiserar kring fyra olika sociotekniska områden. Författaren nämner tekniska faktorer, omständigheter som beror på mänskliga faktorn, situationer som orsakas av att organisatorisk kontroll samt förhållanden som är baserade på uppdateringar hos leverantören.

De områden som Summerville (2009) nämner bygger på författarens tanke om varför en organisation väljer att gå över till molntjänster och det är detta som ligger till grund för antagandet. Summerville (2009) summerar möjliga antaganden för att en organisation väljer att använda molntjänster. Det första antagandet handlar om att organisationen är intresserad av att underlätta samarbetet och användningen av mobila enheter och därför ser möjlighet att använda sig utav vanliga kontrosprogram så som e-postklient och ordbehandlingsprogram i molnet istället.

## Allmänt tekniska

Utöver säkerhet och närliggande områden finns det andra aspekter av teknisk karaktär som även de kan utgöra riskmoment. Graham-Rowe (2009) framhåller problematiken med datamängder som ska färdas långa sträckor såväl geografiskt som antalet nätverksnoder som informationen måste passera. Detta kan ställa till problem för tillexempel ett företag i USA som lagrar information på servrar i Indien. Problemet är enligt författaren teknikbaserat, en teknik som idag använder TCP, ett protokoll för överföring och en av Internets mer centrala funktioner. Whitaker (2010) visar på ytterligare svårigheter och menar att det för vissa organisationer ibland annat USA och Europa faktiskt inte är tillåtet att lagra data utanför respektive geografiskt område, där det geografiska området kan begränsas till ett land eller union.

# *Området för ekonomi*

Mycket av fördelarna som diskuteras med molntjänster är just av ekonomisk karaktär (bl.a. Ailamaki et al., 2009; Arbrust et al., 2009; Etro 2009). Dels eftersom företag som migrerar till molnen (helt eller delvis) i teorin kan avveckla, eller i alla fall kraftigt reducera, sin IT-avdelning eftersom support och uppdateringar till stor del hamnar hos tredje part (Khajeh-Hosseini et al. 2010b; Whitaker, 2010), dels eftersom användaren bara behöver betala för det som verkligen används. Etro (2009) framhåller att startkostnaderna är något som blir lägre. Det ekonomiska området går således att bryta ner i två olika aspekter; antingen med fokus på organisation eller med fokus på teknik. De ekonomiska aspekterna varierar något beroende på vilka molntyper som avses (Srinivasa et al., 2009).

### Tekniskt perspektiv

Det tekniska perspektivet möjliggör mer avancerad teknik för samma pris och att initiala kostnader antingen uteblir helt och hållet eller blir väldigt låga (Miller, 2009). Organisationer kan få möjlighet till mer avancerade och en större mängd applikationer till ett lägre pris (Summerville, 2009).

### Organisatoriskt perspektiv

Att bara betala för den faktiska användningen är som tidigare nämnts ett av de områden som är lätta att kommunicera inom organisationen och möjlighet att hyra infrastruktur är en annan. (Armburst et al., 2009)

Det ekonomiska värdet blir enligt Carr (2003) mycket högre om teknisk infrastruktur kan användas av flera aktörer än att bara vara isolerad inom en organisation. Vidare presenterar Carr (2003) en modell för hur IT-investeringar bör gå tillväga för att undvika misslyckanden. Dessa områden handlar om att **spendera mindre**, då studier visar att de organisationer med högst budget för IT-investeringar sällan är de som visar bästa finansiella resultat. Andra punkten handlar om att **Följa, inte leda**, Carr (2003) hänvisar till Moores lag och menar att ju längre en organisation väntar med en IT-investering, ju mer

får organisationen för pengarna. Slutligen menar författaren att en organisation ska **lägga fokus på sårbarhet framför möjligheter**.

### Systeminvestering

Vid investeringar i informationssystem (IS) i allmänhet handlar det ofta om två huvudområden. Dessa är mjukvara och hårdvara. Definitionen av de olika huvudområdena kan skilja sig åt, men principen är den samma. Med kostnader i mjukvara avses t.ex. utvecklingskostnader, kostnader för operations-system, kostnader för programlicenser, kostnader för databaser samt ordbehandlingsprogram. För kostnader i hårdvara avses t.ex. tangentbord, bildskärmar, skrivare, kablage, routrar och servrar. (Boddy et al., 2002)

Om en organisation väljer att flytta hela, eller delar av sin databehandling till molnet bör den ekonomiska aspekten även inkludera ökad nätverkstrafik mellan organisationen och molnleverantören (Internet). Enligt (Leavitt, 2009) är detta en kostnad som ofta glöms då fokus istället ligger på besparingar som kan göras inom annan hårdvara och mjukvara.

### Teknikinvestering

Några av de stora ekonomiska fördelarna med molntjänster, förutom att bara betala för den faktiska användningen (bl.a. Arbrust et al., 2009; Avetisyan et al., 2010; Leadbeater, 2010), är att initiala kostnader är väldigt låga eller uteblir helt och hållet (Miller, 2009). Större tillgång till applikationer an vad som annars är möjligt och även ökad flexibilitet med delad information (Summerville, 2009).

Att en beställare kan få större tillgång till applikationer, beror enligt (Miller, 2009) på att minskade hinder för inträde, gemensam infrastruktur vilket ger lägre kostnader samt, lägre kostnader för förvaltning.

### Kostnader

Förespråkarna till molntjänster framhåller ofta de ekonomiska fördelarna som är en direkt effekt av molntjänster. Detta grundar sig bland annat i att flera beställare kan dela på kostnaderna för avancerad infrastruktur eller liknande. Kondo et al. (2009) menar att den absolut största kostnaden går att relatera till bandbredd. Vidare menar författarna att kostnaden för molntjänster är effektiv för små och medelstora applikationer, men vid stora projekt blir kostnaderna för att använda molnet för höga.

Att använda teknik som inte är standard eller använder en felaktig standard kan leda till höga kostnader och detsamma gäller vid inlåsningar. Kostnaderna i dessa fall handlar om när en organisation vill bryta sig fri från befintlig teknik eller från befintlig leverantör (Nilsson & Wenell, 2009; Rönnbäck et al., 2006). Även juridisk inlåsning kan, via avtalsförbindelse, blir dyrköpt för en organisation (Nilsson & Wenell, 2009).

## *Området för organisation*

Det tredje och sista huvudområdet från förstudien utgörs av området för organisation. Detta område är kanske det som är mest diffust och störst till antalet underliggande aspekter. Anledning till detta handlar framför allt om att organisationen är en del i ett sammanhang och att omvärlden gör sig påmind. Vidare representerar området för organisation såväl politiska och juridiska aspekter som organisationens kultur och de verksammas sociala yttringar. Inom litteraturen är det framför allt juridiska risker som diskuteras.

## Juridiska

Stanoevska-Slabeva och Wozniak (2010) menar att viktiga juridiska aspekter som måste beaktas är vilka avgifter som gäller, avtal om tillgänglighet, prestanda, nertid, uppskjuten service, support, integritet, säkerhet och sekretess. Parrilli (2010) förklarar att juridiska frågor inte utgör något hinder för att investera i molntjänster. Författaren påvisar dock på olika risker och framhåller vikten av genomarbetade kontrakt och avtal.

### Juridisk inlåsning

Förutom teknisk inlåsning som presenterats tidigare kan organisationer hamna i en juridisk inlåsning. Nilsson och Wenell (2009) redogör för tre olika typer av inlåsning; leverantörsberoende, statisk driftsituation och statiskt utnyttjande. Leverantörsberoendet kan te sig i två former. Antingen är det av mer teknisk karaktär (se: teknisk inlåsning) eller en avtalssituation som medför höga kostnader vid avtalets slut.

Statisk driftsituation menar författarna är ett hinder för rationalisering av driften under avtalsperioden för kunden medan statiskt utnyttjande handlar om hinder för kunden att rationalisera användningen under kontraktstiden vilket kan hindra kunden från nödvändiga förändringar, som nya applikationer, ändrade volymer eller avveckling av applikationer eller justera avtalslängden.

Nilsson och Wenell (2009) skriver att det alltid finns inlåsningseffekter, åt båda hållen. En stor kund kan skapa inlåsning för leverantören och en leverantör kan skapa inlåsning för kunden. Det är därför viktigt att identifiera inlåsningseffekterna ur verksamhetens synpunkt och hantera dessa vid utformning av avtal och prismodeller.

## Politiska

Leverantörerna till molntjänster har enorma serverhallar för att kunna lagra all information som användarna flyttar till molnet. Dessa serverhallar är spridda över jordklotet. En av de kritiska frågorna är således hur dessa företag och dessa länder, där serverhallarna är placerade, väljer att hantera denna

känsliga data. Vilket på sikt kan vara en av de områden som kommer påverka utvecklingen, och utbredningen, av molntjänster. (Nelson, 2009)

## Sociala & kulturella

Inom ramen för den sociala och kulturella aspekten märks tillit både till tekniken och till leverantören. Tillit utgör en viktig del inte minst inom e-handel och andra Internetfenomen (Papazoglou & Ribbers, 2006). Framför allt handlar det om att användaren han tillit till leverantören och omvänt.

