LUNDS UNIVERSITET
Ekonomihögskolan

# COBIT

## Vid migrering till molnet

Kandidatuppsats, 15 högskolepoäng, SYSK02, Informatik

Framlagd: 2012-05-25

Författare: Tobias Gullberg

Jakob Karlsson

Handledare: Anders Svensson

Examinatorer: Björn Johansson & Odd Steen

## Abstrakt

Organisationer väljer molnet då det ger dem möjlighet till kostnadsbesparingar och att få del i skalbara IT-lösningar för att inte bli begränsade av IT-resursernas kapacitet. Att migrera från en plattform till en molntjänstleverantör kan skapa problem för organisationen. Uppsatsen avser att belysa problematiken som uppstår mellan organisationen och molntjänstleverantören vid en migrering till molnet. Vi vill lyfta fram och identifiera problemområdena och visa hur COBIT kan avhjälpa dessa genom att ge en ökad kontroll. Det har skett insamling av empiriskdata genom intervjuer där data samlats in hos informanter med ledande IT-roller inom organisationerna. Resultatet tyder på att många organisationer hänvisar till avtal och tar lite ansvar själva i form av kontroll av sin leverantör. Tillämpandet av COBIT hade i samtliga organisationer gjort en skillnad för deras styrning och minskat deras problem att utsätta sig för risker.

**Innehållsförteckning**

## Figurförteckning



## Tabellförteckning

# 1. Introduktion

## 1.1 Bakgrund & Problemområde

Organisationer möts ständigt av nya teknologiska förändringar, molnet är en av dessa. Molnet kan ha många teknologiska och kostnadseffektiva fördelar. De ekonomiska fördelarna kan innefatta kostnadsbesparingar genom minskade utgifter och utnyttjande av skalfördelning. Molntjänster gör det även möjligt för organisationer att använda sig av flexibelt skalbara lösningar genom att erbjuda ”On-demand” resurser för att möta kunddrivna kapacitetskrav. (Farrell, 2010)

Användningen av molntjänster är en attraktiv lösning för organisationer som vill förbättra sina IT-tjänster. Organisationen kan uppnå nästan obegränsade skalbarhet av IT-infrastrukturen och detta till en kraftigt reducerad kostnad, i förhållande till om organisationen skulle använda endast intern kapacitet. (Beckers, 2011)

Användningen av en molntjänst förutsätter dock att organisationen litar på leverantören och det faktum att leverantören har tillgång till organisationens data och organisationens kritiska information. Ett sätt att säkerhetsställa förtroendet är att behålla en stark kontroll av molntjänsten. (Beckers, 2011)

Att genomföra en migrering från en plattform till en annan innebär oftast att förutsättningarna förändras. Det blir bättre inom några områden, andra blir sämre, problem uppstår. Problem kan hanteras på flera olika sätt. Organisationen kan sätta upp strategier och policys för hur problem ska undvikas. Organisationer kan tillämpa användningen av ramverk och standarder för att minimera risken för att problem ska uppstå. Att migrera från en plattform till en annan innebär att ett antal främmande scenarier uppstår, scenarier som organisationen måste bedöma och ta ställning till. En migrering kan innebära att organisationen ändrar arbetssätt eller struktur och då måste även gamla rutiner, strategier och standarder anpassas till de nya medel som organisationen försett sig med.

Trots att det finns många fördelar med att migrera till molnet kan organisationer inte bortse från att fortsätta hantera områden som berör grundläggande säkerhetsrelaterade problem, det vill säga integritet, spårbarhet, sekretess och tillgänglighet (Farrell, 2010). För att hantera och avhjälpa grundläggande problem, som kan uppstå vid en migrering, kan det vara lämpligt att arbeta med ramverk som förhåller sig till organisationens affärsmål, IT-processer och IT-resurser. (Van Grembergen, 2009)

Vi vill hävda att organisationer inte alltid är medvetna om de problem som de utsätter sig för då de migrerar till en molntjänst. Kontroll över data minskar och beroendet av molntjänstleverantören ökar. Vi hävdar att organisationer negligerar de problem som användandet av molntjänster innebär i det långa loppet. Att migrera till molnet utan att upprätta kontroller kan få konsekvenser.

Detta fick ett antal av molntjänstleverantören Tietos kunder erfara under hösten 2011 då Tietos datacenter havererade. Detta gjorde bland annat att Apoteket inte kunde lämna ut receptbelagd medicin. Stockholms stads intranät slutade att fungera vilket drabbade alla

förvaltningar, bolag, stadsdelarna och ca 70 000 skolelever. Statliga SBAB påverkades även av haveriet då det inte längre gick att ansöka om lån via deras hemsida eller telefon. Nacka kommun, Bilprovningen och Vetenskapsrådet är också exempel på verksamheter som drabbades vid Tietos haveri. (Jerräng, 2011)

Värderande IT-ramverk så som COBIT (Control Objectives for Information and related Technology) borde ha en stor inverkan vid en migrering till molnet, detta för att förhindra, minska och avhjälpa problem. Vi ställer därför följande fråga:

Hur kan tillämpningen av COBIT förebygga och avhjälpa olika problem som kan uppstå då organisationer migrerar till molnet?

## 1.2 Syfte

Vi vill bidra med att belysa problematiken som uppstår mellan organisationen och molntjänstleverantören vid en migrering till molnet. Undersökningen ämnar identifiera och styrka de problemområden som kan uppstå när en organisation migrerar till molnet. Denna undersökning avser att visa inom vilka områden COBIT kan vara vägledande och avhjälpande vid en migrering till molnet, samt hur COBIT kan bidra med en ökad kontroll gentemot tredje part.

## 1.3 Avgränsningar

Att behandla lagar i olika länder är en problematik som förtjänar en egen uppsats, då olika lagar gäller beroende på i vilket land data befinner sig i för stunden. I en molntjänstmiljö kan det vara svårt att förhålla sig till olika lagar då det är tredje part som lagrar och hanterar detta. Det kan även vara så att tredje part har underleverantören som lagrar och hantera data, vilket gör det väldigt svårt att kontrollera var data fysiskt befinner sig. Därför har vi valt att inte behandla lagar som kan ge upphov till problem vid en migrering till molnet i denna undersökning. Avtal är också ett område som inte behandlas i denna undersökning. Det är svårt att bedöma och hantera avtal utan bred juridisk kompetens. Vi anser att problematiken kring avtal är ett område där väldigt många faktorer spelar in, därför har vi valt att behandla detta område i liten omfattning och med ett visst förbehåll. Vi tittar inte på hur molntjänstleverantören förhåller sig i rollen att agera leverantör vid en migrering till molnet. I vår undersökning kommer vi titta på hur organisationen har upplevt och upplever migreringen till molnet, problem är ett nyckelord i vår undersökning. Vi har därför valt att inrikta oss mot COBIT som IT-styrningsramverk eftersom COBIT är ett holistiskt styrsystem, det är generaliserbart och går att anpassa på åtskilliga organisationer.

# 2. Litteraturgenomgång

I litteraturgenomgången behandlar vi de olika teorierna som berör vår undersökning. Vi behandlar grundläggande karaktärsdrag för molnet, molnlösningsmodeller, molntjänstmodeller och de grundläggande IT-säkerhetskoncepten. Sist behandlar vi COBIT, som är det ramverk vi valt att undersöka. Avsikten är att placera molnet i relation till COBIT.

## 2.1 Karaktärsdrag för molnet

Molnet är en modell för att upprätta konstant tillgänglighet överallt, ”on-demand” nätverksåtkomst till en delad grupp av konfigurerbara datorresurser (t.ex. nätverk, servrar, lagring, program och tjänster) som snabbt kan driftsättas med liten insats från leverantören. Molnet består av fem viktiga egenskaper. Dessa är On-demand self-service, Broad network access, Resource pooling, Rapid elasticity och Measured service. (Mell & Grance, 2011)

### 2.1.1 On-demand self-service

”On-demand self-service” innebär att användare kan beställa och administrera tjänster utan att ha personlig kontakt med personalen hos leverantören. Detta kan ske via en webbportal i kombination med ett administrationsgränssnitt. Etablering och avetablering av tjänster och tillhörande resurser sker automatiskt hos leverantören. Detta kräver en hög grad av automatisering för leverantören.(Grobauer et al, 2011) (Mell & Grance, 2011)

### 2.1.2 Broad network access

Bred nätverksåtkomst innebär att funktioner bör vara tillgängliga via nätet och nås via standardmekanismer som främjar användning genom tunna eller tjocka klienter (t.ex. mobiltelefoner, bärbara datorer och arbetsstationer). (Grobauer et al, 2011)

### 2.1.3 Resourse pooling

Leverantörens datorresurser samlas för att tjäna flera konsumenter, med olika fysiska och virtuella resurser som tilldelas dynamiskt i enlighet med konsumenternas efterfrågan. Kunden har i allmänhet ingen kontroll eller kunskap över den exakta placeringen av de tillhandahållna resurser, men kan eventuellt ha vetskap om lokaliseringen på en övergripande nivå (som till exempel vilket land). Exempel på resurser inkluderar lagring, bearbetning, minne och bandbredd. (Mell & Grance, 2011)

### 2.1.4 Rapid elasticity

Resurserna som används kan skalas upp och ner snabbt, antingen enskilt hos varje användare eller hos alla användare samtidigt. För konsumenten verkar funktionerna som finns tillgängliga för anskaffning ofta vara obegränsade och kan disponeras oavsett mängd när som helst. (Mell & Grance, 2011)

### 2.1.5 Measured service

Användarnas resursanvändning övervakas och mäts kontinuerligt, vilket tillåter optimering av resursanvändningen. Detta ger insyn för både leverantör och konsument av den utnyttjade tjänsten. (Mell & Grance, 2011)

## 2.2 Molnlösningsmodeller

Det finns fyra olika typer av molnlösningar inom molntekniken. Dessa är: Public cloud, Private cloud, Hybrid cloud och Community cloud. Det kan vara viktigt för organisationer att förstå skillnaden mellan de olika typerna av molnlösningsmodeller som beskrivs nedan, detta för att skapa en förståelse för vem som har ansvar för vad.

### 2.2.1 Public Cloud

Publika molntjänster ger användaren möjlighet att ta del av molntjänstleverantörens tjänst, antingen är det gratis eller att man betalar när man använder den. Infrastrukturen ägs av molntjänstleverantören och ger allmänheten möjlighet att använda sig av tjänsten. Användaren har ingen kontroll över större modifikationer utav molntjänsten eftersom all kontroll ligger på molntjänstleverantören. Gmail är ett exempel på en publik molntjänst som är gratis. Gmail är Googles eposttjänst som man får tillgång till genom en webbläsare. (Brunette & Mogull, 2009) (Winkler, 2011)

### 2.2.2 Private Cloud

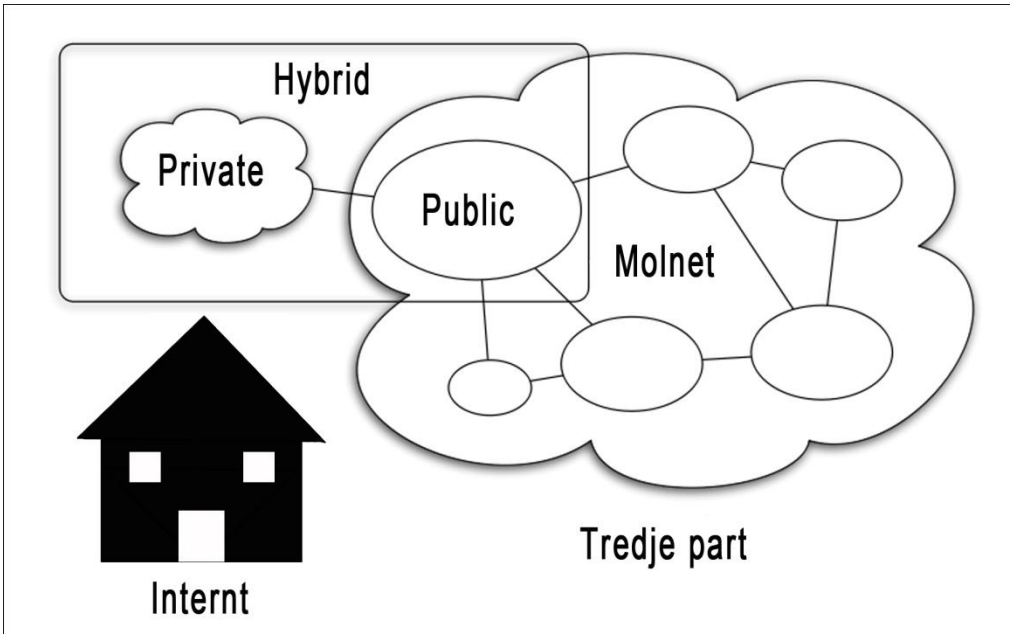
Skillnaden i privata molnlösningar mot publika är att de inte är tillgängligt för allmänheten. De är bara till för en enskild organisation och underhålls enbart av organisationen eller en extern tredje part. En privat molntjänst kan vara placerad externt eller internt, internt hos organisationen eller externt hos molntjänstleverantören.(Brunette & Mogull, 2009)

### 2.2.3 Hybrid Cloud

En hybrid molnlösning är en kombination av flera olika sorters molnlösningar eftersom man då kan köra en del av tjänsterna i det publika molnet samtidigt som en del körs i det privata. Denna kombination består av två eller fler molnlösningar (public, private eller community).(Brunette & Mogull, 2009)

### 2.2.4 Community Cloud

Ett gemenskapsmoln är en molnlösning som delar infrastruktur mellan flera organisationer. Oftast delas det mellan organisationer som har liknande krav på olika faktorer så som säkerhet och inriktning på verksamhet. Denna typ av molnlösning kan finnas fysiskt inom organisationen eller externt hos tredje part. Den kan skötas och underhållas av organisationen eller en tredje part. (Brunette & Mogull, 2009)




**Figur 1. Visuell översikt av Molnlösningsmodeller.**

## 2.3 Molntjänstmodeller

Molntjänstarkitektur kan kategoriseras in i tre olika molntjänstmodeller; Software as a Service, Plattform as a Service och Infrastructure as a Service. Dessa tre molntjänstmodeller är oberoende av varandra. Software as a Service är inriktad på att leverera mjukvara, Platform as a Service är inriktad på att leverera plattform och Infrastructure as a Service är inriktad på att leverera infrastruktur. (Brunette & Mogull, 2009)

### 2.3.1 Software as a Service (SaaS)

Tjänsten som konsumenten får genom att använda SaaS är att leverantören förser konsumenten med applikationer som körs på en molninfrastruktur. Applikationerna är tillgängliga från olika klientenheter genom ett gränssnitt från en tunn klient, så som en webbläsare. Konsumenten hanterar eller kontrollerar inte den underliggande molninfrastrukturen, så som nätverk, servrar, operativsystem och lagring. Konsumenten kan oftast inte reglera individuella applikationers kapacitet. (Brunette & Mogull, 2009)

I vissa fall kan det krävas förberedande arbete för att etablera verksamhetsspecifika behov för tjänsten, så att den tänkta tjänsten integreras med andra applikationer som inte är en del av SaaS plattformen. I en SaaS modell köper konsumenten inte mjukvaran, istället hyr man den genom abonnemang eller ”pay-per-use”. I vissa fall kan tjänsten vara gratis. Tjänsten omfattar ofta hårdvara, mjukvara och support. (Mather et al., 2009)

SaaS modellen är en arkitekturmodell som kan delas av flera användare, vilket innebär att den fysiska bakomliggande hårdvaran delas mellan många olika kunder, men är logiskt unik för varje kund. Arkitektur som används av flera användare maximerar fördelningen av dataresurser mellan användarna, men det går fortfarande att säkert urskilja vilken data som tillhör varje användare. (Mather et al., 2009)

### 2.3.2 Platform as a Service (PaaS)

Tjänsten som konsumenten får genom att använda PaaS är att driftsätta sina förvärvade eller egenutvecklade applikationer på molninfrastruktur. Konsumenten hanterar eller kontrollerar inte den underliggande molninfrastrukturen, så som nätverk, servrar, operativsystem och lagring. Konsumenten har kontroll över de applikationer som satts i drift. (Brunette & Mogull, 2009)

Mather (2009) menar att det är vanligt att leverantören utvecklar verktyg och standarder för utveckling. Mather menar även att PaaS är en variation av SaaS där utvecklingsmiljön erbjuds som en tjänst. Utvecklarna använder fördefinierade kodblock från leverantörerna för att skapa sina egna applikationer. PaaS lösningar är utvecklingsplattformar där utvecklingsverktyget finns i molnet och är tillgängligt genom en webbläsare. PaaS gör det möjligt för utvecklare att skapa webb-applikationer utan att installera några verktyg på datorn och kan därefter driftsätta dessa applikationer utan några specifika systemadministrationskunskaper. (Mather et al., 2009)

### 2.3.3 Infrastructure as a Service (IaaS)

Tjänsten som konsumenten får genom att använda Iaas är att tillhandahålla bearbetning, lagring, nätverk och andra grundläggande datorresurser där konsumenten kan driftsätta och köra valfri mjukvara som kan inkludera operativsystem och applikationer. Konsumenten hanterar och kontrollera inte underliggande molninfrastruktur men har kontroll över operativsystem, lagring, driftsatta program och eventuellt begränsad kontroll av valda nätverkskomponenter som till exempel brandväggar. IaaS modellen tillhandahåller infrastrukturen för att köra applikationer, men molnet gör det även möjligt att erbjuda en "pay-per use" modell och att skala tjänsten beroende på efterfrågan. I en IaaS modell betalar konsumenten endast för till exempel den mängd processorkraft, diskutrymme, som konsumenten förbrukar.(Brunette & Mogull, 2009)

Från IaaS leverantörens perspektiv kan man bygga upp en infrastruktur som hanterar efterfrågan för kundernas krav och lägga till ny kapacitet när efterfrågan ökar.

## 2.4 IT-Säkerhetskoncept

I detta avsnitt redogör vi för fyra grundläggande principer vad gäller IT-säkerhet. Vi kopplar dessa koncept till dess relevans vid användning av molntjänster. Detta gör vi för att styrka att de är relevanta och även går att applicera på molntjänster.

### 2.4.1 Spårbarhet

Inom informationssäkerhet är det nödvändigt att säkerställa att data, transaktioner, kommunikation eller handlingar (elektronisk eller fysisk) är äkta. Det är också viktigt för äktheten att validera att inblandade parter är dem de utger sig för att vara. Detta innebär att data ska kunna spåras samt att man då ska kunna fastställa vem som har gjort vad, när och hur. (Winkler, 2011)

För att garantera spårbarhet i molnet kan olika IT-protokoll användas, till exempel IPSec. Detta möjliggör att skicka och ta emot kryptografiskt skyddade paket utan att de modifieras.

IPSec är ett protokoll som förser två typer av kryprografitjänster. Beroende på behovet kan IPSec förse konfidentialitet och spårbarhet, eller endast spårbarhet. (Zissis & Lekkas, 2010)

### 2.4.2 Integritet

Integritet innebär att data skyddas mot otillåten eller felaktig ändring, samt skydd mot borttagning av information. Integritet kränks när information aktivt modifieras under transporten. Upprätthållandet av integritet medför även att man säkerställer informationens äkthet. (Winkler, 2011)

Integritet i molnet handlar om att en kund till en molntjänstleverantör validerar integriteten av sin data under tiden den finns i molnet, utan att kunden behöver ladda ner och upp denna data. Det finns utmaningar med integriteten i molnet, oftast vet inte kunden på vilken fysisk maskin som data är lagrad eller var detta system är lokaliserat. Dessutom är denna typ av teknik dynamisk och förändras konstant. Dessa ständiga förändringar förhindrar effektiviteten av traditionella tekniker som försäkrar integriteten.(Mather et al., 2009)

### 2.4.3 Tillgänglighet

Tillgänglighet innebär att kunna säkerställa snabb och tillförlitlig tillgång till information när man är i behov av den. Detta innebär att datorsystem som används för att lagra och bearbeta information, säkerhetsåtgärder som används för att skydda den och de kommunikationskanaler som används för att komma åt den måste fungera korrekt. Brist på tillgänglighet uppstår när det blir ett avbrott i åtkomsten till informationen, eller vid problem med användningen av ett informationssystem. System ska ha som mål att hela tiden ha hög tillgänglighet. Trafikstörningar på grund av strömavbrott, maskinvarufel och systemuppgraderingar ska förebyggas. Försäkra tillgängligheten innebär även att förebygga ”denial-of-service-attacker.” (Winkler, 2011)

När det kommer till att säkra tillgängligheten i molnet vad gäller publika molntjänster är det viktigt att tänka på följande:

- Säkerställa sekretessen och integriteten för organisationens överföring av data till och från den publika molntjänstleverantören.
- Säkerställa god åtkomstkontroll till de tjänster som används hos den publika molntjänstleverantören.
- Säkerställa tillgängligheten på internetbaserade tjänster i ett publikt moln som används av organisationen

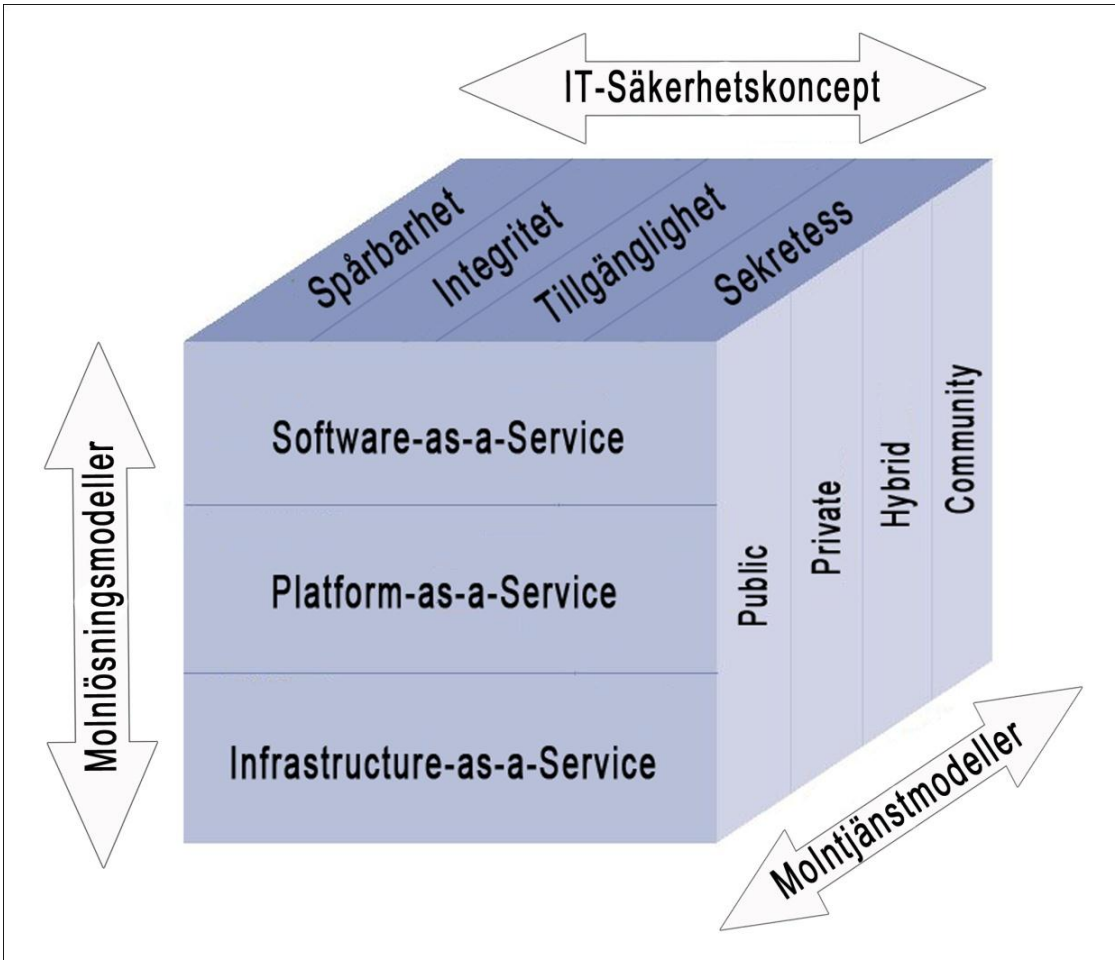
(Winkler, 2011)

### 2.4.4 Sekretess

Sekretess är den term som används för att förhindra utlämnandet av information till obehöriga personer eller system. Sekretess innebär att upprätthålla fastställda restriktioner för åtkomst till information och utlämnande av information. Även åtgärder för att skydda den personliga integriteten och patentskyddad information hanteras under denna kategori. Sekretessen upprätthålls inte ifall obehörig har eller kan få tillgång till informationen. (Winkler, 2011)

