Handelshögskolan
VID GÖTEBORGS UNIVERSITET

IT-revision

En studie av kunskap och förståelse

Sebastian Dolck & Niclas Roos
2009-05-29

Kandidatuppsats i företagsekonomi, Extern redovisning och Företagsanalys,
Handelshögskolan vid Göteborgs universitet, Vårterminen 2009

Författare: Sebastian Dolck och Niclas Roos

Handledare: Pernilla Rehnberg

Sammanfattning

I takt med att de reviderade bolagens verklighet förändras, i och med ökat internationellt ekonomiskt utbyte, ställs också krav på revisionsprocessens anpassning till dessa nya förhållanden. Den ökade internationaliseringen i företagens omvärld har lett till ett behov av effektiviseringar, något som gjorts möjligt med hjälp av informationsteknologi, men även ett behov av harmoniserad lagstiftning då företag verkar globalt över landsgränserna.

Denna harmoniserade lagstiftning har på senare tid influerats starkt av det ökade fokus på interna kontroller som uppstod i USA efter att ett antal redovisningsskandaler resulterat i starkt samhällspåverkande konkurser.

I och med dessa parallella processer har interna kontroller dels fått större fokus i revisionen, och dels börjat präglas av allt mer komplicerade teknologiska lösningar, främst i form av IT-system. Det är naturligt att revisorerna själva inte besitter den tekniska detaljkunskap som många gånger krävs för att på ett tillräckligt grundligt och effektivt sätt utvärdera dessa IT-system, varpå man engagerar en specialist; IT-revisorn.

I regleringen ställs dock utförliga krav på att ordinarie revisor ska kunna leda IT-revisorn i dennes arbete och tolka dennes resultat, detta då det alltjämt är ordinarie revisor som är ansvarig för revisionen och dess resultat. Vår fråga är således om revisorn har tillräcklig kunskap och förståelse för att ge IT-revisorn adekvata instruktioner och utvärdera dennes arbete.

Syftet med denna frågställning är att, med regleringen på området som grund, få klarhet i vad som faktiskt krävs av revisorn gällande förståelse av det arbete som en IT-revisor utför. Samtidigt ställer vi oss frågande till vad som faktiskt kan krävas av revisorn och vari en eventuell diskrepans mellan reglering och praxis ligger.

Uppsatsen är avgränsad till att endast behandla de förhållanden som rör IT-revisionen i större svenska bolag och som utförs av någon av Big Four-byråerna.

Vi har använt oss av sex personliga, öppna intervjuer för att ges större möjligheter att tolka de svar vi fått, och få respondenterna att friare beskriva sina erfarenheter på området utan att bli styrda och hämmade av precisa frågeställningar från vår sida. Dessa svar har vi sedan jämfört med vår teoretiska referensram som utgörs av den reglering som finns på området.

Det finns, enligt våra empiriska studier, vissa skillnader i revisorer och IT-revisorers synsätt på IT-revisorns roll och självständighet. Revisorerna har generellt en bild av att de själva ska ha tillräcklig kunskap och förståelse för att kunna bilda sig en uppfattning om de IT-system som används, och att IT-revisorn blir ett verktyg för mer detaljerad granskning. IT-revisorerna menar att de är ett självklart stöd för revisorn och en auktoritet när det gäller bedömningar och granskningar av de komplexa IT-systemen.

Slutsatsen blir dock att revisorn har den kunskap och förståelse som krävs, men att kravet på den enskilda revisorn blir lägre tack vare att revisionsbyråernas interna metodiker, ansvarsfördelning och kontrollsystem i viss mån substituerar dennes skyldigheter såsom de uttrycks i regleringen.

Vår studie utgår från en övergripande och kvalitativ bedömning av revisorns kunskap och förståelse, och ett förslag på fortsatt forskning skulle kunna vara en mer utförlig, kvantitativ studie av revisorernas kunskapsnivå. Ytterligare ett förslag är att behandla hur motsvarande situation som vi har behandlat ser ut hos mindre revisionsbyråer, utan anställda IT-revisorer.

Författarnas tack

Först och främst vill vi rikta ett tack till våra respondenter som tagit sig tid att svara på våra i vissa fall ovidkommande och konstiga frågor. Vi vill även tacka vår handledare, Pernilla, för hennes stora tålamod med våra konstiga idéer, för att hon inte suckat över våra tokiga idéer och konstiga fokus, men framförallt för all hjälp med värdefulla synpunkter och pekande med hela handen mot mer relevanta områden att studera. Samtidigt vill vi rikta ett tack till medlemmar i vår opponentgrupp som varit snälla och sakliga trots att de har fått läsa en del förvirrade versioner av vår uppsats, främst som ett resultat av vår ständigt omdanade frågeställning. Vidare riktas ett stort tack till vänner och bekanta som inte kunnat njuta av vårt sällskap, men respekterat vår benägenhet till asocialt beteende, under uppsatsens mest intensiva faser.

Niclas särskilda tack går till Hanna, som belastats med allt det hushållsarbete som han själv inte hunnit med, och som inte visats den uppskattning som hon tvivelsutan förtjänar.

Slutligen vill vi tacka Bengt Frithiofsson för hans välformulerade vinrecensioner, levererade på ett sätt som gång efter annan piggat upp den många gånger enformiga uppsatsprocessen.

