EKONOMI
HÖGSKOLAN
Lunds universitet

IT-revisorns bidrag till IT-styrning

Magisteruppsats, 15 högskolepoäng, INFM02 i informatik

Framlagd: Juni, 2010

Författare: Stefan Arnslätt
Hampus Karlsson

Handledare: Lars Fernebro

Examinatorer: Carl Cederström
Claus Persson

Abstrakt

Titel IT-revisorns bidrag till IT-styrning

Författare Stefan Arnslätt
Hampus Karlsson

Utgivare Institutionen för informatik

Handledare Lars Fernebro

Examinatorer Carl Cederström
Claus Persson

Publiceringsår 2010

Uppsatstyp Magisteruppsats

Språk Svenska

Nyckelord IT-styrning, IT Governance, IT-revision, COBIT, Risk IT Framework

Abstrakt

IT-styrning är idag ett omtalat ämne när det gäller informationshantering. Organisationers behov av att hantera och effektivisera sin IT-styrning ökar i takt med systemens kapacitet och komplexitet. IT-styrning kan även ses som ett konkurrensmedel då vissa hävdar att organisationer med en god styrning ges mer i återbäring på tillgångar jämfört med företag med en svagare styrning (Weill & Ross, 2004). I detta avseende kan en IT-revisor assistera och bidra med vägledning gällande organisationers IT-brister, något som i förlängningen kan ha påverkan på IT-styrningen. I denna uppsats undersöks därför i vilken utsträckning IT-revisorns arbete kan påverka IT-styrningen i en organisation samt vilka områden som är mest kritiska för IT-revisorn att beakta i detta avseende. För att uppnå detta har en undersökningsmodell innehållande sju olika temaområden upprättats. Empiriska data har insamlats genom personliga semi-strukturerade intervjuer med IT-revisorer på fyra olika företag. Uppsatsens främsta slutsatser är att IT-revisorernas bidrag till IT-styrning är beroende av att deras rapportering når ledningsnivå samt den tid och omfång som ges varje IT-revisionsuppdrag.

Innehållsförteckning

Tabellförteckning

Figurförteckning

1. Introduktion

1.1 Bakgrund och problemområde

IT Governance, eller IT-styrning, är idag ett omtalat ämne när det gäller informationshantering (Xiao-wen et. al, 2010). Detta har ett samband med att företags processer blir alltmer datoriserade och således hanteras av informationssystem. IT-styrning är ett steg i att kontrollera att dessa processer producerar önskvärda och vinstgivande resultat.

Kapaciteten av IT-system har vuxit märkbart de senaste årtiondena och därmed även deras dynamik och komplexitet. Detta har inneburit att kostnader för misslyckade system har ökat. (Goldschmidt et. al, 2009) Trots en ständig utveckling på marknaden så verkar detta problem vara bestående. En studie utförd av The Standish Group visar att två av tre IT-projekt misslyckas och det finns inga tendenser på att denna trend är på nedåtgående (Nelson, 2007). En anledning till detta kan vara att de som faktiskt implementerar och underhåller system inte besitter en fullgod kunskap avseende IT-styrning. Systemvetare är en yrkesgrupp som ofta har ett stort inflytande vid implementeringen av system. Därför anser vi att det är viktigt att skapa en förståelse för de bakomliggande faktorer som gör IT-styrningen till ett viktigt område att hantera.

I en undersökning från 2008, utförd av ISACA, avseende de mest vitala verksamhetsfrågorna fann man att IT-styrning var en av de två viktigaste aspekterna att ta hänsyn till (Internet 1). En anledning till att IT-styrning anses så viktigt kan vara att företag med en god styrning ger minst 20 procent mer i återbäring på tillgångar jämfört med företag med en svagare styrning (Weill & Ross, 2004). IT-styrningen kan således betraktas som en bidragande faktor till organisationers effektivisering och optimering.

Avseende upphandling av IT-tjänster och deras servicefunktioner så eftersträvas den mest kostnadseffektiva lösningen som bäst möter de uppställda kraven. Detta har inneburit ett ökat behov av att IT-applikationer och infrastruktur fungerar och finns tillgängliga vid efterfrågan. Av stor vikt är således säkerställandet att kritiska informationsflöden är pålitliga så att information kan nås när det behövs. Följaktligen så ställer detta krav på att företags IT-funktioner är organiserade och bearbetade för att kunna möta nuvarande verksamhetsbehov. Att nå framgång avseende hanteringen av kritiska affärsprocesser och informationsflöden är dock inget engångsuppdrag, snarare är det en pågående process som kräver fortlöpande granskningar. (Silva & Chaix, 2008) I detta avseende kan en IT-revisor i egenskap av extern granskare lokalisera och informera om brister i systemen som hanterar företags information. Detta kan i förlängningen ha en inverkan på IT-styrningen genom att vitala system och deras processer granskas och utvärderas löpande. Behovet av kontroller för kritiska verksamhetsprocesser, IT-revision och en förstärkning av IT blir av allt större vikt. (Goldschmidt et. al, 2009) Merhout & Havelka (2008) påpekar i detta avseende att IT-revisioner kan innebära värdeökande effekter såsom förhöjd återbäring genom förbättrad IT-styrning.

Genererandet av dokumentation som IT-revisionen leder till kan även skapa en större och bredare förståelse hos ledningen för en organisations processer. I sin tur kan detta leda till att ledningen kan hantera organisationens resurser på ett mer framgångsrikt sätt. Ett viktigt syfte med IT-

revisionen kan även vara att individer inom en organisation i mindre utsträckning tenderar att utföra oansvariga och illvilliga handlingar om de vet att dessa står under granskning. (Merhout & Havelka, 2008) Det finns indikationer på att IT-revisionen kan bidra med värdefull input avseende organisationers hantering av IT. Det är rimligt att anta att de individer som utför systemgranskningar är de som har störst möjlighet att inverka på IT-styrningen. Det är därför av intresse att undersöka IT-revisorers arbetssätt och skapa en tydligare uppfattning om vilka områden IT-revisionen fokuserar kring. Vidare är det intressant att undersöka hur IT-revisorerna förhåller sig till IT-styrning och vilka delar i deras arbete som potentiellt kan påverka en organisations IT-styrning.

Utifrån det beskrivna problemområdet har följande frågeställningar utformats:

Vilka områden är viktiga för IT-revisorer att beakta avseende IT-styrning?

Vilka faktorer är mest kritiska avseende IT-revisorers arbete, relaterat till IT-styrning?

1.2 Syfte

Syftet med denna uppsats är att skapa en förståelse för IT-revisorns arbete och hur detta kan påverka IT-styrningen i en organisation. För att uppnå detta avser vi undersöka vilka områden inom IT-styrning som kan vara av vikt för IT-revisorer att beakta. Vidare är det av intresse att undersöka vilka faktorer som anses kritiska i detta avseende. Med ovanstående vill vi belysa en sida som normalt inte kommer fram under den systemvetenskapliga utbildningen. I rollen som systemvetare upplever vi det viktigt att ha en bred branschkännedom och förståelse för kollegors och samarbetspartners arbete.

1.3 Avgränsningar

Vår undersökning avgränsar sig från bolag som enbart arbetar med IT-revision då dessa är alltför få till antalet samt att de geografiskt sätt inte anses tillgängliga inom tidsramen för denna uppsats.

1.4 Förundersökning

Då IT-styrning och i synnerhet IT-revision till stor del var främmande områden för vår del och något som inte ingått under den systemvetenskapliga utbildningen så ansåg vi det lämpligt att skapa oss en tydligare bild av dessa områden. Halvorsen (1992) beskriver att ett område i vissa fall kan vara outforskat vilket gör det svårt att utforma en problemställning som når längre än en ren beskrivning av fenomenet ifråga. I sådana fall kan det vara nödvändigt att genomföra en förundersökning för att kunna komma fram till en avgränsad problemställning som lämpar sig för forskning (Halvorsen, 1992). I syfte att få en tydligare bild av en IT-revisors uppgifter och ansvarsområden valde vi att kontakta en IT-revisor för att genomföra en förberedande intervju. Intentionen med intervjun var att den skulle ha en generell och övergripande karaktär med syfte att klargöra IT-revisorns roll i en organisation.

Efter genomförd intervju blev vi även inbjudna till ett seminarie med IT-styrningsorganisationen ISACA som bland annat certifierar IT-revisorer. Den IT-revisor vi träffade under

förundersökningen ansvarade för detta seminarie tillsammans med en annan IT-revisor. Seminariet gick under namnet *IT-revisorns roll i revisionen* och deltagarna var intressenter som ville få en tydligare bild av IT-revisorns roll. Seminariet hölls i Malmö på en stor revisionsbyrås kontor. Vi ansåg att vårt deltagande skulle kunna bidra ytterliggare till vår förståelse för IT-revision, och bedömde det således vara av värde för uppsatsarbetet.

Den information vi fick genom dessa inledande kontakter kommer inte att redovisas separat då syftet endast var att skapa en tydligare förståelse för området i fråga. Det ska dock tilläggas att informationen från förundersökningen till viss del har påverkat valet av litteratur att fokusera på. Vi har således haft förundersökningen i åtanke då vi beaktat relevansen av studerad litteratur.

2. Litteraturstudie

Givet denna uppsats syfte så anser vi att det finns behov av att upprätta en undersökningsmodell. En sådan undersökningsmodell kan skapa en tydligare struktur för uppsatsen och framförallt bibehålla fokus mot uppsatsens syfte. I förlängningen har vi en förhoppning om att denna modell ska underlätta insamlingen av empirisk data samt att möjliggöra en jämförelse mellan datan och den modell vi ämnar skapa.

Som ett första steg mot att utforma en lämplig undersökningsmodell har vi valt att göra en litteraturstudie. Med hänsyn till uppsatsens syfte tar litteraturstudien sin utgångspunkt i allmän litteratur inom IT-styrning. Enligt Willson & Pollard (2009) så täcker IT-styrning ett stort område. Både Willson & Pollard (2009) och Kurtén (2009) anser att *”strategisk anpassning”, ”mätning och uppföljning av IT”, ”IT: s värde”* samt *”riskhantering”* är viktiga ansvarsområden att beakta. Även en mängd andra forskare poängterar vikten av något eller flera av ovanstående områden (Luftman, 2004; Parent & Horner Reich, 2009; Posthumusa & von Solms, 2005; Silva & Chaix, 2008) Dessa områden kommer att ligga till grund för litteraturstudiens omfång och därmed den undersökningsmodell vi avser upprätta.

Under förstudien har det tydligt framgått att ramverk är vanligt förekommande i samband med IT-styrning. Det är behovet av att styra IT och de processer som är relaterade till IT som har lett till uppförandet av ett antal olika ramverk. En rad ramverk för IT-styrning är framtagna för att beskriva verksamhetsprocesser och ger företag möjlighet att ordna aktiviteter på ett mer effektivt sätt, framförallt avseende IT-organisatoriska processer. Dessa ramverk utgör en generell modell som måste anpassas till den specifika kontext som företaget verkar inom. (Goldschmidt et. al, 2009) Ramverk som adresserar något eller flera av ovanstående fyra ansvarsområden har enligt den litteratur vi granskat varit följande: COBIT, ISO 38 500, SOX, Risk IT Framework, ITIL samt Val IT. Av denna anledning har vi valt att titta närmare på dessa. För att skapa en kompletterande bild till vår förstudie avseende IT-revision i allmänhet så har vi även valt att granska litteratur kring IT-revision och IT-revisorns roll i revisionsprocessen.

2.1 IT-styrning

2.1.1 Varför IT-styrning?

Ledningen för organisationer har en förhoppning och förväntan på att investeringar i IT ska resultera i ökat affärsvärde och effektivare processer. Historiskt sett så har det följaktligen funnits stort fokus bland IT-ledningar på användningen av ny teknologi för att adressera affärsproblem. Dessa ansträngningar har dock ofta misslyckats, och för att den här typen av investeringar ska lyckas så krävs det att även den övriga verksamheten tar ansvar för IT. Utan detta stöd är risken stor att IT-investeringar misslyckas och ger oönskade resultat. (Luftman, 2004)

Att det råder en bristande kommunikation och förståelse mellan olika avdelningar av en verksamhet leder ofta till ovanstående problematik. I detta avseende så saknas ofta en tydlig form av IT-styrning. Införandet av en sådan skulle emellertid kunna leda till en bättre struktur avseende projektprioriteringar och fördelning och hantering av IT-resurser. Att utvärdera och bedöma alternativen för IT-styrning är således vitalt för en fungerande hantering av IT. Att en

sådan hantering ska bli framgångsrik kräver vidare att det används lämpliga mått och riktlinjer för att kunna mäta värdet av IT, vilket bör ske kontinuerligt. (Luftman, 2004)

2.1.2 En definition av IT-styrning

IT Governance, eller IT-styrning, är ett begrepp som har definierats på en mängd olika sätt och det råder i vissa fall en osäkerhet bland verksamhetsledare kring vad konceptet verkligen innefattar (Willson & Pollard, 2009). En relativt kort och koncis definition har givits av Webb et. al (2006, s. 7), som preciserar begreppet enligt följande:

> *"IT Governance is the strategic alignment of IT with the business such that maximum business value is achieved through the development and maintenance of effective IT control and accountability, performance management and risk management."*

IT-styrning handlar till stor del om att hantera organisatoriska processer på ett sätt som ger värde för organisationen samt att ta beslut angående anskaffandet och fördelningen av IT-resurser. IT-styrningen är alltså själva modellen för hur organisationen ska använda sig av IT. Viktiga frågor för IT-styrningen är vem som fattar dessa beslut (makt), varför dessa beslut tas (sammankoppling) och hur dessa beslut tas (beslutsprocessen). (Luftman, 2004)

Vidare rör IT-styrningen befogenheter och behörigheter, kontroll, redovisningsskyldighet, roller och ansvarsområden mellan organisationsenheter och deras hantering av beslut angående IT-användande. IT-styrningen involverar även organisatoriska processer och metoder, bland annat för att värdera risker och mäta olika aspekter såsom IT: s värde. Att ha en välstrukturerad styrningsmodell i syfte att kunna ta effektiva beslut är särskilt betydelsefullt i stora komplexa organisationer. (Luftman, 2004)

Strukturer, processer och kontrollramverk är viktiga termer när det gäller IT-styrning. Dessa representerar viktiga koncept och verktyg för att applicera, implementera och utveckla IT-styrning. (Willson & Pollard, 2009) Precis som en fungerande sammankoppling mellan IT-strategi och affärsstrategi är av stor vikt så är det lika betydelsefullt att processerna för IT-styrning är associerade med den övergripande verkamhetsstyrningen. Att säkerställa att det råder en fungerande IT-styrning är endast möjligt genom att undersöka och utvärdera en IT-styrning som har tagits i bruk. Att i detta avseende applicera någon form av kontrollramverk i syfte att vägleda IT-styrningen är väldigt betydelsefullt. (Willson & Pollard, 2009)

Det finns ett antal faktorer som kan ha en påverkan på IT-styrningen, bland annat goda kommunikationsstrategier för att möjliggöra för komplex kommunikation och strukturering samt ett starkt förhållande mellan IT och affärsverksamheten. Ytterliggare en betydelsefull del att beakta är den föränderliga miljö vari IT-styrningen befinner sig, vilken innebär att löpande utvärderingar och granskningar krävs för att möta dessa förändringar. Detta kan göras bland annat genom kontroller och mätningar av IT: s förväntade resultat. (Willson & Pollard, 2009)

2.2 Ramverk relaterade till IT-styrning

2.2.1 COBIT

COBIT (Control Objectives for Information and related Technology) är ett kontrollramverk för IT-styrning, framtaget av den oberoende IT-styrningsorganisationen ISACA. ISACA bildades 1967 när granskningskontroller avseende datorstödda system började bli en kritisk faktor för organisationer att beakta. I dagsläget har ISACA 86 000 medlemmar över hela världen vilka bland annat utgörs av IT-revisorer, konsulter, IT-säkerhetsexperter, CIO: s och interna revisorer. (Internet 2)

Målet med COBIT är att överbrygga gapet mellan affärsrisker, kontrollbehov och tekniska aspekter genom att presentera IT-aktiviteter i en hanterbar och logisk struktur. En av de stora styrkorna med COBIT är dess förmåga att erbjuda tydliga riktlinjer för ledningen. Enligt COBIT är det viktigt att chefer och ledare förstår statusen för deras IT-system och bestämmer vilken grad av säkerhet och kontroll de skall erbjuda. Vad som menas med detta är att det finns ett behov av fortlöpande förbättring när det gäller IT-säkerhet och kontroll. (Pathak, 2005)

COBIT har övergripande och genomgående fokus på verksamheten. För att lämna den information som verksamheten behöver för att uppnå sina mål så behöver verksamheten investera i, hantera och kontrollera IT-resurser. COBIT hanterar detta genom en strukturerad samling processer, totalt 34 stycken, som tillhandahåller de tjänster som leder till den önskade företagsinformationen. I COBIT finns ett antal kontrollmål för varje process och processerna återfinns inom fyra olika domäner. Domänerna är ”*planera och organisera”*, ”*införskaffa och implementera”*, ”*leverera och stödja”* och slutligen ”*övervaka och utvärdera”*. För att möta verksamhetens mål så behöver informationen överrensstämma med de specifika kontrollmål som beskrivs som verksamhetens informationskrav. Kontroll definieras som policys, procedurer, tillvägagångssätt och organisatorisk struktur. (COBIT 4.1, 2007)

COBIT möjliggör för en IT-revisor att granska specifika IT-processer mot COBIT: s kontrollmål och därmed bestämma på vilka ställen kontroller är tillräckliga, eller råda ledningen då processer kräver förbättring. (Internet 3) Genom att implementera COBIT-riktlinjer kan företag exempelvis sätta normer för, och mäta, sina processer gentemot jämlikar i branschen och därmed uppnå en hög konkurrensnivå för IT-säkerhet och kontroll. Genom verktyg såsom nyckelmålsindikatorer (Key Goal Indicators) och nyckelprestationsindikatorer (Key Performance Indicators) kan organisationer mäta resultatet av sina processer och hur väl de presterar. (Pathak, 2005) COBIT besvarar den ständiga frågan ”*Vad är rätt nivå av IT-kontroll för att stödja verksamhetens mål*” (Pathak 2005, s. 154).

2.2.2 ISO 38 500

ISO 38 500 har utmynnat från den Australiensiska standarden AS8015:2005 och är en principbaserad vägledningsstandard som riktar sig till högsta ledningen i organisationen. Syftet är att ledningen ska använda standarden för att utvärdera, styra och övervaka användandet av IT inom verksamheten. (Internet 4) Standarden kan appliceras för att styra ledningsprocesser och hantera beslut som är relaterade till informationen och kommunikationstjänster som används av organisationen. Som potentiella intressenter för denna standard nämns IT-revisorer. (Internet 5)

2.2.3 Sarbanes-Oxley Act

Regelverket Sarbanes-Oxley Act (SOX) utformades efter en rad redovisningsskandaler som resulterade i misslyckande och mycket stora förluster för aktieägarna i stora offentliga företag. Med anledning av detta utformade den amerikanska kongressen därför nya lagar vilket innebar drastiska förändringar avseende krav på den finansiella rapporteringen och bolagsstyrning. En stor del av dessa förändringar var just Sarbanes-Oxley Act, eller SOX, som infördes i juli 2002. Den mest omtvistade aspekten av SOX är sektion 404, vilken kräver att såväl ledningen för ett bolag som externa revisorer rapporterar om tillförlitligheten och effektiviteten för företagets interna kontroller över den finansiella rapporteringen. (Ebrahim, 2010) **S**ektion 404 relaterar specifikt till IT och de kontroller som styrs av IT. Detta har inneburit stora förändringar och utmaningar för organisationsledningar avseende deras IT-hantering. (Warden, 2008)

2.2.4 Risk IT Framework

Detta ramverk har tagits fram av ISACA och fokuserar på IT-relaterade risker med syfte att assistera organisationer i den här typen av frågor. Ramverket är ett komplement till COBIT, ett ramverk som ger ett mer övergripande stöd till styrning och kontroll. (Risk IT framework) Risk IT Framework syftar till att hjälpa IT-revisorer göra en förbättrad analys av risker och assistera IT-revisorerna när det gäller revisionsplanering och skapandet av rapporter (Harrast & Weirich, 2009).

Vidare definieras, och baseras, ramverket på ett antal vägledande principer för effektiv hantering av IT-risker. Dessa principer är baserade på vedertagna riskhanteringsprinciper som sedan har applicerats på IT-domänen. Tre övergripande domäner, *riskstyrning, riskutvärdering* samt *riskbesvarande,* utgör grunden för ramverket. Den förstnämnda domänen fokuserar på aspekter såsom riskaptit, det vill säga den mängd risker en organisation är beredda att ta, och företagets riskkultur i allmänhet. Den andra domänen är fokuserad på vilken affärspåverkan risker kan ha samt beaktningen av olika typer av riskscenarios, det vill säga vilka konsekvenserna kan bli om en risk blir verklighet. Den tredje domänen behandlar hur risker bör definieras, prioriteras och besvaras. Inom dessa domäner återfinns sedan ett antal processer som i sin tur fokuserar på kontrollmål för respektive process. (Risk IT Framework)

2.2.5 ITIL

ITIL (Information Technology Infrastructure Library) består av en samling best practices som baseras på erfarenhet från en rad olika IT-leverantörer (ISP). ITIL ger utrymme för ett systematiskt tillvägagångssätt avseende leveransen av IT-tjänster med hög kvalitet. ITIL ger en detaljerad beskrivning av de viktigaste processerna i en IT-organisation och innehåller även checklistor för procedurer och ansvar vilka kan användas som en bas för att skräddarsys till den individuella organisationens behov. ITIL fokuserar på så kallad IT-service management (ITSM). (Van Bon et. al, 2007) ITSM lägger stor vikt vid kundens perspektiv, det vill säga de som upphandlar och använder systemen, av IT: s bidrag till verksamheten (Galup & Dattero, 2010).

2.2.6 Val IT

Val IT är ett övergripande och pragmatiskt ramverk, framtaget av ISACA, som ger direkt stöd till chefer på alla ledningsnivåer inom både affärs- och IT-organisationer och är ett komplement till COBIT. Val IT hjälper ledningen att fokusera på två av fyra fundamentala IT-styrningsrelaterade frågor. Dessa är ”*Gör vi rätt saker*?” (strategiska frågan) och ”*För vi ut nyttan*?” (värdeskapande frågan) medan COBIT hjälper ledningen att fokusera på att besvara frågorna ”*Gör vi sakerna på rätt sätt*?” (arkitekturfrågan) och ”*Får vi gjort dem bra*?” (leveransfrågan). Val IT omfattas av tre domäner och varje domän innehåller ett antal processer med tillhörande processmål. De tre domänerna är värdestyrning, portföljhantering och investeringshantering. (Val IT)

Värdestyrning har som mål att säkerställa att tillvägagångssättet för att hantera värdet av IT är inbäddat i verksamheten. Detta gör det möjligt att säkra det optimala värdet från IT-investeringar. Ett engagemang från ledningen avseende värdestyrning hjälper företaget med att upprätta ramar för hantering av värde på ett sätt som är integrerat med verksamhetens övergripande styrning. Portföljhantering inom ramen av Val IT finns för att säkerställa att ett företag försäkrar sig om att organisationen får ut ett optimalt värde av hela sin IT-portfölj. Ett engagemang för portföljhanteringen på verkställande nivå hjälper framförallt till med att upprätta och hantera en resursprofil, utvärdera, prioritera och välja nya investeringar samt att övervaka och rapportera om portföljens resultat. Investeringshantering har som mål att säkerställa att företagets enskilda IT-investeringar bidrar till ett optimalt värde. (Val IT)

2.3 IT-revision

IT-revision har sitt ursprung i den finansiella revisionen (Pathak, 2005). Den finansiella revisionen är en oberoende granskning av en verksamhets ekonomi som måste följa en rad riktlinjer och standarder utfärdade av en extern part. Revisionen kan utföras antingen genom att anlita externa auktoriserade revisionsbyråer eller med hjälp av en intern revisionsfunktion. (Merhout & Havelka, 2008)

För att revisionen ska klassificeras som en IT-revision så krävs det att någon form av informationsteknologi granskas. På samma sätt som den traditionella revisionen kan IT-revisionen ske antingen med hjälp av externa eller interna funktioner. De flesta revisioner, IT-revisioner inkluderat, utförs genom ett riskbaserat tillvägagångssätt, vilket innebär att potentiella risker identifieras och prioriteras, kontrollmekanismer utvärderas, och kontroller testas. (Merhout & Havelka, 2008) IT-revisionen är följaktligen ett sätt att säkerställa kvaliteten på informationssystem, och genom detta även kvaliteten på den elektroniska information som ledningen och organisationen i stort använder sig av (Ion et. al, 2008).

Några av de aktiviteter som genomförs under en IT-revision inkluderar att granska dokumentation för affärsprocesser; utvärdera kontroller som ligger inbäddade i olika applikationer såsom affärssystem samt att testa riktigheten och validiteten av data i databaser. Den här typen av granskningar kan ske på en väldigt detaljerad nivå. Analyser på en högre nivå, vilka kräver erfarenhet och expertis för mer specifika teknologier, är även förekommande. När arbetet sker på en strategisk nivå så involveras även personer från ledningen. (Merhout & Havelka, 2008) IT-revision kan således utföras på alla nivåer inom en organisation för att

utvärdera de processer, strukturer och mekanismer som används för att implementera IT-styrning (De Haes & Van Grembergen, 2008; Merhout & Havelka, 2008).

På högsta ledningsnivå kan IT-revisionen användas för att säkerställa att IT-strategin är sammankopplad med den övergripande verksamhetsstrategin samt att specifika IT-policys implementeras och följs. IT-revisionen är följaktligen ett sätt att minska risker relaterade till IT. På en operationell nivå så säkerställer IT-revisionen en korrekt hantering av vardagliga processer och transaktioner. Detta inkluderar att identifiera risker och kontroller som är relaterade till specifika applikationer och affärsprocesser samt att testa huruvida dessa kontroller fungerar på ett önskvärt och lämpligt sätt. (Merhout & Havelka, 2008)

2.3.1 IT-revisionens syfte

Som tidigare framhållits så är det primära syftet med IT-revisionen att bedöma huruvida ett informationssystem möter de organisatoriska kraven och målen samt att säkerställa att system inte skapar en oacceptabel risknivå för företaget (Pathak, 2005). Detta involverar att testa och granska interna kontroller som omger informationssystemen, men även att tillfredsställa ledningens ansvar avseende styrning (Merhout & Havelka, 2008). Den huvudsakliga fördelen som IT-revisionen resulterar i är följaktligen att man med en viss grad av säkerhet kan säga att ett informationssystem fungerar på ett lämpligt sätt. Detta innefattar att systemet bearbetar input till output på ett korrekt vis, att endast behöriga användare kan ha åtkomst till specifika data eller program samt att data lagras korrekt och säkert. (Pathak, 2005)

Andra fördelar som kan nås med hjälp av IT-revisionen är till exempel att organisationer tillmötesgår olika regelverk och standarder och därmed når en ökad och förbättrad systemsäkerhet. Att genomföra IT-revisioner kan även leda till upptäckten av avvikelser såsom medvetna överträdelser gentemot policys, eller omedvetna misstag som innebär lagbrott. En IT-revision kan även bidra till identifiering och dokumentering av kontrollmekanismer i informationssystemen. Att kunna kontrollera dessa aspekter är fundamentalt för ledningen. (Merhout & Havelka, 2008) Detta beskrivs som ytterst viktigt för att kunna utöva en effektiv IT-styrning (De Haes & Van Grembergen, 2008). Dokumentationen som dessa kontroller resulterar i tillåter ledningen att utvärdera hur pass tillfredsställande kontrollmekanismer i förhållande till den operationella effektiviteten är. (Merhout & Havelka, 2008)

2.4 Upprättande av undersökningsmodell

Med utgångspunkt i litteraturstudien har vi valt att utforma ett antal urvalskriterier för att styra vad som ska ingå i uppsatsens undersökningsmodell. Utformningen av urvalskriterierna är gjorda för att begränsa undersökningsmodellens omfattning till att endast inrymma det som upplevs vara mest relevant i förhållande till uppsatsområdet. Urvalskriteriena presenteras nedan:

- Uppsatsens undersökningsmodell ska täcka de fyra ansvarsområdena inom IT-styrning som tidigare presenterats, nämligen *strategisk anpassning, mätning och uppföljning av IT, IT: s värde* samt *riskhantering*.

- Undersökningsmodellen ska rimligen vara förankrad i det arbetssätt som föreligger s*venska* revisionsbyråer avseende IT-revision. Detta för att bidra till en relevant koppling till de företag vi ämnar använda i vår undersökning.

- Undersökningsmodellen ska innehålla material som ska finnas fritt tillgängligt i sin fullständiga orginalform. Detta för att kunna skapa en korrekt förståelse för de underliggande faktorer som ramverken bygger på.

- Undersökningsmodellen ska ge en tydlig koppling till IT-styrning och hantera frågan vad som bör göras för en effektiv IT-styrning.

- Undersökningsmodellen ska kunna knytas till en IT-revisors granskning av organisationers befintliga IT-hantering och därmed inte handla om nya eller framtida IT-investeringar.

- Undersökningsmodellens beståndsdelar ska inte vara så detaljerade att de inte kan besvaras av enskilda respondenter utan detaljkunskap.

Urvalsprocessen har resulterat i följande:

SOX har inte tagits med i uppsatsens ramverk. SOX är ett regelverk vars främsta syfte är att säkerställa att bolagets interna finanser är korrekta och syftar därmed inte till att hantera IT-styrning. Regelverket omfattar endast de bolag som är noterade på den amerikanska börsen vilket har gett oss anledning att tro att endast ett litet antal svenska IT-revisorer jobbar mot SOX: s kontroller.

ISO 38 500 finns inte fritt tillgängligt i sin fullständiga orginalform och då vår förfrågan att i egenskap av undersökningssyfte ta del av det fullständiga materialet nekats har vi valt att inte ta med faktorer från detta ramverk.

COBIT är utformat i syfte att skapa en starkare IT-styrning och riktar sig bland annat till IT-revisorer (COBIT 4.1, 2007). Även Brown & Nasuti (2005) framhåller att COBIT är ett generellt accepterat ramverk för IT-revisorer. De kontrollmål (se avsnitt 2.5.1-2.5.6) som valts från COBIT anser vi täcker in ansvarsområdena *strategisk anpassning* samt *mätning och uppföljning av IT*.

Av dessa anledningar har vi valt att inkludera kontrollmål från COBIT i uppförandet av vårt ramverk.

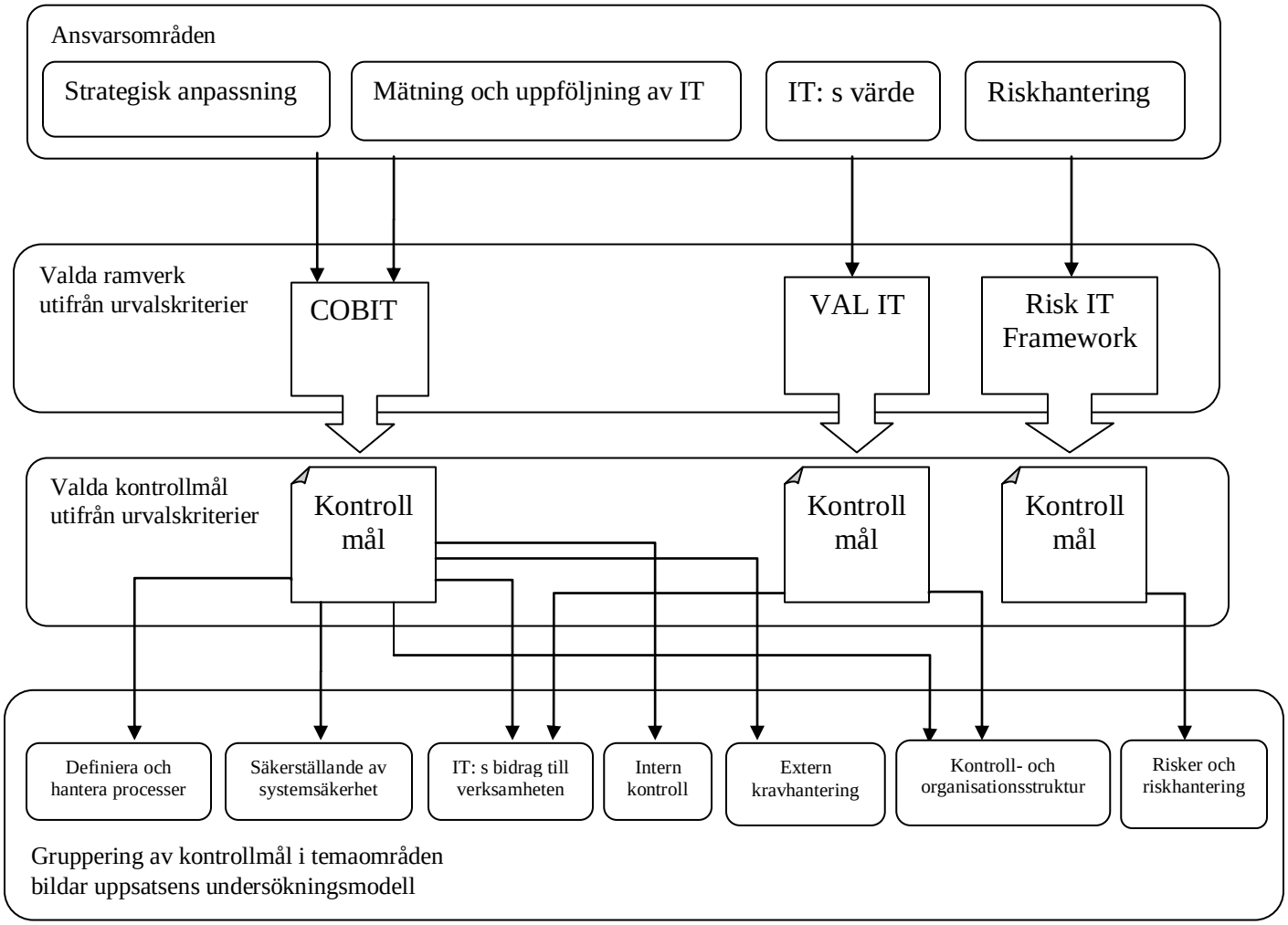
Parent & Horner Reich (2009) gör en uppdelning av IT-styrning och skiljer mellan IT-riskstyrning och IT-värdestyrning. Författarna framhåller att den viktigaste aspekten, och den som bör beaktas först, är IT-riskstyrning. Av de ramverk som studerats är det enda som renodlat hanterar IT-risker IT-risk Framework. Ansvarsområdet *risker* täcks därmed in med kontrollmål (se avsnitt 2.5.7) från detta ramverk.

För att slutligen täcka in *IT: s värde*, vilket utgör ett av ansvarsområdena, har vi valt att applicera kontrollmål (se avsnitt 2.5.3 och 2.5.6) från Val IT.

ITIL saknar tydligt fokus på IT-styrning då detta ramverk koncentrerar sig på hur IT-tjänster ska stödjas och levereras till skillnad från COBIT som lägger fokus på vad som bör kontrolleras och hur det ska mätas (Internet 6). Då ITIL vidare fokuserar på IT-Service Management så återfinns en tydlig inriktning mot kundens perspektiv i förhållande till företaget som applicerar ITIL. (Van Bon et. al, 2007) Detta ligger enligt oss allt för långt ifrån uppsatsens inriktning och därför har vi valt att inte ta med några faktorer från detta ramverk.

Urvalskriterierna har således resulterat i anvädningen av COBIT, Risk IT Framework samt VAL IT. Utifrån dessa ramverk har sedan kontrollmål från respektive ramverk valts ut med utgångspunkt från urvalskriterierna. Dessa har kategoriserats och placerats in inom vad vi kommer att kalla temaområden för att ge struktur till såväl intervjuguiden som att ge uppsatsen en röd tråd. Dessa temaområden bildar uppsatsens undersökningsmodell. Ovan nämnda ramverk har således inte applicerats i sin helhet utan använts som inspirationskällor för att lokalisera temaområden som uppfyller kraven för urvalskriterierna. Nedanstående figur visar urvalsprocessen för upprättandet av denna uppsats undersökningsmodell. Respektive temaområde och kontrollmål ges en mer detaljerad presentation i avsnitt 2.5.

Figur 2.1: Urvalsprocess för undersökningsmodell



Vi är medvetna om att de ramverk som har använts för att lokalisera lämpliga temaområden alla har utformats av samma ISACA. ISACA är en internationellt erkänd organisation och deras ramverk är väletablerade och genomarbetade. Varje temaområde innehåller en inledande text vilket syftar att ge läsaren en övergripande bild av området och dess koppling till IT-styrning. Kontrollmålen ligger på en mer detaljerad nivå i syfte att jämföra mot IT-revisorernas arbetssätt.

2.5 Temaområden

2.5.1 Definiera och hantera processer

Processer är vitala att beakta för att organisationer ska uppnå sina mål (Lodhi et. al, 2009; Harmon, 2007). För att kunna hantera IT-prestanda så krävs det att man övervakar och kontrollerar processer. Detta inkluderar att definiera vilka indikatorer för prestanda som ska finnas, att rapportera prestanda på ett systematiskt och lämpligt sätt samt att agera om det skulle förekomma avvikelser. Att övervaka och kontrollera är följaktligen ett sätt att säkerställa att

”rätt” saker blir gjorda och att dessa överensstämmer med uppsatta direktiv och policys. (COBIT 4.1, 2007)

IT-processer är grundläggande aktiviteter för IT och hanterar utveckling, underhåll av applikationer, stöd för infrastruktur och mänskliga resurser. Antal processer kan variera från ett företag till ett annat baserat på organisationens inriktning. Processer kan delas in i strategiska processer (långsiktiga), taktiska processer (korttidsberoende) och operativa processer (dagliga) och är alla väsentliga för hanteringen av IT. Alla företagets processer är viktiga men de processer som är mest kritiska för företagets framgång och som för närvarande är i förbättringsbehov bör hanteras först. (Luftman, 2004)

Strategiska processer får en långsiktig effekt på företaget. Beslut som fattas i dessa processer kommer att ha påverkan under en längre tidsperiod och det kan ta lång tid innan fördelar från dessa processer uppnås. Strategiska processer kan skapa konkurrensfördelar, leverera kostnadsbesparingar och införa väsentliga förbättringar av affärsprocesser inom företaget. De taktiska processerna svarar vanligtvis mot konkurrenters hot eller försöker uppnå mellanliggande förbättringar av den befintliga verksamheten fram till nästa omgång av strategisk utveckling införs. Majoriteten av IT-personal är involverade i dessa IT-processer. De operativa processerna omfattar många dagliga funktioner såsom produktion, planering, underhåll, resurskontroll och administrativa tjänster. Dessa verksamheter är ibland även de mest kritiska då ett misslyckande på denna nivå kommer att vara synlig för såväl externa som interna partners. Till skillnad från de andra processerna uppmärksammas oftast inte de operativa processerna förrän de visar på brister eller dålig prestanda. (Luftman, 2004)

Den operativa ledningen använder processer för att organisera och hantera pågående IT-aktiviteter. För att uppnå en effektiv IT-styrning måste således operativa chefer utföra kontroller inom ett definierat kontrollramverk för alla IT-processer. Kontroll definieras som policys, procedurer, tillvägagångssätt och organisatorisk struktur vilka bör ge garantier för att verksamhetsmålen uppnås och oönskade händelser förhindras. (COBIT 4.1, 2007)

Kontrollmål

1. Processmål

Definiera och kommunicera specifika, mätbara, utförbara, realistiska, resultatorienterade och tidsenliga processmål för att på så vis effektivt verkställa varje IT-process. Se till att IT-processer länkas till verksamhetsmålen och stöds av passande mättal. (COBIT 4.1, 2007)

2. Processägande

Utse en ägare för varje IT-process och definiera tydligt processägarnas roller och ansvar. Inkludera till exempel ansvar för processdesign, interaktionen med andra processer, ansvarsskyldighet för slutresultatet, mätningsmetoder för processernas prestanda och identifieringen av förbättringsmöjligheter. (COBIT 4.1, 2007)

3. Processers repeterbarhet

Designa och etablera varje nyckel-IT-process på ett sätt så att den är repeterbar och löpande producerar förväntade resultat. Skapa möjligheter för en logisk men flexibel och skalbar sekvens

av aktiviteter som leder till önskvärda resultat som är så pass agila att de kan hantera undantag. Använd konsekventa processer där det är möjligt och skräddarsy endast vid behov. (COBIT 4.1, 2007)

4. Roller och ansvar för processer

Definiera nyckelaktiviteterna och processens slutprodukt. Tilldela och kommunicera otvetydiga roller och ansvar för ett effektivt utförande av nyckelaktiviteter och dess dokumentation så väl som ansvarsskyldigheten för processens slutprodukt. (COBIT 4.1, 2007)

5. Policys, planer och procedurer

Definiera och kommunicera hur alla policys, planer och procedurer som driver IT-processer är dokumenterade, granskade, underhållna, godkända, lagrade och kommunicerade. Utse ansvar för varje aktivitet och vid lämpligt tillfälle, granska om de utförs korrekt. Se till att policys, planer och procedurer är tillgängliga, korrekta, förstådda och aktuella. (COBIT 4.1, 2007)

6. Förbättring av processprestanda

Identifiera en mängd mättal som ger insikt i processers prestanda och resultat. Etablera riktlinjer som reflekterar processmålen och prestandaindikatorer som möjliggör att processmålen kan uppnås. Definiera hur data kan erhållas. Jämför faktiska mätningar med riktlinjer och agera mot avvikelser. Sammankoppla mättal, riktlinjer och metoder med IT: s övergripande prestandaövervakning. (COBIT 4.1, 2007)

2.5.2 Säkerställande av systemsäkerhet

Det är av stor vikt att beakta systemsäkerheten och hanteringen av känslig information inom en organisation (Kim et. al, 2010; Syrèn, 2005). Systemsäkerhet ses ofta som ett tekniskt bekymmer och saknar därför ledningens uppmärksamhet. Säkerheten är dock även en strategisk fråga som i vissa fall dessutom är av rättsliga bekymmer då det är vanligt att företag måste rätta sig efter lagar och bestämmelser. Ett misslyckande kan i detta avseende leda till stränga rättsliga åtgärder. Informationssäkerhet måste hanteras genom verksamhetsstyrning och bör omfatta rapportering och verkställande ledningens redovisningsskyldighet. Styrelsen är ansvarig och redovisningsskyldig till aktieägare och måste se till att verksamheten producerar affärsvärde som ger en rimlig avkastning, vilket goda insatser avseende informationssäkerheten kan bidra till. Dessutom bör det ligga i ledningens intresse att upptäcka alla väsentliga risker och intyga att datasystemet och dess tillhörande teknik kan underlätta för normal affärsverksamhet. (Posthumusa & Von Solms, 2005)

Behovet av att bibehålla informationsintegritet och skydda IT-tillgångar kräver en process för att hantera säkerhet. En sådan process inkluderar att etablera och bevara roller, ansvar, policys och standards för IT-säkerhet. Att hantera säkerhet inbegriper även att utföra säkerhetsövervakning samt att periodvis testa och implementera korrigeringsåtgärder mot identifierade säkerhetsbrister. En effektiv säkerhetshantering skyddar alla IT-tillgångar för att minimera att verksamheten påverkas av känsliga säkerhetsaspekter. (COBIT 4.1, 2007)

Kontrollmål

1. Hantering av IT-säkerhet

Hantera IT-säkerhet på en så hög organisatorisk nivå som möjligt, så att hanteringen av säkerhetsåtgärder överensstämmer med verksamhetskraven. (COBIT 4.1, 2007)

2. Plan för IT-säkerhet

Översätt affärs-, risk- och tillmötesgåendekrav till en övergripande IT-säkerhetsplan, och beakta däri IT-infrastrukturen och säkerhetskulturen inom organisationen. Se till att planen är implementerad i säkerhetspolicys och procedurer tillsammans med passande investeringar i service, personal, mjukvara och hårdvara. Kommunicera säkerhetspolicys och procedurer till intressenter och användare. (COBIT 4.1, 2007)

3. Identifikationshantering

Se till att alla användare (interna, externa och temporära) och deras interaktion med IT-system unikt kan identifieras. Möjliggör en identifiering av användare via verifieringsmekanismer. Säkerställ att användares tillgång till system är i linje med definierade och dokumenterade affärsbehov och att arbetskrav är anslutna till användaridentiteter, vilka bör förvaras i en central databas (repository). Användarrättigheter ska godkännas av systemägarna och implementeras av de säkerhetsansvariga. (COBIT 4.1, 2007)

4. Hantering av användarkonton

Hantera frågor kring begäran, skapande, modifiering och stängning av användarkonton och relaterade användarrättigheter genom att införa procedurer för behandling av dessa. Inkludera i detta en godkänningsprocedur som inbegriper hur data- eller systemägaren ska bevilja tillgång. Dessa procedurer bör gälla för alla användare, såväl administratörer som interna och externa användare. Rättigheter och skyldigheter avseende tillgången till affärssystem och information bör hanteras genom kontrakt för alla typer av användare. Löpande kontroller och utvärderingar av alla konton och relaterade rättigheter bör utföras. (COBIT 4.1, 2007)

5. Testning, tillsyn och övervakning av IT-säkerhet

Testa och övervaka IT-säkerheten på ett proaktivt sätt. IT-säkerheten bör återutfärdas i rätt tid för att på så sätt försäkra att verksamhetens utformningar avseende informationssäkerhet bibehålls. En logg- och övervakningsfunktion kan möjliggöra att upptäckten av eventuella avvikelser kan göras på ett tidigt stadium. (COBIT 4.1, 2007)

6. Definiering av säkerhetsincidenter

Definiera och kommunicera kännetecken för möjliga säkerhetsincidenter på ett tydligt sätt så att de kan klassificeras och behandlas av incident- och problemhanteringsprocessen. (COBIT 4.1, 2007)

7. Skydd av säkerhetsteknologi

Gör säkerhetsrelaterad teknologi resistant mot manipulering, och blottlägg inte säkerhetsdokumentation om det inte är absolut nödvändigt. (COBIT 4.1, 2007)

8. Upptäckande, korrigerande och skydd mot skadlig mjukvara

Skapa förebyggande, upptäckande och korrigerande mått (framförallt uppdaterade säkerhetspatchar och viruskontroller) genom organisationen för att skydda informationssystem och teknologi mot sabotageprogram (till exempel virus och spam). (COBIT 4.1, 2007)

9. Nätverkssäkerhet

Använd säkerhetstekniker och relaterade hanteringsprocedurer (till exempel brandväggar och intrångsdetektering) för att godkänna tillgång och kontrollera informationsflöden till och från nätverk. (COBIT 4.1, 2007)

10. Utbyte av känslig data

Utväxla känslig transaktionsdata endast över en säker väg eller medium som innehar kontroller för att försäkra sig om innehållets tillförlitlighet och omöjliggör tillbakavisande till den ursprungliga källan. (COBIT 4.1, 2007)

2.5.3 IT: s bidrag till verksamheten

En av de enskilt viktigaste faktorerna för att skapa en fungerande IT-verksamhet är att det finns en tydlig förståelse hos både styrelse och verkställande ledning om att IT inte är en sluten del i sig utan ett medel för att uppnå företagets resultat. IT handlar i dagsläget om att frigöra värde genom IT-baserade organisatoriska förändringar. Det är vidare viktigt att ha ett strategiskt ledarskapsinriktat åtagande till att skapa en övergripande IT-styrningskapacitet. För att denna styrning ska fungera så är det för företaget viktigt att se till att värdet bibehålls eller ökas genom IT-investeringar och IT-förvaltning. Det som i många år har saknats är tillgången till ett strukturerat tillvägagångssätt som kan ge styrelser och verkställande ledningsteam praktisk vägledning för att använda IT för att skapa värde för företaget. En fundamental fråga som bör beaktas avseende värdeskapande är huruvida organisationen ”får ut nyttan av IT”. (Val IT, 2008) Organisationer som har förståelse för att IT kan vara värdeskapande och inte enbart är en stödprocess, kan nå en bättre hantering och styrning av IT (Iliescu, 2010; Willson & Pollard, 2009).