När det handlar om sekretesshantering av data som lagras i publika moln finns det två potentiella problemområden. Det första är: Finns det åtkomstkontroll för att skydda data? Åtkomstkontrollen ska bestå av både autentisering och auktorisering (godkännande). Det är vanligt att molntjänstleverantören använder sig av svaga autentiseringsmetoder/mekanismer, till exempel användarnamn och lösenord. Auktoriseringskontrollen för användare tenderar att vara grova. För stora organisationer kan denna grovhet i auktoriseringskontrollen vara ett säkerhetsproblem i sig. (Mather et al., 2009)

Det andra problemområdet är: Hur är data som lagras i molnet egentligen skyddad? Skydd av data lagrad i molnet involverar användningen av kryptering. Det är viktigt att organisationen själva hanterar sina krypteringsnycklar. Det anses inte lämpligt att låta molntjänstleverantören hantera dessa krypteringsnycklar åt organisationen. Det kan vara svårt för organisationer att hantera och förvalta sina egna krypteringsnycklar, det är därför ännu svårare för en molntjänstleverantör att förvalta och hantera alla kunders krypteringsnycklar. Det är därför vanligt att en molntjänstleverantör krypterar all kundens data med en enda nyckel. (Mather et al., 2009)




**Figur 2. Molnet i förhållande till IT-säkerhet.**

*Översikt av sambandet mellan IT-Säkerhetskoncepten, molnlösningsmodell och molntjänstmodell.*

## 2.5 COBIT

### 2.5.1 Definition

COBIT (Control Objectives for Information and related Technology) är ett ramverk som syftar till att överbygga klyftan mellan kraven på kontroll, tekniska frågor, affärsrisker samt att presenterar IT aktiviteter på ett hanterbart och logiskt sätt. COBIT publiceras av Information Systems Audit and Control foundation (ISACA, 2012).(Pathak, 2005)

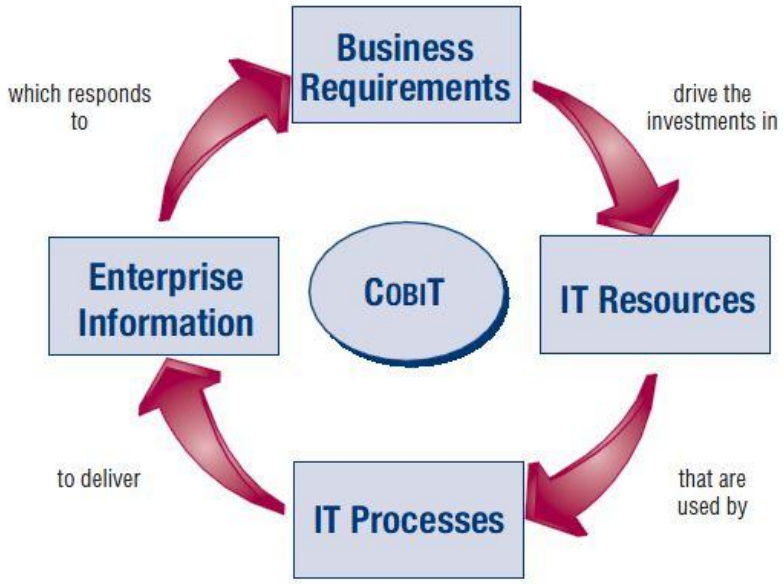
ISACA grundades 1967. Idag har ISACA mer än 95,000 medlemmar i 160 länder. Medlemmarna har IT-relaterade positioner så som IT revisor, konsult, utbildare, IS säkerhetsexpert, CIO och intern revisor. ISACA:s medlemmar arbetar i nästan alla olika näringslivsgrenar så som bank och finans, offentlig redovisning, regering och offentliga sektorn samt tillverkning.(ISACA, 2007)

Enligt Pathak (2005) är en av styrkorna med COBIT att tillhandahålla tydliga riktlinjer till ledningen. Pathak (2005) menar att chefer måste förstå statusen för deras IT-system och bestämma vilken säkerhet och kontroll de ska ge, vilket de kan uppnå genom att använda COBIT. Pathak (2005) menar att detta i praktiken innebär att det kontinuerligt behövs förbättring av IT-säkerhet och kontroll. Genom att följa COBIT:s riktlinjer kan organisationer till exempel jämföra och mäta deras process i förhållande till klienters och organisationens egen strategi, och uppnå en konkurrenskraftig IT-säkerhet och kontroll. (Pathak, 2005)

### 2.5.2 Introduktion

COBIT definierar IT-aktiviteter i en generisk processmodell inom fyra områden. De fyra områden är: Plan and Organize, Acquier and Implement, Deliver and Support och Monitor and Evalutate. COBIT-ramverket förser en hänvisande processmodell och ett gemensamt språk för alla i en organisation att se och hantera IT-aktiviteter. Enligt COBIT (2007) är det ett av de viktigaste stegen i god styrning att införliva en operativ modell och ett gemensamt språk för alla delar av organisationen som är involverade i IT. COBIT är även ett ramverk som omfattar mätning och övervakning av IT-prestanda, kommunikation med tjänsteleverantörer och integrering med bästa ledningspraxis. Med en processmodell så som COBIT uppmuntras processägande, vilket gör det möjligt att definiera ansvar och ansvarsskyldigheter. (ISACA, 2007)

COBIT har tydligt affärsfokus och är utformat för att inte enbart användas av IT-leverantörer, användare och revisorer, utan även för att förse grundliga anvisningar för ledning och affärsprocessägare. För att organisationer ska upprätthålla den information som verksamheten kräver måste organisationen investera i samt hantera och kontrollera IT-resurser. I COBIT sker detta genom att ett antal strukturerade processer tillhandahåller de tjänster som levererar den önskade verksamhetsinformationen (se figur 3). Affärskriterier driver investeringar i IT-resurser. IT-resurser används av IT-processer. IT-processer levererar verksamhetsinformation. Verksamhetsinformationen bemöter affärskriterierna. (ISACA, 2007)



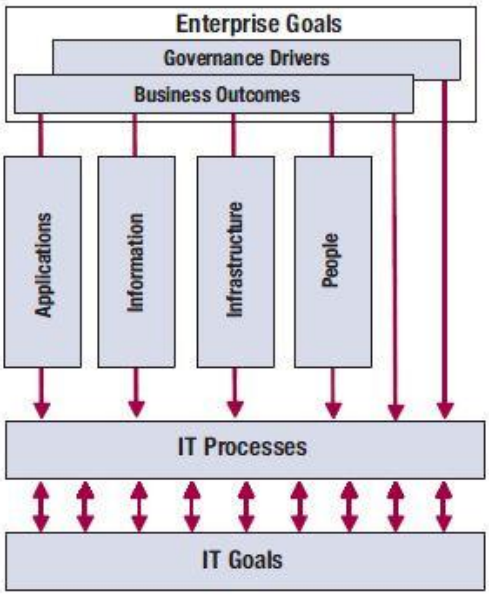

**Figur 3. Grundläggande principer för COBIT. (ISACA, 2007, s.10)**

För att organisationens affärskriterier för IT ska kunna hanteras av COBIT måste organisationen investera i väsentliga resurser som resulterar i önskade resultat (ISACA, 2007).

För en översikt på de IT-resurser som COBIT hanterar (se figur 4). IT-resurserna i COBIT är definierade enligt:

- Applikationer är de manuella procedurerna och de automatiserade användarsystemen som behandlar informationen.
- Informationen är data som finns i många olika former. Den är i form av input där den blir behandlad och resulterar i en output.
- Infrastruktur är den teknologi och utrustning som används. Det kan vara hårdvara, operativsystem och nätverk. Dessa är till för att hantera informationen.
- Människor är personal som är nödvändiga för att planera, organisera, förvärva, genomföra, leverera, stödja, övervaka och utvärdera informationssystemen och tjänsterna. Människorna är efter behov interna, externa eller kontrakterade.

(ISACA, 2007)

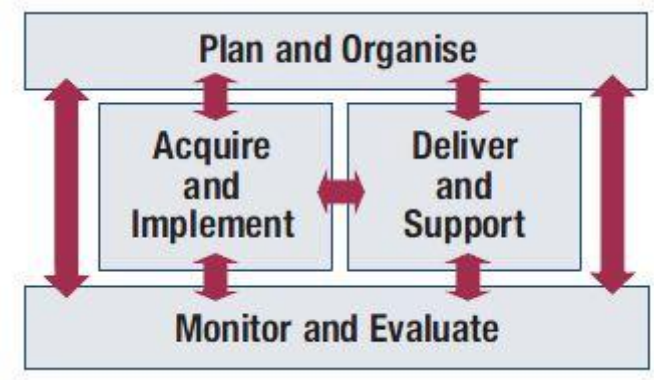



**Figur 4. Hantering av IT-resurser för att leverera IT-mål. (ISACA, 2007 s.12)**

För att få en effektiv IT-styrning är det enligt COBIT viktigt att uppskatta aktiviteterna och riskerna inom IT. COBIT definierar aktiviteterna inom de fyra följande områdena Plan and Organize, Acquire and Implement, Delivery and Support och Monitor and Evaluate. Områdena består i sin tur av totalt 34 underprocesser som i sin tur har totalt 316 aktiviteter. Se figur 5 för de fyra sammankopplade områdena i COBIT. (ISACA, 2007)

De fyra områdena i COBIT är:

- Plan and Organize - ger vägledning om lösning till leverans (Acquire and Implement) och leverans av tjänst (Deliver and Support)
- Acquire and Implement - ger vägledning om lösningar och skickar dem till att omvandlas till tjänster.
- Deliver and Support - tar emot lösningarna och gör dem användbara för slutanvändarna.
- Monitor and Evaluate - övervakar alla processer för att försäkra att den förutsatta riktningen följs.
  (ISACA, 2007)




**Figur 5. De fyra sammankopplade områdena i COBIT. (ISACA, 2007 s.12)**

**Plan and Organize**
Denna del behandlar strategi och taktik och avser identifiering av hur IT bäst kan bidra till att uppnå affärsmålen. Förverkligandet av den strategiska visionen bör planeras, kommuniceras och hanteras i förhållande till olika perspektiv. En korrekt organisation samt en teknologisk infrastruktur bör införas. (ISACA, 2007)

**Acquire and Implement**
För att förstå IT-strategi måste IT lösningar identifieras, utvecklas eller förvärvas. De måste även implementeras och integreras in i affärsprocessen. Dessutom är förändringar i och underhåll av existerande system inräknade i detta område för att säkerställa att lösningarna fortsätter att möta affärsmålen. (ISACA, 2007)

**Deliver and Support**
Leverans och stöd behandlar leverans av tjänster, hantering av säkerhet, support för användare och hantering av uppgifter. (ISACA, 2007)

**Monitor and Evaluate**
Detta område behandlar kontroll och att IT-processer måste bedömas regelbundet för att säkra kvalitén för de olika kontrollkraven. Monitor and Evaluate behandlar verksamhetsstyrning, intern kontroll och styrning. (ISACA, 2007)

## 2.6 Problematiska områden vid migrering till molnet

I detta avsnitt behandlar vi problematiska områden som uppstår vid en migrering till molnet. Dessa problem är kända sedan tidigare. Därefter identifierar vi processer i COBIT som kan knytas till dessa problemområden.

De specifika problemen beror på organisationen och dess individuella krav. De gemensamma säkerhetsproblemen i alla organisationer (genom hela spektrat) är att säkerställa sekretess, integritet, spårbarhet och tillgänglighet på de tjänster och den data som levereras i en molnmiljö. (Small, 2007)

De viktigaste informationssäkerhetsrelaterade problemen en organisation som migrerar till molnet måste ta ställning till sammanställs nedan. På grund av det breda omfång som omfattar molnet kommer prioriteringen av dessa bero på val av molntjänstmodeller och organisationens individuella omständigheter. (Small, 2007)

**Val av molntjänstleverantör**

Efterlevnad av regler och lagar i olika geografiska regioner kan vara en utmaning för organisationer. Det är viktigt att få en ordentlig juridisk rådgivning för att säkerställa att avtalet anger de områden där molntjänstleverantören är ansvarig för konsekvenserna som följer av potentiella problem. Organisationer ska klara av att efterleva strikta globala krav och välja en molntjänstleverantör som kan möta dessa krav och kan styrka att dessa efterlevs. (Ahmed, 2011)

**Minskad styrning**

Att använda sig av molnet förutsätter att organisationen ger upp kontrollen över sin IT-infrastruktur. För att detta ska fungera på ett smidigt sätt bör molntjänstleverantören göra hantering och underhåll transparant och kontrollerbar för kunden. Detta omfattar lagring av loggar och administrativa sessioner som påverkar den del av molninfrastrukturen som används av kunden. Dessa uppgifter ska på begäran göras tillgängliga för kunden. (Ahmed, 2011)

**Kontrakt för tjänst**

De kontrakt som molntjänstleverantören erbjuder är anpassade så att de ska gynna molntjänstleverantören. De innehåller mindre betungande skyldigheter för leverantören än vad vanliga SLA gör. Det är viktigt att ta upp frågor angående vem som äger informationen och hur svårt det är att få tillbaka informationen vid en förlust av data. (Small, 2011)

**Datasäkerhet**

Berörd verksamhetsdata ska identifieras och klassificeras och det ska anges säkerhetskrav för denna data i form av, integritet, tillgänglighet och sekretess. (Small, 2011)

**Geografisk placering av tjänst**

Juridiska frågorna relaterade till den geografiska placeringen av molntjänstleverantören, tjänsten och data måste identifieras. Det ska framgå att avtalen behandlar dessa problem. (Small, 2011)

**Tillgänglighet**
Kraven på tillgänglighet ska identifieras och det ska kontrolleras att leverantören kan uppfylla kraven på tillgänglighet.(Small, 2011)

**Identitet och åtkomsthantering**
Organisationens krav och behov för åtkomstkontroll och identitetshantering ska definieras. Det ska även säkerhetsställas att dessa krav och behov levereras på ett säkert sätt. (Small, 2011)

**Missbruk av behörighet**
Det ska vara säkerhetsställt att molntjänstleverantören har processer och teknik för att på ett korrekt sätt kontrollera den priviligierade åtkomst till data som molntjänstleverantören har. (Small, 2011) (Gregg, 2010)

**Internethot**
Bestäm nivån av skydd som behövs mot Internet-baserade hot och försäkra att detta efterföljs av både molntjänstleverantören och internt av organisationen. (Small, 2011) (Gregg, 2010)

**Övervaka**
Det ska finnas övervakning av molntjänstleverantören för att se till att molntjänstleverantören överensstämmer med lagar och de verksamhetskrav som kunden har satt upp. Olika kunders data ska även särskiljas. (Small, 2011)

### 2.6.1 Identifierade processer i COBIT
I tabell 1 (se sida 24) visar vi en sammanställning av de processer i COBIT som vi har identifierat i förhållande till de problemområden som beskrivs i avsnittet ovan (se avsnitt 2.6). Alla processer i COBIT som är identifierade och som presenteras i detta avsnitt går att koppla till de problemområden som finns enligt Small och Ahmed. Detta gör vi för att styrka vårt val av processer i COBIT samt för att visa att hela COBIT-ramverket inte är relevant vid en migrering till molnet. Enligt Björngren, Gullberg, Karlsson, Kvarnryd & Mattson (2012) kan dessa processer i COBIT påverka IT-säkerhetskoncepten om de inte efterlevs.

### 2.6.2 COBIT-Processerna
**PO2 Define the Information Architecture**
Denna process behandlar användandet av ett dataklassificeringsschema för organisationen och användandet utav syntaxregler för data i systemen. Denna process förbättrar beslutsfattandets kvalité genom att förstärka att trovärdig och säker information tillhandahålls.

Denna IT-process är viktig för att öka ansvar för integritet och säkerhet av data och för att öka effektiviteten och kontrollen av att dela information mellan applikationer och enheter.

Organisationen ska även fastställ och implementera procedurer för att säkerställa integriteten av all data som lagras i elektronisk form, till exempel i databaser, datalager och dataarkiv. (ISACA, 2007)

**PO9 Assess and Manage IT Risks**
Denna process innebär att bedöma och hantera IT-risker. Ett ramverk för hantering av risker ska etableras i organisationen. Ramverket ska dokumentera en allmän och överenskommen nivå av IT-risker och strategier för riskminskning. Organisationen ska identifiera, analysera och utvärdera oplanerade händelser. Riskreducerande strategier antas för att minimera kvarstående risker till en godtagbar nivå. Organisationen ska på återkommande basis bedöma sannolikheten för, och effekten av, alla identifierade risker med hjälp av kvalitativa och kvantitativa metoder. Sannolikheten för och konsekvenserna i samband med inre och kvarvarande risker bör fastställas individuellt efter kategori. (ISACA, 2007)

**AI2 Acquire and Maintain Application Software**
Processen behandlar organisationens behov av att göra applikationer tillgängliga i förhållande till verksamhetskriterierna. Det innefattar design, säkerhetskrav, applikationskontroller och anpassning till standarder. Detta möjliggör att de automatiserade applikationerna stödjer affärsverksamheten. Detta ska ligga i linje med organisationens dataklassificeringsschema, informationsarkitektur, informationssäkerhet och risktolerans. (ISACA, 2007)

**AI5 Procure IT Resources**
Denna process behandlar upphandlingen av IT-resurser. Detta inkluderar hårdvara, mjukvara, tjänster och människor. Organisationen ska definiera och tillämpa procedurer för upphandlingarna av val av leverantörer och avtal. Detta för att se till att organisationen har alla de nödvändiga IT-resurser som krävs. (ISACA, 2007)

Processen innebär även att organisationen ska skapa en procedur för att etablera, modifiera och avsluta kontrakt för alla leverantörer. Den här proceduren bör innefatta legala-, finansiella-, organisatoriska-, dokumentations-, prestanda-, säkerhets- och immateriella rättigheter. Även uppsägningsansvar och ansvarsförbindelser bör finnas. Alla ändringar i kontrakt/avtal bör granskas av juridiska rådgivare. (ISACA, 2007)

Val av leverantör bör ske enligt en rättvis och formell praxis för att säkerställa att leverantören som väljs passar bäst baserat på organisationens specifika krav. Krav bör optimeras med input från potentiella leverantörer.( ISACA, 2007)

**AI7 Install and Accredit Solutions and Changes**
Efter att utvecklingen och den fullständiga testningen är klar ska de nya systemen sättas i drift. För att driften ska fungera gäller det att det finns en plan för hur systemen ska appliceras i organisationen. Detta görs för att se till att systemen stämmer överens med de förväntade resultaten. (ISACA, 2007)

Organisationen ska förse de anställda med utbildning av de nya systemen. Processen behandlar behovet av att organisationen ska tillhandahålla en strategi för att avsluta eller backa ur tjänsten om det skulle bli aktuellt. Strategin ska genomföras med godkännande av berörda parter.

Processen behandlar behovet av att ha en plan för datakonvertering och infrastrukturens migrering. Det ska innefatta återställnings- och reservplaner. Det är viktigt att genomföra ett

slutligt test av systemen för att förhindra och åtgärda problem som upptäcks i testprocessen. (ISACA, 2007)

**DS1 Define and Manage Service Levels**
Processen behandlar tillgodogörandet av anpassning mellan IT-tjänster och de relaterade verksamhetskrav. Det ska finnas Service Level Agreements (SLA) vilka definierar vad som ska omfattas, såsom kundens åtaganden och support. I SLA ska det finnas definierat vad som kommer att vara kundens åtaganden samt olika typer av mått som kommer att användas för att mäta tjänsten. Det är lämpligt att det definieras krav på tillgänglighet och prestanda.( ISACA, 2007)

**DS2 Manage Third-party Services**
I DS2 behandlas behovet av att säkerhetsställa att tredje part kan tillhandahålla tjänsterna. Detta ska ligga i linje med verksamhetens kriterier. Att säkerhetsställa tredje part innebär att definiera ansvar, förväntningar av avtal och roller. Det ska även ske en övervakning av avtalen för att se till att effektivitet efterföljs. Effektiv hanteringen av tredje part ser till att risker minimeras i förhållande till osäkra leverantörer. Det är viktigt att identifiera och minska riskerna relaterade till leverantörens förmåga att effektivt fortsätta leverera en tjänst på ett säkert och effektivt sätt på en kontinuerlig basis. (ISACA, 2007)

Den här processen behandlar formaliseringen av processen för hanteringen av leverantörsförhållanden för varje leverantör. De inblandade parterna bör samarbeta angående kund- och leverantörsfrågor och kvalitén säkerställs genom att relationen bygger på förtroende och öppenhet, till exempel genom SLA. (ISACA, 2007)

**DS3 Manage Performance and Capacity**
Processen behandlar behovet av att se över och hantera prestanda och kapaciteten för de olika IT-resurserna. En prognos för framtiden ska upprättas för att utvärdera behovet av IT utifrån dagens behov och belastning på IT-resurserna. Detta ska göras för att säkerhetsställa att systemen är tillgängliga. (ISACA, 2007)

Det ska finnas bestämmelser så som prioritering av uppgifter, feltoleransmekanismer och praxis för resurstilldelning ska klargöras. Ledningen bör se till så att beredskapsplaner behandlar tillgänglighet, kapacitet och prestanda för individuella IT-resurser. (ISACA, 2007)

**DS4 Ensure Continuous Service**
I processen behandlas behovet av att genomföra återkommande underhåll och testning av olika IT-scenarier. Testningen innebär att kontrollera att backuper som sker på systemen fungerar. Genomförandet av detta innebär att sannolikheten för IT-avbrott på viktiga affärsfunktioner och processer minskar. Det ska fastställas vilken data som ska finnas med i backupen**.** Det ska ske kontroller där säkerheten hos leverantören utvärderas. Det ska säkerhetsställas att hårdvara och mjukvara är kompatibelt med arkiverad data. Den arkiverade datan ska testas och uppdateras. (ISACA, 2007)

**DS5 Ensure Systems Security**
I DS5 beskrivs behovet av se till att integriteten upprätthålls och att IT-tillgångar skyddas. Detta kräver att det finns en process för säkerhetshantering. Denna process innebär att etablera och underhålla de olika rollerna och ansvarsområdena för IT-säkerhet. En säkerhetshantering ska genomföras återkommande för att åtgärda och identifiera svagheter i säkerheten. Genom att använda sig av en effektiv säkerhetshantering så skyddas organisationens IT-tillgångar och minimerar konsekvenserna vid ett eventuellt säkerhetsproblem. (ISACA, 2007)

Processen innebär att alla användare och deras aktiviteter i ett IT-system ska vara unikt identifierbara. Användaridentifieringen ska aktiveras via autentiseringsmekanismer. Kontroll av användarens åtkomstsrättigheter till system och data ska ske i förhållande till affärsbehov. (ISACA, 2007)

**DS11 Manage Data**
Denna process innebär att datahantering krävs för att identifiera informationskraven. I datahanteringen ska metoder för hantering av backup och återställning av data finnas. En effektiv hantering av data hjälper till att se till att kvalitén och tillgängligheten på data är säkerhetsställd. (ISACA, 2007)

Processen innebär att införa procedurer för hur känslig data ska hanteras när information raderas eller hårdvara avverkas eller förflyttas. Om inte rätt tillvägagångssätt för radering av känslig data, alternativt vid avverkning eller förflyttning av hårdvara existerar, riskerar organisationen att informationen hamnar i obehöriga händer. Procedurer för säkerhetskopiering och återställning av system, applikationer och data ska finnas i enlighet med verksamhetens krav. (ISACA, 2007)

**DS13 Manage Operations**
DS13 processen behandlar kravet på att det ska finnas procedurer för övervakning av IT-infrastrukturen och relaterade händelser. Händelserna ska sparas i loggar för att användas vid en utvärdering och rekonstruktion av händelsen och händelserna runt den. Finns det en effektiv verksamhetshantering hjälper det till att bibehålla dataintegritet och det ser även till att reducera driftkostnader för IT. (ISACA, 2007)

**ME2 Monitor and Evaluate Internal Control**
Processen innebär att övervakning ska vara återkommande och förbättrande. IT-kontrollen och kontrollramverket ska jämföras för att nå upp till organisationens mål. Det ska även ske bedömningar hos tredje part för att se till att deras interna kontroll fungerar. Kontrollen sker för att se till att tredje part följer lagar och avtal. (ISACA, 2007)

**ME4 Provide IT Governance**
Processen avser vikten av att etablera ett ramverk för styrning som innehåller organisationens struktur, processer, ledarskap, roller och ansvarsområden. Detta görs för att se till att investeringarna inom IT är levererade och i linje i förhållande till organisationens strategier och mål. Ramverket ska förhålla sig till organisationens mål och strategier, det ska även fungera i enlighet med lagar. (ISACA, 2007)

**Tabell 1. Problem kopplade till processer i COBIT**

| Problem/Process | PO2 | PO9 | AI2 | AI5 | AI7 | DS1 | DS2 | DS3 | DS4 | DS5 | DS11 | DS13 | ME2 | ME4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Val av molntjänstleverantör | | | | X | | | | | | | | | | |
| Minskad styrning | | | | | | | | | | | | X | | |
| Kontrakt för tjänst | | | | | X | X | X | | | | | | | |
| Datasäkerhet | X | | | | | | | | X | | X | | | |
| Geografisk placering av tjänst | | | | | | | | | | | | | X | |
| Tillgänglighet | | | X | | | X | | X | | | X | | | |
| Identitet och åtkomsthantering | | | | | | | | | | X | | | | |
| Missbruk av behörighet | | | | | | | | | X | | | | X | |
| Internethot | | X | | | | | | | | X | | | | |
| Övervaka | | | | | | | | | | | | | | X |

*Tabellen visar vanliga problematiska områden vid migrering till molnet och processer i COBIT. De olika problemen har kopplats till den eller de processer i COBIT som är relevant för respektive problemområde.*

## 2.7 Motivering för COBIT

I detta avsnitt vill vi styrka varför vi har valt COBIT som ramverk för vår undersökning. COBITS styrka ligger i dess fokus på IT-hantering, kontroll och bredd. COBIT hjälper dessutom ledningen att förstå vad det är de behöver göra för att säkerställa att investeringar i deras IT maximeras kring affärsnytta, inte utsättas för oacceptabla risker samt följer nödvändiga krav. COBIT förklarar dock inte hur detta ska genomföras, utan bara vad som ska genomföras. (Symons, C. Orlov, L. M. Brown, K. & Bright, S. 2006)

> ”COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.” (Sahibudin, S. Sharifi, M. & Ayat, M. 2008, s.751)

# 3. Metod

## 3.1 Angreppssätt

Vi genomförde tre intervjuer. Två av dem genomfördes via telefon och en genomfördes ansikte mot ansikte. En fjärde informant ville endast delta i undersökningen och svara på våra frågor om detta kunde ske skriftligt via mail. Enligt Jacobsen (2002) så finns det fyra olika typer av metoder för datainsamling; den individuella öppna intervjun, gruppintervjun, observation och dokumentundersökning. Eftersom vi bara intervjuade ett fåtal informanter så menar Jacobsen (2002) att det är bäst att genomföra individuella intervjuer. Våra intervjuer utformades efter givet tema, fast ordningsföljd och öppna svar. Vi valde att genomföra de undersökningarna som var via telefon och ansikte mot ansikte som semistrukturerade intervjuer eftersom det gav oss möjligheten att styra frågorna men ändå ge informanterna utrymme att svara öppet. Den intervjun som var utskickad var formulerad på samma sätt som de övriga men det var fortfarande fritt för informanten att svara som denne ville men det gav oss inga möjligheter att ställa följdfrågor på svaren eller för informanten att ställa motfrågor.