### Kulturella

Cooper (1994) beskriver risker som uppstår när det sker en konflikt mellan IT-implementeringen och en organisations kultur vilket enligt författaren kan visa sig på två olika sätt. Det första sättet handlar om att implementering saboteras på olika sätt, antingen redan i designfasen eller genom att underutnyttja systemet när det väl är implementerat. Det andra sättet handlar om att systemet anpassas till den rådande kulturen och därmed går de önskade effekterna om intet.

Jacobsen och Thorsvik (2008) menar även de att organisationskulturen kan begränsa vilken information som accepteras kontra utelämnas. Detta eftersom organisationer ofta söker efter den information som passar in i kulturen och avvisar på så sätt information som kan uppfattas som ett hot mot densamma. Författarna menar att kulturen dels kan ge positiva effekter och nämner informationsfilter, samt att beslut inte alltid måste fattas högst upp i hierarkin. Samtidigt menar Jacobsen och Thorsvik (2008) att kulturen kan generera negativa tendenser och då framför allt genom att bara alternativ som passar till kulturen accepteras. Detta kan enligt författarna leda till en stark betoning på att allt ska förbli som det alltid har varit och en begränsad vilja att ta risker eller ändra sig uppstår.

Författarna Hurwitz et al (2010) diskuterar kulturella aspekter relaterat till molntjänster. Enligt författarna har människor en tendens att ta tid på sig för att acceptera en nyhet. Så har det varit tidigare och med stor sannolikhet kommer det att fortsätta vara så lyder deras tes. Författarna pekar på generella problem i samband med införandet av ny teknik i organisationer och menat att problemet antagligen ligger i dessa punkter som författarna presenterar. Som första punkt menar författarna att användarna inte ser ett behov eller användningsområde. För att förhindra detta är det viktigt att förankra fördelar och utbilda personalen för att kunna motivera övergången.

Nästa punkt som presenteras av Hurwitz et al. (2010) handlar om en osäkerhet, misstro och rädsla för det nya. Personers legitima intressen i anknytning till molntjänster handlar om säkerhet, tillgänglighet och hanterbarhet enligt författarna.

Tredje punkten som tas upp av författarna handlar om att människor kan känna sig hotade av ny teknik eftersom det finns en tro att tekniken ska ersätta deras arbete och således påverka deras framtida försörjning. För att motverka detta är det viktigt att tydligt kommunicera vad konsekvenserna kan bli för den enskilde.

Sist beskriver Hurwitz et al. (2010) att människor har en förmåga att se fördelar med ny teknik men samtidigt svårt att släppa ifrån sig det som tidigare använts. Detta kan enligt författarna bero på att det kan ta tid att helt och hållet lita på det nya.

Vidare menar Hurwitz et al. (2010) att någon eller alla av dessa reaktioner kan förväntas av den organisation som väljer ett införande av molntjänster. Således är det många som kommer att påverkas och det är därför viktigt att jämna ut övergången så att det sker så smidigt som möjligt och genom att kommunicera användningen, satsa på ökad utbildning, låta personalen vara involverad kan övergången ske relativt smidigt. Utöver detta handlar det om att förstå kulturen. Har organisationen arbetat på ett och samma sätt under den senaste tioårsperioden måste det finnas förståelse för att det kan ta tid och viss skeptiskhet.

### Tillit

Grandison (2003) förklarar tillit (trust) och menar att bara för person A känner förtroende för person B att genomföra tester för nätverkssäkerhet innebär detta inte nödvändigtvis att person A kommer ge person B tillåtelse att genomföra testet. Författaren menar att principen är enkel och tilliten behöver inte innebära kontrollrättigheter eller omvänt. Dock menar författaren att i vissa fall kan det vara så att tilliten kan ge viss tillåtelse, men att vara betrodd går inte att likställa med att få tillgång. Tillit kan te sig i flera skepnader, dels tilliten av mer social karaktär, dels tillit till programvara och annan teknik (Dimitrakos, 2009)

Coetzee och Eloff (2005) menar att tilliten mellan beställare och leverantörer av webbtjänster ligger till grund för alla utbyten som sker dem emellan. Författarna menar att det skulle vara opraktiskt att en leverantör av webbtjänster ger samma nivå av tillit och samma accessnivå till kända såväl som okända beställare.

### Support

Khajeh-Hosseini et al. (2010b) lyfter fram riskmomentet vid en implementering och författarna menar att problemet finns då infrastrukturen sköts av tredje part. Risken är bristen på IT-support och författarna menar att problemet kan vara under implementeringstiden eftersom personal kan vara i behov av mer tid för att utföra samma arbetsuppgifter som tidigare eftersom personalen måste lära sig att göra samma saker i molnet istället. Khajeh-Hosseini et al. (2010a) pekar samtidigt på ekonomiska fördelar med att en organisation kan slippa en kostsam supportavdelning. Parrilli (2010) framhåller

vikten av att leverantören är tillgänglig för att kunna lösa eventuella problem. Författaren menar att leverantören bör kunna nås dygnet runt. Detta ska även gälla vid katastrofhantering vilket, vid bristande avtal, kan leda till skadestånd för kunden utan möjlighet till kompensation.

# 5 Modell

*Detta kapitel är uppdelat i två olika faser; en teoridiskussion utifrån teorins huvudområden som följs av en analys av riskområden relaterade till respektive huvudområde. Den andra fasen handlar modellens framtagning.*

## *Teoridiskussion*

Nedan förs en diskussion som baseras på informationen som presenterats i föregående kapitel. Varje huvudområde diskuteras för sig och följs av en presentation av de riskområden som går att utläsa direkt i det teoretiska ramverket eller från diskussionen.

### Teknik

Inom området för teknik presenteras ett antal underliggande aspekter utifrån litteraturens syn på respektive underområde. Vissa aspekter har förekommit mer frekvent än andra och vad detta beror på är inte helt klarlagt. En kvalificerad gissning kan ge förklaringen att vissa områden utgör en större riskfaktor än andra. Det skulle även kunna vara så att vissa områden är mer tydligt definierade och således ges en större möjlighet att relatera till just det området. Om förhållandet påminner om det senare skulle förklaringen kunna vara att vissa områden är relativt närbesläktade.

Ett av de större områden som diskuteras utgörs av säkerhet. Anledningen till detta kan ha att göra med att säkerheten utgör en elementär roll för molntjänster och hela idén bygger på att det går att leverera teknik som ger likvärdig eller högre säkerhet gentemot mera traditionella lösningar. Går det inte att garantera ett systems säkerhet är det nog svårt att motivera en övergång. Ett viktigt perspektiv är dock vilken molntyp som avses eftersom detta kan vara av betydelse. Ett publikt moln kan tänkas vara mer utsatt än ett privat, men det privata molnet kan innehålla känsligare information än det publika och således kan konsekvensen av en eventuell attack få större effekt. Samtidigt kan en attack mot ett privat moln resultera i större informationsförluster än om attacken genomfördes mot ett publikt moln.

Frågan om säkerhetshoten är överdrivna är inte en helt befängd fråga. Kanske har denna aspekt fått ett för stort fokus och andra områden har förbisetts. Ett exempel från litteraturen handlar om ett dokument som innehåller en länk till skadlig programvara. Författarna menar att när detta dokument öppnas inom intranätet finns det brandväggar som skyddar och omöjliggör en tillgång till den skadliga programvaran, men när dokumentet placerades i en molntjänst fanns inte längre skyddet. Av detta går det att ställa två frågor där den första handlar om hur kontakten med molntjänsten såg ut, det vill säga, kan det ha varit en applikation som nåddes via webbläsaren. Nästa fråga att begrunda är således om intranätets skydd inte kunde påverka trafiken via webbläsaren. Sedan slutet av 1990-talet har det funnits olika sorters program för att minska risken för framför allt barn att felaktigt komma åt webbplatser med pornografiskt innehåll. Funktionen blockerar helt enkelt vissa domäner och gör

dessa oåtkomliga. En enklare brandvägg erbjuder säkerligen dessa möjligheter också, eller omvänt, att bara godkända domäner är nåbara. Givetvis är en sådan lösning långt ifrån ett fullgott skydd, men som kompletterande torde vissa risker kunna minska.

Förutom säkerhetsrisker med attacker och illasinnad programvara kan valet eller okunskapen att inte välja en modell som bygger på en standard utgöra såväl en säkerhetsrisk som att öka risken för teknisk inlåsning. Problemet med standarder kan vara att i andra vågskålen ligger flexibilitet och anpassade system. Både flexibilitet och anpassade system kan komma att vara aktuellt för en organisation och då skulle en anpassning till standarder minska. Kontentan skulle då kunna leda till en teknisk inlåsning med svårigheter att byta leverantörer eller system. Således utgör är standardiseringen en balansgång vilket i sin tur gör att en medvetenhet om fördelar och risker underlättar.

Ytterligare faktorer som är relevanta med teknik handlar mer om människans hantering av tekniken. De sociotekniska aspekterna som presenterats kan ses som självklara men detta motiverar än mer en riskfaktor. Genom utbildning och medvetenhet kan riskerna minimeras.