En stor del av utmaningen med att ha en effektiv IT-styrning ligger i svårigheten att utvärdera IT: s värde. Beslutsfattare inom IT tar mer effektiva beslut ju större förståelse de har för företagets värde som skapas från IT. Att spåra IT: s värde kan vidare förstärka organisationens förståelse för IT: s bidrag. (Weill & Ross, 2004)

Kontrollmål

1. Ett övervakande tillvägagångssätt

Detta kontrollmål syftar till att utforma ett ramverk för kontroll och övervakning för att på så vis definiera det omfång och processer som ska följas för att mäta och övervaka IT: s bidrag till verksamheten. (COBIT 4.1, 2007)

2. Definiering och insamling av övervakandedata

Jobba tillsammans med verksamheten för att definiera ett antal balanserade prestandamål och få dessa godkända av verksamheten och andra relevanta intressenter. Definiera utgångspunkter som kan jämföras mot de uppställda målen, och identifiera data som kan användas för att mäta målen. (COBIT 4.1, 2007)

3. Övervakningsmetod

Applicera en övervakningsmetod för prestanda (exempelvis ett balanced scorecard) som kan dokumentera mål; fånga olika mått; erbjuda en koncis, omfattande bild av IT-prestanda. (COBIT 4.1, 2007)

4. Prestandautvärdering

Utvärdera löpande prestanda gentemot uppställda mål, analysera orsaken till eventuella avvikelser, och initiera åtgärder för att motverka dessa avvikelser. (COBIT 4.1, 2007)

5. Motverkande åtgärder

Identifiera och initiera motverkande åtgärder baserade på prestandaövervakning, utvärdering och rapportering. Detta inkluderar att följa upp all övervakning och kontroll. (COBIT 4.1, 2007)

6. Rapportering till ledningen

Utforma rapporter angående IT: s bidrag till verksamheten, med specifikt fokus på bland annat prestandan för verksamhetsportföljen (portfolio). I rapporterna ska bland annat beaktas hur uppsatta mål har behandlats samt på vilket sätt identifierade risker har mildrats. (COBIT 4.1, 2007)

7. Upprätta informerat och engagerat ledarskap

Organisationsledningen bör ha en god förståelse för IT-strategiska frågor, hur beroende av IT företaget är men även insikter i teknik och IT:s kapacitet. Detta så att det finns en gemensam och överenskommen förståelse för IT och de övriga affärsfunktionerna. Företagets ledning bör ha en förståelse för de centrala delarna av styrning som krävs för tillförlitlig, säker och konstnadseffektiv användning av befintliga och nya IT-tillgångar och resurser. Man bör även se till att det finns effektiva rapporteringsvägar som gör att CIO engagerar ledningen till att förespråka betydelsen av IT. Denna rapportering bör stå i proportion till vikten av IT för företaget. Se till att det finns en tydlig och gemensam förståelse för vad som utgör värde för företaget och se till att det rapporteras ut genom hela företaget. (ValIT, 2008)

Målen med denna process är att ledarskapet är engagerat i IT-styrningen så att företaget kan fatta beslut som är baserade på information, vilket resulterar i ett optimalt värde. Det ska finnas en transparens och förståelse för relationen mellan värde, verksamhet & IT-strategier, policys, fördelar, kostnader och risker. (ValIT, 2008)

2.5.4 Intern kontroll

En stor del av IT-revisorns arbete består i att övervaka och utvärdera företags informationssystem. Ett av huvudsyftena med en IT-revision är att testa och granska interna kontroller som omger informationssystemen eller för att tillfredsställa ledningens ansvar avseende styrning (Merhout & Havelka, 2008).

Intern revision är en del av styrningsstrukturen och ser till att fokus finns på de teknologiska resurser som skapar affärsvärde för organisationer och säkerställer ett visst mått av ansvarsskyldighet (Rozek, 2008). Interna kontroller i IT-miljön börjar även få en växande betydelse för att säkerställa att ledningen ges tillräcklig och riktig data. Dessa kontroller inkluderar bland annat procedurer och kontroller för att granska dokument, auktorisering och liknande aspekter som kan kontrollera en organisations aktiviteter. (Pathak, 2005)

För att etablera effektiva interna kontroller av IT så krävs det en tydligt definierad övervakningsprocess. En sådan process inkluderar att övervaka och rapportera om kontrollundantag, resultat från självanalyser samt granskningar utförda av tredje part. En stor fördel med den här typen av intern kontroll är att det underlättar arbetet med att säkerställa effektiva procedurer så att rätt saker blir gjorda. (COBIT 4.1, 2007)

Kontrollmål

1. Kontrollundantag

Identifiera kontrollundantag och analysera och identifiera dessa underliggande orsaker. Rapportera till intressenter på ett lämpligt sätt och vidta nödvändiga åtgärder för att rätta till felaktigheter. (COBIT 4.1, 2007)

2. Självanalys av kontroller

Utvärdera genom en fortlöpande självanalys hur fullständig och effektiv ledningens kontroll över IT-processer, policys och kontrakt är. (COBIT 4.1, 2007)

2.5.5 Extern kravhantering kopplat till IT

Externa krav såsom lagar, regelverk och olika standarder ställer stora krav att företag upprätthåller dessa. Det är även ett faktum att regelverk kan ha en direkt påverkan på företags IT-styrning (Brown & Nasuti, 2005). En effektiv översikt av tillmötesgåendet gentemot externa krav inom en organisation kräver ett skapande av en granskningsprocess som säkerställer tillmötesgåendet gentemot lagar, regulatoriska krav samt kontraktskrav. Detta inkluderar att identifiera krav på tillmötesgående och utvärdera de svar som samlas in. Det är även betydelsefullt att skaffa sig en försäkran om att kraven eftersträvas och integrera IT: s tillmötesgåenderapportering med den övriga verksamheten. (COBIT 4.1, 2007)

Kontrollmål

1. Identifiering av externa krav

Löpande identifiera lokala och internationella lagar, regulatoriska krav och andra externa krav som måste tillmötesgås. Dessa bör sedan inkorporeras med organisationens IT policys, standarder, procedurer och metodologier. (COBIT 4.1, 2007)

2. Svarsoptimering mot externa krav

Granska och anpassa IT-policys, standarder, procedurer och metodologier för att försäkra att juridiska, regulatoriska och kontraktskrav beaktas och kommuniceras inom organisationen. (COBIT 4.1, 2007)

3. Utvärdering av tillmötesgående mot externa krav

Bekräfta tillmötesgående av IT- policys, standarder, procedurer och metodologier med juridiska och regulatoriska krav. (COBIT 4.1, 2007)

4. Tillförsäkran av tillmötesgående

Skaffa och rapportera en försäkran om tillmötesgående och tillgivenhet mot alla interna policys som kan härledas till interna direktiv eller externa juridiska, regulatoriska och kontraktskrav. Detta kan då bekräfta att eventuella korrigeringar för att hantera brister i tillmötesgåendet har tagits av den ansvariga processägaren. (COBIT 4.1, 2007)

2.5.6 Kontroll- och organisationsstruktur

Den mest synbara IT-styrningsmekanismen är den organisatoriska struktur som lokaliserar beslutsfattande ansvar. Det ideala är att varje företag ska engagera både IT och verksamhetsledare i styrningsprocessen, och den beslutsfattande strukturen är ett naturligt sätt att se till att säkerställa detta engagemang. En struktur för beslutsfattande innefattar organisatoriska enheter och roller för ansvaret vid beslutsfattande. (Weill & Ross, 2004)

Att etablera ett effektivt ramverk för IT-styrning inkluderar att definiera organisatoriska strukturer, processer, ledarskap, roller och ansvarsfördelning för att försäkra sig om att bolagets IT-investeringar är sammankopplade med den övergripande affärsstrategin och de uppsatta affärsmålen. (COBIT 4.1, 2007)

Kontrollmål

1. Etablera ett ramverk för kontroll

Definiera, etablera och sammankoppla IT-styrningsramverket med den övergripande verksamhetsstyrningen och kontrollmiljön. Basera ramverket på en passande IT-process- och kontrollmodell och skapa en otvetydig ansvarsskyldighet och arbetssätt för att undvika bristfälliga interna kontroller och översikter. Bekräfta att IT-styrningsramverket tillmötesgår lagar och regulatoriska krav och är sammankopplat med verksamhetens strategi och övergripande mål. (COBIT 4.1, 2007)

2. Etablera organisatoriska strukturer

Organisationsstrukturen kan upprättas genom att fastställa lämpliga styrelser, nämnder och stödstrukturer. Detta inkluderar en IT-strategi kommitté, en IT-planering eller styrgrupp och en IT-arkitektur. Upprätta och upprätthålla en optimal samordning, kommunikation och samverkande struktur mellan IT-funktion och andra intressenter, såsom andra affärsfunktioner, användare (vilket kan inbegripa verksamhetens kunder), företagens funktioner och leverantörer. Processens mål är att nyckelaktörer kopplar sina roller i enlighet med sitt ansvar och att värdeskapande styrningsprocesser implementeras och övervakas. (ValIT, 2008)

2.5.7 Risker och riskhantering ur ett IT-perspektiv

De flesta revisioner, IT-revisioner inkluderat, utförs genom ett riskbaserat tillvägagångssätt vilket innebär att potentiella risker styr vilka områden och frågor som prioriteras (Merhout & Havelka, 2008). En viktig del i riskhanteringsarbetet är den så kallade risk- och konsekvensanalysen som utgör grunden för informationssäkerhetsarbetet. De risker som kan drabba ett företag är både många och skiftande och ett sätt att hantera denna problematik är att utforma en riskkarta. Denna ska innehålla identifierade riskområden och ger en möjlighet att åskadliggöra sambanden och påverkan mellan de lokaliserade riskerna. (Syrèn, 2005)

När man pratar om risk så nämns ofta två olika faser för att hantera den här typen av frågor. Den första fasen fokuserar på en bedömning av potentiella risker medan den andra koncentrerar sig mer på planerings- och kontrollaktiviteter som kan förmildra eller eliminera de upptäckta riskerna. Riskhanteringsprocessen involverar riskanalyser vilket representerar något man vill förändra eller förbättra för att förebygga risker. Förändringar handlar till stor del om olika planer och de beslut som fattas kring dessa planer. En viktig del i riskhanteringsarbetet är att leta efter och identifiera alla potentiella risker, det är då betydelsefullt att skapa sig en uppfattning om vad som verkligen utgör en risk respektive vad som innebär en möjlighet. (Charette, 1996)

Kontrollmål

1. Föreslå risknivåer

Etablera till vilken omfattning en verksamhet är beredd att ta IT-relaterade risker (riskaptit) för att möta sina mål. Uttryck begränsningar för mått som liknar de underliggande verksamhetsmålen samt mot en accepterande respektive icke accepterande verksamhetspåverkan. Beakta de införskaffanden som kan vara nödvändiga för att uppnå nyckelmål i förhållande till ett balanserat risktagande. Föreslå gränser och mått avseende IT-fördelar och värdeskapande. (Risk IT Framework, 2009)

2. Sammankoppla IT-riskpolicyn

Dokumentera riskhanteringsprinciper, riskfokusområden och nyckelmått. Anpassa IT-riskpolicyn efter föränderliga riskförhållanden och uppkommande hot. Sammankoppla operativa policys med risktolerans och utför periodiska granskningar av detta. (Risk IT Framework, 2009)

3. Förespråka en effektiv kommunikation om risker

Etablera och bibehåll en kommunikationsplan för risker som täcker IT-riskpolicys, ansvar, ansvarsskyldighet och risklandskapet (t.ex. hot, kontroller, påverkan och bakomliggande

orsaker). Se till så att planen är tydlig, koncis, användbar och riktad till rätt personer. Skapa utrymme för en fortlöpande kommunikation mellan IT-ledningen och verksamhetsledningen avseende IT-riskstatus, angelägenheter och exponering. (Risk IT Framework, 2009)

4. Etablera och bibehåll en ansvarsskyldighet för IT-riskhantering

Klargör vem de ansvariga för hanteringen av verksamhetens IT-risker är. Ställ upp prestandaförväntningar avseende medvetenhet av IT-risker för högsta ledningen som bär det övergripande ansvaret för IT-risker. Etablera prestandamått och rapporteringsprocesser med lämpliga nivåer för godkännande. Se till att det finns en tydlig struktur och ansvarsfördelning (t.ex. en riskkommitté, en ytterst ansvarig för IT-risker) för att involvera verksamheten med beslut för riskmedvetenheten samt för det dagliga operativa arbetet. Skapa en tydlighet mellan roller knutna till verksamheten (vem som äger och hanterar risker på en daglig basis) och funktioner för riskkontroll. (Risk IT Framework, 2009)

5. Etablera och underhåll en modell för datainsamling

Etablera och underhåller en modell för insamlingen, klassificeringen och analysen av data för IT-risk. Modellen ska stödja mätningen och bedömningen av riskattribut genom IT-riskdomäner och ge användbara data som en drivkraft för en riskmedveten kultur. (Risk IT Framework, 2009)

6. Identifiera riskfaktorer

Organisera insamlad data och belys bidragande faktorer för likartade verksamhetsrelaterade händelser. Bestäm vanligt bidragande faktorer och utför periodiska händelse- och riskfaktoranalyser för att identifiera nya eller uppkommande risker för att skapa en förståelse för interna och externa riskfaktorer. (Risk IT Framework, 2009)

7. Integrera IT-resurser till affärsprocesser

Inspektera verksamhetsprocesser, applikationer och infrastruktur. Skapa en förståelse för verksamhetens nyckelaktiviteter och dess beroende av hanteringen av IT-processer och resurserna för IT-infrastrukturen (t.ex. applikationer, lagringsmedia, nätverk och fysiska faciliteter). (Risk IT Framework, 2009)

8. Avgör IT-resursers affärspåverkan

Bestäm vilka IT-tjänster och vilka resurser för IT-infrastruktur som krävs för att bibehålla den kritiska verksamhetsprocessen. Analysera beroenden och svaga länkar från topplager ner genom de fysiska faciliteterna. Skapa konsensus bland verksamhets- och IT-ledningen avseende företagets mest värdefulla information och relaterade teknologier. (Risk IT Framework, 2009)

9. Bibehåll IT-riskregistret och IT-riskkartan

Fånga riskprofilen genom verktyg såsom en IT-riskkarta. Bygg ut riskprofilen via resultaten från verksamhetens IT-riskbedömningar och pågående riskanalyser. När det gäller IT-riskkartan så bör poäng för varje dimension (t.ex. frekvens, magnitud och affärspåverkan) utformas. Som minimikrav, uppdatera och granska årligen riskkartan för att svara mot betydelsefulla interna eller

externa förändringar. En riskkarta kan användas för att identifiera riskaptiten, det vill säga viljan att ta risker. (Risk IT Framework, 2009)

10. Utveckla IT-riskindikatorer

Utforma mättal eller indikatorer som kan peka på IT-relaterade händelser och incidenter som kan påverka verksamheten på ett betydelsefullt sätt. Indikatorerna måste reflektera den faktiska risken; annars kan mättalet vara uppfyllt trots att den faktiska risken är allvarlig. Fokusera på de mättal som varnar ledningen när de faktiska riskerna överskrider accepterade nivåer. Det är viktigt att ledningen har en förståelse för nyckelriskindikatorerna och deras användbarhet och potential för att de på så sätt ska veta vad som ska göras när dessa indikatorer utlöses. (Risk IT Framework, 2009)

11. Inspektera kontroller

Inspektera de kontroller som finns tillgängliga i riskfokusområdena för att på så sätt hantera risker och säkerställa att de risker som tas är i linje med den uttalade riskaptiten och toleransnivån. Klassificera kontroller och integrera dem till specifika uttalanden avseende IT-risker. Utveckla tester för kontrollernas utformning och tester för dess operativa effektivitet. Identifiera procedurer och teknologi som används för att övervaka användandet av kontroller. (Risk IT Framework, 2009)

12. Implementera kontroller

Vidta lämpliga åtgärder för att säkerställa ett effektiv verkställande av nya kontroller och anpassningar till existerande kontroller. Kommunicera med nyckelintressenter på ett tidigt stadium. Innan man förlitar sig på kontrollerna ska testing och granskning av dataresultat genomföras. Integrera nya och uppdaterade operativa kontroller med övervakningsmekanismer som mäter kontrollresultat över tid. Identifiera och träna anställda för nya procedurer efterhand som de verkställs. (Risk IT Framework, 2009)

2.6 Undersökningsmodell

Nedanstående tabell syftar till att ge läsaren en schematisk bild över uppsatsens undersökningsmodell.

Tabell 2.1: Undersökningsmodell

Temaområde	**Kontrollmål**
Definiera och hantera processer	1. Processmål 2. Processägande 3. Processers repeterbarhet 4. Roller och ansvar för processer 5. Policys, planer och procedurer 6. Förbättring av processprestanda
Säkerställande av systemsäkerhet	1. Hantering av IT-säkerhet 2. Plan för IT-säkerhet 3. Identifikationshantering 4. Hantering av användarkonton 5. Testning, tillsyn och övervakning av IT-säkerhet 6. Definiering av säkerhetsincidenter 7. Skydd av säkerhetsteknologi 8. Upptäckande, korrigerande och skydd mot skadlig mjukvara 9. Nätverkssäkerhet 10. Utbyte av känslig data
IT: s bidrag till verksamheten	1. Ett övervakande tillvägagångssätt 2. Definiering och insamling av övervakandedata 3. Övervakningsmetod 4. Prestandautvärdering 5. Motverkande åtgärder 6. Rapportering till ledningen 7. Upprätta informerat och engagerat ledarskap
Intern kontroll	1. Kontrollundantag 2. Självanalys av kontroller
Extern kravhantering kopplat till IT	1. Identifiering av externa krav 2. Svarsoptimering mot externa krav 3. Utvärdering av tillmötesgående mot externa krav 4. Tillförsäkran av tillmötesgående
Kontroll- och organisationsstruktur	1. Etablera ett ramverk för kontroll 2. Etablera organisatoriska strukturer
Risker och riskhantering ur ett IT-perspektiv	1. Föreslå risknivåer 2. Sammankoppla IT-riskpolicyn 3. Förespråka en effektiv kommunikation om risker 4. Etablera och bibehåll en ansvarsskyldighet för IT-riskhantering 5. Etablera och underhåll en modell för datainsamling 6. Identifiera riskfaktorer 7. Integrera IT-resurser till affärsprocesser 8. Avgör IT-resursers affärspåverkan 9. Bibehåll IT-riskregistret och IT-riskkartan 10. Utveckla IT-riskindikatorer 11. Inspektera kontroller 12. Implementera kontroller

3. Metod

3.1 Forskningsstrategi

Metoden och redogörelsen för denna i en empirisk undersökning beskriver det totala tillvägagångssättet, vilket syftar till att ge möjlighet för replikation och evaluering (Backman, 1998). Denna studie behandlar ett nytt område inom ämnet informatik och syftet med metodavsnittet är således att klargöra omfattningen och inriktningen av studien. Appliceringen av en metod är även tänkt att stödja oss i uppsatsarbetet och hjälpa oss att besvara syftet med undersökningen. Jacobsen (2002) beskriver att det i empiriska undersökningar alltid finns en risk att de resultat man kommer fram till faktiskt har skapats av undersökningen. Det kan då vara själva undersökingens upplägg som skapar utfallet. För att kunna undvika denna effekt och bedöma om resultatet är en korrekt bild av verkligheten så är metoden en vital del.

Denna undersökning kommer följa anvisningarna för en kvalitativ ansats, vilket vi anser ger utrymme för att granska det valda fenomenet ur ett brett perspektiv. Metodvalet har även varit viktigt i det avseende att vi har haft möjlighet att följa tydliga riktlinjer för hur en vetenskaplig studie ska genomföras. Detta anser vi vara viktiga aspekter då det kan påverka validiteten och reliabiliteten av en studie. Metoden har således kontinuerligt fungerat som ett assistansverktyg under rapportens olika steg, framförallt vid granskningen och hanteringen av det insamlade empiriska materialet. Vi har följt en liknande struktur för den kvalitativa forskningsprocessen som beskrivs i såväl Bryman & Bell (2005) som Backman (1998). För denna uppsats har vi gått igenom följande steg:

- Förundersökning
- Problem-/frågeformulering
- Val av analysenhet
- Litteraturgranskning
- Observation/Insamling av data
- Analys
- Rapportering

För att genomföra ett av de viktigaste stegen i en undersökning, insamlingen av data, så kan enligt Bryman & Bell (2005) ett flertal olika instrument och tillvägagångssätt användas. Valet av dessa beror på kontexten av undersökningen och syftet med de olika verktygen varierar. *Enkäter, intervjuer, observationer* eller en genomgång av *skriftliga källor* tillhör de vanligaste tillvägagångssätten. Intervjuer är passande att använda då man eftersträvar flexibilitet och är intresserad av informanternas ståndpunkter (Bryman & Bell, 2005). Av stor vikt för denna undersökning är informanternas åsikter och uppfattningar, och vi anser därför att intervjuer är mest lämpliga för att tillgodose detta behov. Vidare har valet att anta en semi-strukturerad utformning genom en indelning i temaområden gjorts. Detta ger en tydlig struktur till intervjuerna samtidigt som intervjupersonen har stor frihet att utforma svaren på sitt eget sätt (Bryman & Bell, 2005).

3.2 Intervjuer

Vid intervjuerna eftersträvades ett utrymme för öppenhet och flexibilitet och vi ville inte låsa oss vid fasta samtalspunkter. Vi upplevde därför att den kvalitativa ansatsen skulle ge flest fördelar i detta avseende eftersom den sätter få begränsningar på de svar en uppgiftslämnare kan ge och lägger mer vikt vid det unika hos varje uppgiftslämnare (Jacobsen, 2002). Däremot så var det viktigt att se till att informanterna höll sig inom ramen för de områden som uppsatsen berör. Vi valde därför att dela in intervjufrågorna i de teman som legat till grund för undersökningsmodellen, vilket diskuteras mer utförligt i avsnitt 3.2.3.

Jacobsen (2002) diskuterar tre vanliga metoder för den kvalitativa datainsamlingen: *den individuella öppna intervjun, gruppintervjun* samt *dokumentundersökning.* Den förstnämnda är som mest lämplig när relativt få enheter undersöks, när man är intresserad av vad den enskilda individen säger samt dennes tolkningar och meningar om ett visst fenomen (Jacobsen, 2002). Då vår undersökning endast omfattar fem informanter och vi är särskilt intresserade av vad just dessa har för åsikter så ansåg vi att *den individuella öppna intervjun* var mest passande för vårt ändamål.

3.2.1 Urvalskriterier för företag

Beträffande urvalet av företag för denna undersökning så stod det tidigt klart att fokus inte skulle ligga på företag som enbart arbetade med IT-revision. Detta berodde på att det geografiskt sett inte finns några sådana företag i vår närhet men framförallt på grund av att det finns ett litet antal renodlade svenska IT-revisionsföretag. Däremot så sysslar numera alla stora finansiella revionsbyråer med IT-revision. Valet föll således på denna typ av företag.

Vi hade på ett tidigt stadium, under en arbetsmarknadsmässa samt via personliga kontakter, etablerat kontakt med ett antal företag som mötte dessa urvalskriterier. Vi ansåg det därför lämpligt att först och främst kontakta dessa företag med en intervjuförfrågan. Detta kan liknas vid vad Bryman & Bell (2005) beskriver som bekvämlighetsurval, nämligen att urvalet består av sådana personer som för tillfället råkar finnas tillgängliga för forskaren. För att kunna utföra arbetet inom uppsatsens tidsram var det viktigt att företagen och följaktligen informanterna fanns tillgängliga i vår närhet.

3.2.2 Undersökningspersoner

Vid valet av undersökningspersoner var det viktigt att dessa personer hade en god kunskap och uppfattning om de temaområden som utgör grunden för intervjun. För att säkerställa att så var fallet så presenterade vi i samband med vår intervjuförfrågan även nämnda teman. I de fall eventuella undersökningspersoner var positiva till ett deltagande i studien så fick de även ta del av en fullständig intervjuguide (se Bilaga B1) innehållande de frågor vi avsåg ställa under intervjutillfället. Detta resulterade i fyra intervjuer.

Den IT-revisor vi intervjuade i vår förundersökning inför uppsatsen deltog även i själva uppsatsintervjun. En annan av undersökningspersonerna hade vi även träffat och diskuterat med under det ISACA-seminarie som tidigare beskrivits. Vi upplevde dock inte detta som något problem eftersom dessa individer hade olika roller vid de olika tillfällena, nämligen rådgivare i

första skedet respektive informant i andra skedet. Dessutom framhåller Bryman & Bell (2005) att en person, när det gäller kvalitativa intervjuer, kan intervjuas flera gånger. Övriga två personer har endast haft rollen som informant vid undersökningens intervjutillfällen som avser empiriinsamlingen i avsnitt 4.

3.2.3 Design av intervjuguide

Intervjuguiden (se Bilaga B1) som utgjort grunden för våra intervjuer består av 25 frågor vilka delats in i de sju olika temaområden som utgör denna uppsats undersökningsmodell och intervjufrågorna utformades utifrån respektive temaområde. Syftet med denna indelning var att på ett tydligt sätt kunna behandla den empiriska datan samt att kunna ställa undersökningsmodellen mot denna i analysdelen av kapitel 4. Vidare var avsikten att ge undersökningspersonen en tydligare uppfattning om vilka områden intervjun fokuserar på. Teman indelades enligt följande:

- Definiera och hantera processer
- Säkerställande av systemsäkerhet
- IT: s bidrag till verksamheten
- Intern kontroll
- Extern kravhantering ur ett IT-perspektiv
- Kontroll- och organisationsstruktur
- Risker och riskhantering ur ett IT-perspektiv

Det är inte lämpligt att låta intervjun vara längre än en och en halv till två timmar eftersom både intervjuare och intervjuobjekt riskerar att bli uttröttade (Jacobsen, 2002). Detta beaktades vid utformningen av intervjuguiden och antalet frågor anpassades för att försöka hålla intervjun inom detta tidsintervall. Fler frågor än de vi valde skulle kunna minska intresset och fokuset hos undersökningspersonerna. Samtliga intervjuer hölls inom detta tidsintervall.

De inledande frågorna hade en övergripande karaktär och behandlade informantens bakgrund och nuvarande roll som IT-revisor. Detta syftade till att fånga informantens intresse och få denne att känna sig avslappnad samtidigt som det kunde ge en bild av dennes ansvarsområde.

De avslutande frågorna syftade till att återknyta vad informanten sagt tidigare under intervjun genom att låta denne rangordna de faktorer och moment som diskuterats. Vi valde att ge de avslutande frågorna en mer öppen karaktär då formuleringen av dessa kunde tänkas variera beroende på vilken information som framkommit tidigare under intervjun.

Den språkliga strukturen beaktades även vid utformningen av frågorna, och alltför komplexa begrepp och ordval försökte undvikas. Frågorna diskuterades och reviderades även i samråd med handledare för att på så vis få en utomstående bedömning av frågornas relevans.

3.2.4 Genomförande av intervjuer

En viktig fråga när det gäller genomförandet av intervjuer är var intervjun ska utföras. I detta avseende är det viktigt att intervjun genomförs på en plats där undersökningspersonen känner sig

bekväm samtidigt som störningsmoment och liknande undviks. (Jacobsen, 2002) Vi ansåg det därför viktigt att träffa undersökningspersonerna i deras vardagliga miljö, nämligen deras arbetsplats. Alla intervjuer genomfördes således under dessa förhållanden i avskilda konferensrum utan risk för störningar.

Med undersökningspersonernas samtycke så spelades alla intervjuer in med hjälp av en diktafon. För att dessa skulle få en överblick över intervjun fick alla undersökningspersoner även ett exemplar av intervjuguiden att ha framför sig vid intervjun. Vi förklarade även syftet med intervjun och på vilket sätt vi skulle använda informationen.

Efter genomförd intervju så efterfrågades även om undersökningspersonerna ville vara anonyma. Detta var inget direkt krav från deras sida, men vi beslutade ändå att låta såväl företag som informanter förbli anonyma. Detta med hänseende till etiska aspekter, vilket diskuteras närmare i avsnitt 3.4.

3.2.5 Analys av intervjudata

En analys av kvalitativ data handlar till största del om *beskrivning, systematisering* och *kombination* (Jacobsen, 2002). De genomförda intervjuerna har som tidigare nämnts spelats in och sedermera transkriberats. Syftet med detta har varit att skapa en grundlig förståelse för den insamlade datan samt att säkerställa att denna är registrerad på ett noggrannt sätt. Med avseende att underlätta för läsaren och ge denne en övergripande bild av empirin så har datan *systematiserats* och endast den information som bedömts som relevant för uppsatsen har presenterats i kapitel 4. För att ytterliggare förtydliga för läsaren så har kritiska moment sammanställts i tabellform. Läsaren ges dock möjlighet att i uppsatsens bilagor, avsnitt 6.2, ta del av intervjumaterialet i sin fullständiga form. Som ett sista steg i analysprocessen har tolkningar av datan gjorts i form av en analys av respektive temaområde.

Intervjuguiden har samma struktur av temaområden som uppsatsens undersökningsmodell. Detta innebär att vi i de flesta fall funnit informanternas svar på respektive temaområde från de ställen av intervjuerna som behandlat just detta temaområde. Varje temaområde har diskuterats separat vid intervjuerna och informanternas svar har i de flesta fall återfunnits inom respektive temaområde. Eftersom uppsatsens analysdel avser hålla samma struktur som såväl undersökningsmodellen som intervjuguiden har det fallit sig naturligt att behandla varje tema för sig. Den största delen av information inom varje temaområde har behandlats på detta vis. I de fall frågor har återkommit längre fram i intervjun men adresserat tidigare diskuterade temaområden har vi gjort ett medvetet val att placera denna information inom det temaområde som svaret faktiskt behandlar. Information som framkommit innan temaområdet behandlats har hanterats på motsvarande sätt. Information som således inte följt intervjuguiden har lokaliserats med hjälp av nyckelord. Exempel på nyckelord som använts är ”processer”, ”ansvarsfördelning”, ”behörighet” och ”risk”.

3.3 Undersökningskvalitet

Det finns framförallt två krav på det empiriska material som samlas in vid en undersökning. Det första är att empirin måste vara valid, det vill säga giltig och relevant. Det andra är att empirin måste vara reliabel, följaktligen tillförlitlig och trovärdig (Jacobsen, 2002).

I syfte att nå en hög validitet har vi eftersträvat att säkerställa att intervjufrågorna är kopplade till uppsatsens undersökningsmodell. Detta har gjorts genom att noga jämföra uppförandet av intervjuguiden med innehållet i uppsatsens undersökningsmodell. Vidare har det varit av vikt att koppla undersökningsmodellen till den litteratur som legat till grund för uppsatsens. Vi har därför löpande utvärderat vårt arbete och relevansen av detta i förhållande till problemområdet och frågeställningen. Detta har gjorts genom att vi kontinuerligt ställde oss själva följande frågor:

- Går det att relatera detta direkt till uppsatsens problemområde och syfte?
- Är denna litteratur relevant i förhållande till uppsatsens ämne?

I syfte att öka reliabiliteten av den insamlade datan har vi strävat efter att utforma intervjufrågor på ett sådant sätt att repondenten lättare ska förstå dess innebörd och därmed kunna ge relevanta svar. Alla intervjuer har spelats in och transkriberats i syfte att skapa en riktig presentation av datan. Transkriberingerna har även skickats ut till respektive informant för godkännande och felaktigheter har korrigerats på begäran. Detta resulterade i att en av informanterna ville ändra ett ordval, vilket dock inte påverkade informantens svar. Det transkriberade materialet återfinns som bilagor (avsnitt 6.2) till uppsatsen i syfte att ge läsaren en möjlighet att bilda sig en egen uppfattning.

Vi har i vår undersökning valt att avgränsa oss från företag som enbart arbetar med IT-revision. Vi är medvetna om att undersökningens resultat kan skilja sig från det ett resultat som baserats på verksamheter som enbart arbetar IT-revision. Vårt val att fokusera på IT-revisorer med anställning på finansiella revisionsbyråer grundar sig i att dessa är betydligt större till antalet. Möjligheten att jämföra och generalisera empiriska resultat anser vi därmed vara lättare. Vi är dock medvetna om att ett större antal intervjuer än de fyra vi genomförde hade kunnat ge större möjligheter för generella indikationer.

3.4 Etiska aspekter

En undersökning innebär som oftast att man bryter in i enskilda individers privatsfär, vilket kan innebära vissa etiska dilemman (Jacobsen, 2002). För att lättare hantera eventuella etiska dilemman så har vi valt att följa de tre grundkrav som Jacobsen (2002) rekommenderar att en undersökning bör försöka uppfylla. Vi har följaktligen följt anvisningar för att hantera *informerat samtycke, krav på privatliv* samt *krav på riktig presentation av data.*

Den grundläggande förutsättningen när det gäller *informerat samtycke* är att undersökningspersonerna ska delta frivilligt i undersökningen samt att de ska vara medvetna om riskerna och fördelarna som deras deltagande kan resultera i (Jacobsen, 2002). Med detta i åtanke har vi tydligt informerat informanterna om uppsatsens syfte, både vid intervjuförfrågan samt just innan intervjuns start.

En viktig aspekt avseende *rätten till privatliv* är att informanten ska ha rätt till en frizon i livet som inte nödvändigtvis undersöks samt att man bör beakta hur känslig informantens information är (Jacobsen, 2002). I detta avseende har vi låtit informanterna och deras respektive företag förbli

anonyma för att på så vis undvika att exempelvis konkurrerande företag kan utnyttja informationen på ett olämpligt vis. Ett sätt att anonymisera informanter är att eliminera data som kan bidra till identifikation av individer (Jacobsen, 2002). I denna uppsats har informanterna givits namnen A, B, C och D.

Det tredje grundkravet som bör beaktas i förhållande till etiska aspekter, *riktig presentation av data,* handlar om en eftersträvan att återge resultat i rätt sammanhang och på ett fullständigt sätt vis (Jacobsen, 2002). Exempelvis citat kan få en helt annan betydelse om de bryts ut ur ett sammanhang. En *riktig presentation av data* innebär även att data och resultat ej får förfalskas. För att undvika dessa aspekter så har vi låtit alla informanter ta del av det transkriberade materialet och låtit dessa individer verifiera att transkriberingen varit korrekt. I de fall informanterna upplevt felaktigheter så har detta korrigerats.

Ovanstående grundkrav har löpande beaktats under hanteringen av det empiriska materialet och den empiriska undersökningen har utförts i linje med dessa rekommendationer.

4. Presentation av empiriska data och analys

Vi presenterar i detta kapitel det empiriska materialet från studien tillsammans med analysen. Detta syftar till att göra det lättare för läsaren att följa med i resultatredovisningen och analysen. Det är även ett sätt att undvika upprepningar, vilket kan ske om empiri och analys redovisas i separata kapitel. Empirin redovisas först för varje temaområde vilket följs av analysen av densamma, presenterad i en egen underrubrik. Avsnitt 4.8 är en sammanställning av intervjuguidens två avslutande frågor vilket behandlar de mest kritiska faktorerna avseende IT-styrning och utgör således inget temaområde i sig. Kapitlet avslutas med avsnitt 4.9 vilket innehåller en diskussion kring övriga iakttagelser.

Informanter

Fem informanter på fyra företag har legat till grund för den empiriska undersökningen. I tre av fallen har intervjuerna genomförts med en informant men vid ett tillfälle närvarade två informanter vid intervjutillfället. Tre av de fyra företagen tillhör den så kallade Big Four, vilket syftar till de fyra största internationella revisionsorganisationerna; Deloitte Touche Tohmatsu, KPMG, Ernst & Young och PricewaterhouseCoopers (Singh, 2010). Det fjärde företaget är en svensk medelstor revisionsbyrå.

Alla informanter arbetar i nuläget som IT-revisorer men deras bakgrund och erfarenhet skiljer sig något åt. Två av informanterna har en bakgrund som finansiella revisorer medan de andra har en bakgrund inom IT. Informanternas erfarenhet inom IT-revision ligger mellan två till elva år. Alla informanter har arbetsområden inom såväl renodlad IT-revision som konsulttjänster inom IT.

Vi har valt att kalla informanterna för A, B, C, och D för att på så vis undvika alltför många upprepningar av ordet informant. På ett av företagen var det, som tidigare nämnts, två informanter och dessa benämns hädanefter enbart som C. Då informanterna arbetar på samma företag, delar samma metodik och arbetssätt samt att de presenterade en gemensam syn avseende IT-revisionen ser vi ingen anledning att skilja dessa åt. De enda fall en skillnad görs mellan dessa informanter är vid citering av informanterna. I dessa fall benämns dessa som C1 respektive C2 vilket motsvarar R1 och R2 i det transkriberade materialet.

4.1 Definiera och hantera processer

Respondenterna på tre av fyra företag svarar att de gör någon form av översiktlig genomgång av det granskade företaget för att skapa sig en initial bild över vilka processer som bör fokuseras på och för att få en uppfattning om företagets struktur avseende resterande delar av verksamheten som är kopplade till IT-revisionen. A och C anser det vara viktigt att lokalisera hur kontroller är uppsatta, vad processerna ska kontrollera och varför de finns. Här ser samma informanter att det finns möjlighet att jämföra olika företag och ge konstruktiv feedback om bra förfaringssätt då verksamheters processer kan vara väldigt likartade. Samtliga informanter berättar att de tittar på behörighetskontroller, förändringshantering och drift. C granskar dessutom IT-kontrollmiljön ur ett generellt perspektiv då man tittar på klientens mognadsgrad gällande styrning, policys och riktlinjer. Viktiga aspekter i detta avseende är hur god klientens förståelse för IT-kontroller är, om kontrollerna finns på plats, kommunikationsstrukturen samt systemägandet. Systemägandet anses av C vara viktigt för att någon ute i verksamheten ska ansvara för att systemet ska uppfylla

de krav som ställs. A anser att tydlighet gällande rollfördelning, genom bemanning av olika roller, i allmänhet och i synnerhet gällande systemägande är det viktigaste för att IT ska stödja verksamheten. B nämner att systemägande är en viktig roll för kravinsamlingen vilket bidrar till att IT kan förankras till verksamheten. I liknande avseende var även processägande viktigt och informant C1 uttryckte sig enligt följande i denna fråga:

> *"[...] det är viktigt att någon har ansvar för att processen fungerar, att man ser till att de kontrollerna som ska göras faktiskt görs, att den dokumentationen som måste finnas finns och det är också en styrningsfråga egentligen, att se till att någon känner ett ägandeskap att leva efter, att uppleva styrning, att implementera styrning egentligen".*

Samtliga företag svarar att de tittar på den befintliga dokumentationen kring företagets processer. Anledningen till att man tittar på dokumentation skiljer sig något åt mellan företagen. A och C anser att dokumentation är viktigt för att kunna spåra vilka förändringar som verksamheten har gjort i sina system och att hanteringen av förändringar sköts på ett korrekt sätt. B och D anser att dokumentationen är viktig för att kunna förlita sig på sina processer och undvika en ad-hoc hantering av dessa samt göra det lättare att upptäcka avvikelser. Samtliga företag framhöll att säkerställandet av att roller och ansvar hanteras var viktigt. A och B anser att detta är en viktig aspekt för att säkerställa att det finns en tydlig koppling mellan IT-processerna och verksamheten vilket leder till att systemet har en förankring i organisationen. Vidare anser A och C att roller och ansvar bidrar till en mer strukturerad och effektiv hantering av IT-processerna. D ansåg att det var av stor betydelse att de personer som är inblandade i processerna, det vill säga, process- och kontrollägare, verkligen förstår varför de tilldelats denna roll.

Ur ett praktiskt perspektiv så jobbade samtliga företag med att först titta på befintlig dokumentation och utvärdera riktigheten i denna genom intervjuer och stickprov. Visade det sig att det inte fanns någon dokumentation eller att den var inaktuell eller på annat sätt bristfällig så gjorde man djupare intervjuer och uppföjlning kring företagets processer. C1 förklarar detta enligt följande: *"Så även om det inte finns något dokumenterat så kanske dom har en process i huvudet för hur det ska gå till [...] Man får genom intervju försöka förstå om dom har någon struktur kring styrning."* Om man kommer fram till att företagets kontroller kring processerna inte går att lita på så var sista utvägen för att säkerställa riktigheten gällande den information som systemen levererar att substansgranska data. Detta steg innebär att man tar ut en väldigt stor mängd data ur systemet för att granska denna.