Under vår intervju valde vi att inte ha några fasta svarsalternativ eftersom det enligt Jacobsen (2002) är en sådan strukturering ett slags slutning av datainsamlingen vilket inte motsvarar en kvalitativ metod.

## 3.2 Intervjudel

Vi har valt att inhämta det empiriska materialet från ett antal kvalitativa intervjuer för att på så sätt få utförliga svar. Vi har valt att genomföra individuella öppna intervjuer med företagens mest kompetenta personal inom området, som till exempel IT-chefen eller IT-ansvarig. Detta tillvägagångssätt har vi valt eftersom det ger möjlighet att ställa följdfrågor och på så sätt utveckla svaren från informanterna i de fallen när vi inte gjorde en dokumentundersökning. Jacobsen (2002) anser att det är olämpligt att genomföra telefonintervju vid genomförandet av öppna personliga intervjuer. Jacobsen (2002) menar att det är lättare att ej tala sanning i en telefonintervju. Vi anser att telefonintervjuerna har gett oss möjligheten att inte vara geografiskt begränsad vilket gav oss möjligheten att intervjua relevanta informanter som kunde bidra med kvalitativa svar.

Vi har intervjuat tre olika personer på två olika organisationer via telefon. Vi har genomfört en intervju ansikte mot ansikte på en av organisationerna. Enligt Jacobsen (2002) tycks personer ha lättare att prata om känsliga ämnen i intervjuer ansikte mot ansikte än i telefon. Vi anser inte att det har varit någon skillnad i kvalitén mellan intervjuer som genomfördes ansikte mot ansikte och de som vi genomförde via telefon. Svaren som vi fick skriftligt via mail från en organisation anser vi också vara av hög kvalité, då de gav oss utförliga och precisa svar.

### 3.2.1 Urvalskriterier för organisationer

Vi har valt organisationer utifrån följande kriterier:

- Utförd migrering
- De ska ha en molntjänstleverantör

### 3.2.2 Urval av informanter

När vi skulle välja informanter ansåg vi att det var av stor vikt att personen i fråga hade bred kompetens inom området för vår undersökning och våra intervjufrågor. För att vara säkra på att få tala med rätt personer i organisationen bad vi att få tala med organisationens Chief information officer (CIO) vid den första kontakten. I tre av intervjufallen så var det CIO:n som ställde upp på intervju med oss. I ett fall hänvisade CIO:n till en person med specifik kompetens på området. När vi hade fått tag i rätt personer som var villiga att ställa upp på intervju, skickade vi frågorna till dem ett antal dagar innan vi utförde intervjun så att de kunde förbereda sig. I ett av fallen när vi intervjuade en CIO var även en IT-projektledare delaktig.

### 3.2.3 Design av intervjuguide

Intervjuguiden (se bilaga 5) som vi har baserat våra intervjuer på består av fem områden bestående av totalt 22 frågor samt med några följdfrågor. Vi gjorde denna indelning för att på så sätt kunna avgränsa och ge struktur i intervjun. Våra intervjuer varade mellan 45 minuter och lite över en timme. Det är olämpligt enligt Jacobsen (2002) att ha intervjuer som är längre än en och en halv timme. Vi hade lagt upp strukturen så att intervjun började med övergripande frågor för att sedan gå in på mer avancerade frågor. Vi delade in intervjun i följande områden:

- Inledande frågor
- Molnspecifika frågor
- Migreringsfrågor
- Driftsfrågor
- Reflekterande frågor
- Styrningsfrågor

*Intervjufrågor*

*Inledande*

De inledande intervjufrågorna började med att vi skulle få den intervjuade att känna sig bekväm i situationen. Därför är frågorna av sådan art att den intervjuade kan prata fritt om de delar han eller hon känner sig trygg i. De inledande frågorna i sig har ingen avgörande roll i vår intervju, utan ses som frågor för att skapa förtroende och dialog mellan den intervjuade och vi som intervjuar. Vi ställer även frågor för att styrka att den vi intervjuar är kompetent att svara på de frågor som intervjun handlar om. Vi som intervjuar kan ställa följdfrågor om det är något som är oklart eller om vi vill ha ytterligare bevisning för att den intervjuade är kompetent att svara på frågorna som följer.

*Molnet*
Dessa frågor är av den karaktären att det ger en övergripande bild över området och ger oss en förståelse för deras syn på området. Vi frågar även varför organisationen har valt att använda sig av molnet. Detta gör vi för att styrka att de relaterar till de karaktärsdrag som molnet har, dessa behandlar vi under rubriken 2.1 Karaktärsdrag för molnet. Vi vill även ta reda på hur en organisation förhåller sig till begreppet molnet och vilka tjänster de använder sig av i molnet. De olika molntjänststandarderna behandlar vi under 2.3 Molntjänstlösningar. Vi frågar även hur den intervjuade ser på säkerhet i molnet i förhållande till att använda ”icke” molntjänster. Vi frågar även om de ser specifika risker med att använda molnet. Dessa frågor ställer vi för att styrka att de IT-säkerhetskoncepts som vi behandlar under rubriken 2.4 IT-säkerhetskoncept är relevanta och av betydelse.

*Migrering*
Med dessa frågor vill vi få den intervjuade att utförligt beskriva hur de har förhållit sig till informationssäkerhet och olika ramverk och de delar som användes innan och under de valde att byta IT-miljö. Vissa frågor i denna del är specifik och förutsätter att den intervjuade är insatt i och har förståelse för hur organisationen arbetar med ramverk. Vi är medvetna om att det kan vara svårt att svara på då ramverk inte har använts eller om de bara har haft en stödjande roll. Vi vill undersöka om organisationer arbetar utifrån ramverk och vilken betydelse det i så fall har haft vid en migrering. Vi frågar även om organisationen haft problem vid migreringen, detta gör vi för att påvisa ramverks betydelse vid IT-styrning.

*Drift*
Den här delen behandlar tiden efter en migrering, hur organisationen arbetar med uppföljning och kontroll löpande. Vi vill undersöka om det finns något informationsutbyte mellan organisationen i sig och molntjänstleverantören vad gäller ramverk och i så fall om ramverket anpassas till den nya IT-miljön.

*Reflekterande*
Vi vill undersöka om organisationen gått tillväga på samma sätt idag om det hade varit aktuellt att migrera andra IT-enheter till molnet. Vi anser detta vara viktigt för att påvisa om några av de delar i COBIT ramverket som vi har identifierat som kritiska vid en migrering till molnet, skulle vara aktuella (se avsnittet 2.5 COBIT). Vi undersöker även om organisationen anser att det varit värt att genomföra en migrering, baserat på den information och de erfarenheter som de har skaffat sig. Detta gör vi för att påvisa om molntjänster i sin helhet överträffar de eventuella risker som den medför.

*Styrning*
Detta område är direkt relaterat till de processer i COBIT som vi har identifierat som kritiska vid en migrering (se avsnittet 2.5 COBIT). Många av frågorna i denna del förutsätter att informanterna varit med om en migrering. Frågorna är av ”Ja” eller ”Nej” karaktären vilket gör att informanten kan svara kortfattat och inte behöver utveckla sitt resonemang.

### 3.2.4 Genomförande av intervjuer

Oavsett om vi intervjuade personen ansikte mot ansikte eller via telefon så började vi med att presentera vem vi var och vår bakgrund. Vi presenterade även målet med undersökningen. Det var också viktigt för oss att klargöra hur informationen som kommer fram under intervjun skulle användas. På så sätt skapade vi förtroende mot informanten och sökte vi en tillitsrelation mellan intervjuobjektet och oss. Detta fungerade som uppvärmning för de kommande frågorna. (Jacobsen, 2002)

Vi var även noga med att få samtycke från intervjuobjekten vad gäller sättet som vi valde att dokumentera intervjun på. Vi använde en portabel multimediaenhet för inspelning av intervjun. I samtliga fick vi informantens samtycke att spela in intervjun.

Inför varje enskild intervju frågade vi hur informanten ställde sig till anonymitet i undersökningen både som person och för organisation. I alla fall utom ett så ville informanterna att både de själva och deras organisationer skulle vara anonyma i undersökningen.

### 3.2.5 Analys av intervjumaterial

Vi har delat in analysmaterialet i tre faser; beskrivning, systematisering och kombination.

När vi analyserade den data som vi hade samlat in under intervjuerna så började vi med att beskriva data. Detta gjorde vi genom att transkribera intervjuerna för att får en noggrann dokumentation av intervjuerna. Detta gav oss en bra förståelse av den data som vi hade samlat in under intervjuerna. Vi kunde därigenom vara säkra på att data var dokumenterad på ett grundligt sätt utan att vi lade in vår tolkning. (Jacobsen, 2002)

I nästa fas systematiserade vi data genom att reducera och förenkla den för att på så sätt få ut det som var av relevans för oss. Vi har genomfört systematiseringen för att på ett lämpligt sätt kunna förmedla vad vi har funnit.

## 3.3 Undersökningens kvalité

För att validera en undersökning ska man uppfylla två krav för det empiriska materialet. Det första är att empirin måste vara giltig och relevant och det andra är att empirin ska vara tillförlitlig och trovärdig. (Jacobsen, 2002)

När vi skulle säkerhetsställa att kraven uppfylldes för det empiriska materialet såg vi till att få kontakt med högsta ansvarig inom området inom organisationen. I tre av intervjuerna så var det CIO:n i organisationen som svarade på intervjufrågorna. I ett av dessa tre fallen så hade CIO:n en medhjälpare med sig som var kompetent att svara på frågorna. I den fjärde intervjun så hänvisade CIO:n oss vidare till en annan person som var mer kompetent att besvara våra frågor. Genom att vi gjorde så här säkerhetsställde vi att vi uppfyllde kraven för relevansen och tillförlitligheten på intervjudata.

### 3.3.1 Litteraturkritik

Vi har använt oss av två källor som inte är akademiska, ISACA och NIST. Vi använder oss av *NIST Definition of Cloud Computing* skriven av Mell & Grance (2011) när vi förklarar molnet. NIST är en statlig organisation som drivs av USA:s handelsdepartement (Wikipedia 1, 2012).
Många av de akademiska källor vi refererar till hänvisar till NIST i samma utsträckning som vi. Några av dessa är Zissis & Lekkas (2010), Farrell (2010), Grobauer et al. (2011) och Mather et al. (2009).

Vi använder oss av ISACA när vi beskriver COBIT. ISACA har skapat COBIT och är en internationell branschorganisation som arbetar med IT-styrning (Wikipedia 2, 2012).
Många av de akademiska källor vi refererar till hänvisar till ISACA och COBIT i samma omfattning som vi gör i vår uppsats. Några av dessa är Mather et al. (2009). Pathak (2005) och Symons et al. (2006).

## 3.4 Etik

Enligt Jacobsen (2002) så kan en undersökning innebära en del etiska dilemman. Han påpekar att det finns tre krav att följa för att göra en undersökning; informerat samtycke, rätt till privatliv, krav på riktig presentation av data. (Jacobsen, 2002)

Informerat samtycke innebär att informanterna ska delta i intervjuerna frivilligt samt att de ska ha förståelse för riskerna och vinster som det kan innebära av att delta i intervjuerna. I vårt fall har några av våra informanter önskat att ta del av vår rapport och vårt resultat vilket vi anser vara till deras fördel. Jacobsen (2002) delar in informerat samtycke i fyra huvudkomponenter:

- Kompetens innebär att informanterna har förmågan att fatta ett beslut baserat på att värdera nackdelar och fördelar.
- Frivillighet innebär att intervjuperson ska delta frivilligt i undersökningen utan några påtryckningar från andra. Vi anser att våra informanter deltog frivilligt eftersom de hade en så pass hög position inom organisationen att de annars bara hade kunnat delegera intervjun vidare om de inte själva hade velat delta. I en intervju så blev intervjun delegerad till en annan som hade mer erfarenhet inom områden än CIO:n.
- Full information innebär att informanterna ska ha fått full information om undersökningens syfte och fördelar och nackdelar som det kan innebära för dem. Enligt Jacobsen (2002) är detta i praktiken omöjligt att uppnå eftersom det skulle innebära att alla informanter översvämmades med information vilket skulle leda till att de inte kom ihåg något av denna information.
- Förståelse innebär att informanten inte bara ska ha fått full information om underökningen utan även ha förstått undersökningen. Det har därför varit viktigt för oss att betona betydelsen av informerat samtycke.

# 4. Empiriska data och analys

I detta avsnitt presenterar vi de resultat som framkommit genom våra intervjuer. Avsnittet är indelat i fem områden. Dessa är Molnet och risker, Migrering, Drift, Styrning och Reflekterande. Varje område avslutas med en sammanställande analysdel.

## 4.1 Molnet och risker

**Tabell 2. Molnet och risker**

| *Varför har ni valt att använda er av molnet?* | |
|---|---|
| Organisation A | • Plattformsoberoende<br>• Kostnad<br>• Funktionalitet |
| Organisation B | • Ska hålla IT-enheten liten<br>• Inte längre ansvariga för drift<br>• Kostnaden |
| Organisation C | • Skalfördelning via virtualisering<br>• Kostnaden |
| Lunds universitet | • Kostnaden |

Alla informanter ansåg att ett gemensamt skäl för att använda sig av molntjänster var den låga kostnaden. I organisation A var det fördelarna med att få ett system som var plattformsoberoende och funktionellt. I organisation B låg det i deras strategi att hålla IT-enheten liten och därför var molntjänstlösningar aktuellt för dem. De ansåg att de kunde lägga över ansvaret på en extern part istället för att ha hand om det själva. Informant i organisation B uttrycker sig som följer:

> ”*Vilket gör då att just molntjänster är ju extra intressanta då för vi behöver överhuvudtaget inte ens bry oss om maskinerna som står bakom, så fort vi alltså om man tar skillnaderna mellan att vi köper in en programvara som även om den driftas av vår driftleverantör så blir vi ansvariga för att se till att den här programvaran är uppe, men är det en molntjänst så frånsäger vi oss egentligen allt ansvar vi bara förväntar oss att en extern leverantören vi går till ska se till att sakerna är uppe.*”

I organisation C påpekade informanten att det var skalfördelarna som var viktiga för dem i molnet.

**Tabell 3. Molnet och risker**

| *Vilka typer av tjänster/uppgifter använder ni er av i molnet?* | |
|---|---|
| Organisation A | • Google Apps<br>• Sunguard, för backup |
| Organisation B | • Ekonomisystem<br>• Personaladministrativa system<br>• Fakturahanteringssystem<br>• Mediestreamingtjänst<br>• Internationellt ärendehanteringssystem |
| Organisation C | • Google Apps<br>• Ärendehanteringssystem |
| Lunds universitet | • Gmail<br>• Delar av ekonomisystemet<br>• Fakturasystemet<br>• Reseräkningssystemet |

Tre av de fyra organisationerna använder sig av någon eller några av Googles tjänster. Det var bara organisation A som använde sig av en extern partner för backup-lösning i molnet. De andra organisationerna hade olika typer av administrativa tjänster i molnet. Organisation B har även en molnlösning för mediestreaming. De har även ett internationellt ärendehanteringssystem ett så kallat community cloud (se avsnitt 2.2.4) inom EU.

**Tabell 4. Molnet**

| *Hur ser ni på säkerheten i molnet i förhållande mot "icke" molntjänster?* | |
|---|---|
| Organisation A | • Molntjänstleverantören har bättre möjlighet att skydda data |
| Organisation B | • Säkrare än att ta hand om det själva<br>• Professionell driftorganisation bakom<br>• Säkerhetsexperter |
| Organisation C | • Förlust av kontroll av fysisk access |
| Lunds universitet | • Lagra data lokalt är inte lika säkert |

Alla förutom organisation C ser det som en fördel att ha någon annan som sköter säkerheten åt dem. Organisation C ser det som en förlust att inte kunna kontrollera den fysiska åtkomsten till data och servrarna. Två av organisationerna såg det som säkrare att använda sig av molntjänstleverantörer än att ha det själv. En informant i organisation B uttryckte sig som följer:

> *"Och det är också så att normalt om man tittar på den här typen av driftorganisationer så då har de kanske en säkerhetsexpert som… som jobbar där."*

**Tabell 5. Molnet och risker**

| *Anser ni att det finns specifika risker i molnet som inte finns annars?* | |
|---|---|
| Organisation A | • Fysisk plats av data<br>• Molntjänstleverantören går i konkurs |
| Organisation B | • Fysisk plats av data |
| Organisation C | • Fysisk plats av data |
| Lunds universitet | • Har inte kontroll på leverantörernas underleverantörer, var finns data, vem äger den |

Alla fyra organisationerna anser att det finns en risk med att inte veta var data fysiskt lagras. Organisation A såg konkurs av molntjänstleverantören som en risk.

### 4.1.1 Analys av avsnittet Molnet och risker

Vi trodde att den främsta orsaken för organisationer att gå över till molntjänster var kostnadsbesparingar. Detta visade sig stämma då alla organisationerna angav detta som orsak. Organisationer ser det inte längre som sitt ansvar när man använder sig av en molntjänst. De tecknar ett avtal som de sen tar för givet att tredje part följer. Vi trodde inte att detta var ett av skälen till att man valde molntjänster.

De processer som är identifierade i COBIT som relevanta vid en migrering hade organisationerna haft större kontroll om de hade följt ME2 Monitor and Evaluate Internal Control. Det hade ökat organisationernas kontroll över deras data om de hade följt PO2 Define the Information Architecture. Eftersom organisationerna var osäkra på var data lagras så hade de fått en förståelse för det om de hade följt DS2 Manage Third-party Services i COBIT.

Många av organisationerna har använt sig av samma aktör, Google. Vi trodde att det skulle vara vanligare med andra leverantörer eller att organisationerna hade utvecklat egna system på en PaaS-lösning (se avsnitt 2.3).

Vår undersökning visar att organisationerna anser att det är säkrare med molntjänster. Vi har genom intervjuerna kommit fram till att organisationerna har liten kontroll på risker i molnet och att intresset för säkerhetskontroller är väldigt lågt.

## 4.2 Migreringen

### Tabell 6. Migreringen

| *Hur har ni arbetat med IT-kontroller/ informationssäkerhet/ förändringshantering inför migreringen?* | |
|---|---|
| Organisation A | • Testgrupp innan inköp |
| Organisation B | • *Kunde inte svara på frågan* |
| Organisation C | • Ja, men det gjordes efterhand<br>• Kort testperiod innan migreringen |
| Lunds universitet | • Lite demo test |

Tre organisationer hade någon form av testning av tjänsterna innan de blev implementerade. Organisation B kunde inte svar på frågan då de inte var anställda då migreringen genomfördes. Organisation C angav att de valde att testa tjänsten under en kortare period innan beslut om inköp togs.

### Tabell 7. Migreringen

| *Vilka delar av COBIT eller andra ramverk och standarder anser ni har varit viktigast att bejaka vid en migrering till molnet?* | |
|---|---|
| Organisation A | • Inga ramverk användes |
| Organisation B | • *Kunde inte svara på frågan* |
| Organisation C | • De använder ITIL i sitt dagliga arbete med processhantering |
| Lunds universitet | • Kunde inte svara<br>• Använder delar av ITIL i dagligt arbete |

Av organisationerna som vi intervjuade var det bara organisation C och Lunds universitet som använde sig av något ramverk och det var ITIL. Exakt vilka delar av ITIL som användes återgavs ej. Organisation B kunde inte svara på frågan då de inte var anställda då migreringen genomfördes.

**Tabell 8. Migreringen**

| *Hur förberedde ni er inför migreringen?* | |
|---|---|
| Organisation A | • Installation av extra server för migreringsverktyget |
| Organisation B | • *Kunde inte svara på frågan* |
| Organisation C | • Kontroll av inkorg i mail innan och efter migrering |
| Lunds universitet | • Ingenting |

I organisation C gjorde de kontroller av antal brev i inkorgen för mail innan och efter migreringen för att säkerhetsställa att all data hade migrerats. I organisation A så installerade de en extra server för att installera migreringsverktyget för Lotus Notes. Lunds universitet hade ingen form av förberedelse, de startade bara den nya tjänsten och stängde den gamla. Lunds universitet uttrycker sig så här:

> *”… det tog två veckor sen var det klart. Det var alltså… jag har aldrig sett någonting snabbare. Alltså det gick oförskämt bra.”*

**Tabell 9. Migreringen**

| *Uppstod det några problem vid migreringen?*<br>*– Vilka?*<br>*– Förväntade problem?*<br>*– Undveks problem genom att följa ramverk och standarder?* | |
|---|---|
| Organisation A | • Tog lång tid att migrera data<br>• Inga ramverk |
| Organisation B | • *Kunde inte svara på frågan* |
| Organisation C | • Problem med stegvis migrering. Gjorde en stor migrering istället<br>• Problem med data i båda systemen<br>• ITIL var till hjälp<br>• Dålig data i gamla systemet |
| Lunds universitet | • Inga problem<br>• Risk att inte hinna migrera i tid<br>• Funderingar kring integriteten |

Det vara bara organisation C som använde sig av något ramverk under migreringen och det hjälpte till med förändringshanteringen och dokumentationen och hur det ska struktureras. Ett återkommande problem för alla organisationer var att de var oroliga för att inte hinna migrera i tid. I organisation C försökte de göra en stegvis migrering men istället gjorde de en stor för att det inte var möjligt med en stegvis migrering. Organisation A hade problem med att deras migreringsverktyg inte kunde hantera den stora mängd data som bilagor var i.

### 4.2.1 Analys av avsnittet Migreringen

Vi trodde innan undersökningen att organisationerna använde sig av kontroll och styrning i större omfattning. Det visade sig att de inte övervägde användningen av ramverk vid en migrering till molnet.