### Tekniska riskfaktorer

Riskfaktorer som framkommit under studiens gång och går att relatera till området för teknik kan handla om attacker, förlorad data, stulen data eller likande. En annan risk handlar om tillgänglighet och åtkomst. Just åtkomst är en av de grundläggande risker som diskuterats med anknytning till molntjänster och i detta sammanhang handlar det framför allt om vilka personer som har tillgång till vilket material där risken är att utomstående kan komma åt hemliga uppgifter. Men risken kan även utgöras av ett omvänt scenario och då handlar det om att en medarbetare kan komma åt skadlig programvara när ett dokument flyttas till tredje part.

Ett annat riskområde som diskuteras är kontroll, eller rättare sagt, bristen på kontroll. Kan beställaren få information av leverantören var någonstans som den information beställaren lagrar finns. Kontroll kan även handla om vilka möjligheter som finns för att komma åt information eller liknande. Vilket följs åt av ägande. I och med att information hamnar hos en tredje part kan tvister uppstå om äganderätten avser informationen i ren data men även rätten till insticksprogram eller liknande.

Standarder, och då framför allt öppna standarder är ett område som har många förespråkare. Framför allt handlar det om att standarder öppnar för möjligheter som förhindrar inlåsning, ökar säkerhetsnivåer och liknande. Därför utgör bristen på standarder ett säkerhetsproblem. Att beställaren låser sig till en leverantör handlar framför allt om en teknisk och juridisk inlåsning eller var för sig. Teknisk inlåsning handlar om att tekniken komplicerar eller till och med omöjliggör för beställaren att flytta till en annan leverantör. Den juridiska inlåsningen handlar framför allt om att beställaren låser sig till en leverantör genom avtal.

## Ekonomi

Området för ekonomi är kanske det område där kritiken mest varit av positiv karaktär. I en värld med ökad globalisering och internationalisering och ökad konkurrens från bland annat låglöneländer utgör en av de största konkurrensfördelarna kostnadsreduceringar. Att då kunna minska organisationens kostnader med alternativa lösningar tordes utgöra en stor betydelse. Att världen de senaste åren upplevt en lågkonjunktur kan också tänkas bidragit till att lyfta fram ny teknik. Eftersom fokus riktas ännu mer åt kostnadsbesparingar.

Litteraturen visar på vissa risker där molntjänster kan leda till ökade kostnader. En av faktorerna utgörs av att det inte finns någon direkt enhetlig standard. Många leverantörer har sina egna lösningar och en inte alltför okvalificerad gissning skulle kunna vara att leverantörer med viss medvetenhet ser till så att användare är låsta, eller i alla fall komplicerar deras möjligheter att byta till en konkurrerande leverantör. Samtidigt bör leverantören ha en viss öppenhet eftersom organisationer med viss medvetande om inlåsningseffekter, eller med tidigare erfarenheter inte väljer leverantörer där det är allt för komplicerat att byta till en annan leverantör efter kontraktstiden. Andra kostnader som diskuterats handlar om juridiska inlåsningar. För att minimera denna risk bör fokus ligga på att utforma kontrakt som inte medför för stor inlåsning.

Genom noggranna kontrakt och genom att studera leverantörer är det troligt att många ekonomiska risker kan elimineras. Fokus bör även riktas till att försöka hitta dolda kostnader och ökade eventuellt ökade kostnader för bandbredd. Viktigast av allt torde vara en medvetenhet och att inte stirra sig blind på de direkta kostnadsbesparingarna som ofta nämns i samband med molntjänster.

### Ekonomiska riskfaktorer

Mycket pekar på att de ekonomiska effekterna snarare utgör en tillgång än en risk. Detta skulle kunna resultera i att de ekonomiska aspekterna förbises vilket i sin tur skulle kunna ge negativa konsekvenser. Riskområdet som således kräver en närmare granskning utgörs av bland annat en eventuell ökad bredbandsbelastning. Beroende på bredbandsleverantör kan detta leda till ökade trafikkostnader. En annan, kanske mer omfattande, riskfaktor handlar om dolda eller extra avgifter.

## Organisation

Som tidigare nämnts beskriver området för organisation ett relativt vidsträckt sådant. Anledningen till detta har att göra med organisationens del i ett större sammanhang men även eftersom mer mjuka värden, där gränsdragningar kan vara svårare att tyda, förekommer.

Juridiska aspekter utgör en stor del av de riskaspekter som diskuteras i litteraturen och inom detta område går det att utläsa flera risker som kan ha stor påverkan. Inom e-handel behandlas ofta ämnet

tillit vilket bygger på att köparen måste känna ett förtroende för säljaren för att generera ett avslut. Att känna tillit torde förekomma i alla typer av överlåtelser, affärer eller annan likvärdig verksamhet. Saknas tilliten är det svårt att förstå en affärsuppgörelse. Således går det att konstatera att tillit är ett viktigt moment. Relationen mellan köpare (beställare) och säljare (leverantör) bygger troligtvis på någon form av tillit. Det som gör detta riskmoment intressant och komplicerat är att det förekommer hos såväl leverantörer som hos beställaren – dessa båda har ett ansvarsförhållande att uppehålla en tillförlitlighet gentemot sin omgivning.

Vidare finns den kulturella aspekten som skulle kunna utgöra en risk inom organisationen. Dessa delar är inte direkt molnspecifika utan förekommer inom alla organisationer på ett eller annat sätt. Däremot är påverkningsgraden i samband med molntjänster något som gör att aspekten trots allt går att relatera till molntjänster. Eftersom molntjänster utgör ett nytt paradigm måste det finnas en förståelse för att en övergång kan ta tid och genom att få alla berörda delaktiga kan dessa risker minimeras.

En av de faktorer som inom den ekonomiska området brukas se som fördel vid molntjänster framför mer traditionella lösningar är att en organisation inte behöver husera en IT-avdelning i någon större skala för att förse organisationen med programuppdateringar, installationer och liknande utan dessa kan överföras till molnleverantören. Givetvis är detta påstående inte helt sant, eftersom kommunikationen med molnet sker på lokala arbetsstationer och därför kommer det fortsättningsvis att behövas någon form av tekniskt kunnig personal som tar hand om programuppdateringar, supportärenden och liknande inom organisationen. Däremot kan mycket av den framtida programvaran placeras i molnet och därför är det viktigt att undvika riskkonsekvenser genom att inte tydlig ha förankrat vad som avses med support från leverantören till beställaren. En annan faktor som har anknytning till supportärenden bygger på när och varför vissa uppdateringar och förändringar är nödvändiga. En större uppdatering skulle kunna medföra att visningsläget av viss mjukvara är det som beställaren kommer i kontakt med och leverantören bör därför ha ett krav på sig att kunna förankra en planering för liknande aktivitet. Samtidigt kan det tänkas finnas visst behov av vidareutbildning hos de som använder berörda tjänster.

### Organisatoriska riskfaktorer

Riskfaktorer i området för organisation utgörs av bland annat politiska aspekter, eller effekter av densamma, kan utgöra risker. Det handlar framför allt om den geografiska placeringen av information, det vill säga, var någonstans leverantören har sina servrar. Vissa organisationer har restrektioner vilka landregioner information får placeras i och liknande. En annan risk kan handla om ett annat lands lagar och vilka rättigheter som detta ger användaren.

Risker som tidigare nämnts har bland annat utgjorts av avtalsinlåsning, avgifter, ägande, åtkomst. Dessa risker kan påverkas av de juridiska dokument och godkännanden som binder leverantör och beställare/användare. Andra risker inom det juridiska området utgörs av skyldigheter. Vem är ytterst ansvarig för informationsbortfall, angrepp eller liknande.

Vidare är det viktigt att känna till vad som gäller avseende support för såväl applikationer i molnet, lokal hård- och mjukvara eller andra områden som berörs. Det finns risk att supporten som levereras inte förstårs av de som behöver den. Det kan handla om en leverantör som har support på ett språk som den enskilda användaren inte begriper eller liknande.

Ett riskmoment bygger på företagskultur och sociala effekter som grundar på mer personliga plan. Det kan handla om medarbetares kunskapsnivåer, informationsåtkomst och beroendeställning. I de fall där det tillkommer nya applikationer och nya arbetsrutiner finns en risk i att användarna inte har full förståelse eller kunskap i hur de ska nyttja dessa.

## *Design av modell*

De faktorer som presenterats i förstudien utgör de områden som kan tänkas vara kritiska inför en riskbedömning vid en implementering av molntjänster. Den mest betydande faktorn handlar om vilken molntyp implementeringen avser. Riskerna kan variera något beroende på vilka molntyper och molntjänster som avses.