Tabell 4.1: Processhantering

	KRITISKA MOMENT AVSEENDE ARBETET MED PROCESSHANTERING
A	Säkerställa att systemen stödjer verksamhetens IT-processer för att minska glapp mellan IT och verksamheten, en klar och tydlig rollfördelning för att säkerställa detta.
B	Att kontrollera dokumentationen för att säkerställa att den speglar det verksamheten gör.
C	Granskning av IT-kontrollmiljön gällande styrning, policys och riktlinjer.
D	Medvetenheten om varför man har ett visst ansvar. "Om inte människorna är medvetna och känner att de tar sitt ansvar så kommer det aldrig funka"

4.1.1 Analys av definiera och hantera processer

Kontrollmål 1 (se avsnitt 2.5.1) för detta temaområde som till stor del innebär att definiera mätbara processer och syftar till att skapa en koppling till verksamheten kan vi tydligt koppla till IT-revisorernas arbetssätt avseende processhanteringen. A och C uttrycker specifikt att de jämför nyckel-IT-processer företag emellan för att kunna ge konstruktiv kritik om förfaringssätt som uppleves vara framgångsrika och bidrar på så sätt till vägledning. IT-revisorerna kan här hjälpa företag att definiera kritiska processer och ge förslag på hur dessa kan mätas och hanteras. Att processerna stödjer verksamheten är något som A och B lyfter fram som mest kritiskt avseende processhanteringen vilket ger indikationer på att kontrollmål 1 är något man arbetar med.

Med undantag för C så granskar ingen av informanterna explicit processägandet, men alla ansåg att systemägandet var en vital del för att säkerställa att system stödjer verksamheten. C framhöll att det i mindre organisationer sällan talas om den detaljerade nivån som processägande innebär utan att man pratar om systemägande. Systemägandet är i förhållande till processägandet på en mer övergripande nivå men båda nivåerna hanterar problematiken med ansvarssyldighet. Kontrollmål 2 (se avsnitt 2.5.1) som hanterar processägandet har således stora likheter med IT-revisorernas förfaringssätt att kontrollera systemägandet.

Samtliga informanter uttrycker att roller och ansvar är en del i IT-revisionsarbetet framförallt avseende behörighets- och förändringshanteringen. Detta arbete säkerställer att företaget har en struktur som förhindrar att intern information hanteras felaktigt och att de finns en spårbarhet avseende förändringar. Genom IT-revisorernas granskning av dessa delar kan en medvetenhet skapas i organisationen kring vilka roller som existerar och hur ansvarsskyldigheter är knutna till dessa. En tydlig definition av roller och ansvar för processer kan leda till ett mer effektivt utförande av nyckelaktiviteter vilket kontrollmål 4 (se avsnitt 2.5.1) syftar till att uppnå.

En vital del avseende IT-revisorns kontroll av behörighet är att säkerställa att procedurer kring behörigheter är granskade och godkända. Som ett steg i detta arbete framhävde alla informanter att dokumentation kring policys och procedurer granskas genom att kontrollera dess struktur, aktualitet och korrekthet. Genom att skapa en medvetenhet kring detta kan IT-revisorn bidra till att kommunicera ut policys och procedurer som driver IT-processer. Detta indikerar på att man jobbar mot de riktlinjer som är beskrivna i kontrollmål 5 (se avsnitt 2.5.1).

Det framgick även att dokumenteringen av processer var betydelsefull framförallt för att förhindra en ad-hoc hantering av processer samt att lättare kunna lokalisera avvikelser. Kontrollmål 3 (se avsnitt 2.5.1) belyser vikten av att skapa repeterbara processer. Dokumentationen kan således vara ett sätt att ge tydliga direktiv och därmed underlätta för ett säkerställande av att processer hanteras på ett repeterbart sätt. Undersökningen ger inga indikationer på att det finns någon koppling mellan IT-revisorernas arbetssätt och kontrollmål 6 (se avsnitt 2.5.1).

Det har i detta temaområde framgått att IT-revisorns arbete inbegriper att jämföra processhanteringen mellan olika företag, att säkerställa tydliga roller och ansvar (och medvetenheten kring detta ansvar) samt att granska dokumentationen kring organisationens IT-processer. Detta arbete avser att se till så att organisationens IT-processer stödjer verksamheten

samt att effektivisera utförandet av organisationens nyckelaktiviteter. Två aspekter som tydligt bidrar till organisationens IT-styrning.

4.2 Säkerställande av systemsäkerhet

Samtliga informanter framhåller kontrollen och säkerställandet av segregation of duties, det vill säga ansvarsfördelning, som det primära syftet inom området. Det rådde en gemensam uppfattning om varför detta var viktigt att kontrollera vilket kan sammanfattas med följande citat från A:

> *”Alltså, segregation of duties, där gör man aldrig sin läxa [...] när du väl kommer in i systemet så kan det vara så att till exempel på en ekonomiavdelning så kan du göra allt. Du kan fiffla i leverantörsregistret och lägga upp en fejkad leverantör, ditt eget bankkonto, så kan du lägga in en fejkad faktura och se till att den blir godkänd, körd igenom och betald till dig själv, då brister det.”*

A och C anser att syftet med granskningen av systemsäkerhet även är att informationen ska vara tillgänglig, korrekt och skyddad. Vidare anser C och D att man måste kunna förlita sig på viktiga kontroller och rapporter och att granskningen av systemsäkerheten är ett steg i att säkerställa detta.

Ett problem som alla informanter påtalade var problematiken med behörigheter. D beskriver denna problematik enligt följande:

> *”Det är jättevanligt att om man jobbar i en stor organisation och man byter avdelning flera gånger så samlar man bara på sig mer och mer och mer behörigheter, för att dom rensas aldrig och till sist sitter man med jättemånga behörigheter och ingen vet hur det ser ut i systemet.”*

Alla informanters praktiska förfarande för detta område innefattar att granska data genom så kallade stickprov som innebär att IT-revisorerna slumpmässigt kontrollerar data för att säkerställa riktigheten av denna. A och C beskriver att de som ett steg i detta tittar på eventuell dokumentation och genomför stickprov i första hand utifrån detta. I de fall då dokumentation saknas extraheras och substansgranskas data direkt från systemen för att kunna genomföra stickprovskontroller. Substansgranskning är ett tillvägagångssätt som även används av B och D.

Tabell 4.2: Systemsäkerhet

	KRITISKA MOMENT AVSEENDE ARBETET MED SYSTEMSÄKERHET
A	Granska åtkomstkontroller och loggning av händelser i systemet (spårbarhet).
B	Kontrollera behörigheter, konfliktande roller genom registeranalys.
C	Säkerställa att behörigheter är kontrollerade och godkända, backup fungerar och kontroll på filer som skickas mellan system.
D	Kontrollera behörigheter.

4.2.1 Analys av säkerställande av systemsäkerhet

Det största problemet och det som ägnades mest tid av IT-revisorerna inom detta område var granskningen av segregation of duties och behörighetskontroller. Denna av typ av problematik hanteras i kontrollmål 3 och 4 (se avsnitt 2.5.2) för detta temaområde. Det är enligt kontrollmål 3 (se avsnitt 2.5.2) viktigt att användares behörigheter är i linje med definierade och dokumenterade affärsbehov och att arbetskrav är anslutna till användaridentiteter. Granskningen av behörigheter inkluderar tilldelning och avskaffning av behörigheter. Denna aspekt hanteras i kontrollmål 4 (se avsnitt 2.5.2) där det även beskrivs att löpande kontroller av alla konton och relaterade rättigheter bör utföras. Det är således möjligt att betrakta IT-revisorns arbete kring detta som en löpande kontrollmekanism.

En av informanterna framhöll att han granskar loggar i systemet som ett steg i att kontrollera olika händelser och vem som utfört dessa. Uppförandet av logg- och övervakningsfunktioner har inte nämnts som något som IT-revisorerna jobbar med. Däremot arbetar samtliga informanter med att använda dessa för att upptäcka och spåra eventuella avvikelser för att på så sätt övervaka IT-säkerheten i allmänhet och behörigheter i synnerhet, vilket beskrivs i kontrollmål 5 (se avsnitt 2.5.2).

Ett säkerställande av att organisationer hanterar IT-säkerhet på en hög nivå samt en hantering av IT-teknologin var aspekter som vi på förhand trodde skulle vara av vikt för IT-revisorn att beakta. Ingen av informanterna har dock nämnt dessa delar. När det gäller de renodlat tekniska delarna av säkerhetshantering så tittar IT-revisorerna primärt på backuper i syfte att säkerställa att viktig information ej går förlorad. Övriga tekniska aspekter ges ingen hög prioritet. Detta innebär att vi inte kan göra någon koppling mellan IT-revisorns säkerställande av systemsäkerheten och kontrollmål 1-2 samt 6-10 (se avsnitt 2.5.2).

Det har tydligt visat sig att IT-revisorerna främst jobbar med behörighetskontroller och ansvarsskyldighet (segregation of duties) vilka framförallt har en koppling till roller och ansvar i organisationen. Temaområdet täcks således till viss del in av IT-revisorernas arbetssätt och kan rimligen, i detta avseende, bidra till organisationens IT-styrning.

4.3 IT:s bidrag till verksamheten

Samtliga företag anser att det primära sättet som IT-revisorn kan bidra till att IT: s värde förmedlas inom organisationen är genom att lyfta upp sin avrapportering, innehållande iakttagelser kring brister samt rekommendationer, till ledningsnivå. Det främsta skälet till att detta anses vara viktigt är att IT-avdelningar i många fall har svårt att själva driva igenom frågor och få gehör från ledningen gällande hur IT ska hanteras och styras. IT-revisorns avrapportering är då i mångt och mycket ett sätt att stötta IT-avdelningen och se till så att viktiga frågor lyfts fram i rätt forum där frågorna kan hanteras på rätt sätt vilket sammanfattas väl genom följande citat från A:

> *”Det är inte alltid som IT-chefen i en verksamhet är representerad i företagsledningen, alltså sitter med i ledningsgruppen. Det varierar. Ofta är det fortfarande ekonomichefen, eller någon administrativ chef som samtidigt har IT under sitt ansvarsområde. Därför är det viktigt att*

> *vi rapporterar till de som sitter i ledningsgruppen, alltså de som kan hantera frågorna på rätt sätt. Det tror jag är det absolut viktigaste."*

Att IT: s värde i organisationen förmedlas lyfts fram på fler sätt. C menar att de kan få fokus kring IT-styrningsfrågor, IT-effektivitet och IT-kontroller genom att prata om de här områdena i rätt forum hos företaget. B anser att en diskussion kring styrmodeller och systemägande för kravinsamling är en viktig del. A och C anser att en jämförelse mellan olika företag gör det möjligt att förmedla en väl fungerande hantering av IT för nya kunder. Genom att relatera brister inom IT till verksamhetsrisker så anser D att han kan bidra till en förståelse för vad IT verkligen bidrar med i organisationen.

Det framkom även fler svar gällande varför IT-revisorns bidrag till att IT: s värde förmedlas inom en organisation är viktigt. A anser det är betydelsefullt för att bidra till kundens utveckling av verksamheten. För att kunna utnyttja systemets kapacitet så menar C att det är angeläget att se till att kunden utnyttjar systemfunktionerna istället för att göra manuella moment. D framhöll att tydliggörandet av varför en risk faktiskt är en risk var en viktig del i att skapa en medvetenhet kring IT: s värde.

Alla informanter framhöll dock att det ligger en svårighet för IT-revisorerna att kontrollera huruvida IT:s värde verkligen förmedlas inom organisationen. Framförallt upplevs detta som problematiskt då alla informanter jobbar med att följa upp tidigare revisionsarbete men att det inte finns något sätt att ställa krav på att verksamheten ska följa några rekommendationer. Följande citat skildrar denna problematik:

> *"[…] det är ju upp till dem om de vill åtgärda de här bristerna, eller om de vill leva med och acceptera risken."* (D)

> *"[…] det är klart att det kan vara tröttsamt om man kommer till en kund och så ser man vissa brister ett år och så kommer man tillbaka nästa år och så är det samma skit igen. Då är det ju rätt trist. Kunde man ju önska att man kunde sparka de lite i häcken så att de jobbar och gör förbättringar, det är ju rätt meningslöst att komma dit och skriva samma rapport igen."* (A)

Tabell 4.3: IT: s bidrag till verksamheten

	KRITISKA MOMENT AVSEENDE ARBETET MED IT: S BIDRAG TILL VERKSAMHETEN
A	Att rapporteringen når ledningsnivå.
B	Föra fram IT genom avrapportering till ledningsgruppen. *"Har du inte styrning på plats så är det också svårt att förmedla ett mer förfinat budskap av bidraget. För annars kommer ju IT bara bli en försörjare av burk."*
C	Att rapporteringen når ledningsnivå, att man har en syn på IT där verksamheten är kravställare och IT är leverantör.
D	Att formulera rapporteringen på ett förståeligt sätt när den presenteras och koppla den till verksamhetsrisker för att nå ut till ledningen.

4.3.1 Analys av IT:s bidrag till verksamheten

Ledningens förståelse och stöd för IT i kombination med att nyttan av IT kommuniceras ut i organisationen är vitalt för en effektiv IT-hantering, vilket beskrivs i avsnitt 2.5.3.

Vi har inte observerat några indikationer på att IT-revisorerna är involverade i arbetet med att utforma ett ramverk för kontroll och övervakning av IT: s bidrag till verksamheten, vilket beskrivs i kontrollmål 1 (se avsnitt 2.5.3) och även omfattas av kontrollmål 2-5 (se avsnitt 2.5.3).

Det viktigaste bidraget som IT-revisorerna kan ge avseende IT: s värde och dess bidrag till verksamheten är istället att säkerställa att deras avrapportering når ledningsnivå. För att rapporteringen ska kunna förstås och hanteras av ledningen så ansågs det viktigt att den var utformad på ett förståeligt sätt och anpassad efter mottagaren. IT-revisorerna rapporterar endast på de brister som finns i organisationen gällande dess IT-hantering, vilket kan ge en negativ bild av IT. Det är dock möjligt att anta att om ledningen beaktar dessa brister och försöker åtgärda dem så kan man skapa ett större IT-värde.

Det föreligger ett tydligt problem i att IT-revisorernas rekommendationer som återfinns i rapporteringen inte är något annat än just rekommendationer. Det är således svårt för IT-revisorer att säkerställa att deras arbete ligger till grund för företagets hantering av IT: s bidrag till verksamheten då detta till stor del beror på hur mottaglig företagsledningen är för rekommendationer. Av denna anledning är det för IT-revisorerna en utmaning att motivera synpunkter och potentiella utfall av risker på ett sätt som ledningen kan relatera till och därmed tar till sig. Arbetet med att förmedla IT: s värde till organisationen inbegrips inte som ett huvudsakligt mål med IT-revisionen. Trots detta har vi sett tydliga indikationer på att IT-revisorerna i mångt och mycket anstränger sig för att se till att deras utförda arbete ger utslag i organisationen. Enligt vår uppfattning är en av anledningarna till denna ansträngning att IT-revisorerna vill skapa ett mervärde för kunderna i syfte att bibehålla en bestående kontakt.

> *”[…] allting som är av direkt mervärde försöker vi ju bidra med och det är stort fokus hos oss internt att revisionen ska inte bara vara en revision utan den ska tillföra ett bra mervärde till bolaget […]”* (C1)

Ytterliggare en anledning som kan bidra till denna ansträngning är de indikationer vi fått om att IT-revisorn vill känna att arbetet blir mer meningsfullt. Om de kan ta fram relevanta rekommendationer som kunden faktiskt tar till sig och applicerar så gynnar detta såväl kunden som IT-revisorn.

Beslutsfattare tar mer effektiva beslut ju större förståelse de har för företagets IT-värde (Weill & Ross, 2004). IT-revisorernas beskrivna tillvägagångssätt gällande arbetet med IT: s bidrag till verksamheten handlar till väldigt stor del om att rapportera iakttagelser till ledningsnivå. Att förmedla och skapa engagemang för IT är precis vad kontrollmål 6 och 7 (se avsnitt 2.5.3) för detta temaområde behandlar.

IT-revisorerna kan framförallt säkerställa att avrapportering sker till ledningsnivå och att rekommendationerna i denna är anpassade efter mottagaren. Således kan de förmedla IT: s bidrag till verksamheten och på så vis bidra till organisationens IT-styrning. Påverkan begränsas dock

till den grad av mottaglighet för IT-revisorernas rekommendationer som organisationen präglas av.

4.4 Intern kontroll

Samtliga informanter framhöll att det allra främsta syftet med ett företags interna kontroller är att säkerställa den finansiella rapporteringen och riktigheten i finansiell data. B anser att man når en högre kvalitet på rapporteringen genom att ha kontroll på de mest väsentliga processerna och att de blir rätt utförda, är kontrollmekanismerna bristfälliga så måste systemet substansgranskas. Både B och D anser att företagets kontrollmekanismer måste fungera på ett bra sätt för att fel inte ska falla ut. C framhåller att dåliga kontroller påverkar organisationen på samtliga nivåer och bristande kontroller på lägsta nivå bidrar till att kontroller på högre nivåer sätts ur spel.

Utöver det huvudsakliga syftet med intern kontroll, framkom även andra aspekter. C framhöll att det kan vara ett sätt att styra och kontrollera IT. A påpekade att det är ett sätt att förhindra obehörigt nyttjande av företagets tillgångar samt att upprätthålla företagets image. På motsvarande sätt framhöll även D att bra interna kontroller bidrar till företagets hantering av sina risker samt ökar förtroendet mot externa parter.

Det framgick även att interna kontroller betraktades som ett övergripande område som genomsyrade hela IT-revisionen. A uttryckte sig i detta avseende enligt följande: *”[...] allting hänger ihop med intern kontroll som jag ser det”*.

Det sätt som IT-revisorn granskar de interna kontroller varierar. A nämner främst en intervjubaserad genomgång som följs upp av stickprov. Här förekommer hjälpverktyg för att granska säkerhetsinställningar vilket är en effektiv kontroll för att stämma av resultaten mot intervjuerna. B skiljer på systembaserade och icke systembaserade kontroller och hanterar endast de förstnämnda. Dessa säkras främst genom registeranalys. C har ett tillvägagångssätt som innefattar att plocka ut loggar för att spåra tillbaka samt att begära in policys och studera dessa. D gör stickprovstestning vilket föregås av en allmän genomgång av de interna kontrollerna. Om denna stickprovstestning pekar på brister så försöker man att hitta kompenserande kontroller för att åtgärda detta problem. Att hitta kompenserande kontroller i verksamheten för att kunna leva med en iakttagen risk är något som även C nämner. På frågan hur brister i de interna kontrollerna hanteras när det gäller exempelvis behörighet så uttrycker D att *”då blir det ju rekommendation på det, de bör ändra sitt arbetssätt och som jag sa tidigare så kan man kanske hitta kompenserande kontroller i vissa fall för att komma runt den risken”*. I samma avseende påpekar C2 att *”[...] för varje iakttagelse som lyfts så försöker vi eventuellt titta på kompenserande faktorer, alltså kompenserande kontroller i verksamheten som gör att man ur ett visst perspektiv kan leva med den risken som man har iakttagit [...]”*

Tabell 4.4: Intern kontroll

	KRITISKA MOMENT AVSEENDE ARBETET MED INTERN KONTROLL
A	Åtkomstkontroller, ändringshantering och kontroll på backup.
B	Säkerställa fungerande kontrollmekanismer.
C	Behörighet, felaktiga behörighetskontroller gör att man direkt kommer åt information som man inte ska göra.
D	Säkerställa en bra ansvarsfördelning.

4.4.1 Analys av intern kontroll

På förhand trodde vi att granskningen av interna kontroller var ett viktigt delmoment av IT-revisionen. Vikten av intern kontroll var också något som informanterna påpekade. Däremot betraktades inte detta område separat utan var ett genomgående inslag i IT-revisionen. Detta kan ha ett samband med att fokus ligger på att säkerställa den finansiella rapporteringen vari granskningen av interna kontroller utgör huvudsakligt fokus. Det var följaktligen inte helt överraskande att de moment som framhölls som mest kritiska för intern kontroll till största del kan relateras till säkerställandet av den finansiella rapporteringen och dess korrekthet. IT-revisorernas påverkan till organisationens IT-styrning kan därmed bättre relateras genom övriga temaområden varför vi endast kort väljer att analysera empirin mot detta temaområdes kontrollmål. Som beskrivits i avsnitt 4.4 så var kompenserande kontroller ett viktigt inslag för att motverka brister gällande interna kontroller, vilket även kontrollmål 1 (se avsnitt 2.5.4) syftar till att hantera.

IT-revisorerna gör en granskning av organisationens kontroller, däremot så undersöker man inte specifikt vilken kontroll ledningen har över dessa. Detta indikerar följaktligen på att kontrollmål 2 (se avsnitt 2.5.4) ligger utanför ramen för IT-revisorns arbete.

4.5 Extern kravhantering ur ett IT-perspektiv

Samtliga intervjuer indikerade tydligt på det faktum att informanterna inte jobbade mot verksamheters externa krav i någon stor utsträckning. C förklarade att lagar och regelverk som organisationen ska följa men som IT-revisorerna inte är skyldiga att uttala sig om aldrig granskas specifikt. D framhöll att externa krav ofta är en del av den finansiella revisionen och att IT endast blir påverkat av dessa krav till en begränsad del.

Samtliga informanter nämner dock att man generellt försöker identifiera de krav som föreligger organisationen för att se hur man möter upp till dessa krav, i synnerhet gällande SOX som av informanterna sägs vara det enda regelverk som IT-revisorer är skyldiga att uttala sig om.

Tabell 4.5: Extern kravhantering

	KRITISKA MOMENT AVSEENDE ARBETET MED EXTERN KRAVHANTERING
A	Fånga upp de krav där de själva riskerar att bli utsatta.
B	Uppgav inget svar.
C	Att IT-revisorerna följer de regelverk som föreligger externa krav.
D	Uppgav inget svar.

4.5.1 Analys av extern kravhantering ur ett IT-perspektiv

I avsnitt 2.5.5 beskrivs att bolag omges av en rad olika regelverk, lagar och standarder som ska tillmötesgås. Vi trodde på förhand att IT-revisorerna kunde ha en stor del i att granska huruvida organisationer motsvarade dessa krav och regler.

Externa krav var dock det temaområde där vi fann minst likheter mellan IT-revisorernas arbete och undersökningsmodellens kontrollmål. Till viss del arbetade man med att identifiera externa krav, i synnerhet med företag som var noterade på den amerikanska börsen och således var tvungna att rätta sig efter de krav som föreskrivs i SOX. Detta ansågs dock inte ligga inom ramen för IT-revisionen utan behandlades till störst del av de finansiella revisorerna. Vi kan konstatera att samtliga kontrollmål (se avsnitt 2.5.5) för detta temaområde ligger utanför IT-revisorns ansvarsområde. Enligt denna undersökning bidrar därmed IT-revisorerna inte till organisationens IT-styrning gällande extern kravhantering.

4.6 Kontroll- och organisationsstruktur

Informanterna på tre av fyra företag ansåg att framförallt granskningen av organisationsstrukturen är en viktig del i IT-revisorns arbete för att skapa en övergripande uppfattning om organisationens mognadsgrad. C1 förklarade detta enligt följande:

> *”[…] den här första domänen (IT-kontrollmiljön) ger väl en bild lite av hur det fungerar, hur man styr sin IT och det kan också ge föraning om vad vi kommer att se i de andra domänerna. Och det är egentligen det viktigaste för oss att förstå mognadsgrad och sådär, för det hjälper oss att identifiera riskerna i de andra domänerna. Om de säger att de inte har några styrande dokument överhuvudtaget, ja då kan vi dra slutsatsen om att risken är förhöjd i de andra, att vi ska hitta felaktigheter då […]”*

D anser inte att organisationsstrukturen i sig är viktig men att den granskas för att identifiera beslutsfattare på olika nivåer i organisationen vilket behöver göras för att kunna ge tydliga rekommendationer kring ansvarsfördelning.

Vidare påpekade A att organisationsstruktur är viktig för att *”möta gränslandet mellan verksamheten och IT”*. Ett vanligt sätt för en organisation att hantera detta är enligt informanten att skapa ett IT-råd/IT-styrgrupp innehållande representanter dels från IT och dels från verksamheten. I de fall då det finns bristande kommunikationsvägar anser sig informanten kunna lokalisera och ge förslag på förbättringar som kan innebära en tydligare struktur och styrning av den finansiella informationen, exempelvis genom att rekommendera en IT-styrgrupp. B anser att om man inte ser

över stödstrukturen så minskar graden av förmedlat IT-värde i takt med att organisationen expanderar. En bra organisationsstruktur kan på så sätt se till att IT stöttar organisationen på rätt sätt så att de *”levererar mer än burk”*. C anser att det är viktigt att kunna se syftet med en kontroll, varför man har den och varför man jobbar efter ett visst kontrollmål. De menar att en förutsättning för att en kontroll ska fungera är att ha strukturstöd i organisation, att det finns ansvariga för kontroller samt att kontrollerna följs upp och bevakas. Detta kontrolleras genom att man genomför intervjuer och begär in policys.

4.6.1 Analys av kontroll- och organisationsstruktur

Granskningen av organisationsstrukturen genomförs för att skapa en övergripande uppfattning om organisationens mognadsgrad gällande IT och görs som det initiala steget i IT-revisionsprocessen. Att etablera en organisatorisk struktur genom att upprätthålla kommunikation och en samverkande struktur mellan IT och andra funktioner är beskrivet i kontrollmål 2 (se avsnitt 2.5.6). En effektiv organisatorisk struktur är en förutsättning för att viktiga interna kontrollmekanismer ska fungera på ett tillfredsställande sätt vilket framgår i avsnitt 4.6. Det är följaktligen möjligt att IT-revisorernas granskning av detta kan skapa en dialog inom företaget kring organisationsstrukturen, exempelvis gällande ansvarsfördelning, och därmed påverka kvaliteten på de interna kontrollerna. Effektiva interna kontroller kan även i förlängningen underlätta för IT-revisorerna att kontrollera riktigheten i den finansiella rapporteringen.

Vidare framgår det i avsnitt 4.1 att IT-revisorerna granskar standardiserade sätt att hantera IT-processer och ansvarsskyldigheter för att undvika bristfälliga interna kontroller. Det framgår även i avsnitt 4.6 att det är viktigt att se syftet med en viss kontroll och vad ansvarsskyldigheten innebär. IT-revisornernas hantering av den här typen av frågor indikerar på att man skapar förutsättningar för att organisationen ska kunna etablera ett ramverk för kontroll, vilket är beskrivet i kontrollmål 1 (se avsnitt 2.5.3) för detta temaområde.

Det arbete som IT-revisorerna utför, gällande den organisatoriska kartläggningen och rekommendationer kring denna, kan bidra till att hanteringen av organisationsstrukturen förbättras. Detta förhöjer organisationens förutsättningar att påverka verksamhetens IT-styrning på ett positivt sätt.

4.7 Risker och riskhantering ur ett IT-perspektiv

Att titta på fysiska aspekter i allmänhet och backuphantering i synnerhet för att förebygga förlust av data är något som alla informanter anser vara en naturlig del av riskhanteringsarbetet. D menar att *”[...] riskerna handlar ju ofta om att data försvinner, att data förstörs, det är inte lika vanligt att data skulle förändras för det hanterar man ju i sådana fall genom att ha andra kontroller för det, behörighetsåtkomst, förändringsprocess och så vidare.”* Vidare ser alla informanter helst att företaget har en riskanalys upprättad och rekommenderar i de fall det saknas att en sådan bör tas fram. Om en riskanalys är upprättad så svarar alla informanter att de granskar denna och för en diskussion med respektive företag kring upprättandet och utformningen av denna i syfte att ge viss vägledning. D framhåller dock i detta avseende att *”det är ändå företagen som vet vilka som är deras största risker. Vi har ju många företag inom många olika branscher så det är omöjligt för oss att vara bäst på att veta vilka risker alla företag står inför.”* Även C1 påpekar gällande detta att *”det är ju inte vår huvudkompetens, riskanalys så att säga, det finns ju bolag som enbart jobbar med det”*.

A beskriver att klassificering av risker görs indirekt och att det är viktigt för att veta vilka kontroller som behövs. I detta avseende anser informanten att företag ofta har kontroller men att dessa sällan är upprättade på rätt sätt utan endast med intentionen att *”de är nog bra att ha”.* C anser att ett minimumkrav är att kontroller ska vara förankrade till riskhanteringsarbetet. De är framförallt intresserade av att se att företaget har gjort en ordentlig utvärdering av riskerna, vilket informanterna granskar genom att begära ut bolagets egen klassificering av risker och ifrågasätta hur man har tänkt kring riskerna och vad man har gjort för att åtgärda dem. C framhåller vidare att det är viktigt att de finns ansvariga för att hantera olika riskaspekter. D gör en egen bedömning av riskhanteringsarbetet om han anser att föreslagna åtgärder är tillräckliga för att IT-revisorerna ska känna sig trygga, framförallt gällande påverkan på den finansiella redovisningen. B anser att man bör titta på om organisationen tänkt i termer av IT-risk och att ledningen har varit involverad i genomförandet av riskanalysen och menar vidare att *”IT-risken är egentligen inte frikopplad från bolagsrisken”*.

IT-risker anses av informanterna även vara kopplat till hur stor betydelse IT har för verksamhetens processer. Det är enligt alla informanter viktigt att betrakta konsekvenserna av eventuella risker. B påpekar i detta avseende att *”[...] man får göra en liten enkel analys själv. Vad händer om jag rycker pluggen till IT på det här bolaget? Vilka processer kommer att stanna?”.*

Både B och D framhöll att riskhanteringen kan skötas med hjälp av ISO-standarden för informationssäkerhet (ISO 27 000). Dessa informanter uttrycker att det inte är tvunget att sträva efter en certifiering, utan ISO-standardens innehåll kan användas som riktlinjer för riskhanteringsarbetet. C menade att hjälpmedel som kan användas i riskhanteringsarbetet är IT-riskverktyg som gör det möjligt att jämföra kunder som är i samma bransch och situation vilket ger en bild över normala risker som bör finnas**.** D påpekade att det är av värde att jämföra olika kunder och på basis av erfarenhet beakta eventuella risker. A ansåg sig inte använda någon form av hjälpmedel för detta ändamål.

Tabell 4.6: Riskhantering

	KRITISKA MOMENT AVSEENDE RISKHANTERINGSARBETET
A	Att relatera risk till sannolikhet att risken inträffar samt konsekvensen av denna.
B	Att se till att företaget håller sig uppdaterade. *”Vet man om att detta är trettonde revisionen av någonting som togs fram för tre år sedan, då är det ju ett dokument man jobbar med löpande.”*
C	Att riskerna är dokumenterade och löpande följs upp i syfte att utvärdera förändringar i riskmiljön. Se till att riskaptiten är förankrad i organisationen samt medvetenhet om konsekvenserna av att en risk faller ut. *”Struktur är ju egentligen nyckelordet.”* (C1)
D	Klassificeringen av risker. *”[...] annars är det ju risk att du jobbar för att åtgärda fel sorters risker när det finns andra som kanske är mycket mer allvarliga.”*

4.7.1 Analys av risker och riskhantering ur ett IT-perspektiv

Den avrapportering som IT-revisorerna ger innehåller iakttagelser, rekommendationer och eventuella riskscenarion. Trots att informanterna framhåller att företagen själva är bäst medvetna om sina risker så kan IT-revisorernas rapportering rimligen användas som beslutsunderlag för organisationen för att själva kunna göra ett ställningstagande till om riskens verksamhetspåverkan

är på en acceptabel nivå. Det har även framgått att i de fall en riskanalys är genomförd så tittar IT-revisorerna på dess tydlighet, användbarhet och vem den är riktad mot. Dessa aspekter belyses i kontrollmål 3 (se avsnitt 2.5.7).

Ett av de mest kritiska momenten gällande riskhanteringen var att genomföra löpande uppdateringar av riskmiljön (se tabell 4.6). Detta hanteras även av de delar i kontrollmål 6 (se avsnitt 2.5.7) som beskriver att periodiska riskfaktoranalyser ska utföras i syfte att identifiera nya eller uppkommande risker i såväl extern som intern miljö. Detta tyder följaktligen på att IT-revisorernas arbete inbegriper det som är beskrivet i kontrollmål 6.

Samtliga informanter framhåller att risker bör betraktas i förhållande till eventuella konsekvenser och att IT-riskers påverkan varierar beroende på IT: s betydelse i organisationen. Framförallt kontrollmål 7 och 8 (se avsnitt 2.5.7) behandlar att det bör skapas en förståelse för verksamhetens nyckelaktiviteter och dess beroende av hanteringen av IT-processer. IT-revisorerna framhåller att de är medvetna om ovanstående och försöker ge viss vägledning inom detta område. Det är följaktligen möjligt att IT-revisorerna kan bidra till riskhanteringen i en organisation då deras granskningar fokuserar på brister i verksamheten, vilket kan leda till en ökad medvetenhet kring de risker som eventuella brister kan innebära.

Övriga kontrollmål (se avsnitt 2.5.7) som syftar till att skapa en systematisk struktur kring IT-risker, med kontroller som avser mäta och följa upp risker, är delar inom riskhanteringsarbetet som IT-revisorerna uppger att de inte arbetar med. Vi ser därmed tydliga indikationer på att dessa kontrollmål inte ligger inom ramen för IT-revisorernas arbete. Detta stämmer bra överens med det faktum att IT-risker varken är ett huvudsakligt fokus- eller kompetensområde för IT-revisorerna vilket framgick i avsnitt 4.7.

IT-revisorns bidrag till IT-styrning avseende arbetet med risker och riskhantering är begränsad. Dels till den tid som läggs ner på detta arbete och dels till det material som organisationen själv producerat. Samtliga intervjuer indikerar på att ju längre organisationen har kommit avseende riskhanteringsarbetet, desto större möjlighet har IT-revisorn att påverka.

4.8 Mest kritiska faktorer avseende IT-styrning

Det framgick tydligt vid samtliga intervjutillfällen att IT-revisorns största möjlighet att inverka på organisationens IT-styrning var via sin rapportering. I detta avseende var det mest kritiskt att säkerställa att rapporteringen hamnar på högsta ledningsnivå samt att den är utformad på ett begripligt sätt för mottagaren. Följande citat illustrerar detta:

> *” Framförallt genom att rapportera våra iakttagelser till rätt person. Med rätt person så menar jag att det ska upp på företagsledningens bord. Det är inte alltid som IT-chefen i en verksamhet är representerad i företagsledningen, alltså sitter med i ledningsgruppen. Det varierar. Ofta är det fortfarande ekonomichefen, eller någon administrativ chef som samtidigt har IT under sitt ansvarsområde. Därför är det viktigt att vi rapporterar till de som sitter i ledningsgruppen, alltså de som kan hantera frågorna på rätt sätt. Det tror jag är det absolut viktigaste.”* (A)

” Det vi fokuserar mycket på nu är ju egentligen att få företagsledningen involverade [...] varför det är så viktigt för företagsledningen att bry sig om IT, bristande kontroller och vilka konsekvenser det kan få.” (A)

” Eftersom jag alltid, ja i 99 fall av 100, ger förslag på hur man ska hantera det på ett bättre sätt så hoppas jag ju att min rapport kan ligga till grund för att VD:n säger att vi måste göra så istället.” (B)

” En sak som vi kan rapportera på och som inte har direkt finansiell påverkan är ju kanske om dom saknar policys och så för styrning. Alltså avsaknaden av policys höjer inte direkt risken för felaktighet i finansiell data, men det är sannolikt att viktiga kontroller i övrigt kanske inte finns då.” (C1)

” Jag tycker att alla moment ger, beroende på hur vi ser det, någon form av mervärde egentligen och det kan ju vara dels till företagsledningen i allmänhet som får veta hur IT-avdelningen fungerar eller inte fungerar men också om IT-direktören har tagit fram ett bra ramverk för styrning och han får feedback från oss att det fungerar inte riktigt som du hade tänkt så ger ju det ett väldigt stort mervärde för honom i sin roll som IT-direktör [...]” (C1)

”Rapporten vi ger till företaget då med rekommendationer, det är ju väldigt viktigt att den är formulerad på rätt sätt så att läsaren förstår annars så kommer vi inte få igenom några av våra rekommendationer, att det inte tas på allvar så att säga.” (D)

Nedanstående tabell har utformats på basis av svaren som framkommit på fråga 24 och 25 i intervjuguiden. (se bilaga B1).

Tabell 4.7: Mest kritiska faktorer gällande IT-styrning

	SAMMANSTÄLLNING AV DE MEST KRITISKA FAKTORERNA I IT-REVISORNS ARBETE RELATERAT TILL IT-STYRNING
A	• Avrapportering till ledningsnivå • Se till att företag har identifierat ett systemstöd som stödjer verksameten för en länk mellan IT-avdelningen och verksamheten • Se till att man får en aktiv involvering av ledningen • Riskanalyser som besvarar frågan om vilken skyddsnivå som behövs • Organisationsstrukturen framförallt gällande ansvarsfördelning
B	• Avrapportering till ledningsnivå • Kontrollera organisationsstrukturen och beslutsägande • Kontroll av att kravinsamling kommer från verksamheten så att IT kan stödja denna • Se till att det finns tydliga kommunikationsvägar mellan IT och verksamheten
C	• Avrapportering till ledningsnivå • IT-kontrollmiljön är viktigast eftersom den involverar granskning av styrdokument och intervjuer med IT-direktören angående hur han faktiskt styr sin verksamhet • Säkerställa att verksamheten är systemägare och kravställare så att IT ges möjlighet att leverera det som verksamheten kräver. • Informera företagsledningen om hur IT påverkar organisationen
D	• Avrapportering till ledningsnivå • Kontrollera att det finns en medvetenhet kring ansvarsfördelningen i organisationen och vilken påverkan detta har för IT-arbetet • Kontrollera att faktiska kontroller finns på plats i organisationen

4.8.1 Analys av mest kritiska faktorer gällande IT-styrning

Nedan presenteras tabell 4.7: s sammanställning relaterat till undersökningsmodellens temaområden vilket avslutningsvis presenteras med en figur.

Samtliga informanter nänmde att avrapporteringen till ledningen är en av de mest kritiska faktorerna. Vidare nänmde A och C, som en separat faktor, att involveringen av ledningen är en kritisk faktor. Denna information hanteras i uppsatsens temaområde för IT: s bidrag till verksamheten.

A, B och C hävdade att en kritisk faktor är att se över organisationsstrukturen. A nämner detta framförallt gällande ansvarsfördelning, B gällande beslutsägandet och C gällande IT-kontrollmiljön. Undersökningen indikerar på att organisationsstrukturen är viktig av två anledningar. Dels för att få en övergripande uppfattning om organisationens struktur överlag och dels för att säkerställa ansvarsfördelning. D framhöll att det var viktigt att säkerställa medvetenheten kring ansvarsfördelningen inom organisationen. Organisationsstrukturen behandlas i temaområdet kontroll- och organisationsstruktur medan ansvarsfördelning och

beslutsägande tas upp i såväl temaområdet definiera och hantera processer som säkerställandet av systemsäkerhet.

Ovanstående faktorer ligger således inom temaområdet kontroll- och organisationsstruktur respektive säkerställande av systemsäkerhet.

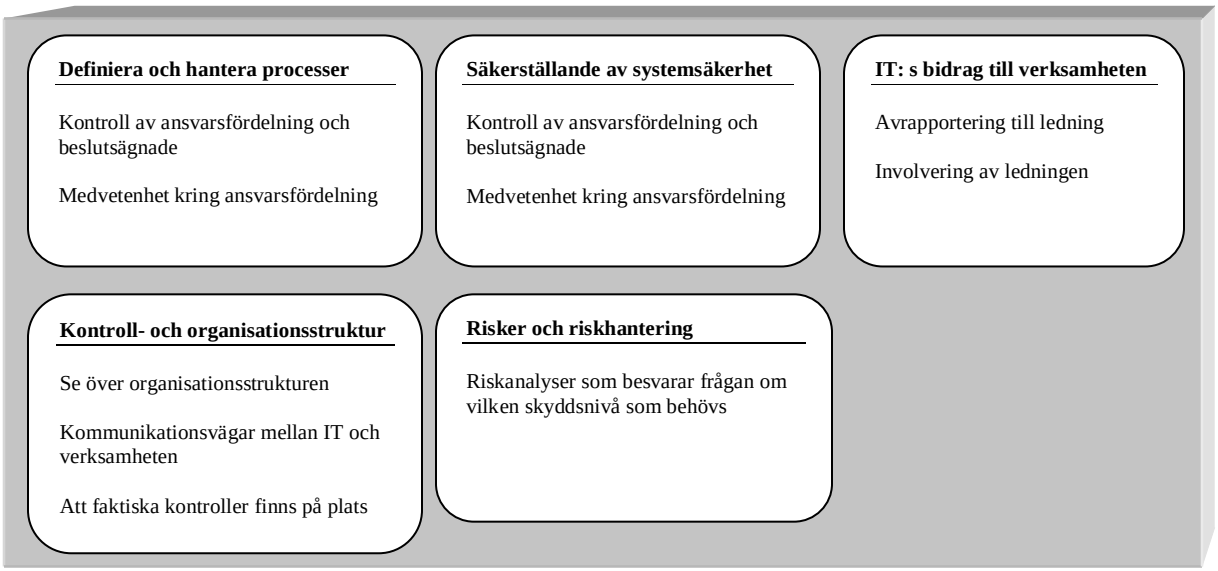
B ansåg att en kritisk faktor är att se till att det finns tydliga kommunikationsvägar mellan IT och verksamheten. D ansåg att det är en kritisk faktor att kontrollera att faktiska kontroller finns på plats i organisationen. Dessa är faktorer som tagits upp i kontrollmålen för kontroll- och organisationsstruktur.

A påpekade att en kritisk faktor är att granska riskanalyser som besvarar frågan om vilken skyddsnivå som behövs i organisationen vilket adresseras i temaområdet risker och riskhantering.

D framhöll att det var viktigt att säkerställa medvetenheten kring ansvarsfördelningen inom organisationen, en faktor som behandlats inom dels temaområdet säkerställande av systemsäkerhet och dels temaområdet definiera och hantera processer.

Att det är en kritisk faktor att arbeta för att organisationen ska ha ett systemstöd som stödjer verksamheten framhöll A, B och C. Detta arbete inbegriper framförallt hanteringen av kravinsamling, vilken verksamheten och inte IT-avdelningen bör ansvara för. Detta är ett område som ligger utanför denna uppsats undersökningsmodell och har således ingen direkt koppling till något av temaområdena. Av denna anledning inkluderas denna faktor inte i nedanstående figur.

Figur 4.1: Mest kritiska faktorerna i IT-revisorns arbete relaterat till IT-styrning



4.9 Diskussion kring övriga iakttagelser

En intressant iakttagelse är att samtliga informanter framhöll att syftet med den renodlade IT-revisionen är att säkerställa den finansiella rapporteringen. Vi hade efter uppsatsens litteraturgenomgång en uppfattning att IT-revisorerna fokuserade på IT-relaterade frågor överlag. Det har dock under undersökningen framkommit att det primära syftet med en IT-revision är att stödja de finansiella revisorerna och därmed säkerställa att interna kontroller gällande de finansiella aspekterna fungerar tillfredsställande. IT-revisorerna framhöll att de även kan arbeta åt kunden med andra typer av IT-frågor, men de gör då en viktig särskiljning mellan rollen som IT-revisor respektive IT-konsult. Detta beror på att de vill undvika att förlora sin ställning som oberoende part. Som alla informanter nämner så kan inte för mycket konsultation ges kring ett revisionsuppdrag då detta innebär en risk att det egna arbetet granskas, vilket kan innebära att jäv uppstår. Samtliga informanter framhöll även att tidsbegränsningar och IT-revisionens omfång ofta avgjorde hur pass omfattande de kunde vara i sin konsultation. Merhout & Havelka (2008) framhåller att tid och omfång ofta avgör hur stort värde revisionen kan bidra med. Det är följaktligen möjligt att dessa omständigheter kan ha betydelse för IT-revisorernas bidrag till organisationens IT-styrning.