Tre av organisationerna svarade att de hade använt sig av någon form av testning av tjänsten innan den implementerades fullt ut i organisationen. Detta är i enlighet med COBIT AI7 Install and Accredit Solutions And Changes. Eftersom de omedvetet har följt processen i COBIT för testning så har de minimerat risker för tjänsten.

I organisation A installerades en extra server för att sköta migreringen av data. Detta ligger i närheten av det som behandlas i AI7 Install and Accredit Solutions and Changes. Processen behandlar behovet av att ha en plan för konventering av data till det nya systemet.

Eftersom det bara var organisation C som använde sig av något ramverk så ledde det till att de andra organisationerna inte kunde svara på om problem undveks med hjälp av ramverk. Organisation C fick hjälp av ramverket med deras förändringshantering. Ett gemensamt upplevt problem för alla organisationerna var att de var oroliga för att inte hinna migrera i tid.

## 4.3 Drift

**Tabell 10. Drift**

| *Hur ser ni till att molntjänstleverantören följer era ramverk och standarder?* | |
|---|---|
| Organisation A | • Vet inte |
| Organisation B | • Inga ramverk<br>• Avtalsfråga<br>• Går inte kontrollera |
| Organisation C | • Kan inte påverka det<br>• Får anpassa sig efter leverantören |
| Lunds universitet | • Kunde inte svara |

Denna fråga var svår för organisationerna att svara på. Organisation B menar att detta ska regleras i avtalet mellan molntjänstleverantören och organisationen, de menar även att det är svårt för organisationen att kontrollera att molntjänstleverantören följer organisationens ramverk. Organisation C anger att de inte kan påverka huruvida molntjänstleverantören anpassar sig till organisationens ramverk och standarder, de menar istället att organisationen ska anpassa sig efter molntjänstleverantörens ramverk och standarder. Organisation C uttrycker sig så här:

> *”Vi har en väldigt svår möjlighet att påverka de bitarna. Vi får anpassa oss mycket efter deras grejor.”*

**Tabell 11. Drift**

| *Vet ni om molntjänstleverantören använder sig av några ramverk och standarder* | |
|---|---|
| Organisation A | • Nej |
| Organisation B | • Genom avtal |
| Organisation C | • Ja, men vet inte vilka |
| Lunds universitet | • Ja, men vet inte vilka |

Det var tydligt att organisationerna inte hade koll på vilka ramverk som leverantören använde för att kontrollerar sin IT-miljö. Organisation C och Lunds universitet angav att deras molntjänstleverantör använde ramverk, men de var inte säkra på vilka. Organisation B menade återigen att detta ska regleras i avtalet mellan molntjänstleverantören och organisationen. Organisation B uttrycker sig som följer:

> *”Jag tror inte att vi någonsin skulle gå in och försöka kontrollera det här, alltså det skulle vi inte ha tid eller jag vet inte knappt ens möjlighet heller…”*

### 4.3.1 Analys av avsnittet Drift

Vi trodde att det skulle ligga i organisationernas intresse att övervaka sin leverantör för att se om leverantören använder sig av ramverk. Det visade sig dock att de inte var intresserade av det så länge allt fungerade enligt avtalen. Det fanns inte något intresse för att få molntjänstleverantören att anpassa sig till organisationens ramverk.

Vi tycker att det är konstigt att organisation C anser att de ska anpassa sig efter molntjänstleverantörens ramverk och inte vice versa.

Hade organisationerna följt ME2 Monitor and Evaluate Internal Control så hade avsaknaden av kontroll hos molntjänstleverantören inte varit problem eftersom den processen behandlar vikten av att återkommande förbättra och jämföra IT-kontrollen och kontrollramverket för att nå upp till organisationens mål.

Genom att inte kontrollera molntjänstleverantörer berörs DS2 Manage Third-party services. Detta eftersom organisationen inte kan definiera vem som har ansvar för vad, vilket ökar problemen relaterade till leverantörens förmåga att leverera tjänster på ett säkert och effektivt sätt.

## 4.4 Styrning

**Tabell 12. Styrning**

| *Sker det återkommande riskbedömningar?* | |
|---|---|
| Organisation A | • Inte direkt |
| Organisation B | • *Kunde inte svara på frågan* |
| Organisation C | • Ingen skillnad mot den interna |
| Lunds universitet | • Ja, för hela organisationen |

Det är ingen av organisationerna som har återkommande riskbedömningar för molntjänsten. Det är dock två av organisationerna som har riskbedömningar för hela organisationen och dess olika delar. Organisation C säger att de gör återkommande riskbedömningar, men inga specifika för deras molntjänster. Organisation C uttrycker sig så här:

> *”Vi hanterar inte den på något speciellt sätt utan de ingår i standard drift liksom.”*

**Tabell 13. Styrning**

| *Har ni en exitstrategi för att kunna lämna molnet?* | |
|---|---|
| Organisation A | • Nej |
| Organisation B | • *Kunde inte svara på frågan* |
| Organisation C | • Nej, flyttar till ny molntjänst istället |
| Lunds universitet | • Nej, treårsperspektiv<br>• Byta eller stänga ner tjänsten |

Organisationerna vi undersökte hade inga exitstrategier för att lämna molnet. Lunds universitet och organisation C ansåg att man byter molntjänstleverantör istället. Lunds universitet ansåg även att ett alternativ var att stänga ner tjänsten helt eftersom det aldrig kommer att vara aktuellt att gå tillbaka och tillhandahålla tjänsten själv igen. Lunds universitet menade även att det är svårt att förutse vilka tekniska möjligheter som skulle vara aktuellt om några år, därför gör man bedömningar utifrån ett treårs perspektiv. Lunds universitet uttryckte sig så här:

> *”Vi kan inte planera för mycket mer än tre års sikt framåt. För mer än tre års sikt så blir det liksom fånigt.”*

**Tabell 14. Styrning**

| *Hur gick det till när ni valde molntjänstleverantör?* | |
|---|---|
| Organisation A | • Billigare än att uppgradera det befintliga |
| Organisation B | • Kostnaden<br>• Kraven |
| Organisation C | • Genomlysning av marknaden<br>• IT-chefen bestämde i slutändan |
| Lunds universitet | • Val mellan två stora aktörer<br>• 20 studenter fick rösta |

För Lunds universitet var det ett val mellan Google och Microsoft. För dem hade det ingen betydelse av vilken tjänst som skulle användas så studenterna fick rösta om vilken som skulle användas. Det blev en klar majoritet för Googles tjänst. För Organisation B och C så var det kostnaden som avgjorde när de valde molntjänstleverantör. I organisation C genomfördes en genomlysning av marknaden men i slutändan var det IT-chefen som bestämde vilken molntjänstleverantör som skulle användas.

**Tabell 15. Styrning**

| *Hade ni någon utbildning av de nya systemen för användarna?* | |
|---|---|
| Organisation A | • Ja<br>• Skedde i grupper av 10-20 personer |
| Organisation B | • Ja<br>• Hur man använder systemen<br>• Öka medvetenheten med säkerheten |
| Organisation C | • Ja<br>• Utbildning efter typ av arbetsuppgifter |
| Lunds universitet | • Ja<br>• Kommer inte till dem utan utbildning<br>• Expertsystem<br>• Säkerhetstänkandet |

Alla organisationerna hade någon form av utbildning för de nya systemen. Återkommande för en del av organisationerna var att öka säkerhetsmedvetenheten. På Lunds universitet har man inte tillgång till expertsystemen såsom ekonomisystemet om man inte har genomgått en utbildning för det.

**Tabell 16. Styrning**

| *Testade ni tjänsten innan den implementerades fullt ut?* | |
|---|---|
| Organisation A | • Testade med 20 användare |
| Organisation B | • *Kunde inte svara på frågan* |
| Organisation C | • Kortare testperiod |
| Lunds universitet | • Ja<br>• Testinstanser<br>• Demotester<br>• Kontakt med andra universitet |

De tre organisationerna som kunde svara på frågan hade genomfört någon form av testperiod innan molntjänsten implementerades fullt ut. Lunds universitet hade varit i kontakt med Linköpings universitet och ett att de största universiteten i Canada för att dra nytta av deras erfarenheter.

**Tabell 17. Styrning**

| *Hur sker backup av er data hos leverantören?* | |
|---|---|
| Organisation A | • Finns på flera servrar |
| Organisation B | • Genom avtal |
| Organisation C | • Vet inte, men har en tjänst för det |
| Lunds universitet | • Inga kontroller<br>• Sker genom avtal |

Organisation B och Lunds universitet angav att det inte sker några kontroller. Skälet till att det inte sker några kontroller av backupen är att detta styrs och regleras genom avtal. Organisation C har en tjänst för backup, men ingen kontroll på hur den fungerar. Organisation A har fått information från Google att deras data finns på cirka sex olika servrar.

**Tabell 18. Styrning**

| *Hur begränsas och kontrolleras användarnas åtkomsträttigheter till systemen?* | |
|---|---|
| Organisation A | • Genom namn och lösenord |
| Organisation B | • Individuella användarnamn och lösenord<br>• Använder AD |
| Organisation C | • Användarnamn och lösenord<br>• Gemensamma konton och lösenord |
| Lunds universitet | • Personliga användarnamn och lösenord |

I samtliga organisationer har de individuella användarnamn och lösenord. I organisation C finns det gemensamma konton och lösenord inom vissa grupper. Organisation B använder sig av Active Directory som är en katalogtjänst från Microsoft som innehåller information om olika resurser i en domän till exempel datorer, skrivare och användare. Dessa klassificeras som objekt och kan hanteras samt skyddas i den egna domänen.

**Tabell 19. Styrning**

| *Vet ni om leverantören har procedurer för hur data behandlas vid radering av information eller vid modifikationer i hårdvara?* | |
|---|---|
| Organisation A | • Google lämnar inte ut information om det |
| Organisation B | • *Kunde inte svara på frågan* |
| Organisation C | • Finns procedurer men har inte koll |
| Lunds universitet | • Ingen koll |

Ingen av organisationerna kunde svara på om de visste att det fanns procedurer för hur data behandlas vid radering av information eller vid modifikation i hårdvara. Organisation A angav svaret att deras molntjänstleverantör, Google, inte gav ut information till sina kunder angående denna process. Organisation A svarade så här:

> *”Google lämnar inte ut information om detta. Man få helt enkelt lita på dem.*”

### 4.4.1 Analys av avsnittet Styrning

Vi trodde att organisationer som gick in i molnet hade en plan för den dagen då de skulle vilja lämna molnet. Det visade sig att alla organisationerna saknade exit-strategi för att lämna molnet. För att undvika detta problem i framtiden skulle de använt sig av COBIT processen AI7 Install and Accredit Solutions and Changes. Processen behandlar vikten av att tillhandahålla en strategi för när man vill avsluta eller backa ur tjänsten.

Inga av organisationerna hade någon specifik riskbedömning för molnet. Hade de följt PO9 Assess and Manage IT Risks så hade riskerna reducerats och de hade haft en större kontroll på riskerna. Hade organisationerna gjort riskbedömningar hade de fått en bättre kontroll på riskerna och dess effekt och sannolikhet om de hade drabbat organisationen.

Vi var inte förvånade när tre av organisationerna svarade att de hade gjort val av molntjänstleverantör efter kostnad. Det vara bara organisation C som ett val gjordes efter en genomlysning på marknaden. Detta är i enlighet med COBIT-processen AI5 Procure IT resources där det behandlar behovet av att välja en leverantör som passar bäst på organisationens specifika krav.

En annan process att ta hänsyn till vid val av molntjänstleverantör är DS2 Manage Third-party Services. Processen innebär att leverantören kan tillhandahålla tjänsterna. Detta ska säkerhetsställas av organisationen. En del av organisationerna hänvisar till avtalen.

Alla organisationerna hade utbildning av anställda för användning av de nya systemen i molnet. Detta är i enlighet med AI7 Install and Accredit Solutions and Changes där processen tar upp att organisationen ska förse de anställda med utbildning av de nya systemen.

Organisationerna testade tjänsterna innan de implementerades fullt ut i organisationen. Detta följer processen AI7 Install and Accredit Solutions där det behandlas att testning av systemen ska ske innan implementering.

Vi trodde inte att organisationerna skulle har så lite kontroll på hur backup sker hos molntjänstleverantören. Det vara bara organisation A som hade fått information på att deras data fanns på ungefär sex stycken servrar. Att inte ha kontroll på sin backup ligger inte i linje med processen DS4 Ensure Continuous Service där det ska bestämmas vilken data som ska finnas i backupen.

Alla organisationerna använde sig av unika användarnamn och lösenord. Detta följer DS5 Ensure Systems Security då det möjliggör användaridentifieringen och åtkomstkontrollen till systemen. Organisation C hade gemensamma lösenord för några av delarna i organisationen. Detta ligger inte i linje med processen och det resulterar i att spårbarheten (se avsnitt 2.4.1) påverkas negativt då man inte kan knyta användaren till en viss individ.

Organisationerna hade ingen kontroll på hur och om det fanns några procedurer för hur data behandlas i avseende vid radering av information eller vid modifikationer i hårdvara. För att få kontroll på detta problem skulle de ha följt processen DS11 Manage Data. Processen innebär att procedurer ska finnas för detta problem.

## 4.5 Reflekterande

**Tabell 20. Reflekterande**

| *Vad hade ni gjort annorlunda idag om ni hade utför en liknande migrering till molnet?* | |
|---|---|
| Organisation A | • Tvinga fram åtgärder hos anställda |
| Organisation B | • Ökad kontroll |
| Organisation C | • Migreringen hade varit samma<br>• Den interna förändringshanteringen |
| Lunds universitet | • Hade gjort likadant idag<br>• Diskussionen runt hade varit annorlunda |

De informanterna som kunde besvara frågan ansåg att de hade gjort samma idag. Organisation A hade infört ett tvång på rensad inkorg och på så sätt slippa problemen som uppstod vid migreringen med bifogade filer som inte gick igenom migreringsverktyget. Både Lunds universitet och Organisation C hade gjort på samma sätt idag. Organisation B menar att de vill ha ökad och tydligare kontroll för respektive system som flyttas till molnet. Organisation B säger så här:

> *”… hur viktigt det är då att man inte förlorar data, alltså, står det upp mot dem kraven vi har för det systemet? Så, det är en typisk sån sak som vi skulle kontrollera den dagen vi skulle gå över i molnet med något annat system som vi har här.”*

**Tabell 21. Reflekterande**

| *Anser ni att det var värt att utföra migreringen med den information och kunskap som ni har idag?* | |
|---|---|
| Organisation A | • Ja<br>• Bättre samarbete |
| Organisation B | • Ja<br>• Billigare |
| Organisation C | • Ja<br>• Ökat samarbete |
| Lunds universitet | • Ja<br>• Inget negativt |

I samtliga fall så ansåg informanterna att det har varit värt att genomföra migreringen av sina system. I två av organisationerna ansåg informanterna att migreringen till molntjänst hade ökat samarbetet inom organisationen. Organisation B anser att det har blivit billigare att underhålla IT eftersom stora delar av deras system är baserade i Molnet. IT-enheten har även minskat i organisationen på grund av migreringen, vilket också har bidragit till kostnadsbesparingar.

### 4.5.1 Analys av avsnittet Reflekterande

Samtliga organisationer ansåg att det var värt att utföra migreringen trots de problem som uppstod för en del av dem. Två av organisationerna ansåg att migreringen hade ökat deras samarbete inom organisationen.

Två av organisationerna hade genomfört en liknande migrering på samma sätt som de gjorde denna gång. De andra två hade ökat kontrollen för att underlätta migreringen. För att uppnå önskan för ökad styrning så skulle organisationerna följt COBIT-processen ME4 Provide IT Governance. I processen ska det etableras ett ramverk som innefattar organisationens struktur, processer, ledarskap, roller och ansvarsområden.

# 5. Diskussion

I detta avsnitt resonerar vi utifrån vår empiri och analysdel. Vår avsikt är att diskuterar kring forskningsfrågan: Hur kan tillämpningen av COBIT förebygga och avhjälpa olika problem som kan uppstå då organisationer migrerar till molnet?

Syftet med undersökningen var att vi ville belysa problematiken som uppstår mellan organisationer och molntjänstleverantören vid migrering till molnet. Vi har identifierat problemområden och styrkt problemområden som kan uppstå vid en migrering. Vi visar på några relevanta områden inom COBIT som kan vara vägledande och avhjälpande. COBIT bidrar med en ökad kontroll gentemot tredje part.

Det har framkommit i vår studie att organisationerna som vi undersökte hade väldigt lite kontroll över sin molntjänstleverantör. Vi menar att det är konstigt att det inte sker fler kontroller för att säkerhetsställa att molntjänstleverantören följer avtal. Att organisationerna inte kontrollerar att molntjänstleverantören sköter sin backup anser vi vara fel eftersom det borde ligga i organisationernas intresse att se till att deras data är säker vid ett eventuellt haveri.

Organisationerna hänvisade och gömde sig bakom avtalen med molntjänstleverantören. Man kan fråga sig om att enbart hänvisa till avtal är samma sak som att kontrollera sin leverantör.

Att migrera till molnet innebär att organisationen förlorar kontroll genom att bli beroende av tredje part, detta för att uppfylla organisationens IT-behov och IT-relaterade affärsmål. För att upprätthålla kontrollen måste organisationer övervaka sin molntjänstleverantör och förhålla sig till områden som kan vara problematiska. Om organisationen negligerar eller om de inte är medvetna om problem som kan uppstå genom att migrera till molnet leder till att organisationen utsätter sig för risker (se avsnitt 2.4 IT-Säkerhetskoncept och 2.6 Problematiska områden vid migrering till molnet). Att värdera och förebygga problem när tredje part kontrollerar och hanterar information borde ligga i organisationens intresse.

Organisationerna har i viss utsträckning arbetat på ett sådant sätt att delar av deras arbete med migreringen kan kopplas till processer i COBIT. Exempel på detta är att organisationerna hade utbildning av systemen och att de testade tjänsten innan implementeringen (se tabell 15 Styrning och tabell 16 Styrning).

Några organisationer kunde inte ge information om hur migreringen hade gått tillväga, eftersom de som hade genomfört migreringen inte längre fanns inom organisationen. Detta kan bli ett problem för organisationerna i framtiden, då det inte finns några referenser till hur och om de borde göra något annorlunda vid en liknande migrering.

Organisationerna börjar använda sig av en molntjänst utan att veta hur de ska göra den dagen då de vill avsluta tjänsten och flytta data från leverantören. Att inte ha en plan för att avsluta tjänsten kan resultera i att de blir fast hos molntjänstleverantören och inte kan få ut och tillbaka all data. Att inte veta vad som händer med data när organisationen avslutar en tjänst anser vi vara ett problem. Det finns inte någon kontroll på om data sparas hos leverantören

och hur länge den finns kvar. Dessa problemområden kan avhjälpas och förebyggas om COBIT hade tillämpats (se avsnitt 2.6.2 COBIT-Processerna).

De organisationer som vi undersökte använde sig alla i någon omfattning av tjänster från Google. Att en leverantör har stort inflytande på marknaden kan få konsekvenser den dagen de vill byta leverantör eftersom det då kanske inte finns någon leverantör som kan möta organisationens behov. Detta kan i sin tur leda till att man blir låst till sin gamla leverantör.

Ingen av organisationerna hade någon specifik riskbedömning för molntjänsten. Detta är problematiskt eftersom de inte får någon uppfattning av de risker som de utsätter sig för när de går över till en molnlösning. Det kan vara så att organisationerna gör bedömningen att de köper sig fria från ansvar och ser det som molntjänstleverantörens problem. Organisationer migrerar till molnet för att det är kostnadseffektivt. Om de då själva ska behöva genomföra riskbedömningar så är detta oftast förknippat med en kostnad vilket gör molntjänsten mindre kostnadseffektivt.

När organisationen går över till molnet kommer de inte undan de grundläggande IT-säkerhetskoncepten relaterade till integritet, spårbarhet, sekretess och tillgänglighet (se avsnitt 2.4 IT-Säkerhetskoncept). Dessa grundläggande IT-säkerhetskoncept upphör inte att gälla vid en migrering till molnet, de måste hanteras oavsett vilken plattform som tillämpas om grundläggande säkerhet ska upprätthållas.

# 6. Slutsats

I detta avsnitt framlägger vi vår slutsats kring undersökningen i förhållande till forskningsfrågan: Hur kan tillämpningen av COBIT förebygga och avhjälpa olika problem som kan uppstå då organisationer migrerar till molnet?

Organisationerna borde inte förlita sig på avtalen och överlåta allt ansvaret till molntjänstleverantören. Även om ansvaren är definierade i avtal måste organisationen kontrollera om det uppfylls eller inte. Användandet av COBIT hade förbättrat kontrollen av molntjänstleverantören.

COBIT är ett ramverk som värderar och talar om vad som ska göras, inte hur det ska göras. Hade alla problem som en migrering till molnet innebär förhindrats om COBIT används fullt ut? Det är svårt att säga om alla problem hade förhindrats. Det är många faktorer som spelar in. COBIT är kanske inte optimalt för ändamålet, men om det kompletteras med delar i andra ramverk och standarder kan en optimal lösning skräddarsys för varje enskild organisation. Att inte ha någon värdering eller bedömning av problem relaterade till migrering till molnet är en mindre bra lösning. Att använda sig av COBIT är bättre än att inte använda sig av något värderande verktyg överhuvudtaget eftersom COBIT talar om vad som ska göras för att avhjälpa och förebygga problem.

Vi tror inte att tillämpningen av COBIT hade gjort att problemområdena hade ökat, tvärtom tror vi att COBIT minskar, förhindra och avhjälper många av de problemområden som organisationer måste ta ställning till vid en migrering till molnet.

Att bedöma risker och problem är något som är förknippat med en kostnad för organisationen. Många organisationer anger att minskade kostnader är en viktig faktor i valet att migrera till molnet. Om organisationen ska behöva kontrollera sin leverantör tror vi att det kommer innebära en kostnad, något som organisationen vill undvika. Att migrera till molnet utan att hantera och värdera IT-relaterade problem kan skapa problem för organisationer, kanske inte omedelbart, men så småningom.

Som resultat av arbetet har vi kommit fram till att organisationer arbetar omedvetet med delar i COBIT då vissa delar är grundläggande inom IT-säkerhet. Det slutgiltiga resultatet är att organisationerna i vår undersökning hade fått en bättre kontroll över IT-styrningen om de hade använt sig av de identifierade processerna i COBIT på ett mer medvetet sätt för att därigenom minska eventuella problem då en migrering till molnet ska genomföras.

# Bilagor

## Bilaga 1

Svar på frågor från organisation A.

**Inledande**

*Kan ni berätta lite kort om företaget/organisationen?*

Organisation A är ett klädföretag med egen design och egna butiker. Produktion sker för det mesta i Asien. Det finns cirka 600 anställda i 4 länder: Sverige, US, UK och Frankrike. Dessutom finns partners i cirka 30 länder till som säljer Organisation As produkter. Huvudkontoret ligger i Sverige men ägarna finns i Schweiz.

*Berätta om er och er roll i företaget/organisationen.*

Jag är IT chef Organisation A med ansvar för personal, IT drift och underhåll här i Sverige. Vi har också en IT global manager som ansvarar för IT i hela företaget.

**Molnet**

*Varför har ni valt att använda er av molnet?*

Vi körde ett föråldrat mail system (Lotus Notes) och var tvungen att byta ut den. Den orkade inte med belastningen och mail klienten för Macintosh var dåligt. Dessutom var funktionalitet väldigt dåligt. Webbklienten var också knappt användbar.

Det fanns några kriterier som gjorde att vi valde Google apps:

- Ingen tung mail klient: Måste vara webbaserad.
- Plattformsoberoende: Vi kör mest Mac på kontoret men vissa avdelningar kör Windows. Även Linux finns med i bilden. Vi är också utsprid i fyra länder.
- Bra funktionalitet: Tidigare hade vi bara mail & kalendrar. Nu fick vi även chat, video chat, Docs plus extra funktioner via Google marketplace.
- Låg underhålls kostnader: Vi minskade IT personal kostnader med en halv tjänst.
- Lägre kostnad: Vi betalar 40€ per användare per år och alla användare få cirka 30 Gb lagring var. Att implementerar en sådan lösning själv med t ex Exchange skulle ha varit avsevärt dyrare.

*Vilka typer av tjänster/uppgifter använder ni er av i molnet?*

Vi använder Google apps för mail, kalendrar, Docs, sites och singel-sign-on.

Dessutom använder vi Sungard för molnbaserat backup och Rackspace för vår nya e-com platform.

*Hur ser ni på säkerheten i molnet i förhållande mot "icke" molntjänster?*

Det finns en del säkerhets risker i molnet men det kan vara väldigt stora skillnader mellan olika leverantörer. Vi hade webbaccess till Lotus notes med samma sorts loginsystem som Google så det har inte ändrats mycket. Vi kan implementera 2 faktor inloggning till Google men har valt att inte göra det.