Författarna
Göteborg den 29 maj 2009

_____ _____

Sebastian Dolck Niclas Roos

Begrepp och definitioner

Big Four-byråerna	De fyra största revisionsbyråerna i världen; Deloitte Touche Tohmatsu, Ernst & Young, KPMG samt PriceWaterhouseCoopers
Ordinarie revisor/revisor	Revisor som är ansvarig för revisionsuppdragets utförande och/eller är ansvarig för påskrivandet av revisionsberättelsen (i de fall det är av värde att göra en distinktion mellan påskrivande revisor och arbetsledande revisor nämns detta i ingressen till stycket och sedan benämns arbetsledande revisor endast som revisor)
IT-revisor	Specialist på bedömningen av IT-system vid en revision
IT-system/system	Datoriserade affärssystem och/eller redovisningssystem som är föremål för revision

Förkortningar

ABL	Aktiebolagslagen
CGEIT	Certified in the Governance of Enterprise Information Technology
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
EU	Europeiska Unionen
FAR	Föreningen Auktoriserade Revisorer
IFAC	International Federation of Accountants
IS	Informationssystem
ISA	International Standards of Audit
ISACA	Information Systems Audit and Control Association
IT	Informationsteknologi
RS	Revisionsstandard i Sverige
SOX	The Sarbanes-Oxley Act

Referenssystem

Om delar av den teoretiska referensramen nämns tidigare än i dess specifika teoridel hänvisas läsaren till gällande teoristycke genom not. Vidare källhänvisningar angående stycket står således att finna i teoridelen.

I förekommande fall ges även förtydliganden om ord och uttrycks innebörd genom not.

Då vissa stycken behandlar explicita lagar och regler framgår källan av rubriksättningen, något som dock kompletteras med källhänvisning i slutet på varje stycke då det uteslutande är information från samma källa i hela stycket. I annat fall, liksom för uppsatsen i övrigt, används referenssystem utifrån APA-manualen löpande i texten.

I empiridelen har vi valt att inte koppla specifika uttalanden till enskilda respondenter varför referenser utelämnats i sin helhet i detta stycke. Vi inser att detta medför en viss påverkan på uttalandenas trovärdighet, men en presentation av detta slag var, enligt vår bedömning, nödvändig för att tillmötesgå respondenternas krav på anonymitet. Det är vår åsikt att den anonymitet vi erbjudit varit en förutsättning för respondenternas möjlighet att lämna mer elaborerade och uppriktiga svar.

Disposition

Figur 1 beskriver uppsatsens övergripande disposition och ger kortfattade beskrivningar av de olika delarnas innehåll.

Figur 1 Disposition (Fritt efter *Bara Sport*)

Innehåll

1 Bakgrund

1.1 Definition

> ”Revision är att kritiskt granska, bedöma och uttala sig om ett företags redovisning och förvaltning”
> (FAR, 2003)

1.2 Revisorns roll

Revisorns granskning syftar i första hand till att objektivt bedöma huruvida den information som företagsledningen har lämnat i årsredovisningen ger en rättvisande bild av företaget. Revisionen är konkret uppdelad i en förvaltningsrevision och en räkenskapsrevision, vilka ska utmynna i revisorns uttalande i förvaltningsberättelsen[1]. (FAR, 2006)

En revision kan genomföras utifrån två olika ansatser, nämligen genom substansvärdering och genom test av intern kontroll. Substansvärdering fokuserar på att kontrollera huruvida de ekonomiska värden som företaget uppger är framräknade i enlighet med de lagar och rekommendationer som finns på området. Testandet av de interna kontrollerna ska säkerställa att de bestämmelser och rutiner som företagets ägare, genom styrelse och ledning, har beslutat om åtföljs inom organisationen, samt att kontrollera att företagets resurser används på ett ansvarsfullt vis. Utöver dessa två delar kontrollerar man även företagets byråkratiska rutiner med hänseende på exempelvis registrering, arkivering och ansvarsfördelning för att försäkra sig om riktigheten i företagets presenterade saldon. (FAR, 2006)

1.3 Historik

Revision har varit en tämligen central del i modernt svenskt företagande sedan 1983 då den nu så omtalade revisionsplikten uppkom på nytt. Historiskt och internationellt har dock revisionen varit ett möjligt inslag i företag sedan 1200-talet, medan den första svenska revisionen tycks emanera från 1600-talets bildande och drivande av handelshus. Den moderna revisionen, däremot, har sitt ursprung i den senare delen av 1800-talet, då externa revisorer i Storbritannien började göra objektiva granskningar av företags räkenskaper, en tradition som sedan spreds vidare i västvärlden. (FAR, 2003) Exempelvis stipulerar den svenska aktiebolagslagen från 1895 ett revisorskrav, ett krav som sedan reviderats i omgångar, och Svenska Revisorssamfundet bildades redan 1899 (www.farsrs.se, 2009).

1.4 Utveckling

Trots det gemensamma ursprung som nämns ovan präglas den fortsatta utvecklingen av skillnaderna mellan de två dominerande redovisningsskolorna, den anglosaxiska och den kontinentala. Den kontinentala skolan har tydligt definierade krav om en oberoende revisor, vilket hör ihop med en lagstiftning som är utformad för att tillgodose

[1] Se rubrik 4.4 Revisionsprocessen

borgenärers