En faktor som kan öka värdet och kvaliteten på IT-revisionen är användandet av en revisionsmetodik som följer standarder och best practices (Merhout & Havelka, 2008) Tre av undersökningens fyra företag beskriver att de checklistor som ligger till grund för deras IT-revision är resultatet av den övergripande metodik som framtagits av respektive företag. Denna metodik grundar sig i management-ramverket COSO gällande den allmänna revisionen och i COBIT avseende IT-revisionen. Checklistorna har sedan utökats med IT-revisorernas erfarenheter och kräver viss anpassning till olika typer av IT-miljöer som deras klienter verkar inom. Det fjärde företaget nämner att de har en övergripande metodik inom företaget där IT-revisionen återfinns som en del. Checklistor är i detta fall framtaget på basis av best practices.

Ovanstående ramverk hanterar styrningsfrågor vilket indikerar på att IT-revisornernas arbete har en tydlig koppling till just IT-styrning.

En återkommande fråga under empiriinsamlingen var huruvida IT-revisorerna fokuserade på mättal, uppföljning och utvärdering inom de olika temaområdena för att mäta organisationens IT-prestanda. Denna aspekt anågs dock av informanterna vara av mindre vikt i deras IT-revisionsarbete. Detta kan förklara varför den typ av kontrollmål inom temaområdena som behandlar mätning och mättal för IT-prestanda ligger utanför ramen för IT-revisorernas ansvarsområde.

Det framgick vid samtliga intervjutillfällen att i de fall de fall det inte fanns några kontrollmekanismer för IT-processer eller att de innehöll grova brister så var IT-revisorerna istället tvugna att substansgranska data från systemen. Detta arbete krävde betydligt mer tid och resurser varför man föredrog att kunna säkerställa organisationens kontrollmekanismer. Genom att försöka se till så att organisationen har fungerande kontrollmekanismer för sina IT-processer, är det rimligt att anta att både IT-revisornernas jobb underlättas samtidigt som det bidrar till klientens IT-styrningsarbete.

5. Slutsats

Uppsatsens syfte har varit att skapa en förståelse för IT-revisorns arbete och hur detta kan påverka IT-styrningen i en organisation. För att uppnå detta har vi undersökt vilka områden inom IT-styrning som kan vara av vikt för IT-revisorer att beakta. Vidare har uppsatsen adresserat de faktorer som av informanterna ansetts kritiska i detta avseende.

Frågeställningarna i denna undersökning har varit följande:

Vilka områden är viktiga för IT-revisorer att beakta avseende IT-styrning?

Vilka faktorer är mest kritiska avseende IT-revisorers arbete, relaterat till IT-styrning?

Det framgår att IT-revisorer inte lägger fokus på mättal, uppföljning och utvärdering som en del i arbetet. Dock används checklistor, som i mångt och mycket har sin grund i COBIT, för säkerställandet av den finansiella rapporteringen. Detta har resulterat i att många av de kontrollmål som återfinns i uppsatsens undersökningsmodell som inte direkt fokuserar på mätning, uppföljning och utvärdering faktiskt har behandlats. Uppsatsens analys har gett indikationer på huruvida respektive temaområde varit väsentliga för IT-revisorn och dennes arbetsprocess. De temaområden som visat sig ha starkast koppling till IT-revisorns roll, och därmed kan ha betydelse för IT-styrning är följande:

- Definiera och hantera processer
- Säkerställande av systemsäkerhet
- IT: s bidrag till verksamheten
- Kontroll- och organisationsstruktur
- Risker och riskhantering

IT-revisorns arbete kan påverka IT-styrningen inom delar av uppsatsens temaområden men inte i den utsträckning som litteratur inom området framhåller. Detta kan ha att göra med de begränsningar som IT-revisorerna upplever. De omständigheter som har visat sig vara avgörande för hur stark påverkan IT-revisorerna har på IT-styrning i allmänhet är den tid och det omfång som ges varje IT-revisionsuppdrag. Vidare påverkar organisationens mottaglighet för rekommendationer IT-revisorns bidrag till IT-styrningen.

Som figur 4.1 visar ligger de mest kritiska faktorerna i förhållande till IT-styrning inom ovanstående fem temaområden. Detta med undantag för den kritiska faktorn som syftade till att säkerställa att ansvaret för kravinsamlingen för en organisations system ligger hos verksamheten. Denna faktor ligger således utanför uppsatsens undersökningsmodell.

Vidare har avsnitt 4.8 visat att IT-revisorernas största möjlighet att bidra till organisationens IT-styrning är deras avrapportering till ledningsnivå samt att skapa ett engagemang för IT i ledningen. Det intressanta i detta avseende är att det är möjligheten att rapportera till rätt nivå i organisationen och utformningen av rapporteringen som sägs vara det avgörande för hur IT-revisorns rapportering kommer att påverka organisationen. Ett problem som ofta belyses när det gäller IT-styrning är ledningens brist på förståelse för IT och vad IT kan bidra med, vilket har

förklarats i avsnitt 2.1. I detta avseende indikerar undersökningen på att IT-revisorn kan påverka ledningens medvetenhet för IT. I många organisationer saknas IT-representanter på högsta ledningsnivå och då är IT-revisorns avrapportering en möjliggörare för en tydligare hantering av IT-styrningsfrågor.

5.1 Reflektion kring uppsatsens metod och slutsats

Utformningen av en undersökningsmodell har underlättat i vårt arbete att besvara de frågeställningar som legat till grund för uppsatsen. Vi är medvetna om att resultatet av undersökningen hade kunnat bli annorlunda om andra urvalskriterier applicerats. Det finns en möjlighet att detta hade medfört att andra temaområden skulle legat till grund för undersökningsmodellen vilket därmed hade haft påverkan på uppsatsens empiriinsamling och analys av denna.

Tre av företagen i denna studie ingår i revisionsvärldens så kallade Big Four. Det fjärde företaget är ett mellanstort svenskt revisionsbolag och det fanns en möjlighet att deras tillvägagångssätt skiljde sig från de större globala bolagen. Vi såg dock inga sådana tendenser i vår undersökning och vi anser därför inte att resultatet hade blivit annorlunda om alla Big Four-byråer inkluderats i studien. Däremot är det möjligt att resultatet hade blivit annorlunda om endast bolag som enbart arbetar med IT-revision hade legat till grund för undersökningen. Bolag som sysslar med både IT-revision och finansiell revision kan möjligtvis ha annorlunda synsätt gällande hur en IT-revision bör bedrivas.

Bilagor

B1. Intervjuguide

Inledande frågor

1. Beskriv kortfattat Dina arbetsuppgifter samt Din position i organisationen?
2. Hur länge har Du jobbat som IT-revisor och vad var det som fick Dig intresserad av området?

Definiera och hantera processer

3. Vilka moment anser du bör gås igenom vid en granskning av ett företags processer?
4. Hur kan man praktiskt jobba med dessa moment (exempelvis vad som dokumenteras och hur det används)?
5. Av de moment (faktorer) som nu diskuterats, vilka anser Du vara mest kritiska i förhållande till IT-styrning och varför?

Säkerställande av systemsäkerhet

6. Vad är syftet med att granska företags säkerhetsrutiner?
7. Vilka moment bör granskningen av ett företags säkerhetshantering fokusera på?
8. Hur kan man praktiskt jobba med dessa moment?

IT: s bidrag till verksamheten

9. På vilket sätt kan IT-revisorn bidra till att IT: s värde förmedlas inom en organisation?
10. Anser Du detta vara viktigt och i så fall på vilket sätt?
11. Hur kan IT-revisorn kontrollera att IT: s bidrag till verksamheten blir synbart för hela organisationen?
12. Vilka moment i arbetet gällande IT: s bidrag till verksamheten anser Du vara mest kritiska?

Intern kontroll

13. Vad anser Du vara syftet med ett företags interna kontroller?
14. Vad anser Du att bra interna kontroller kan ge för effekt för företaget?
15. Hur kan IT-revisorn kontrollera/granska de interna kontrollerna?
16. Vilka moment gällande detta arbete anser Du vara mest kritiska?

Extern kravhantering ur ett IT-perspektiv

17. På vilket sätt kan IT-revisorn kontrollera att företag tillmötesgår de externa krav de omges av?
18. Vilka är de mest kritiska faktorerna i detta arbete?

Kontroll- och organisationstruktur

19. Anser Du det vara viktigt för en IT-revisor att granska organisationsstrukturen för kontroller och beslutsfattande, i så fall varför?
20. Är detta något som ni jobbar med, i så fall hur?

Risker och riskhantering ur ett IT-perspektiv

21. Hur bör IT-risker/IT-riskpolicys hanteras och granskas i relation till följande områden:
    a) klassificering av risker
    b) kommunikation
    c) ansvarsskyldighet
    d) åtgärder/kontroller
22. Vilken typ av hjälpmedel eller verktyg kan användas för ovanstående ändamål?
23. Vilka moment anser Du vara mest kritiska gällande riskhanteringsarbetet?

Avslutande frågor

24. Vi har diskuterat en mängd olika faktorer som är viktiga att beakta vid en IT-revision, hur skulle du rangordna (prioritera) dessa faktorer i relation till IT-styrning?
25. Finns det några andra områden gällande IT-styrning som Du anser vara viktiga i ert arbete?

B2. Transkribering av intervjuer

B2.1 Intervju Företag A

Transkribering av intervju med Respondent från företag A 3 maj 2010

S = Stefan Arnslätt
H = Hampus Karlsson
R = Respondent (Informant)

S: Ja, då börjar vi intervjun här med Respondenten från Företag A som har gått med på att vi spelar in samtalet
R: Ja…
S: Mmm, börjar vi första frågan om du skulle vilja beskriva kortfattat dina arbetsuppgifter samt din position här på Företag A?
R: Mmm, jag är ju såkallat, vad ska man säga, manager är min titel på Företag A här och vad det innebär, det är ju egentligen en intern nomenklatur för befattningar som vi har, vi har även senior managers och parters och partners är ju då de som är delägare. Så det indikerar en viss nivå i organisationen. Eh, mina arbetsuppgifter är ju då att jag tillsammans med en kollega, vi är två stycken, arbetar med IT-revision här på Företag A i Malmö och jag har gjort det sen 2003, den rollen jag har nu. Jag är vanlig dödlig revisor i botten så jag har även en examen, alltså en revisorsexamen på första nivån enligt de nya reglerna så jag jobbar brett. Just att ha förståelse för finansiell revision kan vara en fördel när man jobbar på en byrå som Företag A till exempel för att kunna stötta revisorerna på ett bra sätt.
S: Ja, du svarade ju på det precis men hur länge har du jobbat som IT-revisor och vad fick dig intresserad av området?
R: Ja, det var en ren tillfällighet att jag hamnade här. Det var ju så att jag började jobba, jag har jobbat här på Företag A som revisor sen 1991, sen 1998 lämnade jag och jobbade med affärssystem ett antal år tills 2003 då jag av en ren tillfällighet kom tillbaks och såg att det fanns en roll här där det gavs möjlighet att kombinera kompetenser från de två yrkesroller jag hade haft tidigare…och sen har det bara blivit roligare och roligare.
H: Passar dig som handen i handsken helt enkelt?
R: Ja, det skulle man kunna säga va….Jag har stor nytta av konsulterfarenheten plus att jag förstår vad revision går ut på så att det har liksom varit ganska lätt att kombinera men sen behöver man ju alltid lära sig saker och ting på vägen. Men så är det.
H: Du har kanske fått en viss systemförståelse i och med konsultbiten?
R: Ja, det var ju tur det (skratt) alltså ingen formell utbildning på området utan jag är civilekonom med redovisning och finansiering i botten. Så är det.
H: Ja, då tänkte vi, vi har lite olika områden här som vi tänkt gå igenom och det första handlar om att definiera och hantera processer och då undrar vi då vilka moment du anser bör gås igenom vid en granskning av företagets processer?
R: Ja, alltså det där görs ju på olika sätt. Det är ju inte bara jag då som i egenskap av IT-revisor sysslar med processgranskning utan det gör ju även mina kollegor då va.
H: Mmm.
R: Men det jag tycker är viktigt, det är att i första hand, jag tycker att man ska ha en top-down approach, man börjar titta på vad är det för affär, vad är det för verksamhet bolaget sysslar med och så får man då fundera, okej vilka processer är det då som är viktiga till exempel order to cash och vissa delar i den och inköp till betalning och delar i den processen. Och alla de här bör rimligen kunna beskrivas på papper, verbalt, på ett sätt så att alla begriper det.
H: Att företaget har gjort den dokumentationen?
R: Ja, gärna…vi ser gärna att de gör det men det förekommer inte så ofta.
H: Nej, i de fall det inte gör det, vad gör ni då?
R: Då går vi ju intervjuvägen, går igenom processerna lite kort, sen nästa steg som jag tycker är väldigt viktigt som vi kanske då tycker att de vanliga revisorerna tappar bort är att se vilka system som finns som stödjer de här processerna i verksamheten, och hur används dom. Samtidigt får man fundera på, är det rätt system för

verksamheten? Det är väl kanske i normalfallet i ett granskningsuppdrag en biuppgift, det är inte det viktigaste men på något sätt så har man det med sig.
H: Precis ja. Man tänker på processmål, det var lite det du pratade om där innan.
R: Ja
H: Det som bör vara beskrivet men som kanske inte alltid är det?
R: Ja, precis.
H: Ser du någon fördel om processmålen skulle vara beskrivna och vilken är den i så fall?
R: Det är i så fall tidsbesparingen
H: För er del eller?
R: Ja, det är det ju. Sen säger det en hel del om företaget som sådant, tycker jag att om man gjort den här läxan att dokumentera sina processer. Det säger att de vill ha ordning och reda, man vill ha saker och ting på plats, man tycker det är viktigt med dokumentation vilket oftast syns när man kommer vidare in på kontinuitetsplaner och sådana bitar.
H: Mmm.
R: Processer kring säkerhetsfrågor och så, då finns de oftast också på plats.
H: Jag tänkte på det här med att man mäter och följer upp sina egna processer, alltså att man själv kontrollerar sina processer i viss utsträckning, hur ser du på det?
R: Att man gör det?
H: Ja, är det någonting ni kontrollerar att företaget mäter och följer upp sina egna processer?
R: Nej det kan jag inte säg, inte uttalat nej. Det är inte, om jag ser det utifrån, när du säger mäter, då tänker du på att man utifrån, hur effektiv man är i exempelvis leverantörsfakturahantering. Är det så du menar?
H: Ja men just att man mäter mot de processmålen man har ställt upp?
R: Mmm. Alltså finns målen uppsatta så tittar man naturligtvis på det utifrån det. Då är det liksom, det är svårt för oss att komma in och säga nä men ni bör ju mäta er mot detta istället. Utan vi utgår ju alltid från att företaget förstår sin verksamhet bäst.
H: Okej.
R: Vi är ju experter på den finansiella revisionen och hur den behandlas. Verksamheten kan de bäst själva så att säga. Det är liksom vår utgångspunkt.
H: Då tittar ni inte på roller och ansvar?
R: Jo alltså internkontrollmässigt gör vi ju det.
H: Den som hanterar vilka processer och så där?
R: Ja, det är en viktigt bit när det gäller informationssäkerhet och hur rollfördelningen ser ut att det är rätt personer som gör rätt arbetsuppgifter, göra då att det avspeglar sig i systemet och med profiler, behörighet och rättigheter och så.
H: Men det är mer för att hantera säkerhetsfrågor och så?
R: Ja, mer så ja.
H: Ja, där är det samma när det gäller de procedurer som företaget har kring sina processer antar ni att de själv på något sätt förstår sig på bäst?
R: Ja. Men det är klart, när man sedan kommer in då på den nivån, alltså hur man arbetar kan jag naturligtvis ha synpunkter för att de enskilda momenten är väldigt likartade från företag till företag.
H: Vilka moment är det du tänker på då?
R: Det kan vara hur du, ta leverantörsfakturaflödet igen som exempel, hur det ser ut och hur du har satt upp kontroller, var i processen kontrollerna finns och så vidare. Det är ju väldigt internkontrollriktat. Så där jämför vi mellan våra kunder och det är där också vi tror att kunderna förväntar sig att vi kommer med synpunkter och förbättringsförslag.
H: Ja, av de moment som vi diskuterat här, vilka tycker du är mest kritiska i förhållande till IT-styrning och varför?
R: Ja, i förhållande till just styrning av IT-verksamheten tycker jag framför allt, det är egentligen att man har system som stödjer verksamhetens övergripande mål, att man har tänkt till där. Man sätter ju ofta upp strategier, det är exempelvis marknadsföringsstrategier, vi ska nå dem och dem målen detta året och nästa år och så vidare. Ofta men inte alltid så spiller det över och innebär att vi måste göra någonting på systemsidan och så vidare. Det är inte alltid man får det med sig. Just det systemstödet kontra verksamheten är faktiskt en av de viktigaste bitarna när det gäller IT-stryning och IT-verksamhet.
H: Det som du var inne på lite innan att systemen ska stödja…
R: Ja precis och att man har tänkt igenom hur man har organiserat. Vi ser gärna att IT ska vara en stödorganisation, det ska finnas en kund-leverantörsförhållande mellan IT och den övriga verksamheten.
S: Upplever du där när du tittar på dessa bitar att det finns någon form av glapp mellan IT och verksamheten, du pratade om verksamheten mål där, att de inte är överrensstämmande…

R: Ja alltså det är ju, det varierar väldigt mycket, det kan det göra. Jag tycker väl kanske att det blir mindre och mindre vanligt att IT-avdelningen lever sitt eget liv som man ofta såg förr att de skötte sig själva. Intresset för verksamheten ökar mycket bland IT-chefer idag samtidigt som intresset för IT ökar på verksamhetssidan så man håller väl på att mötas där. Men lik förbaskat ser man ofta att verksamheten inte ställt tillräckliga krav på IT-verksamheten. Det är ändå fortfartande många gång som man märker att saker och ting faller mellan stolarna, enkelt exempel, verksamheten säger att ni ska ta backup och säkerhetskopiera men svarar inte på frågan vad, hur ofta, hur mycket data kan vi tillåta oss att riskera att tappa och så vidare, hur många generationer ska sparas, sådant saknas oftast. Då står IT-avdelningen där och måste själva fundera ut det och då kan det hända att det blir problem när det väl smäller.
H: Men det här att du ser IT som en stödorganisation mot verksamheten och så berättar du att IT får mer och mer insikt i verksamheten och vice versa…
R: Mmm
H: Tycker inte det på två olika saker, alltså att IT är mer än ett stöd, att IT är involverat mycket mer i organisationen?
R: Ja men för att kunna ge ett bra stöd så måste de ju förstå vad företaget sysslar med. Så är det ju.
H: Mmm, jag bara tänkte att man går förbi det här att se IT bara som ett stöd kanske…att de är likvärdiga verksamheten på något sätt att man ser IT som en stor roll i verksamheten…
R: Alltså så länge man har rollfördelningen klart för sig, och bemannar olika roller så som systemägare och den här typen på rätt sätt, att den rollen finns tydligt i verksamheten, att det är ekonomi som äger ekonomisystemet och så vidare, så tror jag inte att det är någon större fara faktiskt. Det är alltså gränsdragningen där emellan som är viktig.
H: Lite om säkerställande av systemsäkerhet då. Vad tycker du är syftet med är säkerställa företagets säkerhetsrutiner?
R: Mmm, det är ju egentligen så att, om vi säger systemsäkerhet eller menar vi informationssäkerhet i allmänhet?
H: Jaa…alltså det blir väl det som krets runt system…
R: Ja det går ju ofta ihop så som vi ser det men systemen finns ju till för att kunna leverera rätt information i rätt tid till rätt mottagare och den ska då vara skyddad för obehörig åtkomst och det där är ju, syftet är ju egentligen att man när de målen, att man helt enkelt har en god intern kontroll kring systemen och den information som finns lagrad i den. Vi tänker väldigt mycket informationssäkerhet egentligen. Och det är ju egentligen en gränsdraning där för vi jobbar just sällan djupt inne i systemen och tittar på hur man praktiskt hanterar vissa intern kontrollfrågor i systemet utan det är ju mycket rutinerna runtomkring. Att man har kontroll av hanteringen är det vi jobbar med.
H: Företagets interna kontroller kring systemsäkerheten?
R: Ja precis.
H: Vilka moment gällande den här granskningen tycker du att företag bör fokusera på?
R: Av säkerhetsgranskning?
H: Ja.
R: Man kan säga att de två absolut, där vi brukar lägga ner mest krut är ju åtkomstkontroller och loggning av olika händelser i systemet, spårbarhet.
H: Är det som ni fokuserar på eller som företaget bör fokusera på?
R: Det är som vi fokuserar på och jag tycker att det är någonting som företagen också bör fokusera på, vilket de inte alltid gör. Framförallt logging brukar vara lite bristande. Behöver man utreda en fråga eller på något sätt spåra en viss transaktion så är det ju en förutsättning att det finns. Man väljer ofta bort det för att det är många extra transaktioner som ska lagras och det tar mycket plats och så. Men det tycker jag är viktigt, sen tycker jag också att det är viktigt med hanteringen av förändringar i systemet.
H: Kodmässigt då eller?
R: Ja både kodmässigt men inte bara, många system kan idag genom att man ändrar vissa konfigurationer bete sig helt annorlunda och det kanske kan man inte vill. Ofta är dessa parametrar och styrtabeller väldigt lätta att ändra och sker av misstag och kan få konsekvenser som är oönskade.
S: Kommer ni ofta in när företag anskaffat ett nytt system eller gjort några ändringar, kommer ni in då och tittar på det?
R: Det händer att vi är med i samband med att man inför nya system och stöttar företaget med rådgivning på olika sätt. Det har blivit vanligare och vanligare de sista åren. Det är för att just det här med intern kontroll är gärna något vi kollar.
S: Ja, för att vi pratade om det här tidigare att man har system som säkerställer verksamhetens mål och att ni kommer in där och säkerställer det på ett tidigt stadium…
R: Det händer ju att man får hjälpa till att göra kravspecifikationer också till exempel och deltar i den processen.
H: Ja och där svarade du lite på, eller…hur man praktiskt kan jobba med dessa moment tänkte vi också fråga.

R: Det är ju samma sak där egentligen, i första hand intervjuer och att man kartlägger, hur ser det ut, hur jobbar ni, vad finns det för dokumentation för processerna kring behörighetsadministration till exempel, change management och så vidare. Så försöker man identifiera kontroller i de här beskrivningarna, kontrollpunkter så att säga och sen tar man stickprov helt enkelt, granskar och ser om man har dokumentareat förändringen på ett vättidgt sätt, har man signat av testerna, är det godkänt och imnplementerat.
H: Så ni lokaliserar rutinerna och sen testar ni om de stämmer?
R: Ja…inte alltid, det beror på vad det är för scope på jobbet så att säga.
H: Är det ofta en begränsning med tid och resurs?
R: Javisst.
H: Känner du att du hade kunnat göra mycket mer…
R: Ja…
H: Vilka delar hade ni kunnat jobba mer med?
R: Vi kan hjälpa till väldigt mycket när det gäller segregation of duties, profiler, rättigheter och den biten och undvika säkerhetskonflikter att vissa användare får göra lite för mycket än vad man borde och så vidare.
H: Okej, åtkomst, behörigheter och den biten alltså?
R: Ja…
H: Så det är det största bekymret?
R: Jag tycker att det är ett bekymmer för att man ofta måste lägga det åt sidan och det tar ganska mycket tid att komma igenom det. Man måste nästan komma till kunden och säga att man gärna skulle vilja hjälpa er med det här men det är också ett litet extrauppdrag så att säga. Men tidsramar och sådant lever vi ju alltid med. Man får försöka hitta det mest väsentliga ganska tidigt så att säga.
H: Hur gör ni det då tycker du?
R: det baseras ju på erfarenhet, det märker man. När man gjort några granskningar så vet man ungefär, ofta så känner man, lite kaxigt kanske, ungefär vad man ska skriva i rapporten innan man går till kunden så att säga.
H: Magkänslan eller?
R: Ja, lite magkänsla, sen är det ju om man ska vara riktigt ärlig nästan alltid samma saker som brister…
H: Det här med change management som vi pratade om innan, av vilken anledning tycker du att det är viktigt?
R: Det är just för att systemstödet ska fungera på ett bra sätt och att du inte gör ändringar, det kan vara rapporter du tar fram, sådana enkla saker, du måste vara säker på att den rapporten verkligen levererar rätt information, att du inte missar data och just för att säkerställa att den output som kommer från systemet är rätt och riktig.
H: Den outputen som kan användas vid beslutsfattande helt enkelt?
R: För beslut ja och likaså är det väsentligt när du ska byta release, det finns ju företag som gjort så mycket anpassningar i sina system att de inte kan göra en uppdatering av sitt system utan det handlar om att vi får reimplementera hela installationen för att det är så specifikt genomfört och man har släppt för mycket och har man då inte dokumentation på vad man har gjort så är det hopplöst.
H: Så det är mer ur ett systemutvecklingsperspektiv?
R: Ja det är det ju, det spar ju kostnader och håller sig till standarder så långt som möjligt.
S: Ska vi ta nästa område eller tema.
R: Mmm
S: IT: s bidrag till verksamheten då. På vilket sätt kan IT-revisorn bidra till att IT: s värde förmedlas inom organisationen.
R: Framförallt genom att rapportera våra iakttagelser till rätt person. Med rätt person så menar jag att det ska upp på företagsledningens bord. Det är inte alltid som IT-chefen i en verksamhet är representerad i företagsledningen, alltså sitter med i ledningsgruppen. Det varierar. Ofta är det fortfarande ekonomichefen, eller någon administrativ chef som samtidigt har IT under sitt ansvarsområde. Därför är det viktigt att vi rapporterar till de som sitter i ledningsgruppen, alltså de som kan hantera frågorna på rätt sätt. Det tror jag är det absolut viktigaste. Sen är det ju givetvis, vi ser ju många företag och vi jämför ju naturligtvis våra kunder sinsemellan och kan på så sätt förmedla vad vi tycker är bra på vissa ställen.
S: Hur hanterar ni den här rapporteringen, om ni kommer ut till ett företag och ni inte får rapportera till vem ni tycker är rätt person. Hur hanterar ni det, säger ni till att ni behöver lyfta upp det här högre?
R: I vårt fall här på Företag A så jobbar vi hand i hand med revisorerna som har en direktingång till ekonomichefer och företagsledningen på ett annat sätt och kommer inte rapporten dit så ser de till att den hamnar på rätt ställe. Det tas oftast med då, i den vanliga revisionsrapporteringen. Men sen kan det ju också vara så att det är en IT-chef som beställt jobbet och kanske vill ha någonting belyst i organisationen i allmänhet och då är det ju han som är mottagare av rapporten.
H: Så det beror på syftet?

R: Ja det beror på syftet.
H: Det här med att en IT-chef gör beställningen, vad brukar hans syfte med det vara, vad vill han få ut av det?
R: Det kan vara att skapa underlag för olika förbättringar och framtida projekt. Kanske stämma av sin egen bild av hur saker och ting ser ut och få en second opinion till exempel.
H: Handlar det om rutiner?
R: Det kan handla om rutiner, behörighetsstrukturer. Ibland går man in och göra analyser av data, att man går in och extraherar data och analyserar lite sidoordnad då med separata verktyg. Det varierar ju.
H: Ja tänkte på det du sa innan, att era iakttagelser ska komma till rätt person, tänkte på rapporteringsväger så här, allmänt gällande information och rutiner, är det något som ni tittar på?
R: Alltså hur rapporteringsvägarna ser ut där?
H: Ja precis…
R: Ja det gör vi väl indirekt. Jo, i ett tidigt stadium så brukar vi försöka se hur organisationen ser ut och vem som rapporterar till vem, det är ju ofta rätt väsentligt att förstå. Det är det.
H: Ja, just det är med, kan ni kanske se IT skulle kunna belysas på ett annat sätt, som rapporteringsmedel. Just det du säger att IT-chefen inte alltid sitter med i ledningen, att IT förs upp på bordet. Är det något ni kan hjälpa till med?
R: Jo absolut, det skulle man kunna. Det hade blivit en del i vår rapport, det är klart att vi skulle kunna hjälpa till med det.
H: Har ni gjort det någon gång?
R: Nja, indirekt har man väl fått med det genom bättre fokus och visst, våra rapporter har varit en ögonöppnare många gånger för personer i olika företag och märker att det har direkt medfört vissa åtgärder och medvetenhet för att göra förbättringar.
H: Hur kan en sådan rapport se ut, är den väldigt formell? Jag tänkte på den här revisionsberättelsen, är det den som er rapport utmynnar i?
R: Skriver vi en rapport så gör vi först en samlad bedömning, hur tycker vi det här fungerar, bra, halvdåligt eller skitkasst eller så. En sammanfattning helt enkelt. Sen redogör vi för de punkter vi har, de findings och de brister vi har noterat och lämnar då förslag på hur man möjligt kan göra förbättringar för att kunden ska få ett mervärde av rapporten. Revisionsberättelsen som ni såg häromkvällen är ju ganska torftig, fan det är ju ingen som läser den, den bara finns där.
H: Ja precis, den kan ju inte betyda så mycket i praktiken?
R: Nej den gör ju inte det. Det är ju en kvittens på att detta är hyfsat okej.
H: Mer praktiskt skulle de kunna använda den dokumentationen ni har…
R: Ja, skriver vi en rapport är det ju vår avsikt att den ska komma till företaget och vi vill gärna att de jobbar med den naturligtvis för att kunna ge ett mervärde.
H: Oavsätt, de blir godkända, eller har ni någon…Det är inte det revisionen går ut på, att få något certifikat?
R: Nej så funkar det inte riktigt. Inte i det sammanhanget, nu gör ju inte vi det men jag antar att om man gör en revision utifrån iso-standard så är det ju en annan sak va. Då har du ett antal mål som du ska nå, då har du en certifiering, en iso-certifiering som mål, ett antal krav som du måste uppfylla va.
H: Jaa…vad tycker du syftet med er revision är?
R: Alltså i huvudsak så är syftet med vår revision att, vi finns ju på FÖRETAG A för att vi ska stödja med specialistkompetens kring finansiella system.
H: Okej, så att ni ska hjälpa kunden i de avseendena?
R: Ja, och revisorerna…för att ge dem den specialistkompetens de kan tänkas behöva för sitt arbete.
H: Jaha, okej ni hjälper alltså dem att förstå vissa delar av…
R: Ja absolut, det händer ju att vi…vi brukar säga att vi har olika kunder. En kund kan ju vara våra revisorer här, sen kan man ha kunder direkt som anlitar oss för olika uppdrag. Det är ju också så att när det är revisorerna som vill att vi gör någonting så går vi in i revisionsteamet och kanske inte ens skriver en separat rapport och det arbete vi gjort utan det är liksom…vi lämnar synpunkterna åt våra revisorer och sen tar de hand om det. Det beror på.
H: Okej, jag bara tänkte att det aldrig ställs några ordentliga krav på företaget utan det blir mer uppmaningar om det inte kommer från era kollegor så att säga då?
R: Alltså, det blir ju en uppmaning, det är ju inte så att vi kan sänka verksamheten eller hur vi ska uttrycka det. Det är samma sak när, jaa, iso, följer man inte kraven blir det underkänt och följden blir att vi inte blir certifierade. Likadant har vi Sarbanes-Oxley-regelverket då för intern kontroll, jag vet inte om ni känner till den?
H, S: Jo.
R: Det är ju samma sak där, där granskar man ju faktiskt den interna kontrollen och uttalar sig om det i de företagen och brister det, ja då är det ju fail på det så att säga och då blir det ju synligt på ett annat sätt men i företag där vi har vår vanliga revision där blir det inte lika tydligt. Utan det blir ju på något sätt en del i bedömningen och det är klart

att man kan hota med att om ni inte sätter det är på plats så måste vi göra mer och mer åtgärder och djupare och djupare stickprov och det kostar mer pengar och det blir dyrt för er. Men det är ju sällan vårt arbete medför en oren revisionsberättelse.
H: Ser du något problem i det, att ni inte kan ställa så pass höga krav?
R: Nej…alltså det är klart att det kan vara tröttsamt om man kommer till en kund och så ser man vissa brister ett år och så kommer man tillbaka nästa år och så är det samma skit igen. Då är det ju rätt trist. Kunde man ju önska att man kunde sparka de lite i häcken så att de jobbar och gör förbättringar, det är ju rätt meningslöst att komma dit och skriva samma rapport igen. Det har ju hänt, år ett så gör man en ganska djup genomgång och har ett antal findings sen år två är man tillbaka och vill vara lite effektiv och går igenom rapporterna för vad som är gjort, vad har ni åtgärdat och så säger de att de inte gjort ett skit så du kan skicka samma rapport igen.
H: Ja det är ju svårt då.
R: Ja men då har man å andra sidan kanske inte nått fram på ett bra sätt. Eller så har de inte tid eller har mycket annat för sig. Det finns tusen och en skäl till det.
H: Ni skulle gärna vilja få med det här med att stärka bidraget från IT?
R: Ja absolut.
H: Och sen är det lite upp till dem om de tar den chansen?
R: Ja, så är det ju. Det är klart det kommer ju, intern kontroll är ju fokus idag på ett annat sätt än vad det var för kanske tio år sedan.
H: Så du menar då att det redan blivit bättre?
R: Ja, alltså det blir ju bättre. Börjar man med att skriva rapporter och de hamnar på rätt ställe och ed börjar läsa, det brukar sås ett frö då och att man vill bli bättre helt enkelt.
H: Ja, alltså att man ser att man själva kan få ut någonting utan detta?
R: Ja precis, det är ju helt och hållet beroende på företagets ambitioner och vilja, vilken division de vill spela i så att säga.
H: Har ni mycket kontakt med IT-chefen på företaget?
R: Ja det är primärt de vi har kontakt med faktiskt.
H: Är det stor skillnad på hans ambitioner och ert arbete?
R: Ja, eller det varierar, han har ju sin agenda. Det beror ju liksom på hur pass mogna de är i verksamheten men det är ju sällan så att de inte bryr sig. Jag tror ändå att det finns ett medvetande här…
H: En önskan att bli bättre?
R: Ja…man förstår ju bristerna, det räcker ju med att läsa Computer Sweden dagligen, det finns risker och det händer grejer hela tiden så det gäller att ha koll på läget.
S: Ja du pratade ju om IT: s värde i en organisation och om hur IT-revisorer kan bidra där, är det en viktig del och i så fall på vilket sätt är det viktigt?
R: Ja anser att det är viktigt att mitt arbete bidrar till min kunds utveckling av verksamheten, annars blir det ju rätt trist att jobba. Det här med att vara revisor kan vara lite speciellt, jag brukar vilja säga att jag vill jobba konsultativt som revisor, vi går in och gör granskningar och hitta lite punkter på vad de kan bli bättre på och gör inte så här, gör så. Då känns det bra och absolut roligast är ju när man ser att kunden verkligen jobbar med våra synpunkter.
H: Så det handlar lite om viljan att ta emot ert arbete
R: Ja det är det, man måste ju vara säljande som revisor och ha en bra approach
H: Så det är mer som ett försäljningsjobb det här?
R: Nja, lite är det…man måste ju vara smidig va.
S: Nästa då här, hur kan IT-revisorn kontrollera att IT: s bidrag till verksamheten blir synbart för hela organisationen? Kan ni kontrollera det på något sätt? Vi pratade lite innan om att rapporteringen bör nå rätt personer.
R: Ja…då är man lite inne på, vad får vi för de pengarna som IT-avdelningen kostar egentligen. Blir synbart…ja…
H: Om man till exempel tänker på prestandautvärdering, att ni kontrollerar att det följs upp
R: Normalt sätt. Vi kanske tittar på det fast ur andra aspekter då. Det kan vara ett sätt för oss att se, hur tillförlitliga är systemen egentligen, hur mycket upptid har man och så va, man får göra en bedömning men vårt syfte är ju inte riktigt då att se till att det blir synbart för hela organisationen. Det ligger lite långt ifrån normalt sätt.
H: Ja…de moment som vi diskuterat kring IT-styrning, vilka tycker du är mest kritiska?
R: Du menar genom IT: s bidrag till verksamheten?
H: Ja precis, att man får med sig IT: s bidrag till verksamheten.
R: Mmm…Det gäller ju då att utifrån det här kund och leverantörsförhållandet hitta KPI:er som man kanske kan följa och som man möjligen kan publicera på intranätet eller på något annat bra sätt och framförallt så tror jag att det är viktigt för IT att göra sig synliga i verksamheten, berätta om problem som uppstått och varför de har uppstått. Vi fick in virus nu och det var antagligen genom USB-minne så vi påminner nu om att…

H: Men inte bara nersidan kanske, vad som IT verkligen bidrar med tror jag är något som sällan lyfts fram…
R: Ja men det håller jag verkligen med om, det är ju svårt att mäta, vad ska vi ta som exempel, vi behöver en applikation för de och de….Javisst, du kanske gör någon form av kalkyl som säger att om vi gör den här investeringen för så och så många miljoner så sparar vi si och så mycket men om det följs upp alltså det har jag svårt att uttala sig om.
H: Ja, men man får den här uppfattningen lite att IT bara ses som problemet, när det uppstår problem, men man ser aldrig den goda biten av kakan så att säga.
R: Nej det har du säkert rätt i.
H: Det är lite som du säger här, att kanske göra IT synligt i verksamheten men även för de bra sidorna.
R: Ja, det tror jag och det handlar ju då liksom att jobba med saker där användarna ute i verksamheten verkligen upplever förbättringar.
H: Ja, kan ni bidra till det på något sätt?
R: Nja, där är vi kanske lite långt ifrån tror jag.
H: En annan sak du sa här innan var att ni ser till att rätt person får den här informationen med iakttagelserna.
R: Ja själva rapporteringen ja…
H: Det kanske är den viktigaste biten?
R: Det är den viktigaste biten absolut ja, en bra skriven rapport är liksom kärnan i det hela va. Pedagogiskt uppbyggd som ger en förklaring till varför vi tycker som vi tycker. Det är absolut vårt viktigaste bidrag som kunden kan jobba vidare med.
H: Okej, då går vi över till interna kontroller som är ett ganska brett område men om du försöker tänka på vilket syfte företagets interna kontroller har.
R: Sett ur vårt perspektiv som finansiella revisorer så handlar det om att säkerställa en korrekt finansiell rapportering men det kan ju också vara att förhindra bedrägerier, obehörigt nyttjande av företagets tillgångar och intern kontroll är också ett sätt att upprätthålla sin image. Det är ju inte bara de här hårda grejerna utan det handlar ju till exempel om att…för Ikeas del är det väsentligt att man inte utnyttjar barnarbetare, att man har kontroller över det och att det finns processer som säkerställer det att den här underleverantören ska vara schyst och följa lagar, så intern kontroll är ju ett oerhört vitt begrepp. Syftet generellt är ju att det är en verksamhet som fungerar schyst, det här fungerar bra.
S: Vi pratar då om att fungera bra, vad anser du att bra intern kontroll kan ge för effekt för företaget?
R: Bättre image, ha kontroll över dina flöden så är det inte det att du får påminnelser från leverantörer, blir känd som en god betalare, fakturerar i tid, levererar i tid, levererar rätt saker, alltså allting hänger ihop med intern kontroll som jag ser det.
S: Högre effektivitet överlag skulle man kanske kunna säga?
R: Mmm, det kan man säga.
H: Och att systemen levererar de som de är tilltänkta att göra kanske?
R: Precis, och rätt information i rätt tid.
H: Ja, hur kan ni kontrollera eller granska de här interna kontrollerna?
R: Ja…generellt sätt så sker stickprov och intervjuer, det är samma sätt. Internkontroll i en viss process, man intervjuar, hittar kontrollerna och så går man in och tar stickprov. Det kan ju hända att man använder verktyg, vi har ett Sekchek heter det som vi använder för att granska säkerhetsinställningar i en windowsserver till exempel, det funkar för AS400- och Unixmiljöer också. Det är ett ganska effektivt sätt för då får man ut inställningar och hur de ser ut och man kan ganska snabbt stämma av att det som är sagt vid intervjuerna stämmer eller inte va.
H: Ja precis, det var det jag tänkte lite på innan. Hur man kontrollerar det.
R: Hur man verifierar ja, man kan också gå och kollar hos någon annan och göra en kompletterande intervju eller ber att få titta på hur det ser ut. Hur passwordpolicyn ser ut, så det är mycket stickprov.
H: Ja, okej. Det här du pratade om KPI innan, i vilka fall kommer det in i bilden?
R: I samband med intern kontroll?
H: Ja, jag tänkte om det är någonting där som ni jobbar aktivt med?
R: Nej det är det väl inte, om vi tittar på företagens nyckeltal, KPI:er , så är det mest för att göra en bedömning men det är sällan det används för att verifiera interna kontroller. Det blir lite långsökt.
H: Okej, jag menar att det finns redan uppställda mål och KPI från företaget?
R: Det kan det finnas. Det är klart, det är kanske inte just den typen av kontroller man tänker på men att mäta upptiden, antal ärenden i helpdesk och så. De kontroller vi testar kanske är behörighetskontroller och så.
H: Vi vet att interna kontroller är ett väldigt vitt begrepp för både er och oss men vilka moment gällande det tycker du är mest kritiskt?
R: Det är åtkomstkontroller och ändringshantering tror jag är det som vi lyfter fram mest i våra granskningar sen är det naturligtvis viktigt också att du har kontinuiteten, kontroll på backuper, planer för det, att det finns åtgärdsplaner

om någonting skulle hända. Systemutveckling är det inte många som sysslar med internt så att säga. *Respondenten svarar i telefon*
H: Ja var var vi…
S: Du pratade om åtkomstkontroller, change management
R: Ja…
H: Det var kanske det?
R: Ja, det är ju mycket där det kretsar, det är det ju absolut.
S: Okej, vi går vidare till nästa område då, externa krav. På vilket sätt kan IT-revisorn kontrollera att företag tillmötesgår de externa krav de omges av? Och är det något ni jobbar med.
R: Hmm, externa krav…
S: Du nämnde SOX här innan, men det är kanske inget ni jobbar så mycket med?
R: Jo det händer och då är det ju, då finns det ju någon form av god sed, vad ska man nå, och cobit och de här bitarna som ligger bakom och som man då granskar emot. Det gör man helt enkelt genom att testa av, man får identifiera de krav som finns och så får man granska och se hur de möter upp till de kraven helt enkelt.
S: Just Cobit när ni jobbar mot det, kontroller som finns i Cobit, är det dem ni granskar det emot så att säga?
R: Ja, det kan man väl säga. Så är det…Det är mycket, nästan alla, både FÖRETAG A-interna checklistor och frågelistor, att tänka på sådär, nästan allting bygger ju på Cobit idag va, det finns ju i bakgrunden och COSO då för övrig intern kontroll. Det är lite av samma typ av sak.
H: Ja vad är det för typ av checklistor ni har med er ut?
R: Vi har ju, det är egentligen egenproducerat faktiskt. Man har någonting i grunden i våran revisionsmanual som man utgår ifrån där det finns vissa mål som man anser att man bör nå, sen så har vi fyllt på själva med frågelistor baserade på våra erfarenheter som vi efterhand jobbat med.
H: Så någon form av egenproducerade checklistor?
R: Ja…
H: Ja det är bra
R: Absolut…det är ju någonting man förbättrar ständigt va. Naturligtvis finns det andra standardiserade checklistor och så men det använder man mer som en åtgärdsbank och så för att du kanske inte kan granska allt och ofta är det så att det kommer ut som en del i den finansiella revisionen och då har man ju begränsiningar när det gäller tid och pengar och det gäller att skjuta in sig på det som man bedömer som det absolut viktigaste. Och det är klart, då kan man ju inte titta på alla kontrollmål gentemot Cobit till exempel.
H: Nej, så det är tid som avgör det?
R: Ja det är det…så då får man försöka hitta det viktigaste men sen är det ju inte alla som veta vad Cobit är överhuvudtaget.
H: Om man tittar på Cobit, vilka områden anser du vara de viktigaste eller ligger närmast tilhands?
S: Om man tittar på de fyra stora domänerna till exempel, är där någon som du anser vara viktigast i ert arbete?
R: Nej egentligen inte, på något sätt så är hela processen viktig. Det tycker jag. Men åter igen, det är ju det med åtkomsten man skjuter in sig på i allmänhet.
H: Men det är väl dokumenterat i Cobit också?
R: Ja, det finns.
S: Men då är det kanske delivery and support som blir viktigast i Cobit?
R: Ja…det blir det väl.
S: Vilka vägar informationen tar så att säga.
H: Ja…gällande extern kravhantering, vilka är de viktigaste faktorerna att jobba med för er?
R: Extern kravhantering, ja…
H: Det kanske inte finns några uttalade?
R: Nej…vad ska man säga…vi måste naturligtvis fånga upp de krav där vi själva riskerar att bli utsatta. Men jag menar i ett SOX-uppdrag måste man följa det och det måste få kosta och det är alldeles för hög risk att missa någonting.
S: Jag bara tänkte på att du nämnde ansvarsskyldig här va? Du pratade om att fånga upp kraven. Ni kunde bli ansvarsskyldiga, är det något ni tittar på även hos företagen, vem som är ansvarsskyldiga där?
R: Ja det ingår ju som en del i vad vi kallar förvaltningsrevision och på något sätt se till att de följer lagar och regler för verksamheten som helhet så att det finns ju med hela vägen.
H: Det här, nu kom jag att tänka på en grej du sa i början på intervjun här. Det här med processägare, det tittar ni på via interna kontroller. Hur fungerar det rent praktiskt? Hur lokaliserar ni det?
R: Vem som är processägare?
H: Ja…och varför kanske just den personen är det?