Överlag så tror jag att Google har bättre möjlighet att skydda vår data än vi har.

*Anser ni att det finns specifika risker i molnet som inte finns annars?*

Vi vet inte längre var vår data är och kan inte återställa som förut. Om jag raderar ett konto så har jag en vecka på mig om jag skulle ångra mig. Annars är det borta för alltid. Vi har nu köpt backup tjänsten från Postini för att åtgärda detta problem.

Man måste kunna lita på moln leverantören. Vid en eventuell konkurs kan man förlora allt.

Man kan inte styra utveckling på samma sätt som förut. Alla kör samma version. Vi har kunnat komma runt detta problem delvis genom att köpa tilläggs tjänster från marketplace. T ex "Rename" för att byta namn på användare och "Dito" för att kunna hantera mail listor.

**Migreringen**

*Hur har ni arbetat med IT-kontroller/ informationssäkerhet/ förändringshantering inför migreringen?*

Vi hade en test grupp som provade köra Google apps innan vi bestämde oss för att köpa tjänsten. Vi körde redan privat Google mail för att kunna kommunicera med leverantörer i Asien så vi väl insatt i hur det fungerade.

*Vilka delar av COBIT eller andra ramverk och standarder anser ni har varit viktigast att bejaka vid en migrering till molnet?*

Har inte använt COBIT eller andra ramverk

*Hur förberedde ni er inför migreringen?*

Installation av extra Windows server med Lotus Notes för att kunna köra Google Lotus migreringsverktyg.

*Uppstod det några problem vid migreringen?*
*– Vilka?*

Det tog lång tid att migrerar allt data. Vi migrerade små grupper åt gången men en del användare hade så många mail att det kunde ta upp till en vecka att få över alla mail.

Bilaga storlek var också ett problem. Google mail klara bilaga storlek på max 25 Mb men migreringen klarade bara av 15 Mb.

*– Förväntade problem?*

Största problemet var övergång från en mail klient till en web lösning. Fram för allt trådade mail skapade problem för en del personal.

*– Undveks problem genom att följa ramverk och standarder?*

Hade inte använt något ramverk.

**I drift**

*Hur ser ni till att molntjänstleverantören följer era ramverk och standarder?*

Har inte kollat om Google följer något ramverk

*Vet ni om molntjänstleverantören använder sig av några ramverk och standarder?*

Nej

**Andra tankar/Reflekterande**

*Vad hade ni gjort annorlunda idag om ni hade utför en liknande migrering till molnet?*

Jag skulle ha tvingat användare att rensa mailen först. Trots flera påstötningar så rensad nästen ingen sin inbox innan migrering.

*Anser ni att det var värt att utföra migreringen med den information och kunskap som ni har idag?*

Införande av Google blev en stor lyft för Organisation A. Vårt sätt att jobbar och samarbeta har förbättrats.

Hela vår infrastruktur håller på att ändras. Vårt nya intranät kommer att vara kopplad till Google apps genom att vi använder Google kontot för single-sign-on.

**Styrning**
*Sker det återkommande riskbedömningar?*

Inte direkt men man håller koll på utveckling som sker på nätet.

*Har ni en exitstrategi för att kunna lämna molnet?*

Nej. Vi blir mer och mer integrerade med Google

*Hur gick det till när ni valde molntjänstleverantör?*

Vi var tvungen att göra något åt vår mail lösning och uppgradering av befintlig skulle vara för dyrt och skulle inte lösa de problem som vi hade med Lotus Notes

*Hade ni någon utbildning av de nya systemen för användarna?*

Vid utrullning utbildade vi små grupper med 10-20 personer. Efter utbildning satte vi igång med migrering av alla mail för gruppen samt satt upp en mail-forward från den gamla mail server till Google mail. Då fick användarna köra Google mail men kunde fortfarande öppna mail på det gamla systemet.

*Testade ni tjänsten innan den implementerades fullt ut?*

Vi körde en pilot med 20 användare först för att utvärdera lösning innan vi köpte. Vi hade dock redan testat systemet eftersom flera hade gmail konto privat.

*Hur sker backup av er data hos leverantören?*

Enligt Google finns all data på cirka 6 olika servrar

*Hur begränsas och kontrolleras användarnas åtkomsträttigheter till systemen?*

Namn& Lösen

*Vet ni om leverantören har procedurer för hur data behandlas vid radering av information eller vid modifikationer i hårdvara, flytt/avverkning?*

Google lämna inte ut information om detta. Man få helt enkelt lita på dem.

## Bilaga 2

Transkribering av intervju, Organisation B.

I1 = Informant 1

I2 = Informant 2

T = Tobias

J = Jakob

I1: Vi har ju dina frågor här.

T**:** Ja.

I1: Eeh… om ni vill veta först då om Organisation B, så kan man egentligen ta det som finns på nätet kanske?

T: Ja, precis. Ja, det kan vi göra ju.

J: Sen är det lite om er roll i företaget, lite om vad ni gör?

I1: Vi jobbar på IT-enheten och det är en enhet som ligger på den administrativa avdelningen. Vi ä fyra personer här, Namn 1 här är en och sen har vi två andra… eeh… Vi är tre IT-projektledare och en IT-chef.

J: Mm. Okej.

I1: Vi sitter ju mer som en beställarorganisation.

J: Ja, okej.

I2: Så vi arbetar egentligen väldigt lite praktiskt med datorer och sånt där utan vi beställer väldigt mycket, framför allt då kring drift sidan. Vi har ju hela… hela driften outsourcad då och sen så stötar vi upp mycket kring systemutveckling gentemot verksamheten här, men då handlar det väldigt mycket om att hjälpa verksamheten att beställa system eller systemutvecklingsprojekt. Där tror jag att det är… större delen av det vi gör då.

J: Ja, okej. Ehm…

T: Jag tyckte det var en bra beskrivning av er roll i organisationen så vi kan väl hoppa vidare till frågorna om molnet?

I2: Först en liten fråga här då… så att vi vet vad ni menar här med molnet… tittar man lite grann här på… till exempel räknar ni att vi har outsourcat våran drift är det samma sak som molnet för eran undersökning?

J: Det blir det, tekniken är den samma, det är mer namnet bakom det… vad använder ni för typ av tjänster idag?

I1: Vi har ju… dem sköter ju vår drift sen har dem vår help-desk och eeh… sköter om våra skrivare…

J: Så ni har mailtjänster och allting då utlagt hos dem?

I1: Ja.

T: Mm. Men då klassar vi det som att ni använder er av molnet.

I2: Japp.

T: Det är kanske mer ett modeord, molnet.

J. Ja, det har ju funnits ganska länge det är ju mer att man kallar det nu istället.

I2: Ja, bortsett ifrån det här då alltså själva outsourcingen av driften så lägger vi ju ut några system dessutom som är typiska väldigt tydliga molntjänster då… alltså, Agresso till exempel vårt ekonomisystem, det är ju en sån tjänst som ligger utanför och den ligger ju alltså inte hos våran driftleverantör utan den ligger hos Agresso. Så att ehh… Palasso är också ett annat system, det personaladministrativa systemet då, det är också en sån tjänst som vi köper då, som helt enkelt är i drift av en annan organisation där vi egentligen bara köper några användare av den leverantören så vi har ingen koll på driften överhuvudtaget.

J: Okej, men det är en typisk molnlösning där…

I2: Ja, de är ju mer en definitionsmässigt en molntjänst på det sättet då…

J: Ja.

I2: Medans outsourcingen den är ju… där har vi ju fortfarande kontroll över våra servrar vi vet ju vilka våra servrar är vad de heter om vi vill gå in och starta om en server så gör vi ju det om vi har något problem i någon ut av tjänsterna där då. Men när det kommer till Agresso och Palasso så har vi ingen kontroll överhuvudtaget då.

J: Ja, okej.

I2: Av den anledningen så frågade ni vad ni egentligen menade med molnet.

J: Då är det egentligen Agresso och Palasso som du pratade om det är mer den typ utav molntjänst som vi kollar på.

I2: Ah, men då är vi med.

I1: Och då har vi ytterligare ett par stycken såna som ligger…

J: Ja, okej.

I2: Kontempus.

I1: Kontempus, som är vår fakturahantering då… ååh… eeh… Sen är det lite såna här småtjänster också av till exempel Streamy, jag är lite osäker där då, men det handlar om film som man kan visa via den tjänsten då… Men eeh… det är ju verkligen någon sån där lite liten grej. Sen så är det ju att hela vår… det kan ju vara så att… att vi har mer grejor som vi på IT inte har hundraprocentig koll på nu när det gäller såna här molntjänster då för… eeh…

I1: I och med att vi inte blir inblandade så kan avdelningarna ha egna avtal så att säga…

J: Ja, okej.

I2: Men eeh… När jag får prata här så kommer jag ju på en typisk sån tjänst. Nu pratar jag inte med er här utan nu pratar jag med Informant 1. Eeh. Den här eeh… CPCS, är ju en typisk sån… CPCS är ju också en sån tjänst som vi har då där ärenden… internationella ärenden hanteras… och det är ju en tjänst som vi har tillsammans med eeh… jag tror hela Europa, alltså EU då.

I1: De som använder sig av det…

I2: De som använder sig av… Ja, det här systemet i EU då, så man ska kunna eeh… hålla koll på andra…

I1: *[ohörbart]*

I2: Aah... så vi har lite molntjänster då …

T: Om vi backar lite och går på frågan; Varför har ni valt att använda er av molnet?

I1: Eeh… ja, nä… Jag kan ju tänka mig att det var ju säkert smidigast och sen från leverantörens sida att vi erbjuder dem en tjänst som var enklast… betydligt enklare för oss att köpa än att ha klienter här.

I2: Det ligger ju i linje med hela… hela arbetet som vi har här på Organisation B kring IT, att vi ska hålla IT-enheten liten så att säga. Vi ska ha egentligen, just det här att vi ska vara en renodlad beställarverksamhet då … Vilket gör då att just molntjänster är ju extra intressanta då för vi behöver överhuvudtaget inte ens bry oss om maskinerna som står bakom, så fort vi alltså om man tar skillnaderna mellan att vi köper in en programvara som även om den driftas av våran driftleverantör så blir vi ansvariga för att se till att den här programvaran är uppe, men är det en molntjänst så från säger vi oss egentligen allt ansvar vi bara förväntar oss att den externa leverantören vi går till ska se till att sakerna är uppe. Så att det ligger i linje med våran IT-strategi som säger att vi just ska arbeta med, alltså egentligen i första hand välja molntjänster då… eeh… förutsatt att det är ett okej pris på det. Så att det är ett strategiskt beslut som togs för… några år sedan och då, tyvärr var varken Informant 1 eller jag här på den tiden när den här sista strategin sattes då… men eeh… det handlar mycket om, för oss då i all fall om att ha en effektiv IT-verksamhet, det kan man väl sammanfatta det som…

J: Ja, okej… Men hur ser ni nu här på säkerheten i molnet i förhållandevis till det gamla systemet om man hade haft, om ni inte hade haft molntjänster hur ser ni på säkerheten där i förhållandevis då?

I2: Ja… eeh… i grunden så… nu blir det lite åsikter här då… kan man väl säga… men… men… i grunden är det ju så att jag vill ju påstå att det här är säkrare då än om vi tar hand om det själva. Därför att man får en professionell driftsorganisation bakom sig då…

I1: De har kanske en produkt att ta hand om och vi har tusen olika…

I2: Aah… Och det är också så att normalt om man tittar på den här typen av drift organisationer så då har de kanske en säkerhetsexpert som… som jobbar där. I en organisation som Organisation B så har vi ingen möjlighet att ha den typen av kompetens här inhouse det skulle bli alldeles för dyrt då, medans en driftorganisation de som driftar för många olika eeh… kunder då… de har råd att ha den här typen av kompetenser då… så att eeh… så ska man väl säga, ser jag på det lite grann då… men det är ju inte något ställningstagande som vi har tagit gemensamt för Organisation B då, men sen kan man väl säga så här också då och det är ju viktigt att tänka på när det gäller för vår del att vi har inte nån direkt hemlig information här, varken hemlig eller känslig information. Så att vi är… vi har det ganska… eeh… lätt på det sättet.

J. Okej. Då kanske ni inte ser att det finns några specifika risker då i molnet?

I2: Det kan man nog säga att vi ser inte… det är precis som du säger att vi ser inte det då, så är det.

I1: Sen så kan man också säga att dem system som Agresso och så här, det är ju välkända system från välkända leverantörer, så det är inte någon vi tar så utan det är… det är ju upphandlingar och avrop innan vi tar in något nytt.

I2: Så att… så att vi skulle ju aldrig… vi skulle ju inte på samma sätt lägga ut ett system om vi hittade något billigt ekonomi system som de driftar i Ryssland… det skulle vi inte ha… då skulle vi tänkt annorlunda då.

J: Ja, okej.

I2: Eeh… utan det är kända företag.

J: Okej. Det var allt på molnet, kan vi gå över på migreringsfrågorna om ni inte har något att tillägga?!

I2: Ja, det går bra.

J: Då ska vi se, den första frågan, hur har ni arbetat med IT-kontroller, informationssäkerheten inför den här migreringen?

I2: Lite problem, man kan ju säga så här nu då, här kommer det här problemet att de tjänster som vi har här då är uteslutande sånt som hände innan egentligen nån här på IT-enheten tror jag, som vi har av oss fyra fanns här.

J: Ja, okej.

I2: Så att det är ett litet problem för oss då… att svara på just de här frågorna då…

J: Ja, då blir det kanske svårt att svara på hela migreringsfrågorna här då?

I2: Ja… alltså, det… det… tyvärr så är det nog så.

J: Ja, då kan vi nästan ta driften där, eller använder ni några ramverk eller standarder när ni kontrollerar era molntjänstleverantörer eller det överlåter ni helt till dem?

I2: Ja, det kan man säga… det gör vi… vi använder definitivt inte några ramverk och standarder så är det… utan… ett exempel är ju som vi pratade om då förut då att… att… eeh… nämen vi tittar vad det är för företag till exempel innan vi lägger ut något stort system. Ekonomisystemet till exempel, jag menar det kan man inte lägga var som helst… men det är på den nivån att… man kan väl tänka lite grann så här att okej om vi skulle lägga ut någonting stort idag och fundera lite på det sättet så skulle vi nog, det handlar nog om att väldigt mycket funder över just vilken är leverantören, fråga såna saker som vart har de serverhallar ehh… ååh… eeh…

I1: Vi kan helt enkelt sätta såna krav när vi gör avrop eller upphandlingar… om det är någon standard som vi är intresserad av eller så…

J: Ja, okej.

I2: Det är som Informant 1 säger att skulle det handla om det så skulle vi ju sätta… det blir en avtals… det blir en avtalsfråga i slutändan att vi ställer krav på, jag menar låt oss säga att vi ställer krav på en ISO certifiering av något slag, jamen då skriver vi ju det i det avtalet då att…

I1: Att de ska vara certifierade…

I2: … certifierade, ja! Eller om vi nu vill att de ska följa nått ramverk till exempel ITIL då, så ställer vi de kraven via avropet eller via avtal. Så det är helt och helt på det sättet det här skulle kastas. Jag tror inte att vi någonsin skulle eeh... gå in och försöka kontrollera det här, alltså det skulle vi inte ha tid eller jag vet inte knappt ens möjlighet heller, alltså att börja kontroller till exempel haft ett krav på Agresso, nån ISO certifiering att de följer det här det skulle ju inte vi någonsin göra en revision på eller nån eeh… uppföljning på utan de… eeh.. där litar vi nog på leverantören och vad vi har kommit överens på i avtalen…

J: Ja, okej.

I1: Vi går ju ofta på statliga ramavtal också så de är ju godkända sen innan…

I2: Aaah…

I1: Den här leverantören…

I2: Aaah…

T: Mmm…

J: Sen har vi lite andra frågor också som vi tänkte ställa. Har ni någon form av strategi om ni skulle vilja lämna molnet inom någon framtid, hur ni får ut all er data då och liknande?

I2: Nej, det har vi inte.

J: Okej. Vi har några fler frågor, men de är nog svåra för er att besvara eftersom ni inte var med när de började använda systemen.

I2: Ah, nä, det är lite… lite…

T: Men man kan ju vända på det och fråga hur de hade gjort idag liksom?

I2: Du tänker på de här sista, vad hade ni gjort annorlunda om ni hade utfört en liknande migrering? De frågorna ni tänker på eller?

J: Jaa…

T. Dels de sen så har vi lagt till några ytterligare, som har kommit till här nu…

I2: Okej…

T: … efter tidigare intervjuer som vi har haft… frågor som har kommit upp hos oss också… de riktar väl sig framför allt att till de som varit med om en migrering då, och det blir kanske lite svårt i det här fallet…

J: Ja, här är ju vissa frågor som ni säkert kan svara på ändå som om ni vet hur backup och liknande av er data hos leverantören, vet ni om det sker eller är det samma sak där att ni litar på att det sker?

I2: Det är samma sak… ja, vi litar på att de gör dem… så att vi... det är egentligen så att det är ju det vi köper oss fria från när vi köper just den här typen av molntjänst… när det kommer till våran normala driftleverantör där måste vi se till att, jamen, hur ofta gör ni backuper, vi måste ställa krav på det och vad är det som det ska göras backup på. När vi köper en tjänst som Agresso till exempel nä men då… då förväntar vi oss att det ska göras backuper på det, så är det ju…

J: Ja, okej.

I2: Så vi gör inte någon kontroll där.

I1: De har ju säkert ofta såna här paketlösningar också där det ingår backup och så vidare. Tillgänglighet och spårservice… ja, vad det nu är för någonting…

I2: Men där kan man ju säga så här att typiska såna här saker som den… den dagen vi gör en ny. Alltså om vi ska lägga upp nått nytt där då så, den typen av backup fråga är en typisk sån sak som vi kontrollerar då, alltså kommer kontrollera innan så att vi vet att det kommer göras backuper och hur ofta kommer det göras backuper och beroende på vilket system då… eeh… hur viktigt det är då att man inte förlorar data, alltså, står det upp mot de kraven vi har för det systemet så det är en typisk sån sak som vi skulle kontrollera den dagen vi skulle gå över i

molnet med något annat system som vi har här. Där det så att säga skapas data, genereras data av verksamheten.

J: Mm. Det var bra där… sen en sak här också där, de här olika systemen hur begränsas de olika användarna åtkomst rättigheter till dem, har ni gemensamma inloggningar eller har alla individuella?

I2: Ja, alla har individuella. Det går igenom hela vår eeh… om det idag finns några allmänna lösenord överhuvudtaget på Organisation B så är det ett misstag kan man säga, det ska inte överhuvudtaget existera utan alla lösenord och alla användare ska ha specifika lösenord som man är… så man kan peka ut enskilda, så att säga man ska kunna se vem det är som är inne och har gjort någonting då.

J: Okej, har ni olika för de olika systemen eller har ni nått gemensamt system som kontrollerar åtkomsten till de andra delsystemen då så att ni loggar in på ett ställe sen kommer ni till allting då eller har ni olika användarnamn och lösenord för de olika tjänsterna?

I: Det är olika för olika tjänster så är det… däremot så är det ju så att vi försöker ju ändå hålla ner det här med lösenord lite grann då… vi har ju, jag vet ju inte hur insatta ni är då men vi har ju något som vi kallar för ett AD… Active Directory

J: Ja…

I2: Ja, och så länge som det är Windows baserade E-produkter så stödjer de ju alltid inloggning via Active Directory så att där är det interna system så är det väldigt många som inte behöver använda sig av lösenord, men det där blir ju ett problem när man går över till en molntjänst därför att eeh… i de flesta fall så i de här molntjänsterna stödjer inte det här att man kan koppla in ett internt AD med en extern tjänst, så att där har ni ett problem med molntjänster va? Att det blir fler lösenord för användarna och det i sig om vi ska gå tillbaka till det här med säkerhet då så är det ju en typisk sån här grej att när det blir för många lösenord så tröttnar användarna på många lösenord och då börjar de skriva upp det på lappar istället…

J. Ja…

I2: Ja, så att där… om man går tillbaka till frågan där i början så det där är ju faktiskt ett säkerhetsproblem att molntjänster inte klarar av det här allihopa. Jag är lite osäker, det finns säkert molntjänster där de har börjat bygga in det här och se till att det här funkar men det är väl ingenting som vi… eller det är bara vad jag tror… hur som helst ehh… för vår egen del så kan man väl säga att det där är förmodligen, det är någonting som sänker säkerheten vad gäller…

I1: … eller både ökar och sänker den egentligen…

I2: Aah… så kan man ju också…

J: Okej…? Hur är det med de nya systemen som ni har, har ni någon utbildning för användarna så de lär sig hur de ska använda det?

I2: Ja, det har vi…

J: Ja, okej…?! …eemmm….

I2: Och det är samma där, jag vet inte om ni är intresserade av det vi… även vad gäller… om man tittar… det är ju sånt vi har ju utbildning inte bara för nya användare utan även för befintliga användare då… kring till exempel IT-säkerhet och hur man ska använda några system över huvud taget då, det är egentligen en väldigt viktig del i säkerhetsarbetet just den här… eeh… utbildningen jämt emot användare och att öka medvetenheten då…

J: Ja…

I2: … om säkerhetsfrågor för det… man kan inte få användare att bete sig… alltså, de kommer aldrig bli säkerhetsexperter på något sätt, men däremot kan man ju öka medvetenheten hos dem så att de kanske tar det lite mer försiktigt iallafall, det är en del av säkerhetsarbetet.

J. Ja, okej.

T: En sista fråga då. Har ni planer på att utföra fler migreringar så att säga med facit i hand, ni har ju en del molntjänstlösningar just nu. Skulle ni kunna tänka er att ha fler?

I2: Ja, utan tvekan.

I1: Ja, absolut. Ibland på vissa områden så har vi ju inte ens system idag utan det hanteras ju med papper och penna helt enkelt… och det eeh… och då ser jag det som att det är säkert mycket billigare att skaffa oss en molntjänst än att vi ska ha systemet här själva eftersom vi inte är så många användare heller…

I2: Nä… och de… eeh… molntjänster är alltid… ska alltid vara ett alternativ när vi tar in ett nytt system, så att vi när vi… åtminstone utvärderar det då… sen är det ju en annan sak om vi tar in det som molntjänst, men det får man ju säga att det tillhör våran IT-strategi. Att molntjänster är något, jag menar kostnaden är rätt och det ger rätt så att säga användarvänlighet och det står upp mot de kraven då, så ska vi gå på molntjänst.

J: Ja, okej… men då tror jag nog vi har fått svar på alla våra frågor.

I2: Ja!

J: Men då tackar vi så jättemycket för att ni ville ställa upp på denna intervju.

I1: Jadå, tack själva lycka till.

T+J: Tack så mycket.

I1+I2: Hej! Hej!

T+J: Hej!

## Bilaga 3

Transkribering av intervju, Organisation C.

I = Informant

T = Tobias

J = Jakob

T: Eeh… du sa du hade frågorna va?

I: Jajamen.

T: Japp.

T: Ja, men då kör vi då… ehm…

I: Mmm…

T: Den första här då… kan du berätta lite kort om ert företag och om er organisation?

I: Visst kan jag det… känner du till någonting i förväg?

T: Eeh… Nä, jag vet ju att ni har eeh… vad är det? Butik 1och Butik 2.

I: Precis! Vi har en huvudorganisation som är Organisation C det är ett helägt bolag av Koncernen 1 och i Organisation C så har vi flera under ehm… bolag som Butik 1, Butik 2, Butik 3 och Butik 4 i Norge. Vi har försäljning i tre olika länder Norge, Sverige, Finland och vi har inköpskontor i Asien, för närvarande tre kontor i New Delhi, Hong Kong och Singapore.

T: Okej.

I: Så ser organisationen ut, övergripande. Sen har vi då att, själva IT som ni kanske mest är intresserade av…?

T: Mmm.

I: Det är en av de små centrala funktionerna som ägs då av Organisation C i den centrala organisationen. Sen i varje del i bolaget, de själv stående företagen som Butik 1 och Butik 2 dem har en IT-ansvarig, sen finns det även inom delade funktioner så som logistik, också en IT-ansvarig. Så har vi en intern beställarorganisation där ehm… IT äger budget för IT-frågorna och ehm… de olika delarna av organisationen får då planera sina förändringar och ta med vad de vill ha för någonting och hur de vill göra det, så att vi mappar upp det. Så att vi inte tar alla investeringar och styr upp det så att vi inte ser till att ha rätt underhåll och att vi kan använda det till alla delar och att vi får synergieffekter av vår storlek.

T: Ja, okej.