Riskvärdering handlar om att utvärdera sannolikheten av att en riskhändelse kommer att inträffa och vilka konsekvenser detta i så fall skulle få för projektet (Tonnquist, 2006). För att kunna minska riskerna vid en implementering underlättar det att känna till dessa. Miniriskmetoden (Tabell II) är ett enkelt verktyg för att göra detta (Tonnquist, 2006). Verktyget bygger på sannolikheten att något inträffar och konsekvensen att det skulle inträffa. Genom att gradera sannolikhet och konsekvens från 1-5 där 1 står för låg och 5 står för hög och sedan multiplicera dessa värden erhålls ett riskvärde. Varje riskområde kan presenteras med en åtgärd, samt vi vissa lägen utökas med tidsaspekt och ansvarsfördelning. Det yttersta ansvaret ligger således på personen som ansvarar för implementeringen och det är även denna person som bestämmer var nivån ligger som ska föranleda åtgärd. (Tonnquist, 2005)

| RISK | SANNOLIKHET 1-5 | KONSEKVENS 1-5 | RISKVÄRDE (S x K = …) | ÅTGÄRD |
|---|---|---|---|---|
| Kunskapsnivån är låg | **2** | **4** | **8** | Utbilda personalen |
| Projektet överskrider budget | **1** | **5** | **5** | Bevaka |
| Projektet försenas | **2** | **2** | **4** | |

**Tabell II:** Exempel på Miniriskmodellen

Sannolikheten och konsekvensen kan variera beroende på vilken typ av organisation eller del av en organisation som avses. Även verksamhetsområde, samt molntyp(er) och tjänstemodell(er) har betydelse. Såväl är sannolikhet som konsekvens mer eller mindre projektunika vilket medför att det inte går att ge någon generell bedömning av dessa.

Sannolikheten kan tas fram genom värden som framkommer av en SWOT-analys (SLU, n.d.). En SWOT-analys används för att hitta styrkor (Strengths), svagheter (Weaknesses), möjligheter (Opportunities) och hot (Threats). (Eriksson-Zetterquist et al., 2005; Kotler & Armstrong, 2009)

## *Undersökningsmall*

Nedan presenteras den mall (Tabell III) som är resultatet av teoridiskussionen. De riskområden som presenteras är de som områden som diskuterats här ovan. Riskområdena har utökats med förslag på åtgärder.

| RISK | SANNOLIKHET 1-5 | KONSEKVENS 1-5 | RISKVÄRDE (S x K = …) | EV. ÅTGÄRD |
|---|---|---|---|---|
| Teknik | | | | Kryptera information |
| Åtkomst | | | | Se över vilka som har tillgång till vad |
| Kontroll | | | | Kontrollera/anpassa avtalet med leverantören |
| Ägande | | | | Kontrollera/anpassa avtalet med leverantören |
| Standarder | | | | Motivera inlåsning, alt. byte av leverantör |
| Inlåsning | | | | Tillämpa standarder |
| Ekonomi | | | | Hitta ev. dolda kostnader/intäkter |
| Politik | | | | Styra geografisk placering |
| Juridik | | | | Kontrollera/anpassa avtalet med leverantören |
| Support | | | | Kontrollera/anpassa avtalet med leverantören |
| Kultur | | | | Planera för utbildning och information |

**Tabell III:** Undersökningsmodell

# 6 Analys

*I detta kapitel presenteras de åsikter och synpunkter som respondenterna bidragit med efter att de tagit del av undersökningsmallen som presenterats i föregående kapitel med sammanfattande förklaringar av riskområden. Analysen avser intervjumaterialet från appendix II.*

Första frågan i undersökningen handlade om ifall respondenterna tycker att mallen kan vara till nytta vid en övergång till molntjänster. Respondent 1 säger sig se mallen som ett visst möjligt stöd för ett initialt arbete med att analysera möjligheten till molntjänster och skriver ”[…] en start upp för att tänka till […]”. Respondenten menar att just i dennes organisation är den situation som mallen syftar till komplex och mallen ger en allt för ytlig bild av läget. Efter att respondent 1 uttryckt en komplex situation vid en övergång till molntjänster görs en återkoppling till mallen och respondenten menar återigen att mallen har kvalifikationer som introduktion och tankeväckare. Vidare uttrycker respondent 1 att mallen kan få en större nytta i en mindre organisation eller ett mindre företag jämfört med en stor komplex organisation med höga säkerhetskrav.

Respondent 2 svarar på samma fråga att mallen saknar en ingångsdel ”[…] där respondenten får värdera varför man behöver molnet och vilka saker det är som man önskar få löst med molnet […]”. Respondenten menar att det är först efter en sådan del som mallen kan fungera och skriver angående mallens riskområden ”[…] rubriker fungera som en reflektion över vad det är för saker man bör värdera vid en molnövergång […]” Respondent 2 menar att det kanske skulle vara en fördel att gruppera rubrikerna för att på så sätt kunna hålla ihop frågeställningarna. Respondent 2 ger som exempel på grupperna ”Kontroll – Ägande – Kultur”, ”Teknik – Åtkomst - Standarder”, ”Politik – Juridik”.

Respondent 3 svarar att mallen skulle kunna vara till nytta för beslutet om en övergång till molntjänster och motiverar detta med ”[…] den visar på vilka områden som behöver tas upp i en riskanalys inför en övergång”

Respondent 4 inleder sina svar med att skriva att frågan känns lite lösryckt ur sitt sammanhang men att respondenten antar att materialet som bifogades frågorna bara utgjorde en liten del av underlaget. Med detta utgångsläge presenterar respondent 4 några funderingar. Respondenten skriver ”Informationen är ju det riktigt viktiga oavsett om detta gäller privat eller offentlig verksamhet” och vidare ”[…] här vill nog samtliga organisationer/företag verkligen ha kontroll över detta”. Respondent 4 tillägger att om denna kontroll saknas utgör det i sig en mycket hög riskfaktor.

Respondent 4 skriver ”[…] i högra kolumnen förslag på åtgärder kopplat till ett antal risker” vilket följs av en motfråga från respondenten ”Är detta bara exempel på åtgärder eller hur har du kommit

fram till dessa?”. Vidare undrar respondenten vad frågorna (appendix II) är riktade till för målgrupp och vad som är syftet med frågorna.

Respondent 4 tillägger att det är viktigt att ha en klar och tydlig bild av vad som avses med mallen och skriver ”Molnet kontra ’normal upphandling’ […] fundera noga på vilket svar du ger”. Respondenten återkopplar till mallen och skriver att ”[…] med fördel kunna gruppera ihop ett antal frågor för att det skulle bli mer överskådligt. Jag tänker t.ex. på Ägande-Kontroll-Ekonomi”.

Respondent 4 uttrycker ytterligare en osäkerhet med vad som avses med mallen och skriver ”Ur vilket perspektiv har du tagit fram mallen […] ett privat företag eller en offentlig organisation så har säkert ägaren ett perspektiv och nyttjaren/brukaren har säker ett annat” och tillägger ”Bestäm vilket du utgår ifrån”.

Den andra huvudfrågan i e-postintervjun handlar om ifall respondenten saknar något område eller att något område är onödigt. Responden 1 svarar att kultur är en punkt som utifrån den beskrivning respondenten tagit del av istället borde heta ”Medarbetare”. Vidare menar respondent 1 att de problemområden som lyfts fram i kategorin helt klart är relevanta men samtidigt att de inte på något sätt är unika just för molntjänster. Respondenten tillägger ”[…] samma problembild finns även vid andra driftsformer.

Vidare nämner respondent 1 att det borde finnas en kategori med mer fokus på säkerhet och skriver ”[…] som hanterar säkerhet där det lyfts fram mer specifika frågor gällande säkerheten kring att lägga ut funktioner i molnet”. Respondent 1 framhåller en ökad risk för ”cyber-attacker” i och med molntjänster och flera användare från andra organisationer arbetar mot samma plattform som ett exempel.

Respondent 1 går vidare och skriver ”Ytterligare ett område jag inte riktigt får in i någon av kategorierna är inlåsningseffekten […]”. Inlåsningseffekten som respondenten resonerar beskrivs som ”[…] styrd av leverantörens utbud”. Vidare framhåller respondent 1 att en effekt av att inte äga tjänsten själv handlar om minskad flexibilitet och skriver ”[…] man blir till viss del låst av konceptet och de ramar som avtalet utgör”. Respondent 1 menar att just detta, med minskad flexibilitet kan komma att påverka vilka tjänster som lämpar sig för molnet och lyfter fram e-post som en möjlig molntjänst och affärssystem som mer komplext.

Respondent 2 tycker det är otydligt till vilket ändamål mallen kan komma att användas och undrar om den kommer användas med ”[…] kvalitativa metoder för att särskilja olika respondenters syn på molntjänster […]”. Som exempel nämner respondent 2 synen hos privata företag kontra offentlig verksamhet. Vidare undrar respondent 2 om avsikten med mallen istället är att ”[…] eller har du för

avsikt att kvantifiera resultaten i en matris för att tydliggöra var ’kunderna’ befinner sig idag”. Respondent 2 tillägger att bristen i förståelse för mallens syfte gör att det blir svårt att svara.

Respondent 2 anser även att support är ett område som är svårare att formulera sig kring vad gäller molntjänster återkopplat till tidigare, och skriver ”Det beror ju återigen på vad som skall in i molnet” och menar vidare att det är skillnad på om det är datalagring, virtualisering av applikationer eller tjänster. Respondent 2 får medhåll av Respondent 4 som också anser att support är ett svårt område och undrar vad som avses med detta. ”[…] är det support om systemet (applikationen) eller nyttjandet av detsamma?”.