R: Det är inte alltid den personen man pratar med, det är inte alltid det finns processägare.
H: Vad är fördelen med att det finns det i de fallen?
R: Om det finns och hanteras på rätt sätt så känner man att det finns någon som tar ett ansvar för processen och dokumentationen av densamma. Att det är någon som ser till att det blir gjort får man förmoda.
H: Så det är åter igen det här med att se till att systemet stödjer processerna? Att det blir ett steg närmre en bättre hantering av processerna?
R: Ja, precis. Det är uppgifter som processägare och systemägare också att man ser att någonting fungerar på ett tokigt sätt och att det här borde man kunna göra på ett bättre sätt, komma med förslag på förbättringsåtgärder, komma med beställningar, vi vill göra så här och göra den anpassningen och att det då hanteras i företaget.
H: Ja…lite om kontroller och organisationsstruktur.
R: Ja
H: Anser Du det vara viktigt för en IT-revisor att granska organisationsstrukturen för kontroller och beslutsfattande?
R: Ja, det är ju en del av kontrollarbetet och är oerhört viktigt. Man kan väl säga att det som är vanligt idag just för ett sätt att möta det här gränslandet mellan verksamheten och IT är något man kallar för IT-råd eller IT-styrgrupp finns också ofta på den nivån. Där det finns representanter dels från IT och dels från verksamheten, IT-chefen är med och den som ansvarar för IT i ledningsgruppen finns med, systemägare, processägare, de som är lite så. Ofta fungerar det ganska bra där man har ett forum för att hantera gränslandet så att säga.
H: Så det är syftet, att det inte ska hamna mellan stolarna?
R: Ja precis, att du täcker upp och fångar upp de frågeställningar som finns. Det händer ju att det finns bristande kommunikationsvägar och det finns någon användare som vill ha en förbättring gjort i systemet och de vet inte vart de ska vända sig, då är det svårt att få det gjort också.
H: Så det här med bristande kommunikationsvägar, bara som ett exempel då, kan ni lokalisera dem och…indikera på förbättringar?
R: Det är klart att vi kan göra det…det är inte ovanligt att man möter verksamheter där IT har koll på produktionsstyrningssystem och många sådana bitar men sen när man kommer till ekonomin och hur finansiella system hanteras, ah det sköter de själva, det har vi ingen aning om hur det hanteras.
H: Mmm, vad kan era förslag innebära i så fall?
R: Kan innebär förbättrad intern kontrollmiljö, struktur, styrning av den finansiella informationen.
H: Men just det här med att koppla in IT, det ingår där kanske?
R: Ja.
H: Det här med styrgrupp, om det inte finns, det är inget ni rekommenderar?
R: Nej inte konkret, men det skulle man mycket väl kunna göra om man känner att det är lägligt. Det beror lite på vad det är för person man möter, är det någon man känner som behöver mycket hjälp i sitt arbete, så kan man rekommendera. Det är så individuellt men visst skulle vi kunna rekommendera det om vi känner att det är på plats.
H: Just som en faktor i det här med organisationsstrukturen?
R: Ja absolut…Det finns företag där man har utsett systemägare och jättefina beskrivningar av saker och ting men frågar man sedan en person som är utsedd så har de egentligen ingen aning om vad det innebär. Det handlar egentligen väldigt mycket om att syna korten i vårt jobb kan man säga, komma bakom det på olika sätt och se.
H: Är det vanligt att fasaden utåt sätt ser bra ut?
R: Javisst, jättevanligt.
H: Det gnistrar om det nästan men sen när man kommer in bakom…
R: Ja…lite sprickor här och var.
S: Nästa område då, risker och riskhantering. Hur tycker du att IT-risker och IT-policys bör granskas då i relation till följande områden, vi har delat in det i fyra olika områden här: Först klassificering av risker, hur bör det hanteras? Är det något ni arbetar när ni kommer ut, att ni försöker klassificera risker, prioriterar, kanske rangordnar?
R: Jo det är klart, det gör man ju indirekt. Alltså riskerna är ju viktiga i perspektivet vilka kontroller behövs och internkontroll finns ju mycket till för att hantera risker också…så visst gör vi det.
H: Men om du istället berättar lite fritt kring hur ni jobbar med riskhantering om ni jobbar med det vill säga?
R: Det primära är ju att se till att företaget har sina egna riskanalyser och riskhantering, att de har tänkt igenom det, vi går det ju inte åt dem. Det är ju mer att de, okej vilka risker har vi, vad ska vi göra för att minimera dem, vilka åtgärder behövs…det varierar väldigt mycket, det är sällan det är gjort på ett bra sätt faktiskt.
H: Ja…vad kan ni hjälpa till med där?
R: Vi kan ju i så fall ge viss vägledning om hur man bör arbeta med det. Vi upprättar ju inte då riskanalyser, det gör vi ju inte.
H: Men det är alltså likadant där att ni kan gå in och ge stöd och input för hur de bör hantera det?
R: Ja.

H: Hur tycker du att det bör hanteras då, är det viktigt med strukturen, att man har en tydlig hantering för det?
R: Ja…alltså framförallt tycker jag att det är viktigt att man kokar ner det till att man har en risk och konsekvensen av att det inträffar, kontra sannolikheten då att den ska inträffa och att du sen anpassar dina skyddsåtgärder efter det. Det är på något sätt kontentan av det hela. Utan en riskanalys tycker inte jag att man kan göra en ordentligt kontinuitetsplan, du måste ju veta vad det är du ska skydda och vad det ska få kosta.
H: Är där några specifika hjälpmedel ni har för att hantera det här?
R: Nej det kan jag inte påstå. Det är vårt eget huvud. Vi jobbar ju inte så aktivt med just den biten så det är väldigt fokuserat kring de kontroller som finns.
H: Det är inga sådana interna checklistor här då?
R: Nej inte just kring risker specifikt.
H: Och de moment du anser vara mest kritiska?
R: Det är väl att de överhuvudtaget tänker igenom sina risker. Har man gjort det så tycker jag nog att man komma ganska långt baserat på vad vi har sett. Det är ju inte det att det inte finns kontroller men man har väl kanske inte gjort det i rätt ordning utan inför kontroller för att det är nog bra att ha. Ibland kan man till och med göra onödiga saker…det förekommer det med.
H: Ja det var nog den sista frågan angående de områdena.
S: Så bara avslutningsvis, vi har pratat lite om olika moment ni går igenom, olika faktorer då som är de viktigaste delarna i ditt arbete, alltså i själva IT-revisionen. Skulle du kunna rangordna dessa faktorer på något sätt i relation till IT-styrning? Bara för att hjälpa dig på vägen, vi har pratat en del om bland annat rapporteringsvägar, och att ni tittar på processmål och att systemen stödjer verksamhetens mål.
R: Ja egentligen så tycker jag att det viktigaste att man har identifierat systemstöd som stödjer verksamheten på ett bra sätt, det är ju steg ett på något sätt. Sen är det viktigt att man organiserar sin IT-verksamhet och att man får en länk mellan verksamhet och IT-avdelning, det är nog prioritet nummer två. Sen kommer då riskanalyser, vilken skyddsnivå behöver vi.
H: Är det det här med åtkomst?
R: Ja, och även kontinuitetsplaneringen. Alltså möjligheten att ha bra segregation of duties beror väldigt mycket på hur organisationen är som helhet och det kräver att man är ett antal personer och att man fördela arbetsuppgifter på många händer och kan du inte göra det så är det omöjligt.
H: Mmm…om vi börjar med det är med organisationsstrukturen, du har kanske svarat på det redan, men varför är den så viktig tycker du?
R: Ja alltså ansvarsfördelningen, organisationer och ansvar, ansvar för olika arbetsuppgifter och fördelningen är alltså grundläggande för en bra intern kontroll.
H: Okej, och den här kontinuitetsplaneringen, kan du utveckla det lite?
R: Vad som är viktigt där?
H: Ja.
R: Det handlar om att systemen ska vara tillgängliga, att informationen ska finnas tillgänglig när man behöver den. I kontinuitetsplanen ingår alltifrån backup och säkerhetskopiering, behöver vi ha reservmiljö kanske, är vår verksamhet så kritisk och hur klarar vi driften vid ett elavbrott och hur länge klarar vi oss, en vecka, en dag eller en timme, inte alls. Vad är det för typ av information vi hanterar och är vi ett försäkringsbolag så har vi väldigt höga krav till exempel får då finns hela verksamheten i burkarna kan man säga. Likadant i bankverksamhet ställs det väldigt höga krav medan i andra verksamheter kan man ta lite större risker. I mindre företag kan kanske rent av kan ha helt manuella rutiner så att går den sönder så klarar vi oss tills vi hittar en ny. Det är mycket det som det handlar om med den planen.
S: Ja…finns det några andra områden när det gäller IT-styrning som du anser vara viktiga i ert arbete utöver det vi har diskuterat som ni på något sätt kan påverka eller bidra till gällande IT-styrningen?
R: Det vi fokuserar mycket på nu är ju egentligen att få företagsledningen involverade. Vi hade ett seminarium i fredags då för våra kunder, varför det är så viktigt för företagsledningen att bry sig om IT, bristande kontroller och vilka konsekvenser det kan få. Det skulle jag nog vilja säga, att det är nog fortfarande väldigt viktigt.
H: För att det brister?
R: Ja precis ja.
H: Det du säger nu med bristande kontroller, menar du att det ligger lite på ledningens bord att ta hänsyn till att de finns?
R: Absolut. Det är deras ansvar och ingen annans egentligen och det är som jag säger, IT-chefen kan sätta upp den maskinen där med den konfigurationen där med den storleken och den kapaciteten, ska den vara i den storleken eller lite mindre? Alltså en IT-chef kan inte jobba om han inte får krav från verksamheten framför sig, då har han liksom ingen input att göra si och så.

H: Det kanske inte är krav i detaljnivå?
R: Nej, men alltså övergripande. En inriktning, i den här verksamheten är de så specifika att det ska vara egenutvecklade system, kostar så mycket, då måste vi ha egna utvecklare kanske och så vidare. Ibland är det tvärt om, vi kör helt och hållet på standardsystem, anpassningar är förbjudna, kostar lite mindre kanske, det ska vara Windows rakt igenom. Ja alltså det finns olika inriktningar men företagsledningen måste involveras, det bara är så.
H: Vad är fördelen med det då, att den är involverad?
R: Ja det är ju alltså att det sker rapportering och att det berättas om det, nu körde vi ju seminarium i fredags, det är ju ett sätt.
H: En sak som jag fastnade lite för innan som du sa var att det är alltid samma saker som brister, vilka är de sakerna?
R: Alltså segregation of duties, där gör man aldrig sin läxa, du kan ha åtkomstkontroller, visst du har loggin, individuella konton och användare i det och så vidare, visst du har lösenord och det följer ofta best practice och så. Det är inte det som är problemet utan det är just att när du väl kommer in i systemet så kan det vara så att till exempel på en ekonomiavdelning så kan du göra allt va. Du kan fiffla i leverantörsregistret och lägga upp en fejkad leverantör, ditt eget bankkonto, så kan du lägga in en fejkad faktura och se till att den blir godkänd, körd igenom och betald till dig själv, då brister det. Det är väldigt vanligt att det är så. Det är en viktig bit, sen är det här med katastrofplanering, kontinuitetsplanering, att man inte riktigt har det på plats där. Att man inte tänker till, man kanske tycker att man gjort en jättebra lösning, en kontinuerlig spegling till en sekundär sajt som man tar bandad backup på löpande men vad händer om vi tappar en fil i den primära miljön och sen dröjer det lite för lång tid, kanske ett dygn innan vi upptäcker det, har den kopierats över och har man sen inte ett antal generationer sparade så kan man kanske inte återskapa det. Alltså att man inte riktigt tänker igenom, återigen verksamhetens krav som brister. Ofta är det de bitarna.
S: Ja, då var det allt. Då får vi tacka så väldigt mycket.
R: Tack själva.
H, S: Tack.

B2.2 Intervju Företag B

Transkribering av intervju med Respondent från företag B 3 maj 2010

S = Stefan Arnslätt
H = Hampus Karlsson
R = Respondent (Informant)

S: Ja, då börjar vi intervjun här med Respondenten från Företag B som har gått med på att vi spelar in samtalet. Och vi börjar med ett par övergripande inledande frågor. Den första då, om du vill beskriva kortfattat dina arbetsuppgifter samt din position här på Företag B?
R: Ja, jag arbetar som IT-revisor här, jag arbetar med IT-relaterade frågor i förhållande till våra kunder kan man kanske säga. Det är ju mer än bara IT-revision, det är ju även till exempel bistånd vid upphandlingar, organisation- och ledningsfrågor och så vidare. Position i organisationen, jag är väl ansvarig för IT-revisionen här på Företag B.
S: Ja. Och hur länge har du jobbat som IT-revisor och vad var det som fick dig intresserad av det området?
R: Renodlat som IT-revisor har jag jobbat sen 99. Jag började som finansiell revisor, men skarvade inom vissa bitar av IT-revisionen redan från 97. Sen har jag därefter jobbat som IT-revisor parallellt med IT-ansvar fram till 2008.
H: Vad säger du, vad är syftet med IT-revision?
R: IT-revision i den kliniska formen är ju ändå att säkerställa siffrorna som hamnar i årsredovisningen, precis som vi pratade om på seminariet. Det är ju det primära syftet ur ett finansiellt bolags inriktning, alltså en finansiell revisionsbyrås inriktning. Sen kan det ju finnas andra bitar i att man hjälper kunden, men ska vi titta kliniskt på processen så bör det ju vara där som är det primära syftet. Sen att dagen består av kanske 20-30 procent av sådana frågor och resten är andra frågor, det är en annan sak.
H: Ja, så om man tittar på revisionen ur ett perspektiv, förutom att titta på att siffrorna stämmer överens, vad är det mer då?
R: Ja det är väl i så fall kanske IT-styrning, upphandling. IT-styrning i så fall i termer av att man tittar kring regeldokument och så vidare, att man tittar kring varför inte IT bistår i processen i bolaget. Vad finns det mer för någonting? Vi har ju pratat om upphandling och...ja riskbiten kan ju vara en fråga där också. Även om den kan tycker jag ofta vara mer kopplad till revisionsspåret.
H: Men dom riskerna som är relaterade till IT borde väl vara, ligga på ditt bord så att säga?

R: Absolut. Men, jag tänker går man ut till en kund och gör en så kallad ITGC, alltså generella IT-kontroller, då ligger ju mycket av dom här riskbitarna med i dom här generella IT-kontrollsfrågorna. Sen kan det kanske bli så att man gör en djupdykning i någor projekt eller att man gör en djupdykning i någonting. Men risk hanteras ur ett styrperspektiv mestadels från det här som kallas ITGC.
H: Ja, kan du berätta lite mer om det, hur det funkar?
R: Ja, vi har ju skapat en checklista med ett par hundra frågor som handlar just om de generella IT-kontrollerna, sen är det ju långt ifrån alla som är tillämpliga på alla verksamheter. Tanken från början när jag skapade frågeformuläret var ju lite att man börjar utifrån och sen går man inåt i företaget. Så när jag kommer till parkeringen så kan du börja titta på, hur ser det fysiska skyddet ut kring lokalen, och sen så tittar du på inpassagekontroller när du kommer till receptionisten, och sen forstätter du inåt i lokalerna. Så man liksom skruvar sig neråt, så att man kan lösa många frågor på vägen, eller på vandringen.
H: Ja, så att man inte missar något där. Den här checklistan, är det som du sa att du själv har utformat eller hur har den dykt upp så att säga?
R: Allting har väl egentligen COBIT på ett eller annat vänster i bas. Men de konkreta frågorna är ju skapade själv, alltså textmässigt så.
H: Men just med vilka bitar som finns med kanske COBIT har bidragit till?
R: Ja.
H: Ja. Det här du sa innan, med den här frågan kring varför inte IT bistår i processen till bolaget, hur förhåller man sig till det?
R: Hur tänker du?
H: Vad gör man om ett sådant fall inträffar? Kommer ni med rekommendationer om hur det borde se ut?
R: Det beror ju lite på hur grava frågor det är. Är det så att man gjort en outsourcing och outsourcingen inte mappar mot organisationen då är det ju en sak, har man en intern IT-avdelning då kan det ju vara känsligare att gå in och ha åsikter. Det är den ena frågan, den andra frågan har att göra med om det är ett revisionsuppdrag eller ett konsultationsuppdrag. Man kan ju inte dra ett revisionsuppdrag hur långt som helst i konsultationen, av jävsproblem. Så svaret på din fråga är, beroende på kund.
H: Det här du säger, särskiljer ni på det, revisionsuppdrag och konsultationsuppdrag?
R: Oh ja, visst gör vi det.
H: Det finns liksom, det är ganska tydliga gränser där emellan eller?
R: Det finns någonting som heter analysmodell, i FAR. Och den får man ju titta på i så fall, om man kommer i konsultläge. Och så får man kommunicera det med uppdragshavaren. Då är det upp till hans samvete. Men det är klart att vi ger rekommendationer. Och sen är det, som jag sa, olika från bolag till bolag vad de önskar sig, och hur man kan uttrycka sig.
H: Ja, det var lite om det då. Sen går vi in här på definiera och hantera processer som är ett av de tema som vi tittar på. Och då undrar vi. Vilka moment som bör gås igenom vid en granskning av ett företags processer?
S: Alltså vilka bitar du tittar på när det gäller processer.
R: Ja...det beror ju på vad det är för granskning. Jag börjar alltid med att göra en översiktlig scanning om vi säger så, för att hitta de problemområden som finns. Och sen får man försöka beta sig igenom processerna efter hand. Och processer, det finns ju olika processer i alla företag.
S: När det gäller en sån här översiktlig scanning, vad är det vanligaste som brukar dyka upp så att säga? Vad är det du oftast brukar titta på om vi säger så?
H: När vi säger processer så menar vi då processerna som är relaterade till IT då.
R: Mmm jo, jag förstår det. Nej men i så fall är det ju, utifrån vår checklista, den här ITGC-checklistan. Där är det ju, där tittar man på processer kring nyanställning, avveckling av anställda, man tittar på backuper, ja egentligen säkerhetsprocesser, man tittar på rutinmässiga processer. Man tittar på förändringsrelaterade processer. Jag vet inte riktigt vilken nivå ni vill att jag ska gå in på.
H: Nej, men alltså framförallt där IT har som störst roll i företaget då, verksamheten. Så dom stora processerna som är relaterade till IT.
R: I så fall då den största processen mellan IT och företaget det är väl i så fall hur man anskaffar nya system, hur beslutsstödet ser ut för att skaffa nya system. Hur systemägandet ser ut, hur kravspecen ser ut och så vidare, kan jag tycka. Så det är IT som kravspecar, IT hittar problemet, kravspecar beställer, implementarar och försöker föra ut. Okej är det nya skrivare så är ju inte det nått bekymmer, men är det ett nytt affärssystem så är det ju en helt annan pilsner.
H: Alltså det här med förvaltningen av systemen, det måste ju finnas många relaterade processer, IT-relaterade processer, när det gäller förvaltningen helt enkelt? Är det någonting ni tittar på, att dom överensstämmer med

verksamhetens krav så att säga? Finns det processmål, finns det roller kopplade till processer...det här med processägande till exempel.
R: Det är klart att vi tittar på det men här är ju liksom ingen knivskarp gräns mellan vad man gör och inte gör. Det är ju ändå så att man jobbar utifrån vad man tycker är väsentligt, vad som är riskfyllt, i en revisionsprocess. Är det en konsultinggrej så kan det ju vara vad som helst. Så att om vi skiljer på konsulting och revision då är det klart att man tittar på processer. Är det någon av processerna på IT-avdelningen som man märker inte stöttar IT-avdelningen på rätt sätt, eller är det bekymmer eller är den dåligt byggd, då har man ju synpunkter på det såklart.
H: Hur går det praktiskt till, att titta på...hur vet man om de överensstämmer eller inte överensstämmer så att säga?
R: Man får intervjua sig fram till det. Ofta är det så att folk har mycket åsikter om IT. Så genom att ställa några frågor så får man rätt mycket synpunkter.
H: Är det ett säkert sätt att säkerställa...låt säga, jag antar att det finns en del dokumentation kopplat till processer, eller bör det göra kanske?
R: Det beror vilken storlek på bolag du tittar på. Tittar du på mindre bolag så är ju dokumentation ett undantagsfall, och då kan du ändå titta upp på bolag som omsätter många hundra miljoner, upp mot miljarden också...som i princip saknar dokumentation.
H: Ser du det som ett problem att dom inte har någon dokumentation på företaget?
R: Det är väl klart att det inte är bra att dom inte har dokumentation.
H: Vilka grejor är det så att säga man tjänar på att ha dokumentation?
R: Det är ju lättare för externa parter att se hur man planerat och att man har en tanke i det man gör. Det blir kanske lite för mycket ad hoc annars.
H: Just det här kanske runt IT också, att det som du säger är många som har en åsikt om IT. Om det inte finns någon dokumentation så kan det kanske också vara svårt att veta vilka delar IT bidrar till.
R: Absolut. Och det är ju också relaterat till att det finns ingen dokumentation, organisationen tycker inte att IT gör vad det ska göra, så det är ju liksom, allt det här hänger ihop i en färm klang. Det gör ju att man ibland hamnar i dom här diskussionerna. Sen är ju också frågan vad som är bäst, att ha ett dokument som inte gäller eller att inte ha något dokument alls, det är ju också en fråga.
H: Kontrollerar ni att det finns dokument på processmål, procedurer och så vidare? Tillvägagångssätt man har, fasta tillvägagångssätt. Om ni tittar ni på det, hur vet ni då att det stämmer överens med verkligheten?
R: Man kan ju testa processen. Låt säga att det är en process för nyanställning, eller en process för avveckling av den här användaren. Det enklaste, starten, är ju att man ställer frågan, till organisationen. Används det här dokumentet alltid? Nej svarar alltid organisationen. Där har man konstaterat att då funkar inte processen fullt ut. Så egentligen behöver ju jag inte gräva vidare, om jag fått svar på frågan redan. Annars kan man då gå vidare, till exempel när man tittar på anställda, ta ut data från AD:et och titta på när loggade olika användare på senast och så vidare. Och så ser man att här är någon som inte loggat på på tre, sex, tolv månader. Varför har dom inte gjort det? Jo, dom har slutat. Trots att dom i steg ett sagt att processen funkar. Så det är lite beroende på hur ärlig och öppen den man pratar med är. Och dom flesta man pratar med är ändå, säger att nej det funkar inte. Det slinker alltid emellan. Och det är samma sak i backuphänseende. Backupen brukar också alltid vara oerhört rigoröst uppsatt. Och där kan man ju kika på återläsning...man går in och kikar i backupen och ser hur där ser ut...om dom inte säger att dom har brister där. Säger dom att dom har brister så brukar jag släppa det där.
H: Du släpper det då?
R: Jamen då har dom ju sagt att dom har en brist i backupen. Då behöver inte jag gå in på det djupare. Dom känner till bristen, dom har dokumenterat att dom har en brist i backupen. Frågan är ju alltid vad syftet är med det man gör.
H: Ja, så om vi tittar på det här temat med processer lite stort då...Vilka moment eller faktorer anser du vara mest kritiska i förhållande till IT-styrning?
R: Det svåra är kan jag tycka när man skapar massa papperstigrar, som man inte använder.
S: Hur menar du då?
R: Nej, men egentligen att du precis som i ISO-handböcker...det brukar vara så att man skriver ner alla processer som finns i bolaget och så är det Olle som ansvarar för att han ska veta var pärmarna står. Och sen när det kommer en ISO-revision så tar Olle fram pärmen...det är liksom så långt man kommit...Jag tycker dock att ska man inventera någonting så ska det rimligt väl beskriva det man gör.
S: Så dokumentationen blir väldigt viktig där, att den speglar...
R: Ja, för annars blir det inte meningsfullt att ha den. Det tycker nog jag är steg ett i det hela.
H: Ja...är det vanligt att företag sätter upp mål för sina processer, och har en form av uppföljning på det? Är det någonting ni kan titta på? Att man faktiskt gör det man vill göra med en process.
R: Om man tittar på renodlade IT-processer så är det väl sällan som bolagets ledning är inblandade i dom. Tittar man på ett byte av ett affärssystem där man har satt ett mål att vi ska effektivisera verksamheten eller

lagerhanteringen eller någonting då är det ju klart att man mäter processen, den nya processens...vad ska vi säga, tillförande av mer värde. Men bolags ledning lägger ju sig sällan i processen om hur många som slutar som man har följt alla processteg i. Dom kanske tycker att det är ett bekymmer officiellt, men frågan är om de gör det officiellt.
H: Det här med att ledningen inte är så involverad i IT, ser du det som ett problem?
R: Absolut.
H: Vad är det huvudsakliga problemet med det?
R: Du får ju ett förväntningsgap mellan vad ledningen eller bolaget tror att dom får, och vad du de facto får. Det är ju ett tydligt problem, absolut.
H: Har man ingen insikt i IT så kan man inte heller ställa några...
R: Nej, det är väl den ena biten...
H: Någon press då...
R: Nej, precis. Det är ju, man byter en skrivare istället för att byta affärssystem. Man ger skrivaren till fel människa, om vi liksom är väldigt konkreta. Man springer på fel typ av PC-support och så vidare.
H: Ja, det här med rapporteringsstruktur och så, är det något ni tittar på? Eller hur tar man sig an det här problemet, att ledningen inte finns med i IT-besluten, eller IT-relaterade beslut. Är det någonting ni kan hjälpa till med?
R: Vi som revisorer, återigen om vi går tillbaks till årsredovisningsrevision...så länge IT producerar rätt siffror till årsredovisningen så spelar det ingen roll. Däremot i rapporterna, har man inte en vettig struktur med systemägande, systemförvaltande och så vidare...då brukar jag allid skriva om det i mina rapporter, att jag tycker att man bör föra ut det i organisationen. Sen är ju inte det något som kanske till syvende och sist påverkar siffrorna i årsredovisningen.
H: Men det är ändå något du brukar anmärka på så att säga?
R: Ja, jag brukar anmärka just på IT-styrningsfrågor så.
H: Så hur tittar man på det, ska det vara dokumenterat i så fall, systemägande? Vilka roller det innebär...
R: Det beror ju på hur stort företaget är, vilken typ av system det är...det kan ju vara en kravinsamlare ute i organisationen, det kan ju vara en systemägare i organisationen och så vidare...man kan ju benämna det som olika saker. Men det viktiga är ju egentligen det att systemet har en förankring i organisationen, att man...att medarbetarna i organisationen vet var dom kan analysera frågor och krav. Som sen då den här systemägaren, eller vem det nu är, eller den utsedde det brukar ju aldrig vara. Det kanske är VD som är systemägare för alla system, men att han i sin tur har delegerat detta. Ofta brukar systemägandet ligga lite högt, lite väl högt upp i organisationen. Så man har kravinsamling på lägre nivå kanske.
H: Är det för kravinsamling, tänker du på nyanskaffning av...
R: Nej, förändring, utvecklingsmässiga förändringar också. Nu pratar ju inte jag Office-program och så, utan jag pratar affärssystem kanske, rapporteringssystem. Uppdateringar i generella termer, om vi nu går tillbaks till Microsoft-världen, det rullar ju liksom bara på. Det är ju sällan man har systemägare för Microsoft-familjen.
H: Jag tänkte till affärssystem, konfigurationer och sådär.
R: Precis.
H: Ja.
R: Rapportering sa du...
H: Ja, just det ja. Är det något ni tittar på? Rapporteringsvägar och beslutsfattande och...hur det ser ut?
R: Ja, det ingår ju egentligen i den styrprocessen jag pratade om. Rapportering, ja men det får jag nog säga. Finns det tydligt definierat systemägande då finns det ju rapportering också. På ett eller annat sätt, sen kan man ju alltid diskutera om det är effektivt eller ineffektivt.
H: Men det finns kommunikation...eller hur vet man det då, att det finns kommunikationskanaler bara för att det finns ett systemägande? Som du sa så ligger systemägandet ofta lite högt upp. Det kanske inte är säkert att det fungerar trots uttalat systemägande.
R: Nej nej. Visst, absolut är det så. Nej men man får väl i så fall titta på hur man har byggt processen för ett systemägande, ett systemförvaltande och så vidare. Och i så fall får man väl...låt säga att det finns möte...att man säger att man har en process för kravinsamlingen i systemägandet. Och då får man väl titta på, hur många krav har ni samlat in? Hur ser det ut med insamlingen av krav, hur ser det ut med prioriteringslistan med krav, för att sen dra det till dom som ska utföra det och så vidare. Och sen då, vad får ni för kvittenser från IT-avdelningen. Det är ofta sånt man intervjuar sig fram till.
H: Men det är något som ni identifierar, att se hur informationen i företaget...
R: Ja, det är det. Det får man ofta fram vid intervjun och sen kan man gräva hur djupt som helst i det också.
H: Men det är en fråga om tid och resurser.
R: Ja, absolut. Visst är det så. Vi har nästan diskuterat systemägarfrågan längre här än vad man gör ute hos en kund på en IT-revision, om inte det är ett specifikt område. För ofta får man ett ja eller ett nej, och så frågar man systemägaren eller systemförvaltaren hur han har delat upp det och så får man ett snabbt svar på det. Utifrån det

svaret kan man ofta bedöma om det är välfungerande eller inte välfungerande. För tittar ni i företag som omsätter upp emot 1 till 2 till 3 miljarder, 5 miljarder kanske också så är inte de här processerna på topp, som jag ser det.
H: Vad är nackdelen att de inte är på topp så att säga?
R: Du får ju en mismatch, mellan vad IT och medarbetarna gör, förväntningsgap ochså vidare.
H: Så IT faller lite i skymjundan då, och allt det som inbegrips i vad verksamheten förväntar sig av IT och det som faktiskt levereras, är det det problemet som du ser?
R: Ja, det kan man säga. Man kan väl egentligen säga att IT får oförtjänt kritik ofta, tycker jag att det leder till. Det är ju sällan en medarbetare tycker att IT gör allt den ska plus lite till. Det har jag nog aldrig hört.
H: Nej det tror inte jag heller. Men det känns ju lite så att det som är relaterat till IT ofta är negativt, och när det är problem med IT så hörs det ganska tydligt. Men när det är något som IT faktiskt bidrar till så är det svårt att får fram det.
R: Och sen är frågan, vems är felet att inte en rapport är rätt i affärssystemet till exempel? Är det IT:s fel eller är det verksamhetens fel? Eller att de nyanställda inte får en dator när de kommer. Är det IT:s fel eller är det verksamhetens fel? Det finns ju förresten konkreta exempel på att IT-avdelningen får reda på kvällen innan att imorgon kommer en nyanställd, har ni dator till honom? ehh, nej.
H: Du sa att du skriver gärna det här med systemförvaltande och systemägande i rapporten, vad är det för rapport du tänker på då?
R: Ja det är en vanlig ITGC.
H: Okej. Vad står det mer i en sån då, som du kan tänkas skriva?
R: Kring styrprocesser menar du?
H: Mmm.
R: Jamen där skriver du kring allting...kring säkerhet, kring backuper, om du inte inkluderar det i säkerhet...kring fysiska problem. Kring fysiska och psykiska problem. Den är ju ett par hundra frågor lång om vi säger så. Och sen anpassar man...är det ett företag som sysslar med programmering så tittar man kanske på change-processer, och då skriver man ju om det. Så det är ju svårt att säga exakt i generella...
S: Ja, ska vi gå vidare här till nästa område angående systemsäkerhet, informationssäkerhet. Vad anser du, vad är syftet med att granska företags säkerhetsrutiner?
R: Det primära syftet är väl egentligen att se så att dom har ett uppdelat ansvar. Att se så att inte en och samma person kan göra, har för mycket rättigheter i systemet. Till exempel, det klassiska exemplet att man har en person på ekonomisidan som kan registrera leverantörsfakturor, ändra utbelade bankgironummer, eller postgironummer. Dessutom att ha rättigheter på banken, att lägga upp betalning på banken, och dessutom attestera avslutningsvis. Och sen håller hon dessutom på med avstämningsfrågorna. Att man har någon som sitter på alla behörigheter i en process. Ur revisionsperspektiv är ju det det viktigaste.
S: Är det vanligt att det ser ut så?
R: Tyvärr ja.
S: Så de är viktigaste bitarna att titta på, när du ser över...
R: Absolut är det det.
H: Hur tittar man på det praktiskt sett då? Hur går man tillväga för att se till så att det finns ett uppdelat ansvar?
R: Mycket av det vi gör till vardags är ju rent intervjubaserat. Så om dom inte själva berättar det...det beror lite på vilken miljö vi tittar på. Tittar vi på ett bolag med en spretig struktur och många olika system och så vidare då är det kanske svårare att konkret verifiera att det är fel...än vad det är om du har en stor SAP-miljö. Tittar vi på exempelvis SAP-installationen på Sony Ericson i Lund så har dom ju folk som sitter och jobbar med det här dagligen, just segregation of duties som det heter, SOD. Dom har folk som jobbar heltid med det, konfliktande roller. Tittar du i mindre SAP-miljöer så finns det konfliktande roller, och då får man ta ut och lyfta dom konfliktande rollerna och titta på hur har man löst det och komplettera en kontroll. I så fall är ju det intressanta att man kikar på vad har den här människan gjort. Att man i så fall tittar på en registeranalys, hur många fakturor har vederbörande attesterat, och betalt ut och så vidare...hela kedjan. Och titta på detta.
H: Så kör ni någon form av testning, är det möjligt att göra?
R: Ja absolut, det jag sa nyss.
H: Det är en form av testning?
R: Ja, tar du ut data från systemet och testar så kan du ju få fram det.
H: Ja, är det likadant med utbyte av känslig data och sådär? Hur tar man sig an det? Finns det någon form av utredning mot känslig data, att den hanteras säkert eller någonting sånt. Tittar ni på sådana rutiner?
R: Vi har frågor i vår ITGC kring just dokumentklassning och så ja. Vad som är känsligt för den ena är ju kanske inte känsligt för den andra så. Det är klart att personuppgifter som hanteras vårdslöst det är väl en bit vi diskuterar, på grund av personuppgiftslagen och så vidare. Men, vad är känslig data?

S: Framförallt då också vem som har tillgång till viss information eller viss data.
R: Behörighet och så?
S: Ja.
H: Känslig data kanske är data som är känslig för verksamheten, som inte dom vill ska spridas. Känslig för just deras räkning. Att med hjälp av att hantera detta så tittar du över deras säkerhetsrutiner.
R: Ja, det är klart att vi diskuterar det, vi diskuterar ju behörighet och så vidare. Om man har delat upp behörigheterna, hur de är uppdelade och så vidare...om det nu är ett svar på det. Sen...det är ju alltid så med affärskritisk data, data som har ett värde för marknaden, att oavsett hur många policys, regelverk eller vad det är man skriver så kan ju alltid någon med tillgång till datan få ut den och sälja den till en konkurrent. Och det kan ju vi aldrig via en revision säkerställa att det aldrig sker. Det är ju så man tangerar området. Låt säga att vi har ett bolag där vi gör en vanlig IT-revision som syftar till att säkerställa balans- och resultaträkning. Dom har en stor forsknings en utvecklingsavdelning, och där vet man att där finns data som är känslig. Det är klart att vi frågar hur separeras den datan från er data? Men är det inget specifikt syfte med att just granska deras behörigheter eller om vi extraherar information ur AD:et så vi ser hur ? *ohörbart* (32.33) är uppsatta så är det ju i så fall en intervjubaserad kontroll. Det är ju lite beroende på vilket bolag man är inne i. Och vilket uppdrag man har, och hur stort uppdraget är. Om ni har ett granskningsuppdrag på 40 timmar inklusive avrapportering då kanske man har två dagar på fältet, två dagar hemma och en dag till avrapportering. Och på två dagar så hinner man inte igenom allting.
H: Nej, det kan jag tänka mig att man inte gör.
S: Vad är det man får prioritera då, om man bara har två dagar? Det du sätter i främsta rummet så att säga...
R: Jamen jag ser det som en översiktlig scanning. Jag hinner igenom hela listan på två dagar, den hinner jag igenom på en dag också. Men vad man får göra då är att man kör igenom hela listan, kanske lite ovägt, man känner kanske inte bolaget från början. Och sen får man ge förslag på vidare granskning som gäller framöver. Vi tycker att vi ser detta som ett problemområde, detta är ett problemområde.
S: Och då kan du gräva lite djupare i dom bitarna efterhand så att säga?
R: Ja.
S: Ja, sen här nästa fråga hur man praktiskt kan jobba med de här momenten, det har du väl beskrivit, det var intervjubaserat sa du.
R: Och registeranalyser. Egentligen är det ju två sätt. Det är att man extraherar data ur systemet, eller tillsammans med dom sitter och tittar på data i systemet.
H: Ja. IT:s bidrag till verksamheten. På vilket sätt kan IT-revisorn bidra till att IT:s värde förmedlas inom en organisation?
R: Det är ju i så fall via dom här styrfrågorna inom IT...för diskuterar jag styrmodell i termer av ITIL och andra styrmodeller som kan finnas på ett bolag. Och jag diskuterar ju systemägande och så vidare. Och om man utifrån en sådan diskussion väljer att implementera ITIL eller, vid något tillfälle har jag rekommenderat att man tillsätter någon som hanterar IT-risker till exempel, och dom då gör det. Då kan man väl säga att IT-revisionen har bidragit till ett ökat värde.
H: Vad ligger till grund för att rekommendera ett ramverk som ITIL till exempel? Vad är det för faktorer du tittar på, när du kommer fram till att ITIL kanske skulle varit bra?
R: Det beror på vem du pratar med. Men jag är inte en förespråkar för att man ska ta ITIL rakt av till hundra procent, för det tar för mycket tid och kraft av dom flesta organisationer.
H: Om man tänker IT-styrningsverktyg i stort i stället då?
R: Nej men det är väl snarast det att när man diskuterar vad de har för styrmodeller och de säger att nej vi har inga. Då brukar jag säga att ni kanske skulle...har ni funderat på att införa någon? Jag kan tycka att redan när det gäller enkla processer till exempel i ITIL service desk och change... är saker man kanske bör titta på och anamma. För att få struktur på styrningen. Sen beror det ju på vilken storlek det är på bolaget såklart.
H: Så det är när du ser brister i strukturen så att säga?
R: Ja.
H: Och vad...med struktur menar du...vad tänker du på när du säger struktur?
R: När man får en känsla av att de inte jobbar stringent, målinriktat, enligt ett regelverk, ramverk och så vidare.
H: Lite ad hoc helt enkelt?
R: Ja, precis. En ad hoc hantering av IT.
H: Att man kanske inte har några måloch följer upp dom, att man inte vet vem man ska rapportera till?
R: Alltså det är frågor som kommer fram ganska fort. Och tyvärr...ofta kan man skriva sjuttio procent av rapporten innan man är hos kund.
H: Hur kan det komma sig då?
R: Har man jobbat några år så är man tyvärr fylld av förutfattade meningar som tyvärr besannas gång på gång.

H: Så, jag blev bara nyfiken, vad vet du om ett företag innan du kommit dit då? Innan du kommer till ett företag, så i sjuttio procent av fallen så kan du skriva en rapport som du vet hur den ser ut, vad baserar du det på?
R:Erfarenhet.
H: Jamen jag tänkte att du måste veta något om företaget innan du är där?
R: Ja oftast så kanske man tittar igenom revisionsakterna, man pratar med ansvarig revisor så att man vet lite grand om dom. Hur det ser ut. Ja, sjuttio procent kanske är att ta i och förhäva sig men. Men eftersom till exempel den processen att ta bort konton ur AD aldrig fungerar. Då kanske dom första tre frågorna säger att det fungerar. Sen springer du runt lite och ser att det inte funkar.
H: Så det finns vissa bitar som alltid fallerar?
R: Ja visst.
H: Vad finns det mer för områden som inte fungerar i stort sett?
R: Jag tycker ofta att det är stök i backuperna, AD-hanteringen är inte hundra alltid, uppdateringshanteringen är inte alltid hundra. Någonting kring den fysiska biten på serverrummet brukar aldrig vara hundra, och så vidare.
H: Ja. Det här om vi återgår till IT:s värde i organisationen, anser du att det är viktigt och i så fall på vilket sätt är det viktigt?
S: Att värdet förmedlas så att säga.
R: Ja absolut. Det är viktigt av två skäl. Dels är det viktig för oss som revisorer att se att IT gör rätt saker, men sen...gör dom inte rätt saker eller tycker att dom får dåligt gehör i organisationen då tycker jag att vi kan bidra med att föra fram deras röst. Sen vet jag att det kan bli diskussioner ibland med ansvariga i bolag kring vem som sagt vad och varför. Och frågan är om vi är budbärare eller om vi är opartiska. Det är ju alltid en diskussion om frågan.
S: Hur anser ni att ni kan bidra med att föra fram IT: s röst, är det er kontakt med högre ledningen eller?
R: Ja, det är avrapporteringen till styrelse eller VD någon annan på högre nivå oftare än vad IT-chefen sitter på. Det är ju inte alla bolag där IT-chefen sitter i ledningsgruppen.
H: Är det den rapporten då, den ITGC-rapporten som dom tar hand om?
R: Ja, eller den rapportering vi gör det året. ITGC är ofta första steget sen finns det ju en mängd andra rapporteringar också, som kan ske, beroende då på...har man gjort en ITGC första året så gör man ju inte den andra året. Då twistar man ju lite på den och så jobbar man på andra frågor andra året.
H: Har man en uppföljning på dom?
R: Absolut, jag följer alltid upp föregående årsrapport.
H: Tittar på hur dom har hanterat frågorna sen sist och så vidare?
R: Ja, absolut.
S: Som du sa då så är det den här översiktgliga scanningen där du då plockar ut bitar att foksuera på.
R: I min avrapportering av ITGC:n så förelslår jag alltid nya områden som vi ska titta på djupare nästa år. Och det är någonting som jag kommunicerar med mina kollegor, att det känns som att det området där borta det har vi inte titta tillräckligt djupt på, och det känns inte bra.
S: Om man ser övergripande då, det kanske jag frågade innan, men vilka områden där är det du brukar plocka ut som mest viktiga från den här ITGC:n, generellt sätt?
R: Generellt sätt är svårt att svara på. Det är mer företagsanpassat. Hade det varit känt från början så hade jag kanske skrivit lite mer på granskningen från början.
S: Så det är alltså väldigt kontextberoende när du kommer att till olika företag, vilka områden du väljer att foksusera på?
R: Ofta brukar man väl föreslå att har man gjort en ITGC vid tillfälle ett så gör man kanske mer registeranalyser i läge två för då blir det djupare tester, av till exempel en process. Det är väl i så fall en fördjupning, alltså man fördjupar sig. Och gärna då med en registeranalys.
H: Alltså man kan säga att ni kommer med rekommendationerna det här första året...
R: Ja, men det gör vi alltid vi kommer med rekommendationer år två också.
H: Ja, men sen att ni följer upp de rekommendationerna ni gjort tidigare år så att säga, och det...är det också IT-styrningsrelaterade frågor som ni hanterar?
R: Jaja. I sammanfattningen av vår rapport så har vi då oftast tagit upp både brister och rekommendationer. Och hittar jag en brist ger jag alltid en rekommendation. I 99 av 100 rapporter ger jag alltid en rekommendation.
H: Till exempel att dom bör använda någon form av styrmodell, eller att dom ska ha någon grupp som hanterar IT-risker.
R: Eller att dom ska formalisera någon typ av hantering eller så. Det brukar jag alltid börja året efter med att diskutera igenom, vad som har hänt sedan i fjol. Det gör jag av två skäl. Dels kan man ha gjort tekniska förändringar under det gångna året, och då behöver man ju ta hänsyn till dom i årets revision.