I: Lite övergripande så, helt enkelt…

T: Mmm… eeh… hur ser din roll ut i företaget? Vilka uppgifter har du?

I: Yes, jag har ehm… Jag jobbade tidigare som kommunikationsansvarig, jag var ansvarig för all typ av nätverkstrafik inom hela företaget egentligen ehm… och sen så blev det en ledig position att man fick sök en som hette IT-arkitekt i en ledningsgrupp och jag kunde få den rollen så kunde vi ersätta min position med en gammal kollega till mig som jag tror vi plockade in och när vi gjorde det så höll vi på med flera större projekt och för att kunna korrigera dem och få ihop dem och få tekniken att fungera för alla delar av organisationen med alla system under förändring så skapade vi en roll som kallades för IT-arkitekt. Men det är väldigt mycket hands-on jobb med att hantera små system och hantera småsaker och… liksom utföra massa grejor och samtidigt tror jag att det finns med någon form av teknikaspekt på hur vi driver förändringar. Så det är en lite… diffus roll och den följer inte riktigt om man tittar på vad andra organisationer har som IT-arkitekt.

T: Ja… det var en ganska bred roll.

I: Aah, det… det är det.

T: Ja, eeh… om vi går in här på själva molnet då…

I: Mmm…

T: Och pratar lite om eeh… just ert moln så att säga… eller era molnlösningar, så har vi ju en fråga här som lyder: Varför har ni valt att använda er av just molnet?

I: Mmm… känner ni till någonting om vad vi har för molntjänster?

T: Nej, det gör vi inte.

I: Nä… intressevis så eeh… så stod det för två år sedan nu, tror jag, om att eeh… Organisation C att vi eeh… gjorde Sveriges största migrering till Google Apps…

T: Mmm…

I: Där vi la ut egentligen alla e-post, kalender ehm… all den hanteringen la vi ut till Google Apps. Och vi har egentligen sett det som en outsourcing av information… så att då har vi lyft ut själva e-posthanteringen till en extern part. Vi har inte någon övergripande strategi om att lägga saker i molnet. Eeh… Och molnet som definition då är att vi ser det som en extern part som levererar vår lösning på en delad plattform med massa andra kunder och så samtidigt.

T: Mmm.

I: Sen dess har vi en som i vardagligt tal ofta definieras som molntjänst det är Salesforce som vi använder som ett ärendehanteringssystem. Men vi ser det ju inte som att det är en molnstrategi egentligen. Vi har länge jobbat med outsourcing av olika funktioner. Vårt

inköpssystem och vårt lagersystem har driftats av en extern partner sen åtminstone 81. Och då står de i stordatormiljöer hos en externpart. Så vi har styrt den typen av upphandling eller uppköp. Vi gick över till IP-telefoni för eehm… för några år sedan också. IP-telefoniservrar och djupströmmingsservrar och citrixservrar står hos en extern part och det används av flera företag, flera kunder. Men vi har inte definition att vi kallar det för något moln-IP-telefoni, utan ehm… vi har ingen uttalad strategi av att använda oss av molnet. Vi förutsätter att vi har ingen större liksom aspekter med att vinna något på att ha ett moln. Det vi jobbar mycket med är att virtualisera kring våra system, vi har en ganska stor VWware – miljö där vi istället för att ha en dedikerad hårdvara per system har flera stycken lite kraftfullare maskiner där vi kör många virtuella maskiner i.

T: Mm.

I: Så då väljer vi att se det som en servervirtualisering så att du utnyttjar hårdvara, vi kör mycket av dem bitarna inhouse. Och sen är det specifika funktioner som främst e-post som vi har valt att outsourca till ett extern bolag och den tjänsten kallas då liksom för en molntjänst…

T. Mm.

I: Vi har inga tjänster i dagsläget som använder sig av externt moln som till exempel Amazons moln eller något annat.

T. Nä, precis. Men ni använder er av Google Apps och ni har någon form av inhouse privatmoln som vi har fattat det?

I. Mmm… Vi kallar det inte moln. För mig är som moln bara ett eeh… buzzword någon form av försäljningsgrej som egentligen är odefinierad…

T: Ja.

I: Och vad är ett moln? Tittar man på vanliga liksom eeh… moln på himlen så finns det massa olika typ av moln. Bland annat moln på marken i form av dimma, liksom. Och definitionen av ett moln i datavärlden det är bara ett populärt ord som folk använder för att det ska vara så bra… Så vi tittar ju på respektive tjänst för om vi kan virtualisera den så att den inte är beroende av en hårdvara, vi tittar på hur vi bäst utnyttjar hårdvaran vi har, så då tittar vi på som en vanlig upphandling ehm… vanliga tjänster som vi gjort i alla tider egentligen och då är det en outsourcingaffär. Då är frågan behöver vi stå för hela kostnaden? Det behöver vi sällan göra för att i en outsourcingaffär kanske vi kan nyttja såna servicedesk som massa andra företag använder på en delad funktion, vi kanske nyttjar samma övervakningsverktyg hos den externa partnern som alla deras kunder gör. Och då behöver vi inte sånt för den licensieringen, vi behöver inte stå för alla de kostnader som skulle va om vi hade köpt in alla sakerna och kört inhouse.

T: Mm. Så man kan säga att det är en anledning till att ni har valt att eeh... molnet då så att säga.

I: Ja, fast vi ser inte själva att vi väljer att använda molnet utan vi väljer ett ehm… det är ju egentligen en tjänst från en extern leverantör som kallas molntjänst, och det är egentligen att vi valt att outsourca en del av våra system som inte är verksamhetskritiska, skulle man kunna säga också…

T: Okej…

I: Att det råkar köras på molntjänst ehm… att det är en *[ohörbart]*att vi inte köper hårdvara, att vi inte har licensiering för alltihop det är eeh...*[ohörbart]*egentligen vet vi ju att vi skulle behöva outsourca en Exchange server, som körs på en delad miljö där flera andra maskiner finns så det är ju inte det här att vi behöver betala för hela hårdvaran, att vi inte behöver betala för all bandbredd. Vi har hög kapacitet det finns ganska mycket bandbredd vi kan använda, det finns ganska mycket hårdvara vi kan använda, men vi behöver inte ta hela kostnaden själv.

T: Nä, precis. Men det leder oss lite in på nästa fråga här. Hur ser ni på säkerheten i molnet, i förhållandevis till att inte använda det.

I: Mm. Och där är det samma sak vi bedömer den som en outsourcingtjänst. Och beroende på hur avtalet ser ut och vad de kan leva upp till för någonting så styr jag upp min bedömning därifrån. Till exempel jag har, som jag nämnde inköpssystem och lagerhållningssystem som kör hos externpart, och det har vi gjort sen åtminstone 81. De systemen äger vi inte allihopa och hur den externa parten då hanterar den informationen, vilka personer som är anställda där eller vilken access deras olika tekniker har det har vi inte full koll på. Vi kan inte veta till exempel vilka som har fysisk access till lokalen där maskinerna står.

T: Nä.

I: Ehm… Den behörighetskulturen kan inte vi mönstra ut, den berör ju flera personer det är deras ehm… det till hör ju deras core business också.

T: Mm.

I: Så att då har vi inte något speciellt synsätt på molntjänst mer än att var placeras data, hur godkänner dem eller säkerställer dem att det är just, vilka regler och förordningar gäller. Som en vanlig outsourcing av någon form av funktion.

T: Skulle du säga idag att ni har verksamhetskritisk data i molnet, så att säga?

I: Inte i dagsläget, nej. Det beror lite på att vi har en vag definition på vad som är verksamhetskritiskt.

T: Okej?

I: Och ehm… det är ju så att i e-post ingår det mycket information och vi har ju inte någon… det finns ingen policy som hindrar att Vd:n inte skickar information till berörda av… där man skriver… jag tycker det här är verksamhetskritiskt. Till exempel om han ehm… presenterar nya riktlinjer för hur vi ska driva verksamheten framåt, då kan vi tycka att det är verksamhetskritiskt… så att det är våra stora planer. Skickar han det via e-post så kommer

informationen vara lagrad i molnet, så det är en definitions fråga, men i dagsläget har vi ingenting av den dagliga produktionen som påverkar någonting med någon form av försäljning eller någon form av lagerhållning eller någonting annat som ligger i molnet. Så jag skulle säga… jag skulle säga nej.

T: Anser du att det finns specifika risker i molnet som inte finns annars?

I: På samma sätt där är det att vid outsourcing ehm… affärer så har man specifika risker som man måste ta ställning till med, vilka personer är det som jobbar med det, var finns de någonstans, vad är det för lagar som gäller, vart maskinerna placeras och alla de här aspekterna också. Och att molnet ofta är en delad miljö *[ohörbart]*Och då ehm… vi ser att det finns samma risker i molntjänst som det finns i en outsourcingtjänst av liknande karaktär. Så moln begreppet är mer... så där diffust att prata om.

T: Mm, fast ja… Det vi funderar på lite är ju om man hade haft allting inhouse själv, då får man ju kostnader och hela köret med i paketet men tror du att riskerna försvinner i och med att man har det inhouse så att säga?  I förhållandevis till att ha dem outsourcade i ett moln?

I: Vilka risker tänker du på då?

T: Det kan vara ju… allt ifrån integritet, spårbarhet, äkthet på data...

I: Den problematiken ehm… det är samma sak med en outsourcingaffär…

T: Mm.

I: Om vi lägger ut det på en maskin hos en extern part eller om vi har ehm… kanske servern stående hos oss men den underhålls av en externpart har vi samma problematik.

T: Mm.

I: Vi använder oss inte av att vi själva har byggt en applikation som använder ett publikt moln till exempel Azur eller Amazon som en lagring eller datakraft för molntjänst. Det använder vi oss inte av i dagsläget.

T: Ja, okej… Men då lämnar vi molnet där då och så… ja, det gör vi ju inte med vi går vidare och tittar på eeh… just er migrering, för det har ni ju gjort en?

I: Yes!

T: Eller ett antal kanske?

I: Mm.

T: Och då är vi ju intresserade av att veta hur ni har arbetat med IT-kontroller, med informationssäkerhet och om ni har jobbat med förändringshantering inför en migrering.

I: Mmh. Och eeh… Den migrering till molntjänst som vi gjorde där gick vi igenom och säkerställde data så gott vi kunde från vårt ursprungs epostsystem till det nya. Och ehm… där eeh… där säkerställde vi att vi migrerade samma innehåll till samma personer, det vi gjorde

var att kontrollera att lika många brev som fanns innan migreringen skulle finnas i den brevlådan när den va… hos Google Apps i det här fallet.

T: Mm.

I: Och då kunde vi säkerställa… vi gjorde en kontroll först att antalet stämde, och när antalet stämde så kunde vi göra slumpmässiga kontroller och då kunde vi tycka att informationen är den korrekta. Sen så hade vi på själva förändringsarbetet då påverkade vi våra användare mycket, mycket mer på deras e-post tjänst, blev helt annorlunda. Och då ehm… då hade vi informationsmöten då vi jobbade med vår verksamhet, våra interna kunder i koncernen ehm… så att liksom uträtta de frågetecken som fanns. Vi hade exempel från tidigare migreringar som vi gjort och tog då med frequently asked questions, vissa informationsbitar och lite beskrivning över vad är det de ska göra första dagen de får ny e-post.

T. Ja, okej.

I: Det var egentligen en ganska förenklad grej att hantera dem också. Vi gjorde en… vi höll först på att göra en fullständig grej men det blev så många nya funktioner de skulle ha, det fanns många möjligheter med eeh… jobba med grupper, kontakter och kartor och alla funktioner som finns i Google Apps, jämfört med vad vi hade tidigare.

T: Mm.

I: Så då valde vi att inte göra för mycket liksom… ehm… en överdos av informationen hade varit en större riks än för lite information.

T: Så ni valde att ta det lite i mindre etapper, så att säga?

I: Mm. Informationsbiten… ja… vi gjorde faktiskt allting i en Big bang en helg, gjorde vi. Och själva informationsbiten och förändringshanteringen med informationen valde vi att fylla på med det som behövdes. Och inte ha klart någon helhet.

T: Mm. Eeh… Använder ni er av några ramverk och standarder idag? Alltså, jobbar utifrån, plockar ut delar av dem eller någonting sånt?

I: Det enda ramverk som vi tydligt använder oss av är vårt dagliga arbete med processhantering så jobbar vi med ITIL.

T: Okej.

I: Och så har vi en change hantering som är en förändringsmetodik som vi följer. Så att från att idén kommer till vilken besparing vi ska göra och vilket resultat vi får av den och när den ska införas och vilka som ska informeras, allt sånt. Så har vi med den i vår change hantering. Samtidigt som vi får en uppsättning av incidenter som inträffar och allt sånt.

T. Har ni behövt anpassa ITIL just när ni har migrerat IT-lösningar så att säga till en tredje part?

I: Nä, inte… ehm… inte nämnvärt. Det är mer så att vi försöker anpassa vårt arbetssätt till vad som skulle vara ITIL-best practice.

T: Ja, okej. Uppstod det några problem vid migreringen och i så fall vilka?

I: Ehm… Jag måste tänka efter, vid migreringen som vi gjorde det var flera år sedan… ehm… vi hade först tänkt att göra en stegvis migrering men sen så fick vi problem med hur två system skulle samexistera när vi skulle flytta M/S-pekare, vilka som skulle vara master och så här… hur de skulle uppdatera varandra och då fick vi efter tester ta beslutet att vi fick köra allting i en Big bang. Och då själva data migreringen… under ett par dagar så hade olika personer olika mycket mail i varje system. Men efter en vecka hade vi kört i kapp allting. Så det vi gjorde var att alla kalenderenteties fick synka under helgen och senaste månadens mail, sen fyllde vi på med äldre e-post efterhand. Och det gjorde att visa personer hade all e-post synkroniserad efter tre dagar och vissa andra personer hade… det kom inte till dem förrän senare i veckan.

T: Ja, okej.

I: Och i andra fall så… ehm… hade vi inga större problem. Rena funktionsgrejen med att vid första inloggningen så måste man skriva in en catcher som vissa personer hade problem att läsa, men det var inga migreringsgrejor som var större problem.

T: Hade ni förutsätt några problem eller hade ni förväntat er att någonting kunde bli problematiskt?

I: Ja, vi hade sätt att i vårt ursprungssystem hade vi dålig datakvalité. Vi kunde inte veta vilka medlemmar som var med i alla grupper eller vilka som var deras primära adress i alla grupper och allting så att... vi hade problem med att rensa ursprungsdatan. Och beroende på att själva ursprungsdatan kvalité var lite shaky så hade vi förväntningar på problem och där fick vi mycket, mycket mindre än vad vi trodde. Under… ehm… testfas på grejor i vår så här change hantering så identifierade vi visa såna ställen och då kunde vi lägga till och ta med mer data istället och då fick vi färre fel. Det vi gjorde till exempel var att ehm… i och med att vi har flera olika koncerner så som Butik 1, Butik 2, Butik 3 om en person har jobbat inom alla ställena så kanske de har en e-post registrerad på allihopa, sen ingår man i en grupp som man kallar kanske för… säg… IT-drift. Vilka e-postadresser som är kopplade till personen gruppkonto och till de här grejorna det fanns inte en tydlig rak tråd med vilket entity som skulle vara var. Utan det var istället… i de här fallen där det var *[ohörbart]*tog vi med alla adresserna, vilket gjorde att en person kunde ha många fler adresser än vad som egentligen användes.

T: Okej.

I: Då kan vi minimera problemet som fanns.

T: Kopplade ni dem till varandra då eller hur fungerar det, hur löste ni det?

I: Då fungerar de som att de är alias till de här personerna.

T: Ja, okej. Eeh... Ja, vi har en fråga här som lyder, det står så här: Undveks problem genom att följa ramverk och standarder?

I: Det kan man säga ja. Då är det ITIL som är vårt processarbetssätt, framförallt change hanteringen att man ska dokumentera vad som ska genomföras och man ska strukturera sakerna, och då kunde man tidigare se att ehm… att det fanns problem med till exempel datakvalitén.

T: Mm.

I: Och den är alltid god… det är alltid bra att följa ramverk och standarder. Även om vi skulle kunna göra det ännu bättre genom att ha en tydligare projektmetodik *[ohörbart]*

T. Mm. Okej, då lämnar vi själva migreringsdelen nu då om du inte har andra frågor eller andra funderingar?

I: Äähh…

T: Då gör vi över och tittar lite på hur det ser ut nu när ni har det i drift så att säga. Ehm. Och då undrar vi hur ser ni till att molntjänstleverantören eller så att säga era leverantörer följer era ramverk och standarder, jobbar med er så att säga?

I: Det gör vi faktiskt inte.

T: Det gör ni inte?

I: Vi har en väldigt svår möjlighet att påverka de bitarna. Vi får anpassa oss mycket efter deras grejor.

T: Okej? Så då kommer ju nästa fråga där… vet ni om molntjänstleverantören använder sig av några ramverk och standarder i så fall vilka?

I: Mm. Jag vet att de använder sig av eeh… väldigt många tydliga strukturer och utvecklingsmetodik och allting, jag kan inte bara vilka alla är. I den leverantören som vi har så har vi gått med i deras premium customer network, som det heter. Vilket innebär att vi är i en grupp som har en dialog med leverantören om olika åsikter eller om vad vi vill, tycker fungerar bra eller dåligt. Men vi har väldigt liten möjlighet att påverka, vi är… några tusen konton i deras miljö som har många miljoner och då eeh… har vi ju… alltså… vi har inte hur stor möjlighet att påverka de sakerna.

T: Nä, det är ju klart.

I: I många fall får vi ehm… vi kan ju lyfta åsikter och rapportera fel och få god hjälp och alla såna saker det fungerar utmärkt men ehm… för ställningsprioriteringen, just i det här fallet med vi använder oss av Google och Google Apps där har Google tagit upp någon form av kamp mot sociala medier och Facebook och aktiverat tjänster som Google+ och såna bitar. Och det är väldigt bra att vi får tillgång till alla tjänsterna och vi får tillgång till deras hang out grej och vi kan köra videokonferens i Google+ med deras hang out ehm… och det finns många såna fördelar. Men problemet är att vi inte kan kontrollera hur tjänsten körs och vi kan

inte kontrollera att de inte lägger in tips för hur en användare ska utveckla sin Google+ profil och alla de här sakerna, så att där har vi begränsade möjligheter med att kunna göra egna anpassningar.

T: Om vi går in på den reflekterande delen här, och tittar lite på den, eeh… Vad hade ni gjort annorlunda idag om ni hade utfört en liknande migrering till molnet, är det någonting ni hade gjort på något annat sätt?

I: Inte för den här migreringen egentligen, av våra då, ett par tusen olika konton som vi har i koncernen som har en andra e-post, sen har vi ett registrerat ärende i en användare som sa att den vill ha tillbaka den gamla, och då får vi tycka att utfallet av själva migreringen var väldigt gott.

T. Mm.

I: Och vi ehm… hade kanske gjort det annorlunda med förändringshanteringen intern inom IT-avdelningen, vi hade kunnat förankra på ett annat sätt och fått ett annat genomförande, men för själva molntjänsten i sig så hade vi nog inte gjort någon större förändring.

T: Nä, okej. Anser ni att det har varit värt att utföra en sån här migrering med den kunskap och den information som ni har idag?

I: Ja, utav den här lite nischade delen som vi valt att outsourca så har det varit det. Vår möjlighet att samarbeta har ökat väldigt och att kunna köra just att… man kan bildsätta, man kan skicka… ställa frågor till varandra, man kan dela dokument och jobba med en massa andra saker så att hela den miljön var ett sånt lyft från vår gamla att ehm… den var väl värd att genomföra.

T: Mm. Har ni återkommande riskbedömningar gentemot era molntjänstlösningar så att säga? Bedömer ni riskerna i molntjänstlösningarna?

I: Inte mer än vi gör med andra saker... alltså, det är ju inte någon skillnad mellan outsourcingsbiten och med våra interna saker.

T: Ah. Okej.

I: Vi hanterar inte den på något speciellt sätt utan de ingår i standard drift liksom.

T: Mm. Har ni någon exitstrategi för att kunna lämna molnet så att säga? Om ni en dag väljer att nu vill vi inte ha den här tjänsten längre?

I: Nä då ehm… då ser jag det som en migrering till en ny e-postplattform och då ser vi inte det som en exitstrategi efter molnet utan då ser jag det som att vi byter plattform och då har vi samma migrering som vi har till vilken plattform som helst. Har vi möjlighet att få ut data i ett sådant format som vi kan använda i det nya systemet, det kan vi ju inte veta, vi vet ju inte vad det nya systemet är. Vi kan plocka ut massa… till exempel alla våra kontakter kan vi plocka ut som… jag tror det är… äh, det finns flera olika format kommaseparerade filer, eller vi kanske inte kan läsa in i det nya systemet. Man kanske måste ha det som en XML-format.

Och liksom behöver vi konvertera de då? Så det kan vi inte veta. Så vi har inte någon uttalad exitstategi.

T: Nä, okej. Hur gick det till när ni valde molntjänstleverantör eller hur går till har ni offentliga upphandlingar eller sånt här eller har ni liksom…?

I: Eeh. Vi… ehm… Det beror på vad som ska upphandlas så kan vi ta in en extern part med att stöta en genomlysning av marknaden som kan hitta några kandidater som vi tittar på lite noggrannare. Just för den här biten så var det ju en plattform vi hade inhouse som ehm… vi behövde göra en uppgradering och vi behövde se över hur vi ville göra med de bitarna och ehm… IT-chefen hade nys om den andra plattformen som fanns och tyckte att vi ville gå dit, så egentligen är det… en sån plattform… jämför du den med andra kända plattformar… vi tittade på ehm… Notes from IBM, vi tittade på Exchange från Microsoft, vi tittade på Google Apps från Google jämfört med den plattformen som vi hade. Och då behövde det inte göras någon större upphandling och kontroll på, eftersom vi visste vilka leverantörer vi hade att jobba med, visste olika upplägg vi kunde köra och då ehm… bestämde sig IT-chefen ganska snabbt för vilken väg han ville gå.

T: Mm.

I: Det var en ganska förenklad process. I vanliga fall på andra outsourcing bitar har vi en längre genomlysning, till exempel när vi tittade på IP-telefoni som vi också har outsourcat och då har köpt en lösning där vi har gjort en noggrannare upphandling så har vi ju ett annorlunda angreppssätt. Men det skiljer inte så mycket om det handlar om molntjänst eller om det är en hostad lösning eller hur det går till.

T: Ja, okej. Hade ni någon utbildning av de här nya systemen till exempel av Google Apps för era användare så att säga?

I: Mm. För användarna ehm… så gjorde vi lite olika indelningar, de på huvudkontoret fick möjlighet att gå på utbildningar och dragningar på hur det fungerade. De som skulle vara administratörer och vara inne och administrera och lägga upp nya användare fick gå utbildningar. De som skulle underhålla systemet och ha koll att e-posten går fram och sådär, typ systadmins de fick gå en annan utbildning så vi hade några tillfällen då det var halvdagars och heldagars genomgångar med olika grupper.

T: Mm. Testade ni den här Google Apps innan ni implementerade den i hela verksamheten så att säga?

I: Mm. Vi gjorde ett kort test innan beslutet kom. Sen hade vi tester och kontroller och genomföringar och liksom, själva projektet för genomförandet tog ett halvår. Sen var det sista helgen där det genomfördes, sen var det ett par månaders uppsättning. Men innan beslutet för inköp gjordes ehm… så var det kortare testperiod.

T: Okej, eeh… Vet du idag hur backupen sker hos er leverantör?

I: Eeh… Inte idag vet jag inte, jag har glömt bort det men vi… ehmm… men vi gick igenom det tidigare och jag vet att vi köpt en tjänst med backup och lagring under en längre tid, men hur det genomfördes kan jag faktiskt inte.

T. Nä, okej. Ehm... Vet du hur ehm… användarna kontrolleras och begränsas, alltså, hur deras åtkomsträttigheter är till systemet så att säga?

I: Mm. Vi har inte någon större begränsning för åtkomsten…

T. Okej…

I: Utan det är ehm… webbtjänst som de får lov att använda och gå in för att hantera e-posten, så att ehm… vi har ju styrt upp det så att det ska vara så tillgängligt som möjligt.

T: Men ni ja… Det finns inga såna här grupploggin eller liknande?

I: Alltså, delade konton finns ju hos vissa och ehm… där ehm… är det en person som äger kontot som delar ut behörigheten till det.

T: Okej…

I: Och sen grupper ehm… det är bara att man får breven till sig.

T: Mm? Så då ingår man i en grupp som har behörighet till att kunna läsa de här mailen då?