Utöver synpunkterna på vad mallen är tänkt att användas till skriver respondent 2 ”I själva modellen är min erfarenhet att om du i den ger exempel på åtgärder så kommer rankningen reflekteras över åtgärden och inte rubriken”. Respondent 2 nämner rubriken teknik och skriver att inom den ”[…] kan ju ett oändligt antal fördelar och nackdelar finnas för den enskilda verksamheten […]”. Respondenten tillägger vidare att genom att vända på matrisen och istället presentera risken som ”Informationen är inte krypterad” följt av sannolikhet, konsekvens och uträkning för riskvärde och sedan i högerkolumen rubricera frågans härkomst, skulle kunna vara ett tips på en mer effektiv modell.

Respondent 3 skriver ”Jag tycker att mallen är tillräckligt bred, men lite ytlig”. Respondent 3 tycker framför allt mallen handlar om förslag på åtgärder och använder den tekniska aspekten som exempel och skriver att det är önskvärt med ”[…] fler tekniska aspekter än sådana som löses genom kryptering”. Vidare menar respondent 3 att det är viktigt att sätta sig in i vad som är bäst för just en viss verksamhet och skriver ”[…] att åtgärderna inte är heltäckande är nog bara bra […]” och tillägger ”[…] men för att den [mallen anm.] skulle bli till ännu mer nytta skulle jag önska några underrubriker inom varje område”.

# 7 Diskussion

*I detta kapitel förs en diskussion baserad på det empiriska material som utgörs av synpunkter på mallen (Appendix II). Diskussionsunderlaget baseras till stor del på analysen.*

## *Empirisk studie*

Som tidigare nämnts bygger denna studie på två olika empiriska undersökningar. Förstudien genomfördes inledningsvis för att mynna ut i områden som var aktuella att undersöka och den senare undersökningen för att ge respons på första utkastet av mallen.

Vid båda tillfällena användes e-postintervjuer eftersom denna metod möjliggjorde kontakt med personer som annars skulle vara svåra att nå, samt att studieområdet kan antas vara relativt komplext och därför fanns ett behov att låta respondenterna själva sätta sig in i frågorna. Vid förfrågan i samband med förstudien var svarsfrekvensen relativt låg bland de tillfrågade men de som svarade ställde sig positiva och gärna ville hjälpa till med synpunkter.

Vid andra omgångens förfrågan om ett medverkande svarade i stort sett alla tillfrågade att de kunde hjälpa till att bedöma mallen. Även vid detta tillfälle var det dock förvånansvärt låg svarsfrekvens efter att de tänkta respondenterna mottagit materialet. Detta bidrog till att de som inte svarat inom två veckor vid första tillfället och en något kortare period vid andra tillfället fick en påminnelse om att de inte svarat. Vid första tillfället, alltså vid förstudien, kan den låga svarsfrekvensen bero på att ämnet var relativt nytt och att det råder osäkerhet i definitioner och betydelser för detsamma. Det går heller inte att utesluta att förfrågan kan varit otydlig. Således kan den låga svarsfrekvensen förklaras av att vissa känt sig obekväma med att erkänna bristande kännedom om ämnet. En annan förklaring kan vara att personerna, efter att mottagit frågorna, inte ansåg sig ha tid, eller vidarebefordrade frågan till en kollega vars yrkesroll var mer passande. Det är alltså svårt att säga direkt vad som har påverkat personerna som först sagt sig villiga att deltaga och sedan uteblivit med svar.

Vid andra tillfället är det något svårare att fastställa orsaken till varför de tillfrågade valde att inte inkomma med svar. Detta eftersom erfarenheter från förra gången bidrog till att förfrågan om ett medverkande var tydligare och därför bör samtliga vara införstådda med vad som avsågs. En av personerna som sagt sig kunna ställa upp återkom nästan omgående och bad om en tydligare avsikt med studien. Detta medförde att samtliga personer som sagt sig kunna medverka fick ett nytt e-postmeddelande med den informationen något tydligare uttryckt. Detta extra utskick kan i sig ses som en påminnelse varpå det är ännu märkligare att de personer som sagt sig kunna svara inte gjort detta. Givetvis går det inte att utesluta att personerna som sagt sig kunna hjälpa till inte kände sig motiverade att medverka när de väl fick ta del av mallen. Kanske upplevde de denna som så undermålig att det inte var värt mödan. Att förklara orsaken till varför de inte svarat är omöjligt. Det

går att spekulera i anledningar men det kan lika gärna handla om att personerna blivit sjuka eller prioriterat andra uppgifter eller likande. Vid andra tillfället ställdes det ett större krav på att respondenterna skulle lämna in sina synpunkter inom en viss tid och detta är en faktor som även den kan ha påverkat. Personerna kan ha varit bortresta eller på annat sätt inte haft åtkomst till sin e-post under denna tid eller så fanns det inte utrymme för att svara helt enkelt. Vissa intressanta områden går dock att utläsa från de inkomna svaren, den låga svarsfrekvensen till trots.

## *Respons på mallen*

Alla respondenter som bemödade sig med att besvara frågorna hade åsikter om mallen. Det går att utläsa att respondenternas syn på mallen avgjorde om de såg att det skulle finnas ett användningsområde eller inte för densamma. Givetvis kan detta bero på hur frågorna, eller den inledande förklaring som bifogades frågorna, kom att tolkas. De personer som svarade att mallen kunde användas som tankeväckare eller i ett inledande arbete kan antas ha fokuserat mer på vad som avsågs med undersökningsfrågor medan de andra istället fokuserat på att förklara mallen utifrån sina egna perspektiv. En lärdom av detta kan vara att det är svårt att motivera en frågeställning vid en e-postintervju kontra en traditionell intervju öga mot öga. I ett fall där respondenterna avviker från frågorna skulle det här ha gått att styra tillbaka dem om det handlar om en traditionell intervjusituation.

Trots de olika uppfattningarna av mallen inkom synpunkter som skulle kunna leda till en förbättring. Att inledningsvis förklara till vilket område mallen kan användas till är en åsikt som bör tillämpas eftersom detta tydliggör mallens roll vilket kan leda till en ökad användning då det klart och tydligt framgår vilket användningsområde som avses.

Samtidigt avser inte mallen en djupdykning på detaljnivå utan målet är att ge en relativt allmän översikt och därför bör inte den inledande förklaringen begränsa användandet i allt för stor utsträckning. Däremot är det viktigt att noggrant kommunicera budskapet så att det inte råder någon oklarhet i detta.

Som en av respondenterna nämnde är det lätt att fokus hamnar på åtgärden framför riskområdet. Detta borde kunna bero på betraktarens bakgrund och vilken roll betraktaren har normalt. Om den huvudsakliga arbetsrollen lutar mer åt problemlösning än projektstyrning är det inte helt oväntat att fokus hamnar på fel område. Tanken enligt modellen är ju mer att visa på ett exempel för att motverka en risk. Frågan behandlas även av en av respondenterna som inte ser någon direkt koppling mellan riskområden och förslagen på eventuella åtgärder. En tanke skulle kunna vara att utöka antalet exempel för varje riskområde men detta kan leda till en allt för komplicerad modell.

Istället för att ta fram en egen modellstruktur för att presentera riskområdena, föll istället valet på att presentera riskområdena efter en redan befintligt modellupplägg (miniriskmetoden). Nackdelen med detta blev att vissa åsikter är svåra att relatera om de avser kritik på riskområdena eller kritik mot mallen. Riskområdena bör dock rimligen belysas i ett samband. Eftersom det kan antas vara vanligt med någon form av sannolikhets- och konsekvensbedömning i samband med riskbedömningar och borde därför en struktur som miniriskmetoden vara att föredra eftersom denna metod används i verksamheter i dagläget. Givetvis kan ju respondenterna ha olika erfarenheter av en liknande modell och detta kan ha bidragit till hur de svarat.

Vidare finns det olika uppfattningar om säkerhetens betydelse och givetvis är detta ett stort och näst intill avgörande område för många användare avseende molntjänster. Därför bör en mall tydligare framhålla detta område ensamt, framför att bädda in det i teknik. Samtidigt handlar det som allmänt brukar avses med säkerhet just om tekniska aspekter. Kanske borde riskområdena presenterats med en tydligare hierarki då vissa riskområden kunde få förekomma vid olika tillfällen. Exempelvis utgör säkerhet en teknisk aspekt så som redan nämnts, men kan ju även ha såväl juridisk som ekonomisk karaktär.

Mallens huvudsakliga syfte är faktiskt att identifiera riskområden inför riskbedömningen vid en övergång till molntjänster och detta borde ha kommunicerats tydligare i samband med att intervjumaterialet presenterades för respondenterna. Kritiken att mallen således är svår att sätta in i ett sammanhang är därmed befogad och detta behöver göras tydligare.

Det har även visat sig att det skiljer stort mellan olika organisationers uppfattning om vilka risker som de upplever. Givetvis är det inte svårt att förstå att exempelvis ett sjukhus med patientinformation har större krav på sig, såväl politiskt som integritetsmässigt, att skydda information som ett företag (inom till exempel servicebranschen) som hanterar om bokföringen för en godiskiosk eller en frisörsalong.