H: Ja, så att det finns två skäl till det ja. Och det här har vi nog varit inne på lite innan också. Hur kan IT-revisorn kontrollera att IT:s bidrag till verksamheten blir synbart för hela organisationen?
R: Jamen alltså egentligen är det ju styrmodellen. Har man inte en tydlig styrmodell som är begriplig och den inte är kommunicerad, det är i så fall det vi kan bidra med och säga att de ska skapa eller hjälpa till att göra om det nu är en kund man kan är hos. Men det är klart att ett visst IT-bidrag är alltid synbart i organisationen. Funkar servern, och lagringsytorna och skrivarna fungerar då är det alltid tydligt att dom bidrar med någon form av värde.
H: Det vi tänker är kanske lite högre upp, så att mål för IT då. Ur stragisk synpunkt och så vidare.
R: Det är ju så att vi börjar alltid en IT-revision med att samla på oss dokumenten. Det brukar alltid finnas en IT-policy, det brukar finnas budget, det brukar finnas...IT-strategi finns sällan idag.
H: Vilka moment i arbete gällande IT:s bidrag till verksamheten tycker du är mest kritiskt då?
R: Mest kritiskt. Ja, funkar inte IT så är det ju mest kritiskt. Står det stilla tre dagar i veckan så är det ju det som är det mest kritiska.
S: Att systemen inte levererar så att säga?
R: Mmm. Man får ju börja...man får göra en liten enkel analys själv. Vad händer om jag rycker pluggen till IT på det här bolaget? Vilka processer kommer att stanna? Är det ett bolag med försäljning till exempel, rycker jag pluggen till IT så kanske dom inte kan sälja längre. Då är det kanske det mest kritiska. Ett annat bolag som håller på med order, postorder och fakturering. Rycker du pluggen här så kanske inte telefonväxeln fungerar. Säljarna kan inte lägga order i systemet och så vidare. Dom tappar försäljningskronor. Och det är ju...den analysen är inte alltid helt utförd kan jag tycka. Det är liksom inte en självklar fråga i alla lägen. Vad händer om det inte funkar? Frågan är om det är ett svar på din fråga.
H: Ja, alltså vad är viktigt att förmedla gällande IT:s bidrag. Och det är kanske en medvetenhet om vad IT faktiskt gör för företaget. Precis som du säger, vad händer om vi tar ut pluggen. Och det är kanske viktigt att förmedla IT:s bidrag till företaget, så att dom har den här medvetenheten. Till exempel att kartlägga katastrofhantering så att säga.
R: Sen är det ju styrfrågor också såklart. Har du inte styrning på plats så är det också svårt att förmedla ett mer förfinat budskap av bidraget. För annars kommer ju IT bara bli en försörjare av burk.
H: Ja, då går vi vidare. Jag vet ju att intern kontroll kan innefattas av mycket, ett vitt begrepp liksom. Men i stort, vad anser du vara syftet med ett företags interna kontroller?
R: Syftet med intern kontroll är ju att...ja hur ska jag formulera mig. Att man har kontroll på de väsentliga processerna. Att de blir rätt utörda, och skulle det vara så att de utförs fel med kontrollmekanismer som gör att felen faller ut igen.
H: Kontrollmekanismer som reagerar fel helt enkelt.
R: Ja, ur ett eknomiskt perspektiv är ju det det viktigaste, ofta. Att du inte registrerar ett OCR-nummer i ett beloppsfält, det kan bli mycket pengar. Om du tar ett oerhört konkret exempel.
S: Så det är också något du kan titta på då, kontrollmekanismerna. Hur de fungerar, och att de fungerar?
R: Jo, visst är det så.
H: Så vad anser du att bra interna kontroller kan ge för effekt för företaget?
R: Om vi backar tillbaka till den IT-revisionen som syftar till att säkerställa balans- och resultaträkning så är det ju ändå så att den ökar ju kvaliteten på redovisningen. Har bolaget bra intern kontroll så ökar det kvaliteten på redovisningen vilket i sin tur minskar behoven av revision. Utan då får vi gå över istället och säkerställa dom här processerna och säga att de stämmer. Det är ju precis som vi diskuterade den här måndagskvällen, att finns det inga interna kontroller så får man substansgranska mer.
S: Ja. Hur kan då IT-revisorn eller du som IT-revisor kontroller och granska de här interna kontrollerna? Att kontrollmekanismerna funkar, hur du tittar på dom.
R: Det är ju frågan om dom är systembaserade eller ligger utanför systemet. Ligger de utanför systemet så kan oftast den vanliga revisorn ofta likaväl granska det och bidra. Men är de inbyggda i systemet som inbyggda kontroller, då kan man ju via registeranalyser säkra dom. Till exempel registeranalyser eller att man tittar på behörighet eller att man tittar på...på mer systemrelaterade ting. Men om det är så att Lisa stansar leverantörsfakturorna sen levererar hon dom alltid till Kajsa som fysiskt tittar igenom att hon har stansat rätt, och man har en sådan process. Då bidrar ju inte jag i den processen. Det kan ju likaväl vem som helst göra, den delen.
H: Och det här med vad som är mest kritiskt med dom här momenten, när man tittar på interna kontroller, är det det du var inne på innan? Att man har fungerande koll på kontrollmekanismer...ur det ekonomiska perspektivet?
R: Jag kommer ju med den ryggsäcken. Än en gång, tittar vi på den typen av balansräkning och avdragsgill revision så är det ju där...
H: Kan man på något sätt säga att man effektiviserar, alltså ju bättre kontrollmekanismer man har desto mindre fel, desto effektivare blir man?
R: Så bör det ju vara.

S: Okej. Lite om externa krav, extern kravhantering. På vilket sätt kan IT-revisorn kontrollera att företag tillmötesgår de externa krav som de omges av? Exempelvis regelverk och liknande andra krav.
R: Det är ju som jag sagt tidigare, eller som vi pratade om den här måndagkvällen, det finns ju inte i svensk lagstiftning sådär väldigt mycket regler som säger att man ska ha blåa servrar och gula sladdar, det är ju väldigt lite i svensk lagstiftning som säger det. Däremot är det ju klart att man tittar ju på hur saker och ting hanteras, man tittar ju på...är det bank/finans så finns det ju krav skrivet. Och då får man ju titta på vilka som är applicerbara, och så får man se hur de appliceras. Absolut, det är branchberoende. Men tittar du på Orvars korvar däruppe så är det sannolikt hans kassaregister som är det största bekymret i den verksamheten ur ett ekonomiskt perspektiv.
H: Jag tänker också att externa krav kan ju komma från kunder, från företagets leverantörer.
R: Har inte vi ett specifikt uppdrag från en leverantör att fylla någonting, så är ju det något som har med bolagets generella styrning att göra. Och det är ju ingenting som vi behöver blanda oss i. Det är väl i så fall om man ser att det är tokigt på något sätt, men det är ju inte vårt primär mål, att springa kundernas ärenden. Det är ju samma sak som att under en period så var jag IT-revisor till två bolag som, utan att nämna några namn, säljer exakt samma produkter, verkar på samma marknad genom samma marknadskanaler och så vidare. Exakt. Och hade dessutom samma system i botten. Skillnaden var att den ena hade köpt källkoden och den andra hade inte gjort det, ordinarie leverantor fortsatte utveckla. Dom köper order från samma leverantör och så vidare. Där är det ju inte...dom är oerhört närliggande. Och där gäller det att hålla tungan rätt i mun. Vilket bolag är det man egentligen är på för tillfället. För, var det dom som hade gjort uppgraderingar för det här problemet eller var det dom som hade gjort uppgraderingar för det här problemet? Så att det är ju så att ibland kan det vara så att man kan inte berätta, även om man vet att en leverantör är på väg att kasta ut. Man kanske är IT-revisor hos leverantören och man kanske är IT-revisor hos den som köper av leverantören. Då kan ju inte jag om jag då vet att kunden hos leverantören är på väg att kasta ut leverantören för att han har en dålig hemsida...då kan ju inte jag springa och säga det till honom. Det går ju inte. Så det är ju viktigt också att fortsätt uppträda oberoende även om man vet att A tycker att B gör fel. Sen finns det ju dom här servicebyråintygen som vi pratade om. Dom här RS 402-intygen, till exempel, eller SAS 70 eller vad det nu kallas för...där en extern revisor kräver ett dokument som säger att just detta bolagets verksamhet är sjysst. Det är ju ett konkret läge.
H: Ja, okej. Det var lite om det. Ska vi ta kontroll- och organisationsstruktur då. Anser du det vara viktigt för en IT-revisor att granska organisationsstrukturen för kontroller och beslutsfattande, i så fall varför?
R: Jag granskar ju det som en av mina första frågor när vi kommer med en ITGC, eftersom jag börjar utifrån och går inåt som jag sa. Jag börjar med mjuka frågor sen slutar jag med säkerhet i brandväggen typ. Det är ungefär så jag har trattat ihop det här. Men, det är ju ändå en värdemätare och temperaturmätare på företaget. Har man ingen ordning och reda på den externa biten så har man sannolikt ingen ordning och reda inuti. Det blir en ad hoc hantering. Så att visst är det viktigt.
H: Alltså mer viktigt för din övergripande uppfattning om företaget eller? På vilket sätt, tror inte jag förstod det riktigt?
R: Ja, det är ju ofta viktigt både för min övergripande uppfattning, och ofta kan det ju också vara applicerbart. Även om du inte har allt dokumenterat i pappersform så kan det ju vara så att det beskrivs att du har väldigt goda rutiner som finns. Ska vi se här, svarade jag på frågan, jag är lite osäker på om jag gör det. Men till exempel att man har en bra organisation med systemägare, systemförvaltare och så vidare. Man har en kravinsamlingsprocess och det är på plats. Då tyder ju det på en viss mognad i sin IT-styrning. Och har man den mognaden där då har man ju sannolikt även tänkt på det som finns under huvudet, tekniskt. Man har kanske en change management-kedja för sin brandvägg, eller för om någon kommer eller slutar. Så ofta är det ju så att IT brukar springa ur att man har...att bolaget köper en server, så blir det två servrar, det blir tre servrar. Och sen blir det så många servrar så att man måste anställa någon som hanterar det. Och då anställer man en tekniker. Och den teknikern tittar inte på IT-struktur och styrning, han tittar på vården av burk. Och så blir det fem servrar, tio servrar, tjugo servrar, trettio servrar...och så kanske man anställer nästa kille. Som också jobbar med teknisk drift.
H: Vad är problemet där då anser du? Liksom, vad utmynnar det i för problem?
R: Det utmynnar än en gång i att du kommer tillbaks till det här förväntningsgapet. Att IT levererar inte mer än burk till organisationen. Du stöttar inte organisationen på rätt sätt. Så under någonstans under bolagets resa så måste man ta ett strukturgrepp.
H: För att förmedla värdet och allting som har med IT att göra?
R: Ja. När man är ett bolag med 300...låt säga att vi hade haft ett bolag ihopa och jag hade varit IT-ansvarig. Och så sitter vi på kafferasten och diskuterar, ska vi inte ha gula datorer? Och så är vi överens om det, då är ju alla medvetna om beslutet. Hade vi varit 3000 man på bolaget, då kan man inte sitta på en kafferast och diskutera om man ska ha gula datorer.
H: Lite det här med att rapporteringen försvinner i takt med att man inte har någon IT-styrning.

R: Ja. Den här graden av förmedlat IT-värde minskar ju i takt med att organisationen expanderar. Om man inte någonstans under resans gång lägger om stödstrukturen för det. För beslutsstöd...beslutsdiskussioner kring det.
H: Ja. Är det samma sak när det gäller beslutsfattande tycker du? Tänker på att dom rapporterna som ni levererar, kan dom på något sätt ligga till grund för beslutsfattande i företaget?
R: Ja, det hoppas jag. Eftersom jag alltid, ja i 99 fall av 100, ger förslag på hur man ska hantera det på ett bättre sätt så hoppas jag ju att min rapport kan ligga till grund för att VD:n säger att vi måste göra så istället. Om nu inte IT-chefen säger det så får han veta att vi tänker göra som han säger istället. Så hoppas jag ju på det. Eller att han kanske säger att det är ju ett tokigt påstående, här går det ju inte att revisera. Så kan det ju faktiskt också vara. Egentligen tycker ju jag att det är viktigt att man fattar beslut. Jag kan ju säga att jag tycker att man ska formalisera en process för att jag tycker att den känns viktig. Och bolaget bestämmer sig för att det är en viktig process, ja. Men vi tänker inte formalisera den. Det är fine med mig. Då har de i alla fall fattat beslut. Avsaknaden av beslut är egentligen sämre. Att man liksom flyter runt såhär och inte riktigt vet vad riktlinjerna är.
H: Fast man kan ju tänka att ifall man tar ett beslut så finns det ju en avsikt med det.
R: Precis. Då har man i alla fall gjort så mycket att man vågar sätta ner foten och säga att nu står vi för detta. Vi tänker inte backupa våra servrar. Varför tänker ni inte göra det? Nämen vi har fattat ett beslut på det här grundvalet. Okej. Sen kommerjag att skriva det i alla rapporter, att dom inte backupar sina servrar. Och vi kommer påpeka det till styrelsen. Men är det deras beslut och dom står för det och tycker att det är rätt i förhållande till deras verksamhet så. Fine.
S: Ja. Nästa här, då har vi väl täckt in det, alltså om det är något ni jobbar med och i så fall hur? Allstå organisationsstrukturen, det har vi väl täckt in här?
R: Nu ska vi se, var är du nu?
S: Ja, fråga 20 här.
R: Ja, det har vi nog täckt in va.
S: Ja, precis. Så om vi går vidare till risker då och riskhantering istället. Hur bör IT-risker/IT-riskpolicys hanteras och granskas i relation de här områdena, om vi börjar med klassificering av risker.
R: Att man har tänkt i termer av IT-risk och så vidare. Det är ju, frågan är vilka bolag du gör det på. Ofta på bank/finans gör man ju det ju såklart. Men tänker man utanför bank/finans får du nog gå på rätt stora bolag. Nu är det säkert något ni kommer att märka under intervjuerna när ni pratar med dom på ...(andra företag som ska vara med i undersökningen) som då har en större referensram för bolag än vad jag har. Dom springer säkert på dom här dokumenten oftare än vad jag gör.
H: Gäller det riskhanteringen överlag tycker du? Eller, om du beskriver er approach till riskhantering i stora drag.
R: Till att börja med hur, om ledningen i bolaget har satt sig ned och gjort en riskanalys överhuvudtaget. Då får man ju fundera över hur den är upprättad. Är det så att den är upprättad över två flaskor vin en fredag kväll, då kanske man ska fästa visst värde vid den. Är det så att ledningsgruppen åkt iväg en vecka och verkligen funderat över det här, då är det ju...då ska man fästa ett annat värde vid den. Jag menar om man tänker i termer av risk, eller vad händer om vi rycker pluggen, vad är det värsta som kan hända i vårt bolag. Egentligen tycker jag att IT-risken är ju egentligen inte frikopplad från bolagsrisken. Egentligen ska man ställa sig utanför porten till bolaget och titta på, vad är det hemskaste som kan hända? Och sen börja med ena fingertoppen.
S: Du tittar då på hur deras riskanalys är genomförd och hur den är genomförd?
R: Har dom genomfört en riskanalys, ja då tittar jag på den. Har dom inte genomfört en riskanalys så rekommenderar jag att dom ska göra det.
S: Om dom då har gjort en riskanalys kan du då så att säga bedöma den? Om det finns andra bitar dom borde titta på, eller någonting dom ska lyfta fram mer, eller bort till exempel. Hur hanterar du riskanalysen så att säga?
R: Jag läser igenom den och försöker att konstatera vad där finns för brister i den, eller om man ska lägga tonvikt på den på något annat sätt. Det som är viktigt i en riskanalys är ju egentligen hur den tas fram. Tas den fram på ett seriöst sätt då har den sannolikt en högre kvalitet. Vet man om att detta är trettonde revisionen av någonting som togs fram för tre år sedan, då är det ju ett dokument man jobbar med löpande. Så sannolikt är det ett fokusdokument. Är det ett dokument som togs fram 2000 eller 99, innan 2000-bubblan om vi säger så, då kanske inte den är bra idag.
H: Om man ska ta fram någon form av riskdokument, finns där några riktlinjer som du anser att man bör följa.
R: Ja, det finns ju en ISO-standard som hanterar risk väl, det är ju bra om den är med. Det är väl bra om den kan basera sig på en standard.
H: Ja. Jag vet inte om fråga 22 och 23 ger oss så mycket mer här kanske.
S: Vi kan ju bara dra den här. Vilken typ av hjälpmedel eller verktyg kan användas när man tittar på riskanalysen?
R: Skulle jag gå in i en process och just granska det här med IT-risk mer djupt, för det är ju inget som vi vid en normal revision hinner med. Det är klart vi tittar på risker, det är inte det jag säger. Men, däremot bolagets upprätte. Om vi tittar på Volvo exempelvis, om vi tittar på deras plan av IT-risker. Då hade man ju fått ta fram ISO-standarden

och se om den mappar mot den. Men med största sannolikhet så har dom gjort något eget. För dom har i alla fall historiskt sett valt att avvika allt väsentligt. Så det är klart, då hade jag hellre tagit fram den typen av dokument, och granskat utifrån den typen av dokument för att få stöd. Eller så finns det ju bolag som jobbar med den typen av frågor specifikt, där man tittar på verksamhetsrisker. Och när man tittar på så stora bolag, så har dom ofta olika typer av krisscenarios som dom spelar med olika aktörer. Då får man ju titta på processen där ute. Så det är ju oerhört anpassat till kunden. Återigen, tittar vi på Orvars korvar där nere så är ju hans största IT-risk att någon står med en pistol i ena handen och samtidigt kan få ut kassan med andra handen.
S: Ja. Och sen då vilka moment som är mest kritiska när det gäller riskhanteringsarbetet?
R: Ja, egentligen att man ska hålla sig uppdaterad.
H: På vilket sätt?
R: Ja, strukturen till hur man håller sig uppdaterad och tittar på det tycker nog jag är det viktigaste.
S: Ja, sen har vi två avslutande frågor här. Vi har pratat om olika faktorer, moment då som är viktiga att beakta vid en IT-revision. Hur skulle du rangordna dessa moment i relation till IT-styrning? Vilka faktorer är viktigast att titta på ur ett IT-styrningsperspektiv? Vi pratade lite här om dokumentation till exempel.
H: Organisation- och ledningsfrågor.
R: Jag bara tittar på era rubriker (teman) för att se om man skulle kunna kategorisera dom. Det kan man ju säkert göra för allting finns ju här. Ur ett IT-styrningsperspektiv får man nog börja utifrån, när man står på revisionsbenet. Och se att det finns struktur för det man sysslar med. Det är väl i så fall prio ett. Det är ju klart att intern kontroll är det viktigaste, om vi tittar på balans- resultat revision.
S: Så struktur och intern kontroll?
R: Ja, precis. Struktur och beslutsägande sen kommer nog intern kontroll-frågorna. Då har ni ju i och för sig täckt in allting, på ett eller annat vänster.
S: Finns det några andra områden utöver det vi har pratat om här som du anser viktiga gällande IT-styrning.
R: Vi har inte pratat mycket om den konkreta kravinsamlingen som ligger utanför IT-revisionen, det har vi inte gjort.
H: På vilket sätt kopplar du den till IT-styrning?
R: Jamen samlar du inte kraven på ett strukturerat sätt då är det inte säkert att du kan stödja din organisation, med dom produkterna som behövs. Då är vi tillbaka i det att du byter skrivare när det egentligen är Lisa som behöver nytt tangentbord.
H: Så att du menar liksom att kraven måste komma från verksamheten?
R: Ja, min uppfattning är att IT egentligen för att det ska fungera på bästa sätt så måste IT vara mer en utförare, dom bör inte äga så mycket. Så att ut med beslutsfattandet så långt du kan i organisationen så att du kan...IT måste ju också ut i organisationen så att dom kan lyssna. Så att dom sen kan hjälpa till och stötta IT-processerna. Det är klart att de måste finnas PC-tekniker som servar datorer eller uppdaterar datorer, absolut, det är inte det jag säger. Men IT måste ha öron ute i organisationen, har dom inte det så funkar det inte.
H: Dom måste ha?
R: Öron, ute i organisationen.
H: Och tvärtom också kanske då? Att organisationen måste se till så att dom vet vad IT kan tillföra.
R: Mmm, precis. Men ofta så får ju ofta IT oförskyllt ansvar för problem, som kanske inte är deras problem egentligen. Och det kan man ju egentligen bara komma runt genom en god kommunikation i organisationen. Det är ju egentligen att man har processer som ser till att saker och ting flödar åt rätt håll eller, att dom tar in saker från sitt håll, att dom kommunicerar ut.
H: Ja, kommunikationsvägarna är också en vital del när det gäller IT-styrning?
R: Absolut.
H: Men är det så att ni tittar på strukturen i stort.
R: Om vi backar tillbaks, som jag sagt väldigt många gånger innan, tittar vi på IT-revision och i den termen att vi ska säkerställa balans- och resultatrapport då spelar det ingen roll om allting inom IT går med skohorn om vi säger så, och alla hatar IT för att dom inte gör vad dom ska. Det spelar egentligen inte så stor roll. För har dom bara koll på sina processer när det gäller den här interna kontroll-delen så är det ju fine för en oerhört strikt IT-revision. Tar man bort skygglapparna och tittar vidare så är det ju en annan fråga. Så här dansar man ju hela tiden mellan olika roller, olika möjligheter, olika angreppssätt.
H: Är det något som du slås av ofta, den tanken, vilken roll har jag nu?
R: Dom flesta är ju ändå så, dom flesta kunder...9 av 10 har ju jag jobbat med många år tidigare så jag känner dom som är där. Så då vet man liksom inom vilka ramar man kan jobba.
H: Okej, då är vi färdiga.
S: Tack så mycket för att du ställer upp här.
R: Tack själva.

B2.3 Intervju Företag C

Transkribering av intervju med Respondent 1 och 2 från företag C 5 maj 2010

S = Stefan Arnslätt
H = Hampus Karlsson
R1 = Respondent 1 (Informant 1)
R2 = Respondent 2 (Informant 2)

S: Ja, då börjar vi inervjun här med Respondent 1 och Respondent 2 från företag C som har gått med på att vi spelar in samtalet. Vi börjar med dom övergripande inledande frågorna här. Om ni vill beskriva kortfattat era arbetsuppgifter samt er position här på Företag C.
R2: Ska jag börja, R2 då. Ja, R2 heter jag, jobbar på en avdelning inom Företag C som kallas för Risk Management Services som fokuserar på intern kontrollgranskning i revisionerna. Min roll i den miljön är att granska IT-miljön hos klienter, IT-revisor om man nu vill kalla det för det. Sen har jag även en expertis inom transaktionsanalys som är då en form av revisionstjänst som vi har i vårt tjänsteutbud så att säga. I övrigt det vi gör i gruppen är att vi har även expertis för att granska så att säga affärssystemsetuper, konfigurationer för ERP-system och så vidare...jobbar med processgranskningar för generella affärsprocesser då. Och jag har jobbat på Företag C i fyra år. Och jag har en roll som manager, assistant manager för tillfället. Vad som fick mig intresserad av området? Ja, det var nog mer en tillfällighet att jag hamnade på Företag C. Så att det var väl inget intresse jag hade från början, att utvecklas i en roll som IT-revisor, utan det har blivit så med tiden helt enkelt.
R1: Det är nog ganska få, i alla fall som jobbar här, som visste att dom skulle bli IT-revisorer innan. Ja, jag heter alltså R1 och jag har jobbat på Företag C i åtta år drygt, och jag är manager som vi säger här, vilket är någon slags mittemellan position. Mina huvudsakliga arbetsuppgifter är system- och processgranskningar kallar vi det. Men det betyder ju egentligen att man agerar som IT-revisor och granskar system, vilket egentligen innebär applikationer, databaser och operativsystem. Men jag jobbar också väldigt mycket med att granska vanliga processer, alltså inköp-försäljningsprocesser. Alltså med intern kontroll som fokus då. Och min specialisering det är SAP-system och det är det jag försöker fokusera på då. Om man ska säga något om avdelningen som sådan, vi är typ ungefär hundra personer är vi nu.
R2: Inom vår gruppering på Sverige-nivå ja.
R1: Företag C på Sverige-nivå är ju 3500 personer tror jag. Och i vår gruppering är vi 100 stycken, och i den ryms det dels då system- och processrevisioner då där IT-revisorn ingår. Det finns också folk som jobbar med intern revision, vi har folk som är tekniska IT-specialister. Vi har folk som jobbar direkt med IT-styrning och IT cost på konsultbasis. Vad har vi mer...som jobbar med affärsrelaterade kontroller.
R2M: Ja, alltså affärssystemsidan.
R1: Affärssystemsidan där vi har kompetens inom Movex, M3, Sapta, Navision och så vidare. Så det är ju ett ganska brett spektrum, och då har vi egentligen smalnat ner det. Sen är ju företag C:s burk som ni vet revision, skattespecialiser och så finns det en rådgivningssida som vi jobbar mycket med. Diverse consulting inom ekonomisidan, det är köpa och sälja företag.
S: Ja, då kan vi gå in på det första temaområdet så kallat, definera och hantera processer. Vilka moment då anser ni bör gås igenom vid en granskning av ett företags processer?
R1: Och då menar ni IT-processer då?
S: Precis ja.
R1: Om vi gör en vanlig IT-granskning inom ramen för revisionen då, för att säkerställa att finansiell data är korrekt och så, att ingen kan påverka det. Då pratar vi egentligen om, ja det är egentligen fem domäner va. Och det är IT-kontrollmiljö, programutveckling, programförändring, drift och berhörigheter. Om man ska något kort om dom då. När det gäller IT-kontrollmiljö så är det egentligen det vi tittar på först. Där tittar man på IT-klientens mognadsgrad vad det gäller styrning, mycket policys och riktlinjer, hur ser IT-organisationen ut? Är det bara en person som är inhyrd eller har dom en stor egen organisation med egen kompetens och så. Hur god är klientens förståelse för IT-kontroller? Förstår dom vad en kontroll är och verkar det finnas kontroller på plats? Vilken relation har dom med finans? Pratar man med varandra och jobbar man tillsammans, vem är det som bestämmer över systemen, och finns det systemägare och så vidare? Och det gör man egentligen för att försöka skaffa sig en initial bild av vad kan vi förvänta oss? Det finns ju en massa metodikmässiga aspekter som gör att man kan fatta beslut om det här, om man ska fortsätta, om man ska granska IT överhuvudtaget, eller om man tror att det inte ens är lönt. Dom är så omogna eller för att det inte finns några processer på plats. Sen är det ju programutveckling som är den egentliga första stora

domänen, och det handlar då om större utvecklingsprojekt som man bedriver. Alltså införandet av ett nytt affärssystem, större förändringar i ett befintligt affärssystem, alltså man för in en ny modul eller gör några riktigt stora förändringar. Den tredje domänen programförändringar, det är mindre ändringar i befintliga system. Och det är, vi räknar också in förändringar till databaser, operativsystem här. Även om det är applikationen, alltså SAP eller Movex eller så, som har störst betydelse kan man säga. Så om man vill ändra en inställning i sitt SAP-system så följer det ofta en process med hur man, vem som får göra ändringen och hur man transporterar in den så att den får effekt i live-systemet så att säga, och det är det vi tittar på där. Att den är godkänd och så.
H: Är det företaget som har, om vi säger att de gör en programförändring, change management är det eller?
R1: Ja, precis.
H: Ser ni till att företaget har en bra processhantering för förändringen, är det också viktigt att titta på?
R1: Ja. Och det är ju den vi granskar egentligen då. Så ofta, ja inte alltid, men de flesta bolag har ju nån form av tänkt process. Stora bolag har ju ofta en väldigt fastställd och dokumenterad process som talar om exakt vem som får göra vad och hur det ska prioriteras och när saker och ting ska göras och vem som får programmera och vem som får godkänna programmeringen och så vidare. Medans mindre bolag där kanske det är bara en person som kan programmera och så att säga flytta den mellan olika testmiljöer och utvecklingsmiljöer och så. Så att vi ser ju egentligen hela spektrat, men på stora företag finns det ofta detaljerade processer framtagna, det är nog det som är skillnaden om man ska säga någonting.
R2: Ja, precis. Det som är viktigt där, vi har ju en metodik som vi jobbar efter när vi går ut och granskar de här områdena, så att vi har ju ett visst antal kontroller som vi tycker enligt vår metodik att bolagen ska ha på plats i sin förändringsprocess då till exempel. Men det som är viktigt att ta med sig där är ju att man får anpassa dom frågorna eller dom kontrollerna efter verksamheten, så att vi kan ju inte lyfta in hela vårt kontrollbatteri på en klient för att dom kanske är en eller två personer på en IT-avdelning. Så man får alltid vara lite flexibel där och se hur den faktiska miljön ser ut som dom sitter i. Det är en förståelse man får ha.
R1: Sen kanske man ska lägga till också, det kanske ni redan har räknat ut, men om vi säger att vi är på ett stort företag då kanske deras process är, det kanske är 20-30 sidor som beskriver en process från ax till limpa. Men som R2 säger så har vi en egen metodik som talar om vad är det som är viktigt för IT-revisionen. Och det kanske är 10, eller 5 kontrollpunkter, som vi kommer fokusera på då. Och då dyker vi egentligen direkt in på dom. Så vi kanske inte är jätteintresserade av exempelvis vem som får lägga ett förslag på en ny ändring till affärssystemet. Vi kan fråga hur det funkar, men det är inget som vi...vi skulle ju aldrig gå in och testa bara Kalle Karlsson på ekonomiavdelningen har önskat nya förändringar för det är bara han som får det. Vi kan prata igenom det, men vi kommer bara fokusera på de bitar som vi tycker är viktiga för revisionens skull. Så att det är liksom inte, vi tar inte deras process och ser ifall det är exakt samma utan det handlar mer om att skapa en förståelse.
S: Den här metodiken som vi pratade om, är det någon form av checklista som ni har att gå efter då?
R1: Det kan man säga. Förenklat kan man säga att det blir en checklista för det är det som blir resultatet av metodiken. Sen, Företag C har en globalt utvecklad metodik som gäller för Företag C i alla länder, och den, det som står om IT i den, det är säkert flera hundra sidor som beskriver dom här olika domänerna som jag pratade om. Vad de innebär, vad man ska tänka på och så. Men om man sen kokar ner det till vad vi tar med oss ut när vi ska granska så är det egentligen ett granskningsprogram som säger att det är det här vi ska titta på då. Och sen anpassar vi det då efter vilket system kunden kör, vilken situation, och lite också hur kundens processer ser ut. Så om vi tar ett exempel om kunden har ett system som gör att behörighet, där behörighetsadministration går igenom ett workflow där det slussas runt i olika program som ska godkännas. Då anpassar vi efter det och kanske tittar mer på det hjälplmedlet som bolaget använder snarare än att vi gräver i själva slutsystemet. Man anpassar det efter hur kundens miljö ser ut egentligen.
H: Så vi kommer alltid tillbaks till dom här interna kontrollerna som ni granskar?
R1: Ja. Och det faller alltid tillbaka på regelverket, för det är det som säger att det är så här Företag C bedriver sin revision.
H: Okej, så det ger en kontinuitet i er revision?
R1: Mmm. Går man ut och tittar på hundra av våra stora klienter så kan man i huvudsak hitta samma kontrollpunkter i de olika processerna, som vi har tittat på.
S: Jag tänkte på den här metodiken, grundar den sig i något speciellt, jag tänkte på COBIT och den typen av styrdokument, eller är det något som ni helt själv tagit fram.
R1: Den har ju sin grund egentligen i COSO. Och sen har det brutits ut, nu har jag glömt lite COBIT:s koppling till COSO, men COBIT är väl en nedbrytning av COSO för IT, om inte jag minns fel. Och vår metodik tar egentligen avstamp ur COSO och COBIT då. Så att tittar man på det här två så ser man jättestora likheter. Men COBIT är ju ganska brett att för vår del täcka...
R2: Så det var change...

R1: Mmm, behörighetssidan.
R2: Ja, vi kikar också på rutiner för administration och behörigheter och uppföljning av behörigheter, att man övervakar hur behörigheter är konfigurerade korrekt så att säga. Och det gör vi på olika nivåer ute hos klienterna. Första nivån är egentligen om vi börjar med den fysiska säkerheten så kan det vara så att vi börjar titta i serverrummet och tittar på vem som har fysisk åtkomst där. Nästa steg är då att man kryper närmre applikationen, så då är det nätverksbehörigheter. Och sen applikationer, och databas då slutligen. Och eventuellt också operativ dåpå databasen tittar vi på. Vidare där så kikar vi även på att det finns ett inloggningsförfarande i samtliga skal, att man ska ha ett användarkonto och lösenord som följer våra rekommendationer. Och att man då byter ut och uppdaterar de här lösenorden löpande då.
H: Så då täcker ni egentligen in allt det här med konton, id-hanteringen och skydd för mjukvaran mot intrång och dom bitarna.
R2: Ja, precis. Så det är ju ett väldigt viktigt område i vår revision då eftersom behörigheter medger ju åtkomst till finansiell information och starkar kontroller däromkring gör ju att man begränsar riskerna i extern påverkan på finansiella transaktioner.
R1: Så att i området behörighet, eller åtkomst, lägger man även in saker som säkerhetskonfigurering, lösenordslängd och den typen av parametrar tittar vi alltid på. Då går man in i området behörighet och åtkomst och så.
H: Det här som vi snackade om att ni granskar rätt mycket policys och riktlinjer och så vidare. Hur...då tittar ni på företagets dokumentation så att säga, kring de här frågorna? Vad händer när företag inte har den här dokumentationen, vad gör ni då?
R1: Om företaget inte har dokumentation så försöker vi då genom intervju få en förståelse för vad deras uppfattning är. Så även om det inte finns något dokumenterat så kanske dom har en process i huvudet för hur det ska gå till. Ett etablerat arbetssätt som säger att när vi gör en förändring till affärssystemet, då ska det gå igenom de här olika stegen. Och när vi får våra lösenord, de ska alltid vara åtta tecken långa. Och vi ger aldrig någon behörighet utan att de fått godkännande av den här och den här. Man får genom intervju försöka förstå om dom har någon struktur kring styrning.
R2: Överlag när det gäller dokumentation så är det väl egentligen bara på de riktigt stora klienterna där man ser att de har resurserna att dra hela det området fullt ut. Mindre klienter, där är oftast inte fokus på den typen av dokumentation, dom är kanske lite mer informellt formulerade.
R1: Man kanske ska säga det också att när vi gör IT-granskningar inom ramen för revisionen så sträcker det sig egentligen till spannet från åtta timmar till tusen timmar, på riktigt stora företag.
S: Det beror alltså på hur stor kunden är.
R1: Hur stor kunden är, eller hur miljön ser ut. Och vad dom vill ha. När vi planerar dom större...gör vi ett sånt här åttatimmarsuppdrag så frågar vi aldrig kunden vad är det ni är intresserade av. För det har man inte tid med, då åker man bara ut och så träffar man en person i två timmar, intervjuar och sen åker man tillbaka och så skriver man en rapport. Men på de riktigt stora företagen, om vi ska lägga ner tusen timmar på att granska deras IT-miljö, då sker det alltid ett visst samspel mellan vad skulle ni vilja ha gjort och vad vill vi ha gjort. På de lite större uppdragen så finns det kanske lite mer utrymma för vår del att styra lite efter vad dom kanske vill då, samtidigt som att det är alltid revisionen som styr då. Men det finns alltså lite mer utrymme där.
H: Ser ni att syftet med er IT-revision beror på då? Att det är olika från olika fall?
R1: Nej. Alltså grundsyftet blir alltid detsamma på något sätt, och det är ju att säkerställa att den finansiella informationen är korrekt. Att ingen kan ändra data i en databas, eller att...det hänger ju också ihop med processgranskning. Så om vi tittar på en försäljningsprocess så kanske det i den här försäljningsprocessen så finns det en kontroll som säger att om en kund har överskridit sin kredit-limit så kan vi belägga en ny order på den, eller vi kan inte leverera ut varor till den kunden. Det är ju en automatisk kontroll i systemet. Och genom att ha en fungerande förändringsprocess så vet vi att ingen obehörig har kunnat ändra den kontrollen under året, exempelvis. Så genom att testa IT-miljön så säkerställer vi även att den här typen av automatik som är viktig för affärsprocesserna fungerar under året. Så det är egentligen de två syftena, att data ej har förändrats, att automatik i systemen fungerar som det ska. Och viktiga rapporter är väl egentligen den tredje komponenten. Viktiga rapporter som man använder för beslutsfattande. Och det kan ju vara allt från att man försöker följa upp hur mycket varor man har sålt per månad eller om vi har varor som vi har levererat men inte har fakturerat. Det kanske sitter någon controller, och så plockar dom ut någon rapport. Genom att testa IT-miljön så säkerställer vi även att den här rapporten inte har ändrats under året, så att den kanske visar hälften av vad den borde visa. Det är egentligen huvudsyftet med alla IT-granskningar som vi gör. Sen kan man kanske då på de lite större uppdragen ta emot lite fler önskemål från kunden om vad de vill ha fokus på.
H: Men just det här med rapporter med beslut för företaget, är det inte av intern betydelse väldigt mycket för företagen också?