I: Aah… eller man ingår i en grupp som får mailen till sig eller ja, typ… och den strukturen den ägs av respektive bolag eller respektive del av verksamheten. Då ser de ju vilka anställda de har i varje grupp och där har vi våra systemadministratörer som håller detta uppdaterat.

T: Mm. Vet du om er leverantör har procedurer för hur data behandlas vid radering av information.

I: Eeh… det finns procedurer vet jag… men jag kan inte dem…

T: Men de finns?

I: Ehm… ja… det finns… jag vet att till exempel i Docs så raderar man någonting så är det at det ligger i typ papperskorgen i 30 dagar innan det försvinner, samma sak med brev som handlar i spam innan det försvinner och då vet jag att själva datan som vi har tillgång till finns det olika processer och olika procedurer för hur det hanteras med vad vi deletar och var vad vi kan ta tillbaka. Vi har även köpt en backup-tjänst som lagrar data längre och då har vi också, jag vet inte det finns strukturerade procedurer för vilken typ av data vi kan få tillbaka och under vilka intervaller och såna saker, men hur det ser ut hos leverantören det vet jag inte, och hur de gör ehm… med datan sen efter att det försvunnit från vår vy det känner jag inte heller till.

T: Nä, okej. Ja, det var alla frågor vi hade. Har du någonting övrigt som du vill lägga till?

I: Toppen! Nä inget vad jag kan komma på.

Intervjun avslutas.

## Bilaga 4

Transkribering av intervju, Lunds universitet.

I = Informant, Karl Hagberg

T = Tobias

J = Jakob

J: Ja men då kan vi börja med att berätta lite om Lunds universitet.

I: Ja.

J: Ska vi ta IT-sidan eller ska vi…

I: Ja vi kan ta IT-sidan, eeh... Karl Hagberg heter jag. Jag är ansvarig för IT-LU totalt sätt... ööh… alla it-frågor..ööh ansvarig för en liten enhet som finns här... ääh då som består av tre personer.. ääh… som då är strategisk IT. Så det är liksom topnoden. Det är det som är förvaltningschefens .och ledningens stabsstöd i IT-frågor. Ääh… och vi skriver då uppdraget till vår IT-leverantör som är vår förcentral med 120 anställda ungefär. De har ansvaret för stamnätet, säkerhetsfrågor och epost... lagringsfrågor, lokala nät, allt sånt har de ansvar för. Och sen så har vi ett nätverk med fakultetsföreträdare för de 8 fakulteterna vid universitetet. En företrädare för varje fakultet. Företrädare för biblioteksverksamheterna. Det som är till särskilda verksamheter. Vilket är den utbildning och forskning som bedrivs utanför fakultetsstrukturen. Alltså miljöinstitutet är en sån. Ett par forskningsenheter som ligger utanför fakulteterna. Så det är då ett nätverk det finns en studentföreträdare med också i det. Ääh så det är dem uppdraget LDC och samordning av fakulteten. Och sen så är det då en tredjedel som handlar om att stötta ganska mycket … den gemensamma förvaltningen och kanslierna i att jobba med sina system. alltså på it-spåret och it-management. Och den typen av frågor.

J: Ja, okej.

I: Systemägarskap och budgetering av de delarna för det handlar om mycket pengar. Ääh så det är de tre benen egentligen som koordineras härifrån. Och sen så då det som ni egentligen är inne på introbrevet. Hahaha. Det vill säga omvärldsbevakningen. Det är inget som bara vi gör, det är något som händer på marknaden. Alla de här som jag pratar om, vi träffas ju ibland och bara pratar framtid. Alltså vad är på gång så att säga. Ääh och sen så har vi ju det med kontakter med, en student som är studentrepresentant och han läser på LTH. Som sitter med i denna sambandsgrupp. Vi har honom och hans företrädare som är i studentorganisationen. Lite granna att hålla koll på, vad som är standardutrustning för en student idag. Alltså, haha, alltså så här sitter de på Iphones och paddor. Det gör alla andra också men få en känsla för hur många där är och hur många som vill ha föreläsningarna… ItunesU, hur många kör på det, vilken kanal eller vilka kanaler är just nu... på topp? Det där är lite granna 24 - månaders...

loop på det där. Så att … ja. Det är ett väldigt snabbt it-LU. Eeh… 2009 är den senaste kostnadsestimeringen då låg vi på strax under 400 miljoner... i pengar på IT. Och det är liksom vad är liksom en IT-kostnad? Och det är säkert något som ni har på utbildningen alltså. Är det en IT-kostnad eller en verksamhetskostnad? Och det ja... låt oss skita i vilket i det här läget bara säga att vi har... inklusive systemkostnader och det är det som man mycket diskuterar det här är en IT-kostnad eller är det en kostnad för att driva ekonomifunktionen, ja det är en kostnad för att driva ekonomifunktionen vi måste skära det i systemkostnaden ha koll på hur mycket pengar vi har så att... det någonstans där 400 miljoner kronor.

J: Ehm, ja. Ja och er roll fick vi lite där också, kanske berätta lite mer?

I: Ja alltså. Vår roll vi är som sagt att har ju... tittar man på stora organisationer så jag jobbar på LU, om två veckor passerar jag 5 år. Och dessförinnan varit en managementkonsult och jobbat i stora organisationen... projektledare en massa såna här olika jobb. Eeh har ingen IT-bakgrund egentligen utan jag är ju statsvetare. Ehm men så att säga började jobba 90-tal tidigt 90-tal. Och jag menar yngst in och kunde något om datorer. Hahaha, lite så... lite grann så. Bara början på beskrivning av det. Men eeh så vår roll är egentligen att rita väldigt mycket perspektiv framåt, att ge uppdrag till LDC, att ge uppdrag till fakulteterna. Att prova testa utveckla göra någonting. Ge uppdrag till våra systemägare för de stora systemen typ student-epost. Det här händer på marknaden. Ta in det i era värderingar så finns vi med och stöttar. Agera väldigt mycket ledstång. Alltså vi hjälper dem att hitta en väg fram utan att göra själva innehållsjobbet själv utan att den som är ansvarig för frågan om det är ekonomichefen eller den som gör jobbet som vi stöttar vi tar inte över frågorna.

J: Okej.

I: Så att säga det är ingen linjeorganisation. Det är inte så att alla strukturerna här rapporterar till mig i linje så att säga. Om ni är med på linje och matrisstyrning? De har ju sina chefer ute och jag har innehållsledstång som hjälper dem. Pengarna finns ju där ute jag har ju inte alla pengarna jag har ju inte alla de här 400 miljonerna. Under mitt ansvar har jag kanske 80 av dem... hos mig va. Så det är likadant där att man styr via att stötta andra att göra rätt saker. Just därför att inte ta över ansvaret från dem.

J: Ska vi gå över på molnet då?

T: Mmm.

J: Ehm... Ska vi börja med varför ni har börjat att använda det?

I: Alltså vi använder det ju... molnet är ju en liten svår... vad menar vi med moln? Så att säga.

J: Det är ett modeord.

I: Det är ju ett litet modeord så att säga. Ääh i en väldigt, alltså vi kör ju… hur ska vi börja...alltså i den vidaste beskrivningen av molnet. Så är det ju alla tjänster som hostas av någon annan.

J: Mmm, hmm.

I: Det är en väldigt vid beskrivning. Det är något annat som vi använder som inte finns hos oss… skulle man kunna säga är en molntjänst.

T: Som drivs av någon annan?

I: Som drivs av någon annan. Och där har vi ju en ganska lång tradition av… eeh stora system som sköts alltså, typ fakturasystem reseräkningssystem...eeh scanningsystem och sånt. Som ju vi inte själva har inom vårt LU nät utan det ligger i... står i Stockholm. Eller någon annanstans. Det är ju en sorts molntjänst så att säga. De förfogar över programvaran de förfogar över hela IT-sidan. Men drift av drivbackup och underhåll. Vi bara köper tjänst av dem. Så det är en sortsmolntjänst.

J: Ja precis.

I: Det är någon sorts vid beskrivning. Eeh sen så kom ju då Google på studentsidan. Alltså i modern terminologi. Den riktigaste molntjänsten så att säga. Och då 2009 på hösten som vi lanserade det, tror jag, till alla studenter... eeh ... egentligen... en sån klassisk migreringsproblematik. Dålig dyr tjänst till studenten som ingen använder. Billig... eller gratis tjänst som studenten ville ha. Det var inget svårt byte så utan det som var… tog mest tankekraft och krävde mest diskussion var ju integritetsfrågan eeh… efter studierna vad händer då? Alltså reklamfriheten, ääh vi hade ett antal diskussioner kring alltså Googles i början ganska omogna avtal... för de hade skrivningar om att vid tvist ska det avgöra vid domstol i Kalifornien och så där va. Vi blev anmälda till JO och en kring det ärendet så att säga. Ääh och mer för att Google då ändrat sina krav, det var inte domstol i USA om man var student tvingades in och tvingades in att kunde dömas i domstol om använde dem. Man var tvungen att under utbildningen använda sig av sin Google-adress.

J: Ja okej.

I: Men det var 2009. Det har hänt rätt mycket sen dess. Vi är inne på studentgeneration tre, nästan efter 2009 va. Och om man säger så, användningen ökade dramatiskt mycket sen 2009. Det märks ju på dem tre åren. Och redan då 2008-2009 så hade vi en diskussion om varför vi erbjuder studenterna epost adresser. Alltså varför ska vi som lärosäte erbjuda studenten en e-postadress. Men ni har förmodligen haft epost... sen alltid.

J: Mmm.

I: Hahaha. Men så länge ni kan minnas har ni haft en e-postadress i synnerhet alltså så va sen 10-15 års ålder den första e-postadressen. Sen har den följt med, ni har till det, en till det och en till det. För ni är lite olika personer så i olika sammanhang. En gaming adress och lite mer seriös sådär. Eller rätta mig om jag har fel? Haha.

J+T: Ja.

I: Sen varför ska ni ha en till när man börjar läsa på universitetet?

T: Kanske lättare att samordna det på universitetet?

I: Ja men sen så för att... ska vi alls tillhandahålla någonting? Ska vi inte bara liksom... så… med student eposten. Vi har ju fortfarande koll på vilka studenterna är. Vi kan ju fortfarande be studenterna i katalogtjänsterna att jag vill bli nådd på en här... till den här eposten vill jag ha mina tentaresultat eller till det här Face Bookkontot eller till det här humledumlekontotjänsten vill jag ha mina grejer skickade... skulle man lika bra kunnat göra. Istället för att vi tillhandahåller det så gör du det jobbet och vidarebefordrar. Eeh så det är ju fortfarande aktuellt för eposten kostar ju inte någonting för oss så då kan det lika gärna rulla på va. Och det är en sån sak som vi diskuterar ganska mycket när det gäller epost.

J: Ja.

I: ehm… så egentligen är det ganska okontroversiellt. Och det som är aktuellt nu det är ju lagringstjänster... i molnet. Alltså just på grund av paddor och så där va.

T: Liknande Dropbox och sådant då?

I: Alltså Dropbox liknande tjänster. Ehm... att... väldigt många som använde det kommer alltid diskussioner om säkerhet och integritet å sådär. Vilket har fått till konsekvens att hela högskolesektorn har gått ihop och håller på med en upphandling av Dropbox liknande tjänst... så man skriver ett vanligt avtal med en leverantör av Dropbox liknande tjänster. För att då kunna skriva in säkerhet och spårbarhet och äganderätt på materialet och sådana saker. Så det kanske kommer så småningom såna tjänster som studenterna får lagring i molnet tillhandahållet av LU. Eller snarare universitetet för att man måste kunna byta universitet. Alltså du måste ju nå det var du än är någonstans.

J: Okej. Är det några andra tjänster förutom mailen, scanningen och fakturan.

T: Ekonomisystemet.

I: Det är inte hela ekonomisystemet, det är bara delar av. Ehm… det är väl det hela det.

J: Vi använder ju det här Liveatlund, det ligger väl lokalt?

I: Ja det ligger lokalt. Men det är ju en sak som sån att den är ju förhållandevis klassisk. I sin struktur. Den är gjord av EHL och den står på EHL. Och den sköts ju av den här livegruppen som sitter uppe på andra våningen där inne i hörnet, haha. Där inne i det fönsterlösa rummet. ehm men det finns många andra som kör andra motsvarande live som går som hostade tjänster, blackboard är en annan sån typ av leverantör som de kör på någon institution i Malmö. Finns många som kör på forskningssidan i labbmiljö på BMC och så när de sitter och kör så har de ju labböcker, alltså de dokumenterar helt enkelt. Det finns som molntjänst. Alltid från vilken device som de har med sig. Det finns en det bibliotekstjänster som också är molntjänster med det är egentligen inlänkade databaser kan man väl säga. Stora databaser som vi har en nyckel till som passar motsvarande del som vi har prenumerationer på. Alltså vi tecknar prenumerationer med 50 förlag. En del i fulltext en del i bara abstrakt. Och men LU-inloggningen så kommer man direkt ut till det. Och det är också någon sorts... vanlig nättjänst.

T: Mmm.

I: Det närmar sig som ni är inne på det här området. Det är väl det som är kontentan... ja moln som fenomen är intressant det väcker en tanke hos ganska ovana... beslutsfattare som inte har tänkt på det här i vanliga fall. Men vi som håller på med det här ser ju att det inte är någon dramatisk skillnad mot något annat. Det beror vilket drast man lägger på det.

J: Okej.

T: Då kan vi hoppa in på nästa då.

J: Ja.

T: Hur ser ni på säkerheten i molnet i förhållande till att inte ha det i molnet så att säga?

I: Alltså den frågan dyker ju alltid upp i sådana här diskussioner. Ehm... säkerhet, integritet. Alltså äkthet på dokument och sånt. Hela det här klassiska. Ehm... den finns där samtidigt så bra säkerhet på det vi har idag? Hehe... så att säga. Alltså ja det blir en säkerhetsdiskussion att vi flyttar på det men vad är det som säger att våra miljöer idag är så himla mycket säkrare än de där borta? Nej och då har vi lite olika regelverk som styr att lagra därborta. Vi har lite EU-direktiv som styr så att säga i tredje land. Och vi har PUL som också hanterar tredje land. Vi har det som heter safe harbour som är ett antal länder utöver kontinentala Europa och Nordamerika och kanade som är godkända motsvarande EU inom EU så att säga. Det har varit mycket Facebook, nu vet ju alla i Sverige att det står en facebookserverpark uppe i Kiruna. Det är ju så mycket de här stora har gjort att man bygger... en node i Europa. För då är de compliance med EU-reglerna och då finns det egentligen inte någon anledning för oss att några nationella krav. Då gå det ju emot EU. Fri rörlighet av tjänst och produktion. Så med det så är ju juristerna nöjda, PUL folket är nöjda. Eee... integritetssidan är inte nöjda... men lite svart tolkning... det kommer de aldrig att bli haha, så att säga. Utan det gäller att bara ha ett... en vettig argumentation för det här är bra nog. Det är inte särskilt säkert att lagra lokalt på hårddisken om man tappar datorn. Alltså... det är det här med vem som ska ta bevisbördan. Ska jag bevisa att det är säkert eller ska de bevisa att det är osäkert? Så kontentan är ja det diskuteras mycket och det läggs kraft på det för att ha koll på det. Ehm... och tittar man sen på det... offentlig sektor i Sverige så har ju kommunerna haft lite andra bekymmer för de har ju… alltså universitetsutbildning är ju frivilligt. Hehehe. Det är det va. Grundskolan är ju tvingande och det som kommuner tillhandahåller till elever blir lite andra krav på för att de måste ju gå dit, de måste använda det. Här är det ett erbjudande till studenterna att använda det. Och det blir lite juridiska olikheter i det. Men för vår del så är det... så känns det rätt lugnt. Men att den alltid diskuteras mycket.

T: Vi har en fråga här som är: Anser ni att det finns specifika risker i molnet och med molnet som inte finns annars så att säga?

I: Nja det är ju det här med lagring och safe harbour frågorna. Safe harbour blir ju de som har unpinned contracts med leverantörer som vi inte har koll på. Att man inte har koll på som Amazon och deras underleverantörer. Det har vi inte insyn i så att säga. De bara säger att de är safe harbour compliance. Det är en sak som kommit upp i diskussionerna då om man backar tillbaka lite granna. Och det är ju det som har fått de här stora att bygga i Europa för att

lösa ut den här frågan. Och lokalt i Sverige så har det ju varit att Logica har tagit flaggan och säger att vi är hosting ställe för ett antal av de här salesforce tjänsterna. Då snurrar det i Bromölla istället. Vm-data eller Logicas serverfarm i Bromölla... då har man tagit ytterliga steg in och begränsat det. Svensk lagstiftning då garanterar Logica att det står fysiskt i Sverige.

T: Så man kan säga att frågar är lite att man har koll på var datan är?

I: Ja. Det är det som är med oron över var den faktiskt finns. Och det ständiga då... vem äger… så att säga. Men det är integritet med de delarna.

J: Har du något mer att tillägga på molnet där eller ska vi gå över till nästa del?

I: Inget just nu men kanske får vi något i nästa varv.

J: Då går vi över till migreringen då... hur ni arbetar med loka kontroller och hur ni arbetar med informationssäkerhet inför migreringen, som till exempel det här med mailtjänsten hur ni gjorde där?

I: Alltså själva nu får vi tänkta efter... det här var ju ett tag sen. Ehm och det gjordes ju av vår, alltså vår datacentral LDC-datacentralen student och utbildning. Det är den sektion som sköter om det, det är studentdesken. STIL-kontoret så att säga. Det är de som praktiskt tillhandahåller studentmailen och Google. Det var ju de tre som gjorde det men... ehm rutinen var sådan väl... nu får jag tänka efter här... de som lästa och hade epost i den gamla bara liksom gick in och flyttade på konton och sen så sög Google över... allt som låg i den boxen. Det hör ju till saken ja att ett problem med den gamle mailtjänsten att boxarna var extremt små. Så det var ju ingen data att prata om. Alltså om det var 250 Meg eller någon sånt så gick de sju gig på Google. Så det var ju ingen issue. Google sög över på studentens begäran så att säga, och alla nya studenter sattes det upp för. Så det var ju egentligen oerhört... och sen så lite städarbete och ett halvår senare ungefär så släckte man väl den gamle tjänsten. Eller den släckte sig själv... upphörde att fungera. Eeh... så migreringsprocessen var synnerligen enkel. Det var i och med att det var allt som fanns och det som eventuellt föll bort det var ju inte det här med att studenterna hade ju redan en annan. Det var ju inte den privata mailen så att säga. Så det var ju inte den här absoluta hanteringen av den. Vi gjorde ungefär samma sak något år senare för anställda där vi gick över i en Exchangelösning istället för anställda. Något år senare uppgraderade vi Exchangemiljön från tre till tio var det nog kanske sju till tio, vilket hopp det var. Så det fanns en viss rutin då på mailsidan av att migrera. Så... från mitt perspektiv så dök frågan aldrig upp igen som ett problem. Funkar det så hör jag ingenting. Utan att det är om det går åt skogen så hör man.

J: Använder ni några ramverk eller standarder vid den här migreringen då?

I: Det är jag fel man att svara på. Ääh men... det skulle ni prata om det med dem som gjorde själv jobbet just specifikt med mailmigreringen. Men det kan ni få namn på.

J: Använder ni ramverk och standarder normalt i IT-arbetet?

I: Ja alltså LDC då jobbar ju mycket med ITIL-processer så att säga. De kör ju hela ITIL-ramverket. Det har satsats ganska mycket på att utbilda hela personalen i det då och de har väl implementerat ett antal av de här klassiska… alltså change of problem den här vanliga.. och vi jobbar ju inte specifikt att vi följer ett exakt ramverk by the book så att säga... Jag har hållit på både med ITIL och COBIT och de här andra projektstyrningsvarianterna... det som kommer från, vad heter det nu... OCH, alltså brittiska statens det är mycket de som är ramverksproducenter som sen tweakas om till standarder och de har ofta sin utgångspunkt i det som heter OCG. Brittiska statens standardiseringsstruktur som ger ut en massa böcker och sån kring olika application management och system management och allt möjligt sånt. Sen när det gäller det som vi gör här är mycket av vårt jobb är att ta det bästa av olika standards för att passa den stora organisationen med utgångspunkt att vi inte kan ha specialramverk IT, specialramverk ekonomi, specialramverk personal, specialramverk webb, specialramverk kommunikation som jobbar på olika sätt. Så det som är vårt jobb är att se till att det funkar ihop. Alltså att de här verksamheterna fungerar tillsammans och funkar som styrmedel för organisationen och då kan man inte alltid använda alltid här i från ett ramverk så att säga skruvas om. Däremot kan ju IT-verksamheten IT-operations typ LDC och fakultetens IT-avdelningar vara mycket mer konsekventa i sina tillämpningar av ramverken. Där är det liksom IT-leveransprocesser punkt som de fixar med och då kan man använda det mycket, mycket mer. Vi rör oss på en mer generell managementnivå och då blir det att vi plockar russinen ur kakan. Vi har en uppdragsutförarmodell vi arbetar med SLA och underpinning contracts tankemodellerna så att säga. Vi har IT-systemägare som är ansvariga för underleverantörer och det kommer från… flera av de här olika IT-ramverken. De har ju det i sig på lite olika sätt. Om det går från leveransprocesser i ITIL eller om det går från leverandprocesserna i COBIT. De möts ändå någonstans.

T: Vi pratade lite om det här när ni förberedde er inför migreringen innan.

I: Mmm.

T: Och det var inte så mycket förberedelse?

I: Nej.

T: Det var mest att ni bara stängde ner det ena och startade det andra?

I: Ja i princip. Hehehe.

J: Fick ni några problem över huvud taget med migreringen?

I: Alltså det tog två veckor sen var det klart. Det var alltså... jag har aldrig sett någonting snabbare. Alltså det gick oförskämt bra.

J: Det är ju skönt när det går så också.

I: Ååh… just som migreringsprojekt så har jag sett många som har varit mycket, mycket värre. Men det har ju varit andra sorters. Här tog man bara mailboxen och skickade över mailboxen... det är en i förhållandevis trivial migrering ändå. Det är ju inte så att det var

tvunget att göras över en natt. Det löpte… det nya var uppe på två veckor. Och sen var det upp till studenten under sex veckor att göra jobbet själva. Att tala om att nu ska jag flytta min inbox från a till b vilket gjorde att frågefloden spreds ut över tid. Det var liksom så att det inte var tvunget att alla skulle göra det inför terminsstart. Alla nya studenter hade redan fått det och det funkade. Vi har idag någonstans 140000 konton på Google. Ääh...

T: Det är en del.

I: Men ändå. Det är 0,0001 promille av Googles totala konton. Det är knappt en decimalökning när vi gick in. Vilket gör att deras produktionsapparat bara sväljer... vilket ju ingen... det är ju en skillnad i molnet. Det finns ju ingen annan leveransstruktur med så liten marginalförändring skulle kunna ta emot och skapa 135000 epostkonton där alla får sju gigs lagring. Det hade ju knäckt vilket IT-leverantör som helst i Sverige. Och vår interna hade aldrig fixat det. Det hade tagit dem ett gigantiskt projekt i sex månader och de hade aldrig levererat det. Musklerna så att säga det är det som blir... där är vi ju egentligen inne i kärnan i det moderna molnkonceptet.

J: Ja, skalfördelningen.

I: Skalfördelningen och varje kund blir egentligen bara en marginaleffekt.

J: Ja, ni hade kunnat dubbla mailadresserna över en natt utan att det hade gjort någon skillnad i prestandan.

I: Det hade inte bekymrat dem. Så det är ingen affärsdiskussion om att vi måste ha stafflade priser som att den tusendeförsta blir jätte dyr. De säger, rulla över, hur många vill ni ha, ni får dem gratis. Det är väldigt... det en ovan affärsdiskussion. Där kommer någon som vill ge mig en massa väldigt bra saker, och kostnaden för mig? Ja får vi skriva att ni nu är vår största kund i Norden? Ja… javisst, får de ringa till dig? Vissa utvalda… ja det kan de väl få göra... hehe okej. Alltså lite annorlunda än om man skulle gå till Logica och vilja köpa 135000 mailkonton. Det är ju en molnskillnad. Där skala verkligen har effekt på affärsrelationen.

T: Förväntade problem. Hade ni förutsett något som kunde hända?

J: Värsta mardrömmen?

I: Värsta mardrömmen var egentligen på andra sidan. Att vi inte skulle hinna migrera det gamla innan den dog. Haha. Ehm men lite grann så var det ju på integritetssidan. Det var ändå och är ju fortfarande lite otrampad mark... lagstiftningsmässigt.

J: Borde kanske prövas i en domstol?