Att fokusera bedömningen av mallen till personer inom IT kan ha varit en begränsande strategi eftersom riskområdena behandlade mer än enbart teknik. Således borde personer med ekonomisk och juridisk, samt eventuellt även politisk kunskap, ha deltagit i undersökningen. Ett projekt som skulle kunna komma att använda mallen borde kunna antas ha en person med ett övergipande ansvar. Denne person borde då antingen ha en väldigt bred kompetens för att kunna avgöra riskernas påverkan i olika områden eller mer sannolikt, borde projektledaren ha ett antal experter på varje område att vända sig till. Förutsättningen för detta är dock att det handlar om en relativt stor organisation som kan avsätta en sådan mängd resurser. Om de har möjlighet att avsätta en expertgrupp till detta är frågan om mallen skulle vara aktuell alls, eftersom en organisation med sådan möjligheter då skulle kunna ta fram en egen mall utifrån sina egna kriterier och behov.

I ett liknande fall borde dock mallen, som antytts i svaren, kunna användas för att just hitta inom vilka områden det kan vara aktuellt med en expertgrupp. Dock behöver mallen även för detta ändamål genomgå vissa justeringar så att riskområdena tydligt presenteras, liksom syftet med mallen.

Benämningen på riskområdet kultur avsåg både företagskultur och mer sociala frågor. Detta område var kanske inte lika tydligt beskrivet som vissa andra riskområden. Kultur kan ses som ett relativt mjukt begrepp som går att se på olika sätt beroende på vem som är betraktare. Att då istället byta namn till medarbetare som en av respondenterna föreslår kan ge en tydligare bild av vad som avses ur ett visst perspektiv. Samtidigt försvinner då andra kulturaspekter så det kanske är mer lämpligt att komplettera modellen med en extra aspekt för medarbetare och således behålla riskområde kultur som huvudområde.

Områdena som lyfts fram i mallen saknar enligt en av respondenterna en unikhet för molnet. Frågan är om det alls finns områden som i mallen är unika för molntjänster eller om det i själva verket är sammansättningen som skulle kunna vara det som är unikt, eller i alla fall vara mer relevant för ämnet. Även om riskområdena inte är unika för molnet utgör de riskfaktorer som är relevanta och således bör hänsyn tas till dessa områden. Givetvis finns inlåsning även i annan programvara som inte är unik för molntjänster, för att ta ett exempel. Inlåsningseffekterna när till exempel information ligger hos tredje part och användaren är låst bör ju kunna ses som ett större problem än vad en inlåsning skulle göra lokalt i ett företag. Med det inte sagt att inlåsningen inte skulle utgöra ett problem.

Som en av respondenterna noterat passar inte alla tjänster som specifika molntjänster. Respondenten exemplifierar e-post och affärssystem. Det finns en poäng med detta – tjänster som bygger på en relativt hög grad av standardiserade kommunikationer lämpar sig givetvis bättre än en tjänst som är mer unik. Däremot upplevs det exempel som presenterats av respondenten inte direkt som välgrundat. E-post är ett exempel på en tjänst som egentligen alltid varit en slags molntjänst, även långt innan begreppet började användas. Att därför anse att denna tjänst skulle göra sig bättre i molnet än ett affärssystem känns inte så välmotiverat i sammanhanget. I detta sammanhang går det dock att anta att det handlar om ett exempel och som sådant är det tydlig. Samtidigt utgör just affärssystem ett av de stora områden som faktiskt redan erbjuds som molntjänster. Affärssystem kan i mångt och mycket anses utgöra den perfekta miljön att applicera som molntjänst, eftersom affärssystem kan antas bestå av några relativt allmänna program och vissa mer skräddarsydda eller lokalt anpassade. Givetvis beror detta på affärssystemets art men en tanke kan vara att systemet ska kunna användas av såväl organisationen som även ägare och återförsäljare, systerorganisationer eller liknande. Eftersom det då handlar om flera olika intressenter och antagligen om ganska stor geografisk spridning bör kommunikationen till stor omfattning gå via Internet och detta borde i sig tala för att tjänsten skulle passa som molntjänst.

Givetvis finns det även olika typer av affärssystem. Är det ett system som innehåller mycket känslig information måste såväl informationen som system skyddas på ett annat sätt än system som innehåller mindre känsliga uppgifter. Affärssystem bör kunna antas vara mer komplext än ett system för e-post, men ett vanligt affärssystem som används av ett företag för bokföring och liknande är inte direkt komplext. Sådana system som i princip går att köpa hos en återförsäljare för datorprogram och programmet distribueras via en CD-rom eller DVD bör inte anses vara speciellt avancerat, även om implementeringen och antalet sammankopplade datorer kan göra att det blir komplext. Respondenten har som sagt en poäng och det motiverar än mer att mallen tydligare presenterar vad den avser.

Av åsikterna att döma är det nog i dagsläget inte lönt att en större organisation flyttar alla sina system till molnet. Däremot kan det antas finnas flera mindre system som både kan vara komplicerade att administrera och kostsamma ur licenssynpunkt. Att program som har dessa karaktäristika flyttas till molnet, om säkerheten kan fastställas, kan ge en fördel för organisationen som då slipper fokusera på antalet licenser och administration av systemet. Om fokus för molntjänster läggs på möjligheten att förenkla samarbetet borde flera program kunna passa för detta.

En av respondenterna uttryckte att mallen var ytlig och får medhåll av en annan som menar att en mall med åtgärder lägger fokus på åtgärden framför risken, och som därför efterlyser en omvänd modell. En sådan omvänd modell skulle dock bli mycket mer omfattande om varje åtgärd skulle belysas och syftet med mallen att vara överskådlig går då om intet. Samtidigt bör förslag på definitiva åtgärder ligga hos den projektansvarige och därför bör mallen istället öppna för detta.

Mallen har givetvis sina begräsningar och en av dessa är att den är övergripande och lyfter fram flera riskområden. Detta gör ju att ytligheten i mallen blir relativt påtaglig som respondenten säger. Hade ambitionen med mallen fokuserat på detaljnivå hade möjligheten att sätta sig in i mallen blivit mycket mer komplicerad och av den anledningen kanske inte kommit att användas. För att en mall sak vara lätt att överblicka och vägledande får det inte vara några oklarheter med hur den fungerar. Detta var en av anledningarna till att presentera den enligt miniriskmetoden som just fokuserar på enkelhet och samtidigt fungerar miniriskmetoden som ett underlag till verksamhetens egen riskbedömning. Mallen blir därför ett redskap och inte en färdig bedömning.

En av respondenterna uttrycket det motsatta och menar att flera av områdena skulle kunna grupperas ihop för att göra mallen mer överskådlig. Att mallen ska vara överskådlig är en av grunderna och därför skulle en gruppering kunna vara aktuell, samtidigt som det tydligare bör framgå att mallen är tänkt att användas överskådligt.

Mallen verkar också ha brister i vad som avses med support. Som en respondent påpekar är det inte självklart vad som avses med support och betydelsen kan variera beroende på om det handlar om

support för själva applikationen eller support för nyttjandet av applikationen. Således måste området support definieras tydligare. Det bör alltså inte råda osäkerhet i vad som avses med respektive riskområde.

I övrigt utgör definitionen av vad som faktiskt avses med molntjänster en stor osäkerhet i dagsläget vilket skulle kunna förklara de relativt skilda meningarna om mallens betydelse. Trots att frågorna som ställdes presenterades med en sammanfattande definition går det inte att utesluta att respondenternas olika åsikter om vad som menas med molntjänster har haft en betydande roll vid bedömningen av modellen.

Att använda miniriskmetoden för att presentera riskområdena måste trots kritiken vara att föredra eftersom denna metod erbjuder ett dokumenterat tillvägagångssätt framför en metod som är utformad just för detta specifika fall. Däremot skulle det kunna underlätta presentationen att tillämpa en tydligare hierarki av riskområden såväl som tydligare områdesindelning. Detta medför givetvis att vissa aspekter kan bli aktuella vid flera tillfällen eftersom vissa aspekter berör flera områden. Exempel på detta är som tidigare nämnts inlåsning som kan te sig på flera olika sätt.

Således bör miniriskmetoden användas men utan att eventuella åtgärder presenteras. Detta eftersom det inte tydligt framgick av mallen att åtgärdsförslag bar var exempel, och själva åtgärderna fick för stort fokus framför riskområdena. Det bör även kunna antas att eventuella åtgärder kan te sig olika beroende på vad för organisation som använder mallen. Att åtgärderna kan uppfattas som låsta måste givetvis förhindras och därför är det extra viktigt att varje specifik organisation själv får avgöra hur de avser begränsa konsekvenserna av ett riskområde.

De riskområden som presenterats i mallen bör antas gälla såväl offentlig verksamhet som privata företag. Givetvis kan konsekvenserna skiljas och betydelsen av riskerna således vara olika, men riskområdena kunna antas vara generella för båda organisationstyperna. Det samma borde även kunna gälla beroende vilken måltyp som avses. Handlar det om ett privat moln internet i en organisation kan sannolikheten att en risk inträffat antas vara lägre. Detta måste dock ligga hos ägaren av projektet att bedöma vilket även tydlig måste framgå i beskrivningen av mallen.

Vidare måste riskområdena kommuniceras väl och en tydlig definition av desamma måste komplettera mallen. Vad som avses med mallen är en annan aspekt som tydligt måste framgå och det får inte råda någon oklarhet i detta. Mallen måste även signalera att den på intet sätt är låst till ett viss antal riskområden utan de områden som presenteras är av mer allmän karaktär. Således bör mallen innehålla utrymme för ägaren att lägga till riskområden som är mer organisationsspecifika.

# 8 Slutsats

Studien resulterar i en mall som presenteras nedan (Tabell IV). Mallen är ett verktyg som bör utformas efter den verksamhet som väljer att använda den inför en riskbedömning. För att mallen ska kunna ge resultat måste riskområdena förankras i verksamheten så att det inte råder oklarheter om vad som avses med respektive risk. Det är upp till projektansvarig att bedöma vilken nivå på riskvärde som ska föreligga åtgärd och åtgärden måste stämma överrens med verksamhetens riskområdes-definition. Det står ansvarig fritt att utöka mallen med verksamhets- och organisationsspecifika områden.

**Tekniska**

| RISK | SANNOLIKHET 1-5 | KONSEKVENS 1-5 | RISKVÄRDE (S x K = …) | ÅTGÄRD |
|---|---|---|---|---|
| **TEKNIK** | | | | |
| - Inlåsning | | | | |
| - Support | | | | |
| - Åtkomst | | | | |
| **SÄKERHET** | | | | |
| - Standarder | | | | |

**Ekonomiska**

| RISK | SANNOLIKHET 1-5 | KONSEKVENS 1-5 | RISKVÄRDE (S x K = …) | ÅTGÄRD |
|---|---|---|---|---|
| **EKONOMI** | | | | |
| - Inlåsning | | | | |
| - Kostnad | | | | |
| - Support | | | | |

**Organisatoriska**

| RISK | SANNOLIKHET 1-5 | KONSEKVENS 1-5 | RISKVÄRDE (S x K = …) | ÅTGÄRD |
|---|---|---|---|---|
| **JURIDIK** | | | | |
| - Ansvar | | | | |
| - Inlåsning | | | | |
| - Kontroll | | | | |
| - Åtkomst | | | | |
| - Ägande | | | | |
| **POLITIK** | | | | |
| **KULTUR** | | | | |
| - Medarbetare | | | | |
| - Support | | | | |

**Tabell IV:** Slutgiltig mall

## *Förslag fortsatt forskning*

Slutsatsen i studien visar på en mall med ett antal riskområden som bör beaktas vid riskbedömningen inför en övergång till molnrelaterade tjänster. Ett uppslag för fortsatt forskning skulle därför kunna vara att pröva mallen för en bredare publik.

# Referenser


Affärsvärlden (2006) ”Outsourcing lockar – men undvik fällorna!,” Affärsvärlden April 20, 2006. Available: http://www.affarsvarlden.se/hem/nyheter/article271569.ece.

Allen, R., & Sriram, R. (2000). ”The Role of Standards in Innovation,” Technological Forecasting and Social Change, Volume 64, January, 2000, 171-181.

Anderson, J. E., Wiles, F. A., & Young, K. P. (2008). ”The Impact Of Cloud Computing On IS/IT Academics,” Issues in Information Systems, 9(1), 203-206.

Armbrust, M., Fox, A., Griffith, R., Joseph, Anthony D., Katz, Randy H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., & Zaharia, M. (2009). Above the Clouds: A Berkeley View of Cloud Computing. Technical Report. EECS Department, University of California, Berkeley

Avetisyan, A. I., Campbell, R., Gupta, I., Heath, M. T., Ko, S. Y., Ganger, G. R., Kozuch, M. A., O'Hallaron, D., Kunze, M., Kwan, T. T., Lai, K., Lyons, M., Milojicic, D. S., Lee, H. Y., Soh, Y. C., Ming, N. K., Luke, J-Y., & Namgoong, H. (2010). ”Open Cirrus: A Global Cloud Computing Testbed,” IEEE Computer Society, April, 2010. 35-43.

Backman, J. (2008). Rapporter och uppsatser (2:a uppl.). Lund: Studentlitteratur.

Beizer, D. (2009). ”Cloud computing needs standards to mature, experts say,” Washington Technology. Available: http://washingtontechnology.com/articles/2009/03/23/web-cloud-computing.aspx

Berg, B. L. (2007). Qualitative Research Methods for the Social Sciences (6th ed.). Boston, MA, USA: Pearson Education.

Boddy, D., Boonstra, A., & Kennedy, G. (2002). Managing Information Systems: An organisational perspective. Harlow, England: Pearson Education Ltd.

van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., & Verheijen, T. (2008). ITIL® V3 Foundation Exam – The study guide. Zaltbommel, Netherlands: Van Haren Publishing.

Briscoe, G., & Marinos, A. (2009). ”Digital Ecosystems in the Clouds: Towards Community Cloud Computing,” In: IEEE, (corp. ed.) 2009 3rd IEEE International Conference on Digital Ecosystems and Technologies (DEST 2009). Institute of Electrical and Electronics Engineers (IEEE), New York, USA. 103-108.

Callewaert, P., & Luysterborg, E. (2009). Cloud computing: Security, Privacy and Trust. White Paper, Deloitte Consulting, Belgium.

Carr, N. G. (2003). ”IT doesn't matter,” Harvard Business Review, May 2003. 41-49.

Catteddu, D., & Hogben, G. (2009) ”Cloud computing: Benefits, risks and rekommendations for information security,” European Network and Information Security Agency, ENISA, Nov 2009.

Coetzee, M., & Eloff, J. H. P. (2005). ”Autonomous trust for web services,” Internet Research, Vol. 15. No. 5, 498-507.

Cooke, J. (2009). ”Fyra av tio program i molnet 2011,” CIO Sweden, Nr. 4, 2009. 39.

Cooper, R. B. (1994). ”The inertial impact of culture on IT implementation,” Information & Management, Vol. 27, Nr. 2, 1994. 17-31.

Christodorescu, M., Kinder, J., Jha, S., Katzenbeisser, S., & Veith, H. (2005). ”Malware normalization,” Tech. rep. 1539, University of Wisconsin, Madison. WI. USA.

Dikaiakos, M. D., Katsaros, D., Mehra, P., & Vakali, A. (2009). ”Cloud Computing: Distributed Internet Computing for IT and Scientific Research,” IEEE Computer Society, IEEE Internet Computing, September/October 2009. 10-13.

Dimitrakos, T. (2009). Common Capabilities for Service Oriented Infrastructures – Grid and Cloud Computing. In: Stanoevska-Slabeva, K., Wozniak, T., & Ristol, S. Grid and Cloud Computing: A Business Perspective on Technology and Applications. Berlin: Springer. 123-146.

Ejvegård, R. (2009). Vetenskaplig metod (4:e uppl.). Lund: Studentlitteratur.

Eriksson-Zetterquist, U., Kalling, T., & Styhre, A. (2005). Organisation och organisering. Malmö: Liber.

Ernest & Young. (2009). ”Fler företag outsourcar i kristider”. Retrieved April 10, 2010, from http://www.ey.com/SE/sv/Newsroom/News-releases/Pressmeddelande090319.

Etro, F. (2009). ”The Economic Consequences of the Diffusion of Cloud Computing,” Employment and Output in Europe Review of Business and Economics, Vol. 54, 2. 179-208

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). "Cloud Computing and Grid Computing 360-Degree Compared," abs/0901.0, Issue: 5, Publisher: IEEE, 2008. 1-10.

Gartner. (2009a). ”Gartner Identifies the Top 10 Strategic Technologies for 2010,” Gartner Pressrelease, October 20, 2009. Available: http://www.gartner.com/it/page.jsp?id=1210613

Gartner. (2009b). ”Gartner Survey Shows Outsourcing Activity in Europe Is Growing During Economic Downturn,” Gartner Pressrelease, May 5, 2009. Available: http://www.gartner.com/it/page.jsp?id=967119

Gartner. (2007). ”Gartner Identifies the Top 10 Strategic Technologies for 2008,” Gartner Pressrelease, October 9, 2007. Available: http://www.gartner.com/it/page.jsp?id=530109

Google Trends. (2010). ”Cloud Computing”. Retrieved March 20, 2010, from http://www.google.com/trends?q=cloud+computing

Graham-Rowe, D. (2009). ”A Faster Way to the Cloud,” Technology Review, September, 11, 2009. Available: http://www.technologyreview.com/computing/23451/

Grandison, T. W. A. (2003).”Trust management for internet applications,” PhD thesis, Imperial College of Science, Technology and Medicine, Department of Computing, University of London, London.

Hanseth, O., & Lyytinen, K. (2004). ”Theorizing about the Design of Information Infrastructures: Design Kernel Theories and Principles,” Case Western Reserve University, USA. Sprouts: Working Papers on Information Systems, 4(12).

Hanseth, O., & Monteiro, E. (1997). ”Inscribing behaviour in information infrastructure,” Accounting, Management and Information Technologies, Vol. 7. Issue 4, 183 – 211. Retrieved May 14, 2010, from http://www.ifi.uio.no/~oleha/Publications/siste.enkel.doc.html

Haverblad, A. (2006). IT ur ett affärsperspektiv. Lund: Studentlitteratur.

Heiser, J. (2010). ”Analyzing the Risk Dimensions of Cloud and SaaS Computing,” Gartner Research, Publication Date: 17 March 2010, ID no: G00174873. Gartner Research.