R1: Jo, det är ju en kvalitetssäkring för dom också. Så om man tittar på de stora ramverken som Sarbanes Oxley, där företagen har sina egna kontroller också, så är det kanske ofta samma saker dom testar som vi testar. Att vi gör IT-granskningen är ju också en kvalitetssäkring för dom. Sen beror det också lite på hur mycket vi granskar och litegrann hur stor ansats vi har, hur stor betydelse det får för dom egentligen. Men om man ser det som...att det vi tittar på är också viktigt för bolaget. Så vi har ju egentligen samma syn där. Allt vi gör är också av godo för företaget i slutändan.
R2: Har vi något mer att säga om den domänen.
R1: Jag tror inte det.
R2: Jag hoppas inte det, haha. Sen är det ju, sen har vi computer operations och det vi kikar på där det är väl framförallt batch-hantering och hur man hanterar eventuella systembryggor i sin miljö mellan system. Så än en gång, ur ett revisionsperspektiv, att det inte är några transaktioner man tappar på vägen till exempel. Vad det finns för kontroller runt det flödet. Vi tittar på backuphantering. Enligt metodiken så tittar vi även på change management på hårdvarusidan, att man ska ha liknande rutiner för att testa förändringar på nätverk, hårdvaror. Den beteckningen fungerar kanske inte fullt ut i praktiken. Något mer som ingår under drift?
R1: Driften handlar ju om, det är ju egentligen två sidor som R2 säger. Det är det här med batch-jobb, siffror som går mellan olika system och så, att man ser att allting följer med inne i huvudboken. Och sen är det ju det här med drift, att se till att man har ett fungerande backupande. Man har kanske dieselaggregat så man måste köra systemmiljön vidare även om man har fått strömavbrott.
R2: Patch-hantering kanske också skulle kunna ingå.
R1: Precis. Här kan man ju se, det är jättestor skillnad mellan olika bolag. Om man pratar om IT-styrning och så...vi frågar ofta bolagen, har ni tänkt på hur länge ni klarar er utan ström. Det är klart, är man ett gaming-företag så är det ju katastrof om man är utan systemen i en timme eller två timmar kanske. Medans vissa fabriker säger att vi klarar oss en dag utan det här systemet. Att vi kör ut dom här produktionslistorna på morgonen sen kan vi jobba efter dom hela dagen. Är systemet uppe nästa morgon, då blir det inget avbrott.
H: Jag tänkte på det här...kontrollerar ni företags interna kontroll, alltså att dom mäter och följer upp processerna, att dom fungerar, IT-processerna? Om dom har processmål till exempel.
R1: Inte om det är operationella mål så gör vi inte ofta det. Alltså om det är...om IT-avdelningen säger att vi har ett mätetal som säger att vi ska ha 99 procent tillgänglighet på våra filservrar exempelvis, så att användarna kan komma åt sina filer. Det struntar vi i princip helt och hållet i. Det vi tittar på är egentligen kontroller som...att en förändring i ett affärssystem ska vara godkänd innan den sätts i drift. Men det är ju kanske inte ett riktigt mätetal, men det är ju en kontroll då. Det är vi intresserade av. Eftersom det kan ha påverkan på kontroller eller finansiell data. Däremot, om dom inte når sitt mål med 99 procent tillgänglighet på filservrarna, det har egentligen ingen betydelse för den finansiella rapporteringen, och det är det som är viktigt, grundbulten i IT-revisionen. Sen har vi säkert allsköns uppdrag där vi hjälper IT-avdelningar att sätta upp mätetal och kostnadsfördelning och sådana saker. Men då har vi hamnat lite det här konsultspåret som ligger utanför IT-revisionen då.
R2: Ja, jag håller med dig. Och det man ska ta med sig också, det som trattas ner i form av iakttagelser, det ska ju vara direkt kopplat mot den finansiella rapporteringen. Och där har vi egentligen två dimensioner, impact och likelihood, när vi lyfter en iakttagelse. Dels är det ju...om en incident skulle inträffa på grund av den iakttagelse vi noterat, vad är då påverkan på finansiell rapportering? Och sen då den andra dimensionen, vad är sannolikheten för att den iakttagelse vi noterat ska ha lett fram till en incident helt enkelt. Så därför blir det ju, om man nu tittar på vissa aspekter av IT-driften, IT-kontrollmiljön, så är där kanske vissa kontroller och kontrollmål som inte är direkt kopplade mot finansiell rapportering, om man tar ner det på den nivån. Till exempel om man inte har en change management-rutin för att byta ut en hårdvara på sin infrastruktur, så är det ju väldigt svårt att koppla den iakttagelsen till en påverkan på revisionen kanske.
R1: Om ni tycker att vi spårar ur så får ni säga till. Men jag kan tycka att det finns lite olika typer av saker som kan komma att rapportera på. En sak som vi kan rapportera på och som inte har direkt finansiell påverkan är ju kanske om dom saknar policys och så för styrning. Alltså avsaknaden av policys höjer inte direkt risken för felaktighet i finansiell data, men det är sannolikt att viktiga kontroller i övrigt kanske inte finns då. Har man ingen dokumenterad process för att göra ändringar i sitt affärssystem då är det också ganska troligt att det har skett ändringar som inte varit godkända då eller att det gjorts ändringar av fel person. Så den typen av saker rapporterar vi. Mot både internt och mot företaget då. Och sen är det som R2 var inne på, dels saker som kan ha direkt påverkan, och det kan vara...i de flesta affärssystem så finns det alltid standardanvändare som kommer med paketen, som har väldigt höga behörigheter. Och då vill man att man ska låsa dom, eller skydda dom på något speciellt sätt. Om man inte har gjort det, då finns det alltid en risk för att någon har missbrukat den här användaren. Och det kan vara allt ifrån att man försökt begå något bedrägeri, eller att man skapat leverantörer och betalat ut fakturor till sitt eget bankkonto. Eller bara att man varit inne och fipplat i något som man inte vet...man kan ha ändrat något saldo, kundfordran eller något

sånt där. Sånt rapporterar vi då, och det är mer sånt som har direkt påverkan. Och det rapporterar vi alltid till företaget såklart, men också internt mot våra revisorer då. Och sen kan det vara sånt som R2 säger att man testar inte backupbanden en gång per år, eller man har ingen...man saknar batteri, eller dieselaggregat som kan drivas oberoende vidare. Det rapporterar vi ju också alltid mot kunden, men det kanske inte alltid har en direkt påverkan på den finansiella rapporteringen.
R2: Sen är det så också att för varje iakttagelse som lyfts så försöker vi eventuellt titta på kompenserande faktorer, alltså kompenserande kontroller i verksamheten som gör att man ur ett visst perspektiv kan leva med den risken som man har iakttagit så att säga. Ett exempel kan ju vara som R1 nämnde att man har för höga behörigheter som är lite för vida så att säga, men samtidigt så har kanske bolaget en rutin för att gå igenom en applikationslogg löpande för att se vem som har utfört vilken förändring på känslig data till exempel. Då skulle man kunna tänka sig att det är en kompenserande roll för den iakktagelsen vi hittade då initialt till exempel. Så att man får alltid vara lite flexibel där när man tittar på helheten.
H: Det du sa, R1, det här med avsaknaden av policys, det var lite det här jag tänkte på om företaget mäter eller dokumenterar sina processer. Är det samma syfte så måste det vara viktigt att dom har en struktur?
R1: Ja, för styrningen. Om man tänker sig att om man, ofta har ju större företag flera lager av policys också. På toppen kanske man har...man har alltid IT-policys som kanske är på en sida bara där man säger att vi ska stödja verksamheten eller så. Sen kanske man har en informationssäkerhetspolicy på toppen som säger att alla löseord ska vara komplexa och svåra. Och sen under den så bryter man ofta ner det och säger att, i kanske specifika säkerhetsriktlinjer för ett affärssystem, och då betyder det att dom här parametrarna ska vara satta si och så i affärssystemet för att vi ska hålla oss till den här övergripande informationssäkerhetsstandarden då. Och finns det inte sådana dokument, teoretiskt sett kan allting vara frid och fröjd ändå. Men det är ju ofta genom styrdokumenten som man ser till att man efterlever de högre tankarna som man har om styrning och så.
H: Det kanske ger en anledning till att granska vidare i så fall?
R1: Ja.
S: Ja, då har vi väl täckt in det mesta här med processer. Av de moment eller faktorer som vi nu har diskuterat, till exempel de här fem domänerna, vilka är mest kritiska i förhållande till IT-styrningen, och varför i så fall?
R1: IT-kontrollmiljön är ju den som är mer direkt mot IT-styrningen så att säga. Men alla dom andra domänerna påverkas ju av. Om man säger att det finns en frånvaro av IT-styrning, alltså en frånvaro av styrande dokument och så, så påverkar ju det, eller kan potentiellt påverka de andra domänerna som behörigheter och programutveckling och så vidare. Sen, utan att göra kopplingen mot IT-styrning, så är alltid behörigheter det område som är svårast och känsligast för företag att hantera, och kanske dämred också viktigast att ha hård styrning på.
R2: Ja, nej men jag håller med dig. Behörigheterna är jätteviktigt, och vi kan bara nämna det, i vår metodik, vi är ju bara, vi skrapar bara lite på ytan för kontrollrutiner som klienter har för att bevilja, förändra och godkänna behörigheter. Sen är det behörigheterna i systemen också, hur är systemen konfigurerade så att säga. Vem kan göra vad? Ofta sett, när vi gör en IT-revision, så är vi ju inte nere på den nivån. När vi tittar i själva systemen, på detalj, men det är en väldigt viktig aspekt av behörighetssidan. Det är ofta en tilläggstjänst som vi kan ta fram om man märker att man kanske inte har någon rutin för tilldelning av behörighet, så kan man gå in mer i systemen och se vem som kan göra vad och så vidare. Change är ju också viktig såklart, men vi ser ju en ganska liten andel egenutvecklade system, utan det är mycket standardsystem som används numera, och då är det mindre risk, alltså klienterna har ju inte samma möjlighet att gå in och påverka den underliggande logiken i samma utsträckning. Ofta så har man kanske inte access till databasen, utan det är en tredje part som sköter systemmiljön så att säga. En systemleverantör som tar helhetsansvaret. Så det är väl de områdena som vi hittar flest iakttagelser som är direkt relatarade till finansiell rapportering som vi kan se att här har vi en direkt koppling.
H: Ja. Lite om säkerställande av systemsäkerheten då. Vad tycker ni är syftet med att granska företags säkerhetsrutiner?
R1: Från ett IT-revisionsperspektiv så är det ju att säkerställa riktigheten i finansiell data, och rikitgheten i viktiga kontroller och rapporter i affärsprocessen. Kort och gott egentligen.
R2: Vi kan ju bara säga, alltså inom Företag C så har vi en del granskningsprogram som vi har tagit fram som en standard då, för olika typer av affärssystem. Där man testar exempelvis konfigurationer för Sapta, Navision, SAP. Där vi kan gå in på detalj och fokusera på olika riskområden. Det är ju i och för sig något som ligger utanför den traditionella IT-revisionen också, men då går vi mer liksom på djupet på något av systemen, går den vägen.
H: Vilka moment tycker ni att granskningen bör fokusera på gällande företags säkerhetsrutiner?
R1: Egentligen dom här fem domänerna som vi var inne på innan. Det är det vi alltid applicerar. Och sen, ja det tar för lång tid att gå igenom alla kontrollpunkter som vi tittar på i varje domän, men om man skall genralisera så när det gäller change, det ska vara godkänt och granskat innan man gör en ändring i systemet. Och det gäller även för behörigheter, syftet är att alla behörigheter ska vara godkända. Ska stå i paritet med den anställdes arbetsuppgifter,

till exempel man ska ha behörighet för bara det man har. Sen IT-drift, ja egentligen att man har en rimlig säkerhet vad det gäller att kunna driva verksamheten vidare i händelse av en katastrof. Alltså att man har en backup, och att man testar det. Att man har koll på filer som skickas mellan systemen. Det är väl egentligen dom huvud...
H: Dom två första faktorerna du nämnde där, hur kan man faktiskt jobba med dom?
R1: Du menar när vi granskar dom antar jag?
H: Ja.
R1: När vi testar, vi kan ta några olika exempel från olika områden. När vi testar change. Större affärssystem har ofta loggar över ändringar som har gjorts i systemen, från början till slut. Och det kan vara allt från större kodändringar till någon liten konfigurering, kanske en liten procentsats någonstans. Då plockar vi alltid ut den loggen som är i systemet på faktiskt gjorda ändringar. Sen tar vi då ett urval, vår metodik styr hur stort urval man ska ta. Så exempelvis, har man gjort mer än 250 ändringar i systemet på ett år så tar vi 30, 60 eller 90 av dom och så försöker vi spåra det tillbaka till den dokumentationen som kunden har. Och den dokumentationen innehåller ofta en beskrivning av vad det var för ändring, vem som har programmerat ändringen, vem som godkände den i slutändan och vem som såg till att den kom liksom, in i live-miljön. Och det är vårt sätt att, om vi säger att vi tagit 30 stycken, för vart och en av de 30 så spårar vi det tillbaka till kundens dokumentation helt enkelt. Och hittar vi då dokumentation för alla de 30, då är det ett bevis på att deras dokumentation fungerar som den ska. Samma gör vi egentligen på behörigheten, man plockar ut ur större system ofta en logg med vilka ändringar som har gjorts för behörigheter. Och det kan vara då att den 28:e januari så fick Kalle Karlsson behörighet att posta fakturor exempelvis. Den typen av klocka finns ofta. Då gör vi samma sak där, man tar ut loggen, tittar på hur många ändringar som har gjorts, tar ett stickprov. Och så spårar du det tillbaka, ofta kan det ju vara mail som någon har skickat, man har ofta en säkerhetsadministratör som sitter och fördelar ut nya behörigheter, så då får man gå till dom. Så säger man att nu har jag valt ut trettio stycken här, och så får du visa mig dom mailen du har, och visa att det är en chef som har godkänt den här nya behörigheten.
R2: Den typen av test tillämpar vi ju bara om bolaget har dokumenterade rutiner, och alltså formellt säger att man har en process och kontroller för det här. Har man inte det så tjänar det ingenting till att vi går in och stickprovstestar det, för då har vi ingenting att hänga upp det på så att säga.
R2: Och finns det inte den typen av bevis då får man kanske plocka ut alla behörigheter som finns i systemet, så får man ta lite stickprov där och se att ja Kalle Karlsson han har behörighet till kundreskontragrejor och lite sådana saker, och så får man fråga hans chef, är det det här han jobbar med? Ja, det är det...eller oj, han jobbar inte med kundreskontra längre, det gjorde han för två år sedan. Då skaffar man sig en liten uppfattning om det verkar rimligt då, för det är det som är huvudsaken, att man kan fastställa om det verkar vara rimligt eller inte.
H: Om det inte är rimligt då, kommer ni med önskemål eller rekommendationer för hur företag ska bedriva dom policys, rutiner.
R1: Ja. Så då...i våra rapporter står det alltid egentligen, det är observation, det är risk, rekommendation. Och en observation kan då vara, för tio av trettio nya behörigheter som vi testade, fann vi att det fanns det inget underlag för, eller det var godkänt av fel person. Det kan vara en observation. Och sen så skriver vi då att risken i systemet är att användarna har för höga behörigheter. Och rekommendationen är, det kan vara har dom redan en policy som säger att så här gör vi förändringar för behörigheter, och så ska dom godkännas av den här chefen och si och så. Då skriver vi, om vi tycker att den är bra, att företaget bör följa sin redan etablerade policy. Och har man ingen policy då skriver vi att bolaget bör göra si och så. Och sen har vi kanske också en observation på toppen då som säger, för då när vi granskar den här första domänen, IT-kontrollmiljön, så frågar vi ofta efter policys och så. Säger dom då att dom inte har en sådan här policy, då blir rekommendationen ofta att man bör ta fram en sådan här policy. Så att man dels kanske rent praktiskt hur man vill att en sådan här rutin ska se ut, och då en önskan att man kanske bör ta fram policys som styr det här.
H: Hur mycket i detalj går ni in och rekommenderar hur en sådan policy ska se ut, eller policys överlag?
R1: Ofta på väldigt hög nivå. Det blir ofta, vi rekommenderar, ni tar fram en policy, för användaradministration. Och den bör innehålla de här tre huvudområdena, men inte mer än så. Om man växlar över då, så hjälper vi såklart bolagen att ta fram en sådan policy, om dom skulle vilja. Men då är det ju utanför det vanliga arbetet så att säga.
R2: Precis. Det kan vara viktigt att man mer trycker på att man årligen går igenom aktuella policys och håller dom uppdaterade. För det märker man oftast ibland, att man tar fram en policy och sen har man den liggande någonstans. Den blir ju snabbt inaktuell, så det är ju en viktig rutin eller kontroll för vår del och se att de går igenom aktuella styrdokument, och ser att de stödjer nuvarande verksamhet och hur man jobbar så att säga. Det kanske är mer på den nivån då som vi går in och granskar.
H: Ja, det måste vara viktigt också att kontrollera att även om dom har dokumentationen, att den efterföljs.
R2: Ja, har du ju dokumentation som inte följs upp och är aktuell så är den ju verkningslös.

R1: Ofta försöker ju vi, om vi vet att de på större bolag har policys som vi tycker är bra och som vi vet vad dom säger, då hänvisar vi väldigt ofta till deras egna policys. Alltså ni bör följa den här policyn kring användaradministration eller vad det nu är vi tittar på, säkerhetskonfigurering eller...ni har redan en bra policy så följ den och det gör också att vi, på flera klienter har jag märkt, som är globala eller utspridda, att det finns policys som är framtagna centralt som man inte känner till lokalt, alltså man har tagit fram dom i Stockholm, men i Örkelljunga så vet man inte att dom finns ens en gång. Och då kan vi genom att vi hänvisar till bolagets egen policy med namn och vilken sektio i policyn det handlar om, hjälpa också att offentliggöra policys i bolaget. Sen tror jag, eller jag inbillar mig, att det...för ofta är det kanske en liten grupp som sitter centralt, en informationssäkerhetsgrupp som tar fram de här policys. Och det kan vara svårt att nå ut till alla mindre IT-avdelningar som finns runtom. Då kan vi genom revisionen hjälpa till.
R2: Det är också en väldigt viktig aspekt av, om man nu ska ha dokumentation, vem kan läsa dokumentationen. Var hittar man den här informationen till exempel. För har du en massa dokument, policys, men förmedlar inte ut till de som är berörda var man ska läsa och var man kan ta del av informationen så blir det än en gång verkningslöst.
H: Likadant kanske om det blir för mycket information? Att man får ha någon prioritering på vad som är viktigast.
R2: Ja, precis. Alla blir såklart inte berörda av allting. Dom som blir berörda ska vara medvetna om var dom hittar de här bitarna.
H: Är det ett problem i sig så att säga att informationsflödet för policys i sig blir framtaget så att säga?
R1: Jo, det är inte helt ovanligt att lokala bolag som inte sitter centralt, som inte känner till vilka policys som finns.
H: Ja, för det är ju lite synd då. För då har man en god intention då och så har man gjort halva jobbet eller 75 procent av jobbet
R1: Precis. Man ser det ju ganska tydligt på bolag som är utspridda, ju närmre huvudkontoret man sitter där ofta de här informationssäkerhetsavdelningarna sitter, ju närmre dessa man finns desto större chans är det att man känner till dem och följer dem. Ju längre bort man kommer desto mer skiter man i det egentligen va, man bryr sig inte.
S: Ska vi gå vidare här till IT: s bidra till verksamheten, IT:s värde. På vilket sätt anser ni att IT-revisorn kan bidra till att dess värde förmedlas inom en organisation?
R1: Jag tror att vi kan bidra på ett ganska bra sätt men man kanske också ska nämna att det är svårt för oss att förändra en inställning som redan är cementerad i en organisation. Om man ser IT bara som ett problemområde så är det kanske svårt för oss att ändra det men genom att vi lyfter…vi kan i alla fall få fokus på IT-styrningsfrågor och IT-effektivitet och IT-kontroller genom att prata om de här områdena i rätt forum hos företaget. Ofta tycker jag, om vi bara håller det inom IT-avdelningen, då stannar det där men om vi börjar prata om det här med företagsledningen, ekonomichef motsvarande eller på revisionsutskott och så, då brukar det få mer skruv och det blir också så att det, det är inte helt ovanligt att IT-avdelningarna är ganska öppna med oss och ser lite grann en chans att genom oss förmedla att vi försöker åstadkomma det här men vi har varken tid eller resurser att få till den här styrningen eller de här bra kontrollerna som vi behöver.
H: Mmm
R1: Och det är klart, lyfter vi det i samtal med företagsledningen, man har ofta inom ramen för revisionen ett antal avrapporteringsmöten per år, man har slutrapporteringsmöten där man talar med företagtsledningen om hur revisionen har gått och vad vi har hittat och så. Och på dessa möten talar man om allt från att man har missat att betala in moms till att då kan man välja att lyfta sådana här IT-styrningsfrågor och IT-kontrollfrågor också och då kan det hjälpa till att skapa ett tryck i organisationen och på så vis ge IT-avdelningen antingen en spark i baken om de inte har skött sig men kan också vara mer resurser för att driva igenom någonting om vi säger att det här är viktigt, ja oj det visste vi inte, det måste vi åtgärda.
S: Ni blir lite som en budbärare kan man säga?
R1: Japp, det kan man säga att vi blir, om vi har samma intresse.
R2: Det viktiga är att de rekommendationer vi ger och det vi noterar är av relevans så att det inte blir så att, det är väldigt lätt att saker hamnar hos fel personer som gör sin egen tolkning om man då inte har en gedigen IT-bakgrund och förståelse så kanske man får för sig att kanske vissa aspektera av IT kanske blir väldigt väsentliga och viktiga men det är de kanske egentligen inte ur ett IT-revisionsperspektiv eller IT-driftsperspektiv. Riskanalyser då till exempel, om man årligen går en riskanalys av IT eller inte så ser vi inte att det har någon direkt påverkan på finansiell rapportering utan är en mer operationell risk så hamnar en sådan fråga uppe hos ledningen så kan ju den få skruv rejält då så att säga, så det vi lyfter ska vara av väsentlighet så att säga.
H: Mmm, den rapporteringen ni går, ni säger att den ska komma till rätt forum, var är det normala att den hamnar någonstans?
R1: Jag tror att det är alltför vanligt att den ofta, det beror lite på men normalt sätt, den normala gången är att vi rapporterar av först på IT-avdelningsnivå och man börjar ofta från botten, att de vi hittar stämmer vi av med de vi har intervjuat, stämmer det här, ja det stämmer, sen sätter man ihop en rapport och den tar man med ledningen, IT-

ansvariga eller till ledningsgruppen och sen via rapporteringen internt så kan det också gå upp till företagsledningen men där sker det ofta en slags sollning, att man har en lösenordslängd på 3 istället för 8 tecken kommer inte till företagsledningen men däremot är det katastrof i alla rutiner då kommer det kanske vidare så att man sollar ganska mycket av den information som går uppåt men ungefär så är gången då.
H: Men ni har en rapportering, ni har inte rapportering till olika nivåer då?
R1: Jo det har man egentligen, vi kan skicka en detaljerad rapport till IT-ledningen som kanske är skrivet ur ett tekniskt perspektiv, sen kan vi göra en annan rapportering som är skriven mer, vad ska man säga, allmänt hållen som går upp till företagsledningen och då ändrar man formuleringar och så för att det ska bli begripligt och man pratar inte om vissa säkerhetsparametrar utan mer att säkerhetsstyrningen, säkerhetsmekanismen för verksamheten är bristfällig så att det kan man gott säga att vi har rapportering på flera olika nivåer egentligen, men sen är det inte alltid så.
S: Ja, anser ni det vara viktigt och i så fall på vilket sätt, att IT-förmedlas?
R2: Jag tror att man har en förståelse i de, om man ser på vilken verksamhet idag så har man ju alltid ett IT-stöd i grunden så jag tror att man är ganska medveten om att IT är en viktig del i verksamheten ute hos de klienter vi reviderar och så vidare, sen har vi kanske en möjlighet att där tillföra ett extravärde där om man tänker IT-miljön och applikationkontroller i förhållande till hur man jobbar, vi kan bidra till en mer slimmad process i vår granskning att man utnyttjar systemfunktionerna, istället för att göra en massa manuella moment vid sidan om så utnyttjar man systemet.
R1: Men det kan ju också vara, om man pratar styrning av IT: s värde, det kan också vara att vi kan ju dela med oss av erfarenheter från andra, vi har ju så många olika kunder så kan vi plocka godbitar därifrån vi vet att det fungerar bra, jag vet inte vad man ska ta för exempel men en de företag jobbar ju med att IT-avdelningen fakturerar ut en kostnad för varje användare som finns i systemet exempelvis.
H: Mmm.
R1: Och säger man att vi har sett exempel på att det här fungerar ganska bra som ett sätt att jobba på så kan ju vi förmedla det vidare till den kunden vi här hos just då och som har problem med det så att.
H: Jag tror lite det som ni pratade om innan att man för upp det till ledningen, att man får dem att inse att det kan vara ett problem och sådär och på så sätt ser ni kanske också att ni kan bidra till att det blir en bättre förståelse?
R1: Ja absolut, det är väl egentligen den stora biten som vi kan bidra med, att förmedla upp vad vi tycker är viktigt och vad vi har sett, det tror jag.
R2: Det är också en utmaning för oss att förmedla IT-revisionen till de IT-ansvarige för vi kommer ju in med ett perspektiv mot den finansiella rapproteringen och det är viktigt att kommunicera det och att man som mottagare som IT-chef eller IT-ansvarig på området inte tror att vi kommer in och testar den tekniska set-upen fullt ut för att bedöma den utan att det är mer ur ett revisionsperspektiv och de domäner som vi diskuterat utifrån då så att säga, så att de verkligen förstår vad detta avser göra och varför det är viktigt då.
H: Ja, fråga nummer 11 är hur ni tycker att IT-revisorn kan kontrollera att IT: s värde till verksamheten blir synbart till organisationen men det har vi varit inne på.
R1: Mmm
R2: Vi gör en uppföljning på de iakttagelser som noteras och nästa års revision så följer vi upp status, vad har hänt på de här områdena och då ser man ju lite hur pass mottagliga, hur mottaglig organisationen är på vårt synsätt.
H: Okej, men om ni exempelvis ser att, okej IT verkar vara en väsentlig del i företaget men att det inte förs fram på rätt sätt, kan ni komma med rekommendationer till exempel att här bör ni göra någon form av förändring för att…
R2: Alltså ibland kanske man inte har resurser för att göra som vi rekommenderar, kan vara en bidragande faktor, då kan vi kan ta fram kompenserande rutiner eller kontroller som man kan ha för att hantera de eventuella brister…
R1: Sen hänger det ihop lite grann med att företagets verksamhet och hur vi bedriver våran revision hänger ihop ganska mycket så om företaget har en ineffektiv IT-revision med lite kontroller, då blir det svårare för oss att bedriva en effektiv IT-revision, så att det hänger ihop och det brukar revisorerna som jobbar med finansiell revision vara ganska snabba med att påpeka det också att det här göra att vi inte kan granska effektivt och då får man också ett helt annat kryck i, men det hänger ju ihop så att säga.
S: Sen här, vilka moment gällande IT: s bidrag till verksamheten anser ni vara mest kritiska, det är kanske som ni sa att det förs upp till ledningen just, att det är en viktigt del.
R1: Ja precis, det beror lite på vad ni menar med frågan här men att…Det är klart att IT ska stödja verksamheten så bra som möjligt och om man tittar på system så vill man gärna att önskemål om nya system ska vara drivet från verksamheten, från affärsprocesserna, det är de som ska komma med önskemål om ett nytt affärssystem det ska inte vara IT-drivet. Det som är viktigt för IT, om man frågar en IT-chef vilka system är viktiga för dig så kanske han säger, för mitt dagliga arbete så är det kanske e-post så är det det enda som är viktigt för honom men frågar man ekonomichefen så är affärssystemet det absolut viktigaste, det är de som ska äga och därför är det vitkigt att det är

verksamheten som ska vara kravställare så att säga och sen ska IT ges möjlighet att leverera det som verksamheten kräver.
H: Det här med systemägare och processägare, hur ser ni på det och varför är det viktigt?
R1: Det är bra och det är viktigt därför att någon måste ha ansvaret att dels se till så att systemet gör det som det ska göra men också ska någon vara, om man pratar om kritisk informationsdata, att någon ska äga datan och måste känna att det här är min data, det är jag som bestämmer hur den ska hanteras och så. Och det ska ju också ofta vara någon i verksamheten, är det ett affärssystem då är det verksamheten som ska äga det. Är det ett system som håller reda på nycklar till fastigheten, då kanske det är någon på fastighetsavdelningen som ska äga det för att det är de som kan det , det är de som har nytta av det…
H: Mmm
R1: och processägare, det är viktigt att någon har ansvar för att processen fungerar, att man ser till att de kontrollerna som ska göras faktiskt görs, att den dokumentationen som måste finnas finns och det är också en styrningsfråga egentligen, att se till att någon känner ett ägandeskap att leva efter, att uppleva styrning, att implementera styrning egentligen.
H: Är det vanligt att det står på papper till exempel då, att det är en viss processägare men att det i själva verket inte bedrivs på det sättet?
R1: Det är väl inte helt ovanligt.
R2: I mindre verksamheter så har man kanske inte det på den nivån utan då har man en systemägare, informationsägare och i större klienter kanske man har per process per område.
R1: Jag tror det är en skala också, i de stora bolagen brukar det vara riktigt tydligt därför att man på störr e bolag ofta utsätts för problematik att man kommer till slutsatsen att man måste ha en systemägare, msåte ha en processägare för att hantera de här frågorna. Där finns det också definierat och de vet också vad det innebär att vara systemägare och går man ner på de mindre klienterna så är de oftast, chansen att man ska få mer omogna klienter att man har ingen systemägare, eller att det finns en men han vet inte riktigt vad det betyder.
H: Mmm
R1: Man upplever också på många halvstora bolag att IT-avdelningarna kämpar med att få verksamheten att förstå att de är de som äger saker och ting. Det har varit IT-drivet innan men IT kämpar för att få verksamheten att förstår att det är du som äger det här systemet, det är du som måste bestämma i vilket riktigt det ska gå sen hjälper, realiserar och förvaltar vi då men det är ni som äger det.
H: Ja, nästa tema är interna kontroller och det är ju ett ganska vitt begrepp men om ni tänker på det generellt sätt, vad anser ni då vara syftet med företagets interna kontroller?
R1: det vi är mest intresserade av är ju interna kontroller som påverkar finansiell rapportering och det är egentligen en viss typ av intern kontroll men syftet med den är ju alltid att säkerställa riktigheten i finansiell data, att det som rapporteras är rätt och riktigt. Men sen kan man, vi har ju varit inne och pratat om operationella kontroller innan, och det kan ju vara för att säkerställa att systemen är uppe en viss tid och, så det är ju egentligen, om man säger IT, interna kontroller, dels är ju syftet finansiell rapportering men sen är det ju också för att kunna styra och kontrollera IT som man vill så man kanske gör 5 kontroller om dagen för att kontrollera att systemen är uppe 99 procent av tiden, det är inget vi tittar på inom ramen för revisionen men det är ju för att de ska kunna nå sina mål på IT-avdelningen då så det handlar ju om styrning och kontroll.
H: Och dem kan man väl säga att de kontrollera tittar ni på lite indirekt för att säkerställa det som har med den finansiella rapporteringen?
R1: Ja, de kontrollerna som har direkt påverkan på finansiell rapportering tittar vi ju alltid på, det som är vid sidan av kanske vi berör i samband med att vi pratar styrning och så, men det är ingenting som vi, om man gör det här kontrollerna för att se att systemet är uppe 99 procent av tiden och vi inte tycker att de har direkt finansiell påverkan så tittar vi inte närmre på dem, det kan vara bra att känna till att de finns.
H: Men det kan fortfarande vara en rekommendation, en iakttagelse?
R1: Det kan det fortfarande bli, vi begränsar oss inte alltid så till bara kontroller som har direkt finansiell påverkan men ofta håller vi oss inom de ramarna och sedan rapporterar vi upp.
H: Man kan kanske se det som att det blir något slags mervärde för kunden?
R1: Absolut, allting som är av direkt mervärde försöker vi ju bidra med och det är stort fokus hos oss internt att revisionen ska inte bara vara en revision utan den ska tillföra ett bra mervärde till bolaget och därför delar vi gärna med oss erfarenheter från andra företag, det som fungerar bra och så.
R2: Man kan ju säga att vi tittar på interna kontroller på lite olika nivåer, nu har vi diskuterat IT-miljön här som vi ser som grunden för hela verksamheten, ovanpå den grundläggande IT-miljön så ligger ju applikationerna där har man ju också interna kontroller i form av applikationskontroller, kredit och limits tidigare och sen ovanpå applikationerna sen har man ju sina manuella rutiner i affärsprocesserna har man för att manuella rutiner därutöver så

att säga har man även en viss nivå av intern kontroll. Vilket gör att de här tre lagerna totalt sätt interagerar så att det blir en fullständig harmoniserad intern kontrollmiljö nu då.
H: Manuella rutinerna var nu?
R2: Det är själva affärsprocesserna då, rutiner i affärsflödet som inte hanteras i affärssystemet
R1: (Ritat upp pyramid bild för att illustrera olika företagslager) I botten när vi tittar på IT-verksamheten så ser vi att, i botten är det databaser och operativsystem, applikationer SAP M3 Movex Navision, och sen affärsprocesserna inköp försäljning och så vidare och ofta jobbar man ju direkt i applikationerna så man ligger ju jättenära och sen på toppen analysen och nu pratar vi ju egentligen hela revisionen och interna kontroller hos företaget och analyser typ uppföljning mot budget, marginaler på olika produkter och så va och sen styrning ligger egentligen som något lager över allt i hopa och pratar vi IT-styrning så är det ju IT-säkerhetspolicys och så och styrning för företaget som helhet kan vara allt från policys som gäller riktlinjer för hur man anställer folk och så på jättehög nivå men det är IT som är fokus här va, vi pratar inte om?
H: Ja precis…Jag vet inte om ni har något att lägga till på fråga 14 där, vad anser ni att bra kontroller kan ge för effekter i företaget?
R2: Vi kan bara knyta till den bilden igen som R1 ritade om vi nu pratar om IT då, om man ser på den här pyramiden då, om man inte har en god kontrollmiljö på lägsta nivå så faller egentligen resterande lager också eftersom om vi tittar på en databas och någon kan gå in och ändra information där, då spelar det ingen roll vad vi har för kontroller i applikationen eller processen för att de sätts ur spel i och med att man har en access som medger att man kan förändra information direkt så att säga. Så att det är därför IT är viktigt i revisionen i hela verksamheten.
R1: Sen är det klart att det, effekten på företaget, låt säg att man inte har en intern kontroll på företaget så kan det ju bli väldigt ineffektivt också alltså att man kan, helt plötsligt så börjar man få konstiga fel när man bokar saker i affärssystemet och då kanske det beror på att man gjort något fel på IT-nivån och då får man lägga 200 timmar på att reda ut det på inköpsavdelningen så att det handlar om effektivitet i hela företaget egentligen.
R2: Mm, och sen är här ett operationellt det är så att exempelvis en server och att man inte har en fungerade backuprutin, vad gör man då och man inte kan läsa tillbaka bakcupen så att det är en förutsättning för att man rent operationellt också ska kunna bedriva sin verksamhet.
S: Mmm…
H: För att stödja verksamheten blir det väl? Jag menar, om man effektiviserar IT så effektiviserar man också resterande delar av verksamheten?
R1: Så kan man också säga, precis. IT ska ju stödja verksamheten och om IT ska utveckla någonting så ska det ju vara på begäran av verksamheten och bara det som verksamheten vill ha och inte någonting annat. Det är på så vis man stödjer verksamheten effektivt.
H: Ja, nummer 15 tycker jag att ni har besvarat här.
R1: Mm, det var egentligen de här exemplen vi gav att man tar ut loggar och spårar tillbaka eller begär in policys och läser igenom och…
H: Och vilka moment gällande det här arbetet anser ni då vara mest kritiskt.
R1: Jag skulle vilja säga, alla de domänerna som vi pratat om, de är viktiga, de som har, spontant sätt säger man väl alltid att behörighet är det som har störst genomslagskraft och det hör också ihop med att det är det som är svårast att kontrollera.
R2: Det är de kontroller som ligger närmst den finansiella informationen egentligen, har man en felaktig behörighet så kommer man direkt åt den informationen så att säga.
H: Om man tänker de domänerna i form av IT-styrning, hur skulle ni vilja rangordna dem? Vilka är mest viktiga, jag antar att den första var den som var mest generell?
R1: Precis, det är den som behandlar, som pekar direkt på IT-styrningen, där vi frågar efter styrande dokument och hur de styr sin verksamhet, det är ju den som handlar om IT-styrning och om man ska rangordna de andra, det blir ju lite svårt men om man tänker baklänges då, vad skulle innebära störst risk och felaktigheter i finansiell rapportering om man inte hade IT-styrning överhuvudtaget så är behörighet och programförändringar som skulle få störst genomslagskraft på den finansiella rapporteringen i alla fall
H: Skillnaden mellan den här programutvecklingen och programförändringen var nivån av den?
R1: Ja, och edt finns inget fast. Om du går ut och frågar ett företag om programutveckling är oftast det man kallar för projekt och ofta har företagen kanske till och med en timgräns som säger att en utveckling eller programmering som tar mer än 40 timmar kallar vi för projekt och då kan man säga att det är det som är programutveckling. Kontrollerna är ungefär desamma. Så det är inte så stor skillnad på dem.
S: Nej okej. Om vi går till extern kravhantering då, på vilket sätt kan ni som IT-revisorer kontrollera att de tillmötesgår de externa krav som de omges av?
R1: Tänker ni på exempelvis lagkrav och så?

S: Ja precis, ni nämnde SOX här tidigare till exempel.
R1: I egenskap av revisorer hos en kund så är vi naturligtvis skyldiga att kontrollera det vi ska uttala oss som så när det gäller Sarbanes-Oxley så skriver vi ett utlåtande om vad vi tycker om deras interna kontroller så där är vi ju direkt involverade och då har vi ju också direkt granskning av det. Sen kan det ju finnas andra lagkrav på IT som kommer kanske ifrån Food and Drug administration i USA eller någonting, de tangerar ju ofta det vi tittar på men vi granskar aldrig det eftersom vi inte behöver uttala oss om det så granskar vi aldrig det specifikt heller om de inte begär det. Vi är kanske inne på samma områden men det är klart om jag nu kan FDA-lagstiftningen innan och utan och jag är hos en klient och ser att de inte uppfyller det så skulle jag ju såklart kanske diskutera det med dem men för vår granskning skulle det inte ha någon betydelse mer än att det skulle vara en observation, en brist för oss också om de inte följde lagstiftningen men det är inte så att vi gör en extra verifiering av det utan om det nu är FDA-lagstiftningen som de lyder under då har de egna kontrollanter som säkerställer det.
S: Ja det kanske är svårt att lista de men vilka är de mest kritiska faktorerna i det arbetet med externa krav?
R1: Om vi tar Sarbanes-Oxley som vi är tvingade att uttala oss om…då följer vi ju det regelverk som i det här fallet PCAOB ger ut då som talar om för oss som revisorer som granskar en kund som påverkas av den här lagstiftningen, ni måste göra detta detta och detta så då är det egentligen kritiskt att vi följer det regelverket. Om de påverkas av någon annan lagstiftning som vi inte behöver uttala oss om så skulle man försöka diskutera det med dem, vad de gör och vad de inte gör för att efterleva detta men eftersom vi inte behöver uttala oss om det så behöver vi egentligen inte lägga jättemycket krut på det heller.
R2: Det är ett lite svårdefinierat område, jag tänkte på bokföringslagen där också. Man tänker till exempel, vad är där för arkivering kring data, det finns ju vissa regler, tio år i elektroniskt format ska man ju, man får hålla sig uppdaterad där på vad det är som gäller. Sen är det väl inget specifikt vi dyker ner på, alltså i vår metodik utan det är mer fullständighet och riktighet gällande finansiella transaktioner. Med syfte att säkerställa.
H: Om vi går vidare då till temat organisation- och beslutsstruktur så första frågan då om ni anser det vara viktigt för en IT-revisor att granska organisationsstrukturen för kontroller och beslutsfattande och i så fall varför?
R1: Mmm, vi var inne på det lite grann innan med den här första domänen och det ger väl en bild lite av hur det fungerar, hur man styr sin IT och det kan också ge föraning om vad vi kommer att se i de andra domänerna. Och det är egentligen det viktigaste för oss att förstå mognadsgrad och sådär, för det hjälper oss att identifiera riskerna i de andra domänerna. Om de säger att de inte har några styrande dokument överhuvudtaget, ja då kan vi dra slutsatsen om att risken är förhöjd i de andra, att vi ska hitta felaktigheter då, det är nog det jag skulle säga.
R2: Precis, det är egentligen en förutsättning för att en kontrollmiljlö ska fungera, är att man har en organisation som stödjer, och i kontrollmiljön då att man har någon som är ansvarig som kontroller, följer upp och bevakar hur sakerna utförs. Problemet är, om man nu pratar SOX så, det krävs ju en viss mognadsgrad också hos klienterna och det är viktigt att kunna se syftet men en kontroll också inte bara att man ska ha en kontroll utan man måste förstå varför man jobbar efter ett visst kontrollmål. Det är väl kanske så att man kräver en viss mognadsgrad och tid för att etablera den typen av tänk i en organisation, det såg man ju framförallt på de SOX-uppdrag som dök upp för ett par år sedan när bolagen tvingades in under det här regelverket, man såg bara kontrollerna men hade lite svårt för att sätta sig in i vad syftet var och hur man skulle utnyttja de optimalt i verksamheten.
H: Ja, och på fråga 20, är det något ni jobbar med och det var väl den första…
R1: Ja precis, svaret är ja och vi gör det oftast via intervjuer och begär in policys och så
R2: Det är också en del av vårt revisionsbevis när vi testar en kontroll, att det finns dokumenterade bevis att det är någon som är ansvarig som har signat av en kontroll så att det är så vi förlitar oss på att kontroller har exekverats att det finns ett dokumenterat bevis från en ansvarig person eller något sådant som har det som sitt ansvarsområde.
H: Vi har pratat väldigt mycket om kontroller men just biten för beslutsfattande, är det samma sak där, tittar ni på det också?
R1: Ja, det är klart, olika kontroller innehåller ju beslutsfattande också men det kan ju handla om IT-investeringar och vem som får fatta besluts om det och det gör vi ju oftast fast på uintervjubasis och dyker inte lika djupt i det. Man frösöker skaffa sig en förståelse för hur företaget jobbar.
S: Ja, om vi går över till risker och riskhantering, hur bör IT-risker eller IT-riskpolicys hanteras eller granskas i relation till följande områden, klassificering av risker, kommunikation, ansvarsskyldighet, åtgärder och kontroller, ni kanske kan ta mer övergripande hur…
R1: Här skulle man nästan…om man tar klassificering av risker, det beror nästan på från kund till kund skulle jag vilja säga, om man har en kund som är extremt IT-beroende vi pratade om ett spelbolag och så innan du skulle man ju vara ganska intresserad av att se att de gjort en ordentlig utvärdering av risker framförallt relaterat till deras spelsystem och så. Jag menar om de inte utvärderat risker och inte har rätt skydd så kan ju det betyda att det bolaget kommer att gå i konkurs, om det spelet försvinner från Internet i 2 månader så går de i konkurs. Och hur granskar

man det då, vi skulle begära ut bolagets egen klassificering av risker och egentligen granska den och ifrågasätta hur man har tänkt och vad man har gjort för att åtgärda dessa risker.
R2: Ja, precis det som är vitkigt än en gång tycker jag är att de har en löpande uppdatering på sina aktuella risker och man årligen gör en utvärdering om vad det är som har förändrats dels till vår externa miljö och sen internt också, det kan vara risk att hela sajten går upp i rök, det kan vara en risk att man har något läckage internt att man har behörigheter eller liknande är konfigurerade fel, det beror på vilken nivå man får se riskerna så att säga.
H: är det viktigt på samma som gällande processer, att man har kontroller för risker, att man har ansvarsskyldighet och att man har struktur helt enkelt?
R1: Ja, precis, struktur är ju egentligen nyckelordet också. Man har ju identifierat ett antal risker vilket jag tänker mig att företaget gör då i form av någon workshop eller tar hjälp av några konsulter för att hitta risker, så vill man ju också se att man satt in åtgärder för att hantera de riskerna, man har försäkrat sig mot vissa saker eller att man har kanske dubbla datahallar, brinner den egna upp så växlar man bara över till den andra. Och att det finns ansvariga för att hantera olika saker, har man kanske en katastrofplan, vad händer om datarummet brinner ner, vem ska man ringa och vad ska man göra.
H: Kan ni titta på dessa bitar med?
R1: det gör vi men, på större företag är katastrofplanerna enorma
R2: Det är ju inte vår huvudkompetens, riskanalys så att säga, det finns ju bolag som enbart jobbar med det så att säga, kostar jättemycket pengar men det viktiga här är som vi var inne på tidigare att man ser att man har en uppföljning på risker och att man följer upp det löpande och att man tagit ställning till interna och externa risker.
R1: Men har man gjort en dokumenterad riskanalys så tar man ju ofta in den och tittar på och det är klart, ser vi eller tycker att det fattas någonting så tar vi ju upp det eller tar en diskussion om det, de kanske redan har tänkt på det
R2: man kan ju se risker i allting om man vill, så det är ju en utmaning för oss att hittar rätt nivå, vad är det som för vårt perspektiv då kan vara en risk och inte en risk.
H: Om ni känner att det fattas någonting, är det, hur tar ni reda på det så att säga, använder ni några verktyg?
R1: Det finns, det var längesedan jag gjorde det själv men vi har otroligt mycket verktyg för diverse olika saker internt och det finns även IT-riskverktyg och då skulle man kunna jämföra den aktuella kunden mot andra kunder i samma bransch eller i samma situation på olika, och då få upp ett gäng risker som normalt sätt bör finnas och det är sådana verktyg som vi väldigt ofta använder, för den här typen av situation så finns det följande, bör följande risker finnas eller vanligtvis och sen det är klart, kanske inte alla är applicerbara för just den kunden men…
H: Men det är samma sak där, anpassa efter kunden?
R1: Ja precis, anpassa efter kunden…och man kan använda det för att ifrågasätta varför gör ni inte det här…
S: Och vilka moment anser ni då vara mest kritiska gällande riskhanteringsarbetet?
R1: Det är väl uppföljningen lite som du varit inne på R2?
R2: Löpande…
R1: men uppföljning, att man dokumenterat också, dokumenterat tagit ställning och förankrat det, det här är våra risker det här är vad vi måste göra för att ha en acceptabel, man pratar ofta om riskaptit, vilket typ av riskaptit kan vi acceptera. Och kokar man ner det så är vi lite inne på det vi berörde tidigare, då är vi inne på hur länge kan vi vara utan systemet, det kan vara en aspekt av det, ah det här systemet kan vi vara utan i två dagar utan att det gör någon skada men det här systemet måste fungera inom en timme för annars så kommer företaget att förlora pengar eller det kommer att påverka oss negativt. Att man tagit det hela vägen, att man inte bara satt sig ner i ledningsgruppen och spånat lite kring risker utan att man också har börjat sätta in, vad har vi då för åtgärder som hanterar det här och här har vi något som saknas och då måste vi göra någonting åt det, då får du göra det R2. Att man också är medveten om, faller den här risken ut så kommer det att kosta oss så och så, medvetenhet och ett strukturerat riskarbete.
S: så det här med riskaptit, toleransnivå, trösklar är det sådant ni diskuterar med klienten då?
R1: Ja precis.
R2: Ja precis, i grund och botten om man nu pratar om risker, det är ju framförallt backuprutiner, har man väl fungerade rutiner på den nivån så har man, för att ha en offsite location som man tar sin backup till så är man rätt så garderad i alla fall för externa risker. Men som sagt, man kan se risker i allt och på olika nivåer men det är i alla fall ett minimumkrav som vi tycker att man bör ha förankrat det, kontrollerna på.
S: Ja avslutande frågor här, varit inne på denna ett antal gånger känns det som men vi har diskuterat olika faktorer ju framförallt de här 4 domänerna som är viktiga att beakta vid en IT-revision men hur skulle ni rangordna dem då i relation till IT-styrning?
R1: Mmm, vi har nog nästan sagt det där. Jag skulle vilja hävda att den första domänen där vi faktiskt efterfrågar styrdokument och kanske intervjuar IT-direktören då på hur han faktiskt styr sin verksamhet, det är det batteriet som blir det viktigaste.
H: Och varför, det kanske blir lite upprepning, men varför är det så viktigt att göra den biten?

R1: därför att det säger väldigt mycket om hur mycket ordning och reda är det på resterande områden som vi är intresserade av i vår granskning då och det ger oss input till hur vi ska bedöma riskerna till IT-miljön och det påverkar sedan resten av revisionen också då. Så att ser vi jättestora risker i IT-miljön redan från början så kanske vi väljer att inte ens granska IT-miljön utan då gör vi det vi kallar för substansgranskning då, det kan vara någon som tar ut jättestora mängder data, något som R2 också jobbar med, i detalj istället för att förlita sig på att man har en fungerande IT-miljö då. För ett revisionsperspektiv så säger den första domänen väldigt mycket om vilka risker vi kan förvänta oss att hitta då.
H: var har den domänen som härkomst ifrån?
R1: Jag tror att den kommer från COSO, COBIT.
S: Finns det några andra områden inom IT-styrning då som ni anser vara viktiga i ert arbete utöver det vi diskuterat?
R2: Vi var nog inne på det lite tidigare men man måste ha en förståelse för hur klientens verksamhet ser ut så att vi får anpassa vår testning och kontroller efter deras miljö så att säga, det som vi talade om tidigare, att tillföra ett extra mervärde till klienten och sen får vi ju se på våra kontroller utifrån hur organisationen ser ut så att vi inte trycker in en massa kontroller som inte har något syfte så att säga just i deras miljö.
H: Ser ni det här med extra mervärdet, att det kan vara förankrat till IT-styrning, att ni hjälper dem där indirekt i många moment som ni faktiskt går igenom?
R1: Jag tycker att alla moment ger, beroende på hur vi ser det, någon form av mervärde egentligen och det kan ju vara dels till företagsledningen i allmänhet som får veta hur IT-avdelningen fungera eller inte fungerar men också om IT-direktören har tagit fram ett bra ramverk för styrning och han får feedback från oss att det fungerar inte riktigt som du hade tänkt så ger ju det ett väldigt stort mervärde för honom i sin roll som IT-direktör då så det tycker jag absolut. Så det är egentligen på alla olika nivåer tycker jag, att det ger mervärde.
S: Ja, då är vi nog nöjda där.