I: Ja alltså vi har börjat få en del fall där det är prövat. Prövat och prövat… datainspektionen har uttalat sig i frågan. De har hittills fram för allt behandlat kommunfrågor och skola men det har blivit aktuellt nu med högskolesektorn. Fler och fler pratar om att köra Office 365 och sånt. I och med att det funkar ju oerhört sömnlöst med ett installerat Officepaket. Där du kan välja att öppna det i browsern och köra den i Office 365 eller vill man öppna den lokalt på Office på datorn. Eller om man vill lagra den på Silverlight eller vad Microsofts moln nu

heter. För då flyttar man inte bara plötsligt studenten utan då är det den anställda personalens arbetsdokument som flyttar. Och det är plötsligt en mycket kämpigare fråga. Inte egentligen lagstiftningsmässigt och principiellt för det är samma som med studenterna alltså samma resonemang som tidigare men mentalt. Ska mitt underlag till Universitetsstyrelsens möte ligga i Redwood?  Naah känns otryggt. Så att säga va. Det är den typen av frågor som dyker upp.

T: Ni såg inga problem med det här med att Google är ju en ganska så stor aktör? Om många kommer till samma ställe så får ju de en väldig makt. Att hålla i allas data så att säga.

I: Jo mycket diskussioner.

J: Det är ju ändå en vinstdrivande organisation.

I: Ja men samtidigt så gör vi affärer med andra vinstdrivande som Microsoft och Oracle. Vi har rätt häftiga investeringar i våra serverparker och nät. Det är ju kommersiella spelare allihopa. Det är så att vi nämligen har kört hela.

T: Men vi tänker lite så om de erbjuder en massa space till varje människa och kanske sen om några år ändrar avtalen och då säger ni att det blir jätte dyrt... vi vill flytta och då sitter där väldigt mycket människor på väldigt mycket information i Google som kanske inte kan ta sig därifrån.

I: Ja. Det är en del i bedömningen. Vi har ju varit där och diskuterat väldigt mycket just exit klausulen. Hur gör vi, vilken beredskap måste vi ha för att själva erbjuda tjänsten? Ehm… och pratar vi då om studenterna så var vi ju där lite, okej, Google 2009, då kör vi i tre år. Den bedömningen gjorde vi. Ja, om tre år så står vi ju... Om Google vill att vi ska lämna allt... inte sannolikt men om... då kan vi sätta upp det själva igen...  inte göra det alls som vi pratade om tidigare, bara fimpa tjänsten och bygger den här andra tjänsten istället som skulle kontrollera. Ha det som koncept istället eller någon annan spelare som då har tagit över motsvarande funktionalitet. Vi kan inte planera för mycket mer än tre års sikt framåt. För mer än tre års sikt så blir det liksom fånigt. Så tittar man på världen, i treårs intervaller tillbaka i tiden.

J: Ja det händer ganska mycket på tre år.

I: För tre år sen i Sverige fanns... Iphonen hade kommit 2008...Dropbox fanns inte. Facebook fanns men det var spritt det var...

T: Det var inte lika integrerat.

I: Det var inte lika integrerat i allting. Alltså om man tänker tillbaka var vi stod för tre år sen så har man tagit till sig oerhört mycket andra beteenden. Och att då ha en planeringshorisont för såna här saker mer än tre år känns... sådär meningsfullt.

T: Det är väldigt diffust bara på några år.

I: Ja då är det bättre att det som vi har fokuserat på istället ha en mer kontinuerlig dialog. Och då så tittar vi tillbaka var vi på utbildningsstöd och systemen innan. Vilka möjligheter för ekonomihögskolan Allan T. Malm sommaren 2009 när han tryckte igång jobbet med

Liveatlund? Och vad finns det idag? Finns det samma sak idag? Nej förmodligen inte. Men då hade han inte några andra alternativ. Det är bara tre år.

T: Mmm.

I: Hehe… och vad händer då om era nya kursare som går termin ett eller två, var är de när de går sista terminen och skrivit sina exjobb? Vad har de för grejor? Haha… vad kan den där göra i version fyra eller fem? Så det är lite grann så att man blir lite blind på var man var någonstans.

T: Den här talar ju till en nu till och med.

I: Ja… den talar lite... man måste.

T: Den talar inte så mycket till mig ska jag säga.

I: Den ringer mest upp fel personer när jag provar.

J: Ska vi gå över till nästa del då?

T: Mmm.

J: Driften då... ni hade ju inte något direkt ramverk som ni följde utan ni använde lite av varje. Ser ni till att molntjänstleverantören följer det på något sätt?

I: Alltså där... det är inte min hemmaplan. Utan egentligen… ja det finns garanterat standarder som Google har följt utifrån hur... utifrån de integrationerna som är gjorda mot våra tjänster. Det handlar om studentkatalogen så att säga. Var ska vi få ut konto någonstans. Det följer helt klart något ramverk, jag vet inte vilket men det kan ni bara få kolla via han som är systemförvaltare för tjänsten. Och de som sköter om den lilla del där det finns internt. Det är den lilla integrationen mellan vår katalog och Google. Det är egentligen bättre att prata med dem och vilka ramverk som de har följt och hur den uppsättningen ser ut. Så jag är inte rätt man att svara på det...

J: Hade ni gjort något annorlunda idag eller hade ni gjort likadant med migreringen?

I: Nej jag hade nog gjort ungefär likadant idag... det är alltså rent migreringsmässigt. Diskussionen runt omkring hade varit annorlunda. Man har kommit längre rent mentalt idag. Men på den tekniska delen hade man nog gjort likadant.

J: Så då anser ni att det var värt att göra migreringen?

I: Ja. Det har visat sig vara en av dem... från att studenteposten någonstans var tredje månad var figurerad i pressen som dysfunktionell och att studenternas epost inte fungerade på två veckor och sådär. Sen har det varit knäpptyst sen vi gjorde det. Sånär som på dem som tyckte att de skulle JO-anmäla oss för att vi tvingade dem att de blir tvingade att infinna sig i domstol i Kalifornien. Men... utöver det så är det... tyst för nu håller man på istället att integrera Google. Nu pratar vi om Googleeposten rätt mycket men det som kom till apps... hela appsbiten som man säga va. Och nu har den börjat användas mer och mer integrerat som

i live där är väl någon kartkoppling till Googlemaps eller något sånt och det finns andra som tittar på det här. Tittar på inomhuspositionering med Google att man ska kunna hitta rätt i stora hus och sånt då de använder Googles API. LTH har en studentapp till paddan som är sådär men ändå lite Googleintegrationer. Där finns kartor och sånt klart. Kan lägga in och plotta punkter och sånt där. Det har ju hänt att man använder det istället i andra tjänster... vilket ju har... vi har ju väldigt många läromedel som man kan arbeta med Google-apps i utbildningen. Vad som är smart där och allting sånt... så det har hänt andra saker som våra system inte är kopplade till. Utan de är pedagogiskt kopplade istället.

J: ska vi gå över på de sista frågorna nu?

T: Mmm.

J: Har ni några återkommande riskbedömningar för till exempel Google-tjänsten som vi nu har pratat ganska mycket om?

I: Mmm. Vi har ju… alltså om vi går in på informationssäkerhetssidan eller risksidan så ... görs det på lite olika sätt. Dels görs ju riskvärderingar för hela organisationen. Nu är jag långt ifrån IT utan risken för hela Lunds universitet. Det är ju liksom... fallande forskningsfinansiering, minskat studentunderlag... den typen... bristen på studentbostäder. Alltså vad vilka faktorer... kan så att säga skada. Vilja faktorer ska vi utnyttja för att ha dem som hävstång. Typ ISS och Max och sånt. Ett sånt jobb görs årligen av universitetsledningen och folk omkring. Total omvärldsbevakning. För sen så bryts det ner inom olika områden och när det gäller informationssäkerhetsområdet så ehm... ansvarig för det är säkerhetschefen... som är totalt ansvarig för säkerhetsfrågorna där det handlar om informationssäkerhet. Och det har vi sen härifrån översatt och tagit hand om... att vi i uppdraget till ekonomichefsansvarig... ehm ska de varje år göra en riskvärdering... av sina system. Så om vi tar personalchefen så ska hon titta på de systemen som hon har hos sig. Och tillsammans med informationssäkerhetskompetens göra en värdering... vad händer vid ett avbrott? Finns det återläsningsplaner? Finns det i avtalet med leverantörer överenskommet med överläsningstider och avbrottstider och är det gjort faktiska återläsningar av data? Det klassiska att man har tagit en backup och att man inte kan läsa tillbaka den. Det händer ju fortfarande... och det ligger i uppdraget till dem. Och det är något som det har varit ganska mycket tryck på under de senaste åren inte minst från externa revisorer alltså riksrevisionen. Att man har varit på den här informationssäkerhetsfrågan på systemen ganska mycket. Ääh... och så det är den vägen som det hanteras så att säga och sen så gör ju då alla som är systemägare gör ju det för sina system. Jag gör ju det härifrån som systemägare för nätet och telefoni... core funktionen. Det gör ju vi tillsammans med LDC då som är driftställe eller tjänsteansvarig eller IT-systemägare för dem gemensamma. Sen jobbar man in den hela tiden så att man får in det... vi har ju ett separerat uppdrag till LDC som just handlar om alltså... IT-säkerheten. Där är ju nätscanning, sniffningar, alla peer2peer trafik stoppas ju. All den typen... det är ju inte så att vi gör det då och då vi gör det ju alltid. Det är den mer hårde delen av handson-säkerheten. Som säker lagring och redundans. Redundanta nät och allt det här liksom. De här går ju lite granna in i varandra. Ehm.. fungerar det? Ja hyfsat. Det kommer då och då kritik. Mycket av den kritiken under senare tid har varit att man efterfrågar från

granskningshåll. Tvåfas autentisering på lite mer... alltså på högnivårollerna alltså rootaccessen om man säger så. Så vill man ha två nivåer. Någonting du är, någonting du har så att säga. Med dosa, fingeravtryck, slumpgenerator eller någonting sånt där. Inte bara har användar-id och lösenord utan någonting till. En del vill ha det på alla individer men så räknade man ut vad det skulle kosta och sen så faller frågan igen. Hahaha. Det kostar för mycket liksom. Alltså man kan utrusta högnivåbehöriga med en dosa eller fingeravtrycksscanner eller något sånt där va men att ha det på varje användare så skulle de gå fullständigt ballistic liksom. Man skulle inte orka... ständiga säkerhetsproblemet.

J: Vi pratade lite om det här med exitstrategin innan. Har ni en fullt utvecklad där?

I: Nej. Vi har mer... vi hade det då 2009 men då sa vi liksom… håll till de där treårsresonemanget. Och nu känns det inte som att vi tänker lägga allt för mycket tid på det för att...

J: Precis... sju gig för varje mailadress... 135000.

I: Återställningen att vi skulle ta över och leverera vad Google levererar... finns ju inte. Den varianten existerar inte. Antingen gör Google det eller någon motsvarig eller så lägger vi ner det.

J: Okej.

I: Det är inte... det finns inte på kartan att vi skulle... få för oss att leverera samma sak. Det skulle kosta för mycket.

J: Men hur gick det till när ni valde molntjänstleverantör?

I: Det fanns två möjliga spelare på marknaden då… Google och Microsoft. Microsoft hade precis gått i luften. Ehm student och utbildning som gjorde själva jobbet hade bjudit in studentkårerna för att ha en referensgrupp på ett 20-tal studenter. Lite oklart urval men... 20 intresserade studenter som bidrog med några mötestimmar en vår och en försommar. Och omröstningen slutade 19-2 eller någon sånt där till Googles fördel. Så vi ställde frågan till studenterna, de som var med. Det finns a, det finns b oss kvittar det, det är samma sak för oss. Och då sa studenterna Google. Det var då Google fortfarande levde upp till dont be evil. Hahaha. Microsoft var evil... så var det. Vi som organisation hade inga värderingar alls i det. Utan studenterna valde sen körde vi på det.

J: Okej... har ni någon form av utbildning av systemen för nyanvändarna?

I: Du menar för studenterna?

J: Ja för alla.

I: Ja du kommer inte åt något system utan att passerat utbildning egentligen som anställd. Många av de här systemen är vad vi kallar för expertsystem. Alltså du är ekonom och ska sköta om din enhets ekonomiadministration eller något sånt. Är du IT person och ska sköta om en katalog eller något eller en e-postserver. Antingen kan du det på IT-sidan annars...

J: Är det bara hur man använder det eller är det mer säkerhetstänket också?

I: Det är säkerhetstänket också det ingår inte några separata säkerhetsutbildningar men att säkerhetskomponenten ingår i alla utbildningar så att säga det här med... och sen styr vi ju via ramverken att vi måste ha 8 tecken och att man ska blanda versaler och ha både numeriskt och alfanumeriskt så att säga. Såna inställningar försöker vi ha ungefär samma i de olika öar vi har. Vi har en masternode som är STIL som vi skjuter ut till ett antal tjänster. Och de som har helt egna för söker vi ha ungefär likadant så att man inte har jättehögt där... hyfsat likt säkerhetstänk. Funkar, funkar inte ja...

J: Testade ni tjänsten innan den implementerades fullt ut eller det var det här halvåret innan?

I: Ja man hade lite utvärdering. Man körde lite testinstanser, demotester och sånt där från leverantören. Men mycket var ju det att studenterna själva hade konton. Så det var ju utvärderat den vägen. Lite kontakter med andra universitet såklart. Alltså Linköping var väl några månader tidigare före oss i Sverige. Men det är i ett förhållande litet universitet. Vi hade en hel del kontakt med UBCS och British Colombia Vancouver som är ett av de största universiteten i Canada... som jag råkade springa på en konferens i Seattle. Så pratade vi lite med dem via telefon hur de gjorde och så... referens case internationellt. För det här var ju då Google gick ut med det här 2007 så det var fortfarande lite otrampad mark.

J: Okej. Vet du om det sker och hur det sker backup av datan på era tjänster?

I: Ja det får ju Google fixa. Haha. Vi utgår från at de har kolla på det. Det skriver de att de har koll på i avtalet.

J: Så ni har inte gjort några kontroller på det att det verkligen sker?

I: Nej.

J: Okej.

I: Det... finns... starkare påtryckningsstrukturer än Lunds universitet i det fallet som man kan använda sig av... typ media. Om vad vi tycker... om de säger att de gör det... det känns lite så… vi ska såklart ställa frågan men...

T: Det är kanske så att de bevisar.

I: Det kan vara så att de har läst tillbaka säger de och sen så rullar tjänsten. Och sen så får man titta på när det nu var som med Google hade sitt haveri och de tappade typ någon promille data... Ja då var det en hel jävla hall som brann upp. Ja de klarade den recoveryn rätt bra... ja... ingen issue.

J: Hur begränsas och kontrolleras användarnas åtkomsträttigheter till de olika systemen?

I: Utifrån behov. Vad behöver du för att göra ditt jobb? Du ska bara ha tillgång till så mycket som behövs för att du ska kunna göra ditt jobb. Ehm… den benämningen gör ansvarig chef. Ehm… då om det gäller ekonomi eller personal avdelningen till exempel… vem ska se… vem ska kunna göra förändringar i ekonomisystemet. Sen vem kan göra förändringar i budget

systemet. Du ska ju ha ansvar för att personen klarat utbildning är ju arbetsledande chef. Så det ligger helt och hållet i linje… sen om det är prefekten på institutionen eller studieläraren eller studierektorn vem det nu är, vem som faktiskt har det ska ju säkerhetsställa att studieadministratören vet hur Ladok fungerar. Så att de kan gå in och registrera poäng på kursen. Vilket förutsätter att regelverket följs. Det är på underskrivna examinator och listor så att de inte bara går in och reggar poängen så att säga. Det är ju arbetsledandechef det... den strukturen är genomgående alltså prefektens ansvar ute på utbildningarna.

J: Okej. Vet du om Google i detta fall har procedurer när data behandlas med radering av information som när de tar bort hårdvara eller byter ut hårddiskar? Slängs de eller vad gör de?

I: Det har vi ju ingen koll på utan vi litar på det... alltså återigen deras... bara att referera till branschpress. Som Facebooks datahall i Luleå är liten jämfört med de andra stora som står och mullrar någonstans. Det är ju inte så att de byter ut en hårddisk... De byter ut 500 hårddiskar samtidigt. Alltså om failraten är för hög på de 500 så bara kastar de dem. Smälter ner dem och bygger nytt. Det är ju inte så att de bara byter ut en hårddisk. De byter ut större rackvolymer än vad vi har totals sätt på universitetet. Det är ju skalor... som man inte riktigt fattar.

J: Man behöver nog se det för att förstå.

I: Man behöver nog se det för att förstå hur stort det där är. Nu tycker vi ändå att vi har mycket skrot i källaren... men det är ju ingenting.

J: Jag tänkte på det här med... användare… har ni några gemensamma lösenord och användarnamn? Eller alla har personliga?

I: Alla har personliga. Det är ett ständigt pågående arbete med att rensa ut gruppinloggningar. Men man har hållit på så pass länge nu att den förståelsen är rätt hög. Att man inte ska ha det.

J: Ja man tappar hela spårbarheten annars.

I: Ja precis det är ju... och det är speciellt i de systemen ekonomi och pengar har att göra för där är det extremt viktigt vem som har rätt att generera uttag. Det är dem vi pratar om att höja upp en nivå till två faktor. Så att... ständigt pågående… måste ändå pågå så det betyder inte att håller man inte igång det så... kanske det uppstår igen så att säga. Men mycket av våra tjänster idag går ju genom en sån här CAS-hantering. Som man jackar på som inloggning.

J: det är ju väldigt smidigt att vi loggar in på ett ställe sen kommer man till allt därifrån.

I: Vi har ju valt att inte ha autoinloggning på allting där utan man måste faktiskt logga in men du har samma inloggnings credentials. Inte single utan simplyfied. Om vi pratar SSO. Du måste fortfarande använda din credentials. Inte bara pang är på-loggad... det är den typen av väg som vi har valt. Den ständiga värderingen mellan enkelhet och säkerhet. Det blir alltid en bedömning. Får säkerhetsfolket bestämma blir det en sak, får användarna bestämma blir det något annat och någonstans i mitten ligger svaret.

J: Det var alla våra frågor. Har du något annat att tillägga?

I: Nej… egentligen så tänker jag på skye-tjänster. På en dansk konferens. Det man i Danmark hade fastnat på var ju integritet och var data lagras. Då körde jag mitt resonemang hur många av er har en hostad tjänst. Och vad är skillnaden rent principiellt. Att ha tjänsten hostad i Köpenhamn, Malmö eller Bryssel eller USA? När blir det en molntjänst? Det var ju ingen som kunde svara på det. För de hade fastnat i integritetsfrågan och lagringen... det var totalt stopp i Danmark. Man fick inte använda de här… i offentliga Danmark… fick inte använda Google fick inte använda Dropbox fick inte använda… totalt förbud. De hade gått på den linjen helt och hållet. Men sen så har de börjat luckra upp det. Vi har kanske blivit mer åt andra hållet. Mer pragmatiska från början kanske. Men det är... det har ju gått ett och ett halvt år sen jag var där och det har hänt massor. Det kommer att hända mycket, mycket mer här… väldigt snabbt som vi inte riktigt kan förutse vad det är för något. Vi gör så mycket nya grejor nu som vi inte gjorde tidigare. Nu sköter man ju alla bankaffärer från paddan. Säkert eller inte… visst det kanske är en säkerhetsrisk men om en miljon människor gör det… hur intressant är mina transaktioner i så fall?

J: Jo det är sant.

I: Nej men jag har inte mer.

J: Tackar så mycket.

I: Ni har fått lite källmaterial nu.

# Bilaga 5
## Intervjufrågor

### Inledande

*Kan ni berätta lite kort om företaget/organisationen?*

*Berätta om er och er roll i företaget/organisationen.*

### Molnet

*Varför har ni valt att använda er av molnet?*

*Vilka typer av tjänster/uppgifter använder ni er av i molnet?*

*Hur ser ni på säkerheten i molnet i förhållande mot "icke" molntjänster?*

*Anser ni att det finns specifika risker i molnet som inte finns annars?*

### Migreringen

*Hur har ni arbetat med IT-kontroller/ informationssäkerhet/ förändringshantering inför migreringen?*

*Vilka delar av COBIT eller andra ramverk och standarder anser ni har varit viktigast att bejaka vid en migrering till molnet?*

*Hur förberedde ni er inför migreringen?*

*Uppstod det några problem vid migreringen?*
- *– Vilka?*
- *– Förväntade problem?*
- *– Undveks problem genom att följa ramverk och standarder?*

### I drift

*Hur ser ni till att molntjänstleverantören följer era ramverk och standarder?*

*Vet ni om molntjänstleverantören använder sig av några ramverk och standarder?*

### Andra tankar/Reflekterande

*Vad hade ni gjort annorlunda idag om ni hade utför en liknande migrering till molnet?*

*Anser ni att det var värt att utföra migreringen med den information och kunskap som ni har idag?*

**Styrning**

*Sker det återkommande riskbedömningar?*

*Har ni en exitstrategi för att kunna lämna molnet?*

*Hur gick det till när ni valde molntjänstleverantör?*

*Hade ni någon utbildning av de nya systemen för användarna?*

*Testade ni tjänsten innan den implementerades fullt ut?*

*Hur sker backup av er data hos leverantören?*

*Hur begränsas och kontrolleras användarnas åtkomsträttigheter till systemen?*

*Vet ni om leverantören har procedurer för hur data behandlas vid radering av information eller vid modifikationer i hårdvara, flytt/avverkning?*

# Litteratur

Ahmed, A. (2011). *Using COBIT to Manage the Benefits, Risks and Security of Outsourcing Cloud Computing.* Hämtad från: http://www.isaca.org/Knowledge-Center/Documents/Using-COBIT-to-Manage-the-Benefits-Risks-and-Security-of-Outsourcing-Cloud-Computing.pdf den 3 mars 2012.

Beckers, K. (2011). *Security and Compliance in Clouds.* Wiesbaden.

Björngren, Z. Gullberg, T. Karlsson, J. Kvarnryd, J & Mattson, G. (2012). *Riskbedömning för migrering till molnet.*

Brunette,G & Mogull, R. (2009) *Security Guidance for Critical Areas of Focus in Cloud Computing 2.1*.

Farrell, R. (2010). *Securing the Cloud—Governance, Risk, and Compliance Issues Reign Supreme.* Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 310-319.

Gregg, M. (2010). *10 Security Concerns for Cloud Computing.* Global Knowledge. Hämtad från: http://www.globalknowledge.ae/knowledge%20centre/white%20papers/virtualisation%20white%20papers/10%20security%20concerns%20for%20cloud.aspx den 5 maj 2012

Grobauer, B., Walloschek, T. &Stöcker, E. (2011) *Understanding Cloud Computing Vulnerabilities.*

ISACA (2007). "Obtain COBIT" *ISACA.* Hämtad från: http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx den 3 april 2012

ISACA (2012). "History of ISACA". *ISACA*. Hämtad från: http://www.isaca.org/About-ISACA/History/Pages/default.aspx den 2 maj 2012.

Jacobsen, D.I (2002). *Vad, hur och varför? - Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen.* Studentlitteratur, Lund.

Jerräng, M. (28/11/2011). "Disk-problem bakom Tietohaveri". *Computer Sweden*. Hämtad från: http://computersweden.idg.se/2.2683/1.418561 den 8 maj 2012.

Mather, T., Kumaraswamy, S. & Latif, S. (2009) *Cloud Security and Privacy*. O'Reilly Media, Inc.

Mell, P. & Grance, T. (2011) *The NIST Definition of Cloud Computing.* Gaithersburg.

Pathak, J. (2005). *Information technology auditing - an evolving agenda.*Springer-Verlag. Berlin Heidelberg.

Sahibudin, S. Sharifi, M. & Ayat, M. (2008). *Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations.* Malaysia.

Small, M. (7/11/2011). "Managing Risk in the Cloud". *The Data Chain.* Hämtad från: http://www.thedatachain.com/articles/2011/9/managing_risk_in_the_cloud den 8 maj 2012.

Symons, C. Orlov, L. M. Brown, K. & Bright, S. (2006). *COBIT Versus Other Frameworks: A Road Map To Comprehensive IT Governance.*

Van Grembergen, W. & Haes, S.d. (2009), *Enterprise governance of information technology: achieving strategic alignment and value.* Springer, New York, NY.

Wikipedia 1. (2012), *National Institute of Standards and Technology.* Hämtad från: http://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology den 10 maj 2012.

Wikipedia 2. (2012), *Information Systems Audit and Control Association.* Hämtad från: http://en.wikipedia.org/wiki/ISACA den 10 maj 2012.

Winkler, J.R. (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics.* Rockland, MA: USA.

Zissis, D & Lekkas, D. (2010). *Addressing cloud computing security issues.* Syros, Greece.