Hurwitz, J., Bloor, R., Kaufman, M., & Halper, F. (2010). Cloud computing for dummies. Hoboken, NJ, USA: Wiley Publishing.

Iball, J. (2010). ”Don’t Cloud Data Security,” ITNOW, Vol. 52, Number 2, March 2010. 14-15.

IDG Media (2010). Retrieved April 23, 2010, from http://idgmedia.idg.se/2.3710

Jacobsen, D. I., & Thorsvik, J. (2008). Hur moderna organisationer fungerar (3:a uppl., G. Sandin övers.). Lund: Studentlitteratur.

Johnson, B. (2008) ”Cloud computing is a trap, warns gnu founder Richard Stallman”. The Guardian, September 29, 2008 Available: http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman.

Khajeh-Hosseini, A., Summerville, I., & Sriram, I. (2010a). ”Research Challenges for Enterprise Cloud Computing,” Submitted to the 1st ACM Symposium on Cloud Computing, SOCC 2010, on 19 Jan 2010. Retrieved April 21, 2010, from http://arxiv.org/pdf/1001.3257v1

Khajeh-Hosseini, A., Greenwood, D., & Summerville, I. (2010b). ”Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS,” Submitted to IEEE CLOUD 2010, on 18 Feb 2010. Retrieved April 21, 2010, from http://arxiv.org/pdf/1002.3492v1

Kondo, D., Javadi, B., Malecot, P., Cappello, F., & Anderson, D. P. (2009). ”Cost-benefit analysis of Cloud Computing versus desktop grids,” In Proceedings of the 2009 IEEE international Symposium on Parallel & Distributed Processing, May 2009, 1-12.

Kotler, P., & Armstrong, G. (2009). Principles of Marketing (13rd ed.). Upper Saddle River, NJ, USA: Person Education.

Leavitt, N. (2009). ”Is Cloud Computing Really Ready for Prime Time?,” IEEE Computer Society, Computer, January 2009. 15-20.

Leth, G., & Thurén, T. (2000). Källkritik för Internet. Stockholm: Stiftelsen för psykologiskt försvar.

Liebowitz, S. & Margolis, S.E. (1996). ”Typing Errors,” Reason Online. Retrieved April 18, 2010, from http://reason.com/archives/1996/06/01/typing-errors.

Malmqvist, M. (2009). ”Orderstocken hos outsourcingleverantörerna växer,” Computer Sweden. Retrieved April 10, 2010, from http://www.idg.se/2.1085/1.216597/orderstocken-hos-outsourcingleverantorerna-vaxer

Mell, P., & Grance, T. (2009). Draft NIST Definition of Cloud Computing. Retrieved April 20, 2010, from http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

Miller, M. (2009). Cloud computing: Web-based application that change the way you work and collaborate online. Que Publishing, Indianapolis, IN, USA.

Motahari-Nezhad, H. R., Stephenson, B., & Singhal, S. (2009). ”Outsourcing Business to Cloud Computing Services: Opportunities and Challenges,” Technical Report HPL-2009-23. January 2009.

Movin, S., & Zandelin, N. (2009). IT i Sverige 2009: En bok om trender och utveckling inom IT i Sverige. Stockholm: Exido Internatonal AB och Dataföreningen.

Nelson, M. R. (2009). ”The Cloud, the Crowd, and Public Policy, ” Issues in Science and Technology, Summer, 2009. 71-76.

Nilsson, A., & Wenell, T. (2009). ”Inlåsning och leverantörsberoende i outsourcingavtal,” White Paper, PMCG Scandinavia AB, Stockholm, mars, 2009.

Open Cloud Manifesto (2009). ”Open Cloud Manifesto,” Availabe online: www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf, 2010-05-01

Papazoglou, M. P., & Ribbers, P. M. A. (2006). E-business: Organizational and technical foundations. Chichester, England: Wiley.

Parrilli, D. M. (2010). Legal Issues in Grid and Cloud Computing. In: Stanoevska-Slabeva, K., Wozniak, T., & Ristol, S. Grid and Cloud Computing: A Business Perspective on Technology and Applications. Berlin: Springer. 97-122.

Patel, R., & Davidson, B. (2003). Forskningsmetodikens grunder (3 uppl.). Lund: Studentlitteratur.

Radar Group. (2009). ”Cloud rapport visar att över 18 miljarder kan frigöras ur svenska IT-budgetar,” Pressrelease, Radar Group International. March 20, 2009. Available: http://radargroup.se/se/2009/cloud-rapport-visar-att-over-18-miljarder-kan-frigoras-ur-svenska-it-budgetarna/

Röhne, J. (2008). ”Lyckas med outsourcing - och behåll din inre frid,” CIO Sweden. May 21, 2008. Available: http://cio.idg.se/2.1782/1.113444

Rönnbäck, L., Holmström, J., Hanseth, O., Borg, T., Frykman, A., & Thomsson, S. (2006). ”Changing the Installed Base: Exploring IT integration challenges in the process industry,” Proceedings of IRIS 29.

Sirkemaa, S. (2002). ”IT infrastructure management and standards,” Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'02).

SIS, Swedish Standard Institute. (2010). ”Standard ger säkrare molntjänster,” Press release: Swedish Standard Institute (SIS), 31 mars 2010.

SLU, Sveriges Lantbruksuniversitet (n.d.). ”Kritiska faktorer,” Retrieved 10 maj 2009 from http://processer2.adm.slu.se/projektmallar/kritiskafaktorer.doc

Sloan, K. (2009). ”Security in a virtualised world,” Network Security, Vol. 2009, Issue 8, August 2009. 15-18.

Srinivasa, R. V., Nageswara, R. N. K., & Kusuma, K. (2009). ”Cloud computing: An overview,” Journal of Theoretical and Applied Information Technology, Vol. 19. Nr. 1, 2009. 71-76.

Sriram, I., & Khajeh-Hosseini, A. (2010). ”Research Agenda in Cloud Technologies,” Submitted to 1st ACM Symposium on Cloud Computing, Indianapolis, Indiana, USA, June 2010.

Stango, V. (2004). ”The economics of standards wars,” Review of Network Economics. Vol. 3. Issue. 1, 2004. 1-19.

Stanoevska-Slabeva, K., & Wozniak, T. (2010). Organizational and Governance Challenges for Grid Computing in Companies - Summary of Findings from Business Experiments. In: Stanoevska-Slabeva, K., Wozniak, T., & Ristol, S. Grid and Cloud Computing: A Business Perspective on Technology and Applications. Berlin: Springer. 213-224

Summerville, I. (2009). Socio-technical issues around cloud computing. Retrieved 18 April, 2010 from http://projectnets.cs.st-andrews.ac.uk/stse/ian/files/-1/316/STSEandCloud.pdf

Svenningsson, M., Lövheim, M., & Bergquist, M. (2003). Att fånga nätet: Kvalitativa metoder för Internetforskning. Lund: Studentlitteratur.

Sörqvist, L. (2004). Ständiga förbättringar. Lund: Studentlitteratur

Thurén, T. (2005). Källkritik (2:a uppl.). Stockholm: Liber.

Thurén, T. (2007). Vetenskapsteori för nybörjare (2:a uppl.). Malmö: Liber

Tonnquist, B. (2005). ”Struktur ger frihet i projektledning,” InfoTrend, Vol 60. Nr. 1, 2005. Retrieved 19 maj 2010 from http://www.sfis.nu/Portals/images/default/infotrend/infotrend1_05/struktur.pdf

Tonnquist, B. (2006). Projektledning (2:a uppl.). Stockholm: Bonnier Utbildning AB.

Walsh, J., & Heyes, M. (2010). ”The current and future relevance of cloud computing,” Tenth annual Freshman Conference. March 5, 2010.

Wassermann, G., & Su, Z. (2008). ”Static detection of cross-site scripting vulnerabilities,” Proceedings of the 30th international conference on Software engineering, 2008. 171-180.

Whitaker, C. (2010). ”Cloud Computing – Storm Clouds or is it Smooth Flying?,” East Carolina University. Retrieved May 10, 2010, from http://www.infosecwriters.com/text_resources/pdf/cwhitaker_cloud.pdf

# Appendix I

1. Hur skulle du beskriva begreppet Cloud computing?
2. Begreppet Cloud computing har under det senaste året diskuterats flitigt i media. Hur har detta påverkat dig?
3. Har det gjort att du funderat över om tekniken/tjänsten är något för din organisation? Varför/varför inte?
4. Använder organisationen du representerar någon typ av samarbetsprogramvara/tjänst via Internet I dagläget?
5. I så fall, inom vilket område och vad är din uppfattning?
6. Ponera att er organisation ställer sig positiva till tjänster som körs externt via Internet, inom vilka områden skulle dessa fungera/inte fungera? Varför?
7. Hur skulle en eventuell övergång (inom hela eller vissa områden) påverkas?
8. Vad är viktigt att fokusera över? Skiljer sig detta utifrån att införa andra typer av IS/IT-tjänster?

# Appendix II

1. Är mallen till nytta för beslutet om en övergång till molntjänster?
    a. Ja/Nej
    b. Varför/Varför inte?

2. Tycker du att det är något område som saknas alternativt är onödigt?