B2.4 Intervju Företag D

Transkribering av intervju med Respondent från företag D 6 maj 2010

S = Stefan Arnslätt
H = Hampus Karlsson
R = Respondent (Informant)

S: Ja, då börjar vi intervjun här med Respondent från Företag D som har gått med på att vi spelar in samtalet. Vi börjar med två inledande frågor här. Om du vill beskriva dina arbetsuppgifter samt din position här på företag D?
R: Mmm. Jag jobbar framförallt med IT-revision på våra revisionskunder. Och sen jobbar jag även en del med andra konsultprojekt, management- och konsultprojekt, inom IT-säkerhet skulle man kunna sammanfatta det till. Min position är ju officiellt IT-revisor inom samma affärsområde som dom vanliga revisorerna tillhör, men vi jobbar som sagt inte bara med revision utan även med konsultverksamhet. Så det är lite uppdelat, ungefär hälften av tiden till båda arbetsuppgifterna.
S: Hur länge har du jobbat som IT-revisor och vad var det som fick dig intresserad av området?
R: Jag har jobbat i två år, och det som fick mig intresserad var att man kan kombinera flera olika intresseområden. Jag är intresserad av ekonomi, men även av IT, och även att ha kontakt med människor ute på företag och inte bara sitta bakom en datorskärm. Och då fungerar den här tjänsten bra, och den ligger även i linje med utbildningen då, systemvetenskap, som även är ganska...ja, tvärvetenskaplig är väl fel ord, men den innefattar många olika områden.
H: Bara lite nyfiken, har du en utbildning i ekonomi också?
R: Nej, jag har läst extrapoäng i ekonomi som dom valbara timmarna så att säga, men jag har ingen examen i ekonomi.
S: Okej. Då går vi in på de här temaområdena som vi har, vi börjar med definiera och hantera processer. Vilka moment anser du bör gå igenom vid en granskning av ett företags processer, vi menar då IT-processer?
R: Dom processer vi framförallt granskar när vi gör en IT-revision det är ju processen för programförändringar av affärssystemen framförallt, och behörighetsprocesserna. Om vi börjar med programförändringar, då vill vi ju säkerställa att de förändringar som görs i systemen, som har påverkan på den finansiella redovisningen, att dom ska vara godkända, testade, innan dom förs in i produktion. Så att man vet att det inte är någon programmerare som kan sitta hemma på kammaren och göra lite småförändringar, som han själv tycker är bra att ha så att säga. Allting ska vara godkänt och testat. Och om vi tittar på behörighetsprocessen så tittar vi framförallt på hur går det till att få behörigheter. Vem kan beställa? Vem måste godkänna? Tittar man över de behörigheter som ligger i systemen, att det finns en viss periodicitet. Så att det inte ligger kvar några gamla konton, eller konton på folk som bytt avdelning

eller något. Eller att de kanske har för höga behörigheter. Det är jättevanligt att om man jobbar i en stor organisation och man byter avdelning flera gånger så samlar man bara på sig mer och mer och mer behörigheter, för att dom rensas aldrig och till sist sitter man med jättemånga behörigheter och ingen vet hur det ser ut i systemet. Så därför är det viktigt med en sådan process.
H: Hur jobbar man då praktiskt med de här momenten som du nu har beskrivit?
R: I första hand så intervjuar vi de personer som är ansvariga för det, för processerna. Och ber dom beskriva egentligen hur dom arbetar, och vi ställer frågan har ni den här kontrollen på plats, gör ni det här momentet? Gör dom inte det, då försöker vi hitta andra vägar för att ändå känna en viss säkerhet att det nog ändå ser okej ut i systemet. Men det är ju vanligast att större företag har bra processer för det här. Mindre företag har ofta inte den personalstyrka som krävs för att upprätthålla till exempel segregation of duties, alltså bra ansvarsfördelning. Utan då är det kanske en eller två personer som jobbar med IT, och då gör de allt, som har både med utveckling och behörigheter att göra. Så då är det svårt att upprätthålla bra säkerhet i IT-miljön.
H: Det här du säger om att om det inte går att säkerställa genom intervjuer, att man hittar andra lägen att säkerställa, hur tänker du då?
R: Till exempel om en person har rättighet eller möjlighet att genomföra en förändring på egen hand så kan man i bästa fall se då att de här förändringarna godkänns i efterhand, av en annan person. Så att den personen går igenom alla förändringar som varit i systemet under det senaste halvåret, och i efterhand skriver på att dom här har varit okej. Då kan man ändå tänka sig att det fungerar att låta den första personen ha rättighet att genomföra förändringen. Det blir en kompenserande kontroll i det fallet.
H: Så ni kontrollerar rent praktiskt sett hur det går till. Följer upp liksom
R: Ja.
H: Okej. Hur viktigt tycker du det är med dokumentationen kring processer?
R: Jag tycker att det är ganska viktigt, för att om processen är dokumenterad då vet man att det finns i alla fall möjlighet att alla ska kunna följa samma process. Annars är det risk att någon tror att det är så här processen ser ut och så sprider man bara det genom att prata med folk, och så till slut så sitter bara alla och jobbar på helt olika sätt. Har man ett fastslaget officiellt dokument då vet man att det här är det som gäller, och är det någon som avviker från det så är det lättare att peka på att de faktiskt inte gör det de borde göra.
H: Om det inte finns dokumentation till exempel, hur ser ni på det då?
R: Finns det inte dokumentation, då måste vi ju göra mer djupgående intervjuer, för att veta...vi måste ju ändå kartlägga processen för att veta om vi kan lita på den. Finns det inte dokumentation då finns det oftast inte någon fungerande process heller, utan då gör man det lite mer ad hoc. Och då när vi har granskat, då ger vi rekommendationer, att de bör dokumentera ner sina processer. Och vi ger även rekommendationer hur de här processerna bör se ut.
S: Ger ni rekommendation varför de bör ha dokumentation?
R: Ja, vi visar på vilka risker som kan uppkomma genom att inte ha vissa steg och kontroller i processen.
H: Det här med processägande till exempel, är det något ni tittar på?
R: Inte så mycket i IT-revision, utan det blir mer på SOX-granskningar och sånt. Just för IT-processerna, beror på hur stort bolaget är, men det är nästan alltid IT-chefen som är ägare för de IT-processerna, i alla fall i de mindre bolagen. Sen i de större bolagen, då kan ju vem som helst vara processägare egentligen. Men då blir det mer intressant vem som är kontrollägare i de processerna, det är ju de som verkligen ansvarar för att kontrollerna utförs. Men då är det ju på SOX, då är det inte IT-revision längre.
H: Vad innebär det då, granskning via SOX?
R: Ja, det är ju mycket mycker mer omfattande än att göra en IT-revision, för då ska verkligen alla steg vara dokumenterade, på ett mycket mer detaljerat sätt. Och då ska det finnas en utpekad kontrollägare för varje kontroll, och det kan vara hundratals kontroller då som man ska gå igenom och testa. Så att de verkligen fungerar, och det blir ett väldigt omfattande arbete, att vara utsatt för en SOX-granskning.
H: Det att man behöver en kontrollägare på varje plats, vad är syftet med det tror du?
R: Det är att någon ska vara ansvarig för att den här kontrollen alltid fungerar så att säga. Det ska ju inte falla mellan stolarna, utan den personen har till uppgift att se till att kontrollen alltid fungerar.
H: Jobbar man i så fall även med att följa upp och mäta processerna, till exempel att man har processmål? Att processen verkligen levererar det den ska göra, eller det den är tilltänkt för.
R: Det är ingenting jag i direkt har kommit i kontakt med. Nej. Det blir ju på något sätt att vi granskar det när vi gör vår walkthrough i processerna. Då ser vi ju om de är designade på ett sånt sätt att de skulle kunna fungera så som det är tänkt. Då blir det en granskning. Sen när företagen gör det själva, det...visst vi tittar även på om de löpande ser över sina egna processer och granskar dom, så man kan tänka sig att det är en kontroll från vår sida för att se att dom gör sin granskning över processerna. Men det är ingen jättestor bit, utan finns processen där och den ser rätt designad

ut då får man nästan också utgå från att den kommer att fungera som det är tänkt. Men det ser man ju då när man går igenom och verkligen testar. Och då tar man ju ut stickprov och ser att har de här stickproven verkligen följt processen som de ska.
H: Så vad är egentligen viktigt i hanteringen av processer, är det att man har policys och planer och rutiner för hur man driver dom så att säga?
R: Det viktigaste som jag tycker är att de personer som är inblandade i processerna, processägare, kontrollägare, verkligen förstår varför de har fått den rollen, så att det inte bara står i deras arbetsinstruktioner att du är kontrollägare för den här kontrollen och du ska se till att den funkar. Om man då inte förstår varför, eller syftet med det då blir det väldigt lätt så att det här hanteras med vänsterhanden lite vid sidan av. Man måste förstå väldigt bra varför man sitter där och har den rollen.
H: Av de moment du nu beskrivit, vilka anser du vara mest kritiska i förhållande till IT-styrning, vi ska nog passa på att säga det också att vårt approach till uppsatsen är IT-styrning, så du får gärna tänka i relaterade termer till det.
R: Ja. Jag tycker nog att just medvetenheten om varför man har ett visst ansvar är jätteviktigt, för det är ändå människorna som är inblandade som ska se till att den här kontrollen ska fungera. Sen kan man ha hur många papperstigrar som helst, om inte människorna är medvetna och känner att de tar sitt ansvar, då kommer det aldrig att funka.
H: Kan det vara så att dom har dokumentation, men ni upptäcker att dom följer faktiskt inte den?
R: Ja, det händer, det händer. Och det är ju typiskt ett sånt problem då, att då har man inte överhuvudtaget förstått varför man skrivit ner det i första läget. Då har man inte blandat in någon från de lägre nivåerna. IT-chefen kanske har suttit på sin kammare och författat egna policys och sen inte förankrat det ut, lägre ner i organisationen. Och då blir det ju bara en pappersprodukt.
H: Så vad ser du, vad är syftet med IT-revision?
R: IT-revision för våran del, när vi gör det på våra revisionskunder, det är för att vi ska känna oss trygga med att företagens kontroller fungerar så att säga. Känner vi att företagens kontroller fungerar, då vet vi att den information vi får ut från affärssystemen, den bör vara korrekt. Med stor sannolikhet är det rätt siffror som ligger där inne. Har kontrollerna inte funnits, eller det finns inga kontroller på plats, då kan ju inte vi lita på företagets kontroller. Då måste vi granska dom faktiska siffrorna från grunden, och göra en egen kontroll egentligen, om det är korrekt i systemet eller inte. Och det är ju också mer tidsödande, så det blir ju en mer effektiv revision om vi kan förlita oss på företagets kontroller. Då kan man lägga mer tid på andra saker som ger värde för kunden.
S: När du själv gör en sådan lite större kontroll, plockar du ut all data då, eller du gör ett stickrov eller hur fungerar det då?
R: Det finns flera sätt att göra det, man kan även använda sig av dataanalys, då kan man exempelvis plocka ut hela lagerregistret från systemet och så kör man dataanalyser på det för att identifiera eventuella konstigheter. Till exempel artiklar som legat för länge och kanske inte är värda det värde som de är upptagna i i bokföringen. Och då granskar man allt, då tar man in hela lagret till exempel. Men när vi gör kontrollgranskningen då tar vi ut stickprov, slumpmässiga stickprov. Och så går vi in och följer dom i processen, och tittar om processen har funkat i de fallen.
S: Ja. Om vi går vidare till nästa tema, säkerställande av systemsäkerhet. Vad är syftet med att granska företags säkerhetsrutiner?
R: Det är lite samma syfte som det tidigare området, att vi vill känna oss trygga med att de har koll på sin verksamhet, och att de har identifierat de största riskerna. Det är ändå företagen som vet vilka som är deras största risker. Vi har ju många företag inom många olika branscher så det är omöjligt för oss att vara bäst på att veta vilka risker alla företag står inför.
S: Just det här med risker, även om dom ska känna till det själv, är det något ni tittar på gemensamt med företaget och ser dom här riskerna som kan finnas och hur de ska angripa dom så att säga?
R: Ja, fast det är ofta finansiella risker. IT-riskerna är sällan av den digniteten att de skulle kunna påverka företagets fortlevnad. Och dom finansiella riskerna det är ju någonting som de finansiella revisorerna tittar på, så det gör ju inte vi i IT-revisionen.
S: Vilka moment då bör man fokusera på när man granskar ett företags säkerhetshantering?
R: Ja vi tittar ju då bara på IT-delarna, men vad menar ni egentligen med säkerhetshantering?
S: Ja, om dom har någon policy eller procedurer för att hantera säkerhetsfrågor.
H: Det kan vara lite det här som du var inne på innan, riskkontroller.
R: Mmm. För IT-policy är ju ofta skrivet med slutanvändare i åtanke, i syfte att informera dom hur de får arbeta med IT. Och det är ju för att minimera riskerna i företaget, till exempel hur man får ha med bärbara datorer utanför kontoret och så vidare. Och det brukar sällan vara med där hur man jobbar med behörighetshantering och förändringar i systemen utan det brukar mer vara interna policydokument.
H: Skydd mot nätverk och virusintrång och sånt, är inte det på ditt bord eller?

R: Visst, vi granskar ju att de här basala säkerhetsfunktionerna finns på plats så att säga, men vi granskar ju inte det något djupare, vad de har för typ av skydd och så. Fortfarande är det så, i en IT-revision, man vill kunna förlita sig på deras kontroller så att säga. Alltså vi går ju inte så jättedjupt och granskar på IT-säkerheten för även om dom får...ja visst, ett hackerintrång skulle ju kunna ställa till problem, men vi måste hela tiden se till att vi har ett visst revisionsarvode och företagen vill ju inte att vi använder det som dom enligt lag måste anlita oss för, för att gå jättedjupt in på vissa IT-områden. Man måste ju väga risk mot kostnad. Så det kanske är bättre att granska andra delar av verksamheten djupare, än att lägga allt eller mycket krut på att granska IT-säkerheten. Men vi kan ju självklart göra det om dom ber oss om det, men då blir det utanför den vanliga IT-revisionen.
S: Så man kan säga då att IT-revisionen är mer ett sätt att säkerställa att den finansiella rapporteringen blir korrekt?
R: Ja, precis.
H: Ligger det en tydlig linje då mellan ditt IT-revisionsuppdrag och den konsultbiten?
R: Ja, det är det, det är en tydlig skillnad. I konsultdelen så jobbar vi på uppdrag av kunden, i IT-revisionen så jobbar vi på uppdrag av revisorn. Kunden har ju inte bett att vi kommer dit och granskar deras IT-säkerhet när vi gör en IT-revision. Utan det är ju något vi vill göra för att känna oss trygga.
H: Ja. Så det momentet vi fick fram då var kanske det här med behörighet, gällande säkerställande av systemsäkerhet? Och det har vi varit inne på lite innan kanske, hur man praktiskt kan jobba med det? Ja. Då går vi vidare här till IT:s bidrag till verksamheten. På vilket sätt tycker du att en IT-revisor kan bidra till att IT:s värde förmedlas inom en organisation?
R: Under en IT-revision, eller under konsultarbete? Nästan lättast att svara på IT-revisionsdelen kanske.
S: Och det kan vara både som du känner en direkt påverkan men även indirekt, alltså att ditt material eller det du granskar på något sätt kan bidra, alltså både direkt och indirekt.
R: Ja, precis. Genom att vi gör en genomgång av deras rutiner så identifierar vi ju brister i dom, och presenterar då vilka risker de här bristerna kan leda till. Och genom att åtgärda dom så har man ju säkerställt att IT inte ställer till med något problem så att säga. För IT:s värde, jag ser inte direkt att IT har något egenvärde i en organisation. Det är en funktion som ska fungera, och visst, vissa företag är väldigt IT-beroende, men det är sällan IT driver verksamheter. Utan den ska ligga i linje med verksamheten, alignment det är ett bra ord. Det jag ser är att IT ska vara en möjliggörare för verksamheten.
H: Det här, det ni rapporterar, kan du berätta lite om strukturen på det, och vad det innehåller?
R: Vi rapporterar ju våra slutsatser till revisorerna, om vi anser att IT-systemen går att förlita sig på eller inte. Sen kommunicerar vi även rekommendationer till kunderna, där vi beskriver vad vi identifierat, vilka risker det kan medföra och vad dom kan göra för att åtgärda de här bristerna då. Och det kan vi göra via mail, eller vi kan komma ut på företaget och presentera det. Vissa företag vill alltid att man kommer ut och diskuterar sakerna med dom, för det är ju inte alltid ledningsgruppen förstår. I och med att de kanske inte är så tekniskt bevandrade så kan de behöva en förklaring, varför det här egentligen är en risk. Och då kan det vara bra att komma ut på företaget och beskriva det.
H: Dom här rekommendationerna, vem får ta del av dom i företaget, är det ledningsgruppen som du säger då?
R: Ja, alltså. Ledningsgrupp och IT-chef framförallt som är mottagare av det. Sen är det ju fritt för dom att kommunicera ut det här i organisationen, om de vill åtgärda. För det är ju upp till dom om dom vill åtgärda de här bristerna, eller om dom vill leva med och acceptera risken. Det är ju också ett övervägande, som med allt annat, om det är värt kostnaden. Att ställa risk mot kostnad hela tiden.
S: Du var lite inne på här, just att ni rapporterar till ledningen, kan det vara ett sätt...nu tänker jag på det här just att IT:s värde förmedlas, att ledningen på något sätt får en insyn i IT-frågorna och lyssnar kanske lite på er då, att ni liksom för fram IT:s budskap så att säga.
R: Ja, fast problemet blir ju att vi rapporterar bara brister. Men visst, vi kan ju synliggöra mer hur man jobbar med IT i den verksamheten, det är ju inte alltid att det är så tydligt för ledningen. Och på det sättet så kan man ju få upp ögonen för att IT har en viktig roll i verksamheten. Men samtidigt så går det ju att tolka som att IT bara bidrar negativt, i och med att vi bara presenterar brister. Det finns ju ingen anledning att presentera här fungerar det bra. Det ger inget mervärde. Utan vi presenterar ju dom rekommendationer och brister som vi ser, som behöver åtgärdas.
S: Ja, för du pratade ju lite om det här med medevetenhet. Det kanske skapar större medvetenhet om vad IT faktiskt gör, för även om det är i negativa termer så får man en uppfattning om vad IT syftar till att göra så att säga.
R: Ja, visst. En bra företagsledare skulle ju identifiera då att åtgärdar vi de här riskerna så har vi ju drivit verksamheten framåt och kan, nästa år kanske vi kan göra ännu bättre så att säga.
H: Man kanske tänker på då också, vad händer om vi inte åtgärdar dom? Och då får man kanske en förståelse för hur viktigt IT är. Åtgärdar vi inte de här problemen, dom här riskerna faktiskt faller ut, då står ni inför ett väldigt stort problem.

R: Precis. Det är ju sådant vi skriver till varje observation, och vi skriver ju riskbedömningar, det här kan ske om risken blir verklighet.
H: Så att synliggöra IT:s roll kan vara ett mervärde som ni...?
R: Ja, alltså. En del IT-chefer som vi har pratat med, dom känner kanske att dom inte är så sedda i organisationen, och vill gärna att vi tar med vissa iakttagelser till ledningen som dom kanske själva har påpekat länge, men inte fått något gehör från. Och då kan det vara en annan tyngd om revisorerna kommer och säger samma sak, och då kan IT-chefen säga att titta det här är ju det jag har sagt, och nu har vi fått medhåll. Då kan vi kanske hjälpa fram IT-verksamheten, så på det sättet så kan man kanske förmedla värde då.
H: Mmm. Och då har vi direkt svarat på fråga 11 här också, hur IT-revisorn kan kontrollera om IT:s bidrag till verksamheten blir synbart för organisationen. Så vilka moment gällande det här IT:s bidrag till verksamheten anser du vara mest kritiskt?
R: Det är ju i sådana fall att formulera de här observationerna och riskerna på ett sådant sätt så att den som läser det också förstår, och inte göra det alltför tekniskt, om nu tanken är att man ska presentera det för ledningsgruppen. Så måste man ju kanske knyta det till en verksamhetsrisk också, vad den här IT-risken kan orsaka för verksamheten.
S: Ja, om vi går över till intern kontroll. Det är ju ett väldigt vitt begrepp så du kan försöka tänka i lite generella termer. Vad anser du vara syftet med ett företags interna kontroller?
R: Det är för mig att andra externa intressenter ska kunna förlita sig på det företagets finanser framförallt. Mycket intern kontroll dök ju upp efter Enron-händelsen där investerarna trodde att det var ett företag att lita på, men det visade sig att det var helt tvärtom. Då började man ställa krav på att företag ska ha dokumenterad intern kontroll, till exempel SOX, för att man ska kunna förlita sig på det här. För det måste ju, du måste ju bli godkänd för att få säga att du är ett SOX-bolag. Och då vet man som extern att någon har gått in och gjort de här kontrollerna och kommit fram till att de fungerar. Då är risken mindre för att det ska kunna uppstå konstiga fel i företaget.
S: Ja, och vad anser du att bra interna kontroller kan ge för effekt för företaget?
R: Man hanterar sin risk och man ökar förtroendet utemot externa parter.
S: Hur kan du som IT-revisor kontrollera och granska de här kontrollerna?
R: Vi gör ju det genom att göra de här granskningarna, processgranskningarna i form av walkthrough och test och så vidare. Men i en IT-revision så går vi ju inte in och granskar SOX-kontroller och så i samma utsträckning. Nä men det är ju framförallt, då får man ju ta stickprov, om de har en kontroll, går man in och tar stickprov och kontrollerna funkar till alla de tillfällena.
S: Mmm…och vilka moment då när det gäller interna kontroller och kontrollera dem anser du vara mest kritiska?
R: typ av kontroller som jag anser vara väldigt viktiga är exempelvis bra ansvarsfördelning, segregation of duties, det är ofta också en kontroll som fallerar och det öppnar ju upp för möjligheter att genomföra saker som man inte ska kunna göra i företaget.
S: Är det något som ofta är ett problem, att det är många i organisationen som har väldigt bred behörighet så att säga
R: Ja, man litar väldigt ofta på sina medarbetare i organisation och det gör att man inte är så restriktiv och i Sverige har man en kultur att tillåta väldigt mycket medan i andra länder så låser man ner och öppnar bara upp det som ska kunna genomföras
S: Hur hanterar ni det om man märker att det finns brister där så att säga?
R: då blir det ju rekommendation på det, de bör ändra sitt arbetssätt och som jag sa tidigare så kan man kanske hitta kompenserande kontroller i vissa fall för att komma runt den risken.
H: DÅ går vi vidare lite till extern kravhantering ur ett IT-perspektiv, på vilket sätt tycker du att IT-revisorn kan kontrollera att företag tillmötesgår externa som de omges av? Varit inne på SOX en hel del, kan ju ta det exemplet, till en början.
R: Hur vi kan kontrollera det är ju egentligen bara genom att kolla om de är SOX-godkända eller ISO 27000 certifierade och är de det så har de ju uppfyllt de kraven i sådana fall och om det sen är några andra externa krav, det är ju väldigt individuellt beroende på vilka krav det är så att säga vissa kan man ju säkerligen lätt återskapa och se vilka krav som ställs så att säga.
H: kan ni jobba med dem, låt säg att de har de här kraven från sin omgivning så att säga, kan ni hjälpa dem med att jobba med dessa kraven till exempel som SOX-uppdragen?
R: Ja det kan vi göra fast inte som en del av en IT-revision utan då blir det som ett konsultuppdrag i sånna fall. Det är ju också en oberoendefråga i många av de här fallen, vi kan ju inte vara revisorer och samtidigt skapa kontrollerna åt dem, vi kan ju inte granska oss själva, då tappar vi ju oberoendet. Vissa råd över hur de eventuellt bör jobba men vi kan inte skriva eller skapa kontrollerna åt dem utan det arbetet måste de göra själva annars kan vi inte gå in och granska det året efter.
S: Nej.
H: Så ni kan meddela att de behöver en kontroll men själva skapandet av den är upp till dem?

R: Precis
H: Nu blir kanske den här frågan lite svår att besvara men vilka är de mest kritiska faktorerna gällande extern kravhantering?
R: Nej den kan jag nog inte svara på då.
H: Det är kanske som du sa tidigare att identifiera om de finns en certifiering då?
R: Jaja, om det bara handlar om att se om de uppfyller kraven och det är ett SOX-bolag så är det ju bara att identifiera dem.
H: Kan ni hjälpa dem att identifiera andra krav som de omges av, till exempel, de här kraven brukar finnas, jag tänker att ni kanske granskar liknande företag och så har ett företag en gedigen kravhantering och så kommer ni till ett annat företag och så har ni det i bakhuvudet lite, har ni inte tittat på de här bitarna?
R: Mmm, det ingår ju ofta när man planerar revisionen, alltså när man tittar på omvärldsrisker, omvärldsfaktorer och bedömer man då att det finns ett externt krav mot företaget så måste man ju gå in och granska det som en del i revisionen men återigen är det ofta en del av den finansiella revisionen för det finns mer krav på den sidan än på IT-området. Men IT blir ju givetvis påverkat av de kraven till viss del.
H: Det här med, du sa att ni planerar revisionen, är det en fas i sig?
R: Jo det är det, de som ingår i teamet måste ju sätta sig ner och bestämma hur de ska göra upplägget av revisionen för att veta vilka granskningsinsatser som behövs under året.
H: Vad innebär det för arbete för din del som IT-revisor?
R: Jag måste ju komma med mina åsikter och hur deras hantering ser ut kring IT, exemplev kommer vi kunna förlita oss på deras systemet eller deras kontroller och processer eller måste vi göra någonting annorlunda eller någonting mer för att uppnå den säkerheten vi vill i revisionen.
H: Men vet ni det innan ni går ut och utför revisionen?
R: Ja, vi försöker påbörja vårat arbete ganska tidigt på året för att få en känsla av hur hanteringen ser ut just för att kunna ge input till diskussionerna senare då när man verkligen lägger upp strategin för om man skapar en strategi först och sedan går ut och granskar och kommer fram till att vi kan inte förlita oss till företaget kontroller, då måste man ändra hela revisionsstrategin och då är det bättre att vi går ut och gör vårat jobb tidigt för att kunna lägga upp rätt strategi redan från början.
H: Om vi går över lite till det vi kallar kontroll- och organisationsstruktur, anser du det vara viktigt för en IT-revisor att granska organisationsstrukturen för kontroll- och beslutsfattande, och i så fall varför?
R: alltså organisationsstrukturen i sig tycker jag inte är så vitkig för kontrollerna men om vi tar exemplet segregation of duties igen, där är det ju viktigt att det är olika personer som godkänner men det kanske inte är så bra att kollegan på samma nivå får godkänna en sak, det är kanske chefen för den personen som bör godkänna vissa steg. I de fallen kan ju organisationsstrukturen vara viktig att känna till för annars vet man ju inte vem som är på vilken nivå så att säga. Det är oftast så att ju känsligare information som ska godkännas desto högre upp i organisationen behöver man gå men då försöker man ju också skriva kontrollerna på ett sådant sätt att det är väldigt tydligt vem som får godkänna var.
H: Mmm..och då har vi någon form av lokalisering av beslutsfattande i organisationen så att säga?
R: Ja vi ber dem ofta om organisationsstrukturen när vi gör en granskning.
H: Kan du utveckla det lite, hur ni jobbar med och får in det materialet, tittar på det.
R: Vi får ju oftast in en bild på organisationsstrukturen och sen ligger den då som underlag till senare beslut, det är inte så att vi sätter oss och har så mycket åsikter om hur de har strukturerat sig utan det är ju mer en bild att ställa i relation till när vi får vetskap om hur de jobbar.
S: Risker och riskhantering då, hur bör IT-risker, IT-riskpolicys hanteras och granskas i relation, vi har 4 olika områden då om du kan tänka på det övergripande också men att, om du bara ser till klassificering av risker, hur man bör hantera och granska det?
R: klassificering av riskerna, tänker ni då på att högprioriterade risker är sådana som kan allvarligt påverka företagets fortlevnad?
H: Ja, egentligen vilken typ av klassificering som helst.
R: Men det ser jag mer att man har katastrofplan och riskanalys och så vidare, när jag tänkter IT-riskpolicy, det är mer hur man ska jobba utifrån. Nu har jag aldrig stött på en IT-riskpolicy, IT-policy har jag stött på.
S: det är väl lite också med riskaptit, toleransnivå, trösklar och så vidare, hur man ser på risker helt enkelt om man har en kommunikation med företaget om vilka risker som anses vara mest farliga och hur ni hanterar det då och granskar att de kan kontrollera riskerna elelr att de kan skydda sig mot riskerna.
R: om det har en dokumenterad, jag skulle nog säga, riskhanteringsarbete så kan vi ju granska det och göra en egen bedömning om vi anser att de föreslagna åtgärderna är tillräckliga att vi ska känna oss trycka, men om det handlar om IT-revision så är det framförallt risker som skulle kunna påverka den finansiella redovisningen igen och det

närmaste området handlar ju om att skydda datan och det hanterar man ju genom att ta backup och så vidare så riskerna handlar ju ofta om att data försvinner, att data förstörs, det är inte lika vanligt att data skulle förändras för det hanterar man ju i sådana fall genom att ha andra kontroller för det, behörighetsåtkomst, förändringsprocess och så vidare. Så jag tror inte att vi göra någon jättedykning på just riskerna i en IT-revision.
H: Som du nämnde i början, tittar ni på någon katastrofplan eller någon riskanalys?
R: Finns den dokumenterad så tittar vi på det och gör en bedömning om vi anser att den är tillräcklig men ofta har dem gjort en riktig sådan plan så, många företag har inte gjort någonting överhuvudtaget så man får också ställa det i relation till att man börjar detaljgranska de som verkligen har skrivit någon, det kanske inte är effektivt ur kostnadssynpunkt.
H: Nej det låter ju lite märkligt kanske att man granskar de i detalj som verkligen har gjort en och de som inte har gjort någon låter man passera förbi så att säga. Men vad gör man om de inte har det, är det lite en liten väckarklocka?
R: Jo absolut, vi tycker ju att de bör ha en, det första steget är ju att göra en riskanalys för att veta överhuvudtaget vilka risker finns det som vi kan bli utsatta för, därifrån kan man gå vidare och jobba och få ett helt ledningssystem för riskhantering men första steget är ju att göra en riskanalys som sagt och det skriver vi ju som en rekommendation också om de inte har det på plats.
H: Tar ni det i åtanke när ni gör den här helhetsbedömningen som vi pratade om innan om företaget har ordentliga kontroller eller om ni måste in och substansgranska, ligger det här om de också har uppfört en riskanalys i paritet med det?
R: Nej det gör det inte för det kan inte direkt påverka den finansiella redovisningen, i förlängningen skulle det kunna göra det om det finns en jätterisk att all data bara försvinner. Det är ju i ganska extrema fall, så finns informationen där så kan det inte direkt påverkas av att de inte har eller har en riskanalys.
H: Har ni någon tyd av hjälpmedel om ni nu tittar och granskar och gör en bedömning av företagets katastrofplan eller riskanalys?
R: Ja eller, i och med att vi granskas många företag tidigare så för man ju en känsla för vad som bör finnas där och man kan ju på något sätt jämföra med andra företag inom liknande branscher då men sen finns det ju även rekommendationer från till exempel krisberedskapsmyndigheten som numera heter myndigheten för samhällsskydd och beredskap som ger ut rekommendationer om hur man bör arbete med riskanalyser. Och även ISO 27 000, informationssäkerhetsramverket har ju många bra, alltså man behöver ju inte certifiera sig och följa allt men man kan ju valda delar ur det ramverket för att nå en bättre riskhantering.
H: Är det likadant med SOX när man tittar på interna kontroller?
R: SOX är ju mer att man ska ha kontroll över finanserna så att säga medan ISO 27000 är mer IT-säkerhet så att man kan vara certifiera på både men de går ju in på varandras områden ganska mycket.
H: Jag bara tänkte på att det kan vara hjälp för ert arbete, inte det att de måste vara certifierade.
R: Jaja, visst man tittar ju på de här ramverken och plockar idéer därifrån absolut
H: Ert material mer generellt sätt, vad är det för material du jobbar med när du kommer ut och gör granskningar?
R: Vi har ju en metodik som är genmensam för hela företaget så att granskningarna ska ske på samma sätt oavsätt vem som gör dem och var de görs, vi har ju fastställda granskningsprogram och även hur vi ska genomföra tester och vad vi ska titta på när vi genomför tester
S: Denhär metodiken som du nämnde, kan du berätta lite mer om den, är det några speciella domäner den riktar sig mot, hur den är uppbyggd och så vidare?
R: Den täcker in en hel finansiell revision från början till slut, från första bedömningen om man ska ta in företaget som revisionskund till att man har lämnar över sista rapporten och IT-revision är en del av hela globala metodiken. Just vårat arbete ligger till grund för hur man arbetar med den finansiella revisionen då, de rekommendationer och de slutsatser vi kommer med påverkar ju hur de finansiella revisorerna ska jobba så vi är en integrerad del av den stora globala metodiken så att säga.
H: Mmm, hur har den här metodiken kommit fram så att säga, är den framtagen genom några ramverk som ligger till grund?
R: Metodiken har ju sin grund i de lagkrav som finns och ställs på alla revisionsbolag, vet inte exakt vad de heter men de är ju gemensamma över hela världen så men är ju lite anpassad efter de svenska reglerna också så vi ska uppfylla alla de kraven som ställs så jag tror inte att den skuljer sig jättemycket mellan de stora revisionsbolagen i och med att alla har samma lagkrav att följa så att säga.
H: Mer praktiskt sätt, har du med dig några checklistor när du kontroller?
R: Det finns checkliostor för exempelvis standardsystem, SAP, då kan man få ut ett färdigt granskningsprogram att de här bör du titta på men när det är mindre svenska affärssystem då finns inte samma utan då får man ta den standardiserade granskningen och anpassa den till just det systemet.
H: Mmm, och den standardiserade granskningen, vad är det för typ?

R: Där tittar vi på behörighetshanteringen och programförändringshanteringen och även andra backuper och det är relevant i granskningen. Då har vi ju ett antal kontroller som vi ska gå igenom då inom varje område för att få en helhetsbild av.
H: är det den standardiserade checklistan då som är uttagen från de lagkraven?
R: Nej, för IT-revisionen så är inte lagkraven, tror inte att det finns, finns vissa formuleringar om att man bör beakta riskerna inom IT-verksamheten men vad exakt man ska titta på är framarbetat av företaget globalt sätt, att vi ska titta på samma saker men det, jag antar att man har skapat den utifrån best practice, vad vi ska titta på för att vi ska känna oss trygga med att deras system hanteras på ett bra sätt.
H: och vilk moment som du anser vara de viktigaste gällande riskhanteringsarbetet, var väl kanske då att man hade en riskanalys?
R: Ja, det är ju första steget för att kunna hantera sina risker, först måste man identifiera dem sen kan man ta fram åtgärder för dem eller om man väljer att leva med dem men då måste man fortfarande vara medveten om att de finns.
H: Ja…om man skulle se den här som vi har på fråga 21, A, B, C, D som olika faktorer som man kan jobba med gällande riskhanteringen, vad skulle du anser vara viktigast då?
R: Klassificeringen är nog viktigast enligt mig, för annars är det ju risk att du jobbar för att åtgärda fel sorters risker när det finns andra som kanske är mycket mer allvarliga.
S: Som avslutande frågor då, vi har diskuterat lite olika faktorer som är viktiga att beakta då gällande en IT-revision, hur skulle du rangordna eller prioritera dessa faktorer i relation till just IT-styrning? Vi pratade ju lite om programförändring, att se till att de är testade och godkända och så vidare, behörighetsprocesser, de moment man går igenom och de faktorer man tittar på.
R: Precis, de är ju väldigt viktiga men jag tror att ännu viktigare är att människorna som jobbar i organisationen, att de är medvetna om sin roll och vilken betydelser det har att deras arbete då har en verklig påverkan då på riskhanteringsarbetet. Det är ju lite mer de mjuka delarna men därefter så kommer ju att de faktiska kontrollerna finns på plats också.
H: det här med rapportens utformning, anser du det också vara viktigt då?
R: Om du tänker på den rapporten vi ger till företaget då med rekommendationer, det är ju väldigt viktigt att den är formulerad på rätt sätt så att läsaren förstår annars så kommer vi inte få igenom några av våra rekommendationer, att det inte tas på allvar så att säga.
H: Är det ofta ett problem att ni ger rekommendationer, att ni kommer tillbaka ett år senare och att det inte hänt så mycket?
R: Det händer ganska ofta ja.
H: Hur angriper man det problemet bäst så att säga?
R: Ja, alltså våra rekommendationer är ju ingenting företaget måste rätta sig efter så i alla fall inte inom IT-revision. VI kan ju fortsätta då att påpeka att de här riskerna kvarstår om ni inte åtgärdar den här bristen men har de inget intresse av att åtgärda bristerna så är det inte så mycket vi kan göra då lägger vi inte så mycket energi på det utan då får vi inrikta oss på att granska på något annat sätt så att säga.
H: Granska på något annat sätt, hur tänker du då?
R: Jo men substansgranska.
H: Just det. Finns det några andra områden gällande IT-styrning som du anser vara viktigt i ert arbete?
R: Andra än de vi diskuterat?
H: Precis ja…
R: Nej jag tror nog att vi täkt in det mesta som jag kan komma på nu.
H: Ja, men då så. Då får vi be och tacka så mycket.
S: Tack så mycket.

Referenser

Backman, J. (1998): *Rapporter och uppsatser*. Studentlitteratur, Polen.

Brown, W. & Nasuti, F. (2005): Sarbanes-Oxley and Enterprise Security: IT Governance - What It Takes to Get the Job Done. *Information Systems Security,* Vol. 14, No. 5, pp. 15-29.

Bryman, A. & Bell, E. (2005): Företagsekonomiska forskningsmetoder. Liber Förlag, Slovenien

Charette, R. N. (1996): The mechanics of managing IT risk. *Journal of Information Technology*, Vol. 11, No. 4, pp. 373-379.

Debreceny & Gray (2009): IT Governance and Process Maturity: A Field Study. *2009 42nd Hawaii International Conference on System Sciences,* pp. 1-10.

De Haes, S & Van Grembergen, W. (2008): An Exploratory Study into the Design of an IT Governance Minimum Baseline through Delphi Research. *Communications of AIS,* Vol. 2008, No. 22, pp. 443-459.

Ebrahim, A. (2010): Audit fee premium and auditor change: the effect of Sarbanes-Oxley Act. *Manegerial Auditing Journal*, Vol. 25, No. 2, pp. 102-121.

Galup, S. D. & Dattero, R. (2010): A Five-Step Method to Tune Your ITSM Processes. *Information Systems Management,* Vol. 27, No. 2, pp. 156-168.

Goldschmidt, T., Dittrich, A., Malek, M. (2009): Quantifying Criticality of Dependability-Related IT Organization Processes in CobiT. *2009 15th IEEE Pacific Rim International Symposium on Dependable Computing,* pp. 336-341.

Halvorsen, K. (1992): *Samhällsvetenskaplig metod*. Studentlitteratur, Lund.

Harrast, S. & Weirich, T. R. (2009): New IT Risk Framework. *Journal of Corporate Accounting & Finance*, Vol. 20, No. 5, pp. 49-54.

Harmon, P. (2007): *Business Process Change - A guide for Business Managers and BPM and Six Sigma Professionals.* Elsevier, USA.

Iliesco, F-M. (2010): Auditing IT Governance. *Informatica Economica Journal,* Vol. 14, No. 1, pp. 93-102.

Jacobsen, D. (2002): *Vad, hur och varför?* Studentlitteratur, Malmö.

Kim, H.K.; Im, K.H.; Park, S.C., DSS for computer security incident response applying CBR and collaborative response. *Expert Systems with Applications,* Vol. 37, No. 1, pp. 852-870.

Kurtén, R (2009): *IT-styrning - Vad Ledning och Styrelse Behöver Känna Till om Informationsteknologi*. Uppsala Publishing House AB, Halmstad.

Lodhi, A., Kassem, G., Rautenstrauch, C. (2009): Modeling and analysis of business processes using business objects. *2009 2nd International Conference on Computer, Control and Communication,* pp. 1-6.

Luftman, J. (2004): *Managing the Information Technology Resource - Leadership in the Information Age.* Pearson Education Inc, New Jersey.

Merhout, J. W. & Havelka, D. (2008): Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit. *Communications of AIS*, Vol. 2008, No. 23, pp. 463-483.

Nelson, R. (2007): IT Project Management: Infamous Failures, Classic Mistakes, and Best Practices. *MIS Quarterly Executive,* Vol. 6, No. 2, pp. 67-79.

Parent, M. & Horner Reich, B. (2009): Governing Information Technology Risk. *California Management Review,* Vol. 51, No. 3, pp. 134-153.

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

Posthumusa, S. & von Solms, R (2005): IT oversight: an important function of corporate governance. *Computer Fraud and Security, Elsevier Advanced Technology*, Vol. 2005, No. 6, pp. 11-17.

Rozek, P. (2008): Putting IT Governance into action. *Internal Auditor,* Vol. 65, No. 3, pp. 29-32.

Silva, E. & Chaix, Y. (2008): Business and IT Governance Alignment Simulation Essay on a Business Process and IT Service Model. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*.

Singh, R. (2010): Only one Big Four firm produces UK annual report. *Accountancy Age,* pp. 4-6.

Syrèn, A. (2005): *På egen risk - En handbok om Informationssäkerhet*. SIS Förlag, Stockholm.

Van Bon et.al: (2009) *Foundations of IT Service Management Based on ITIL V3*. Van Haren Publishing, Zaltbommel.

Warden, B. (2008): After Sarbanes-Oxley: IT Compliance Update. *Certification Magazine,* Vol. 10, No. 4, pp. 34-39.

Weill, P. & Ross, J. W. (2004): *IT Governance - How Top Performers Manage IT Decision Rights for Superior Results.* Boston, Harvard Business School Press.

Webb, P., Pollard, C., Ridley, G. (2006): Attempting to Define IT Governance: Wisdom or Folly? *System Sciences,* Vol. 8.

Willson, P. & Pollard, C. (2009): Exploring IT Governance in Theory and Practice in a Large Multi-National Organisation in Australia. *Information Systems Management,* Vol. 26, No. 2, pp. 98-110.

Xiao-wen, L., Xiao-chun, L., Ke-jin, H. (2009): Design and implementation of IT governance planning decision supporting system. *2009 Chinese Control and Decision Conference,* pp. 5629-5632.

Internetkällor

ISACA och IT Governance Institute (2007), *CobiT 4.1*, tillgänglig på http://www.isaca.org/cobit

ISACA och IT Governance Institute (2009), *Risk IT Framework*, tillgänglig på http://www.isaca.org/Template.cfm?Section=Risk_IT3&CONTENTID=53239&TEMPLATE=/ContentManagement/ContentDisplay.cfm

ISACA och IT Governance Institute (2008), *ValIT*, tillgänglig på: http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/Enterprise_Value_Governance_of_IT_Investments,_The_Val_IT_Framework_2_0.htm

Internet 1: *Top Technology Initiatives Survey*. ISACA. Tillgänglig på: http://www.isaca.org/Content/ContentGroups/News_Releases1/20082/ISACA_Partners_With_AICPA_on_2008_Top_Technology_Initiatives_Survey.htm

Internet 2: *ISACA Overview and History*. ISACA. Tillgänglig på: http://www.isaca.org/Content/NavigationMenu/About_ISACA/Overview_and_History/Overview_and_History.htm

Internet 3: *Integrating COBIT into the IT Audit Process.* ISACA. Tillgänglig på: http://www.sfisaca.org/download/Integrating%20CobiT%20Domains%20into%20the%20IT%20Audit%20Process.pdf

Internet 4: *ISO/IEC 38500 - The Corporate Governance of IT*. ISACA London. Tillgänglig på: http://www.isaca-winchester.org/documents/ISACAW%20ISO%2038500%20The%20Corprorate%20Governance%20of%20IT.pdf

Internet 5: *ISO/IEC 38500:2008.* International Organisation for Standardisation. Tillgänglig på: *http://www.iso.org/iso/catalogue_detail.htm?csnumber=51639*

Internet 6: *Governing ITIL with COBIT*. DITY Weekly Newsletter. Tillgänglig på: http://www.itsmsolutions.com/newsletters/DITYvol4iss15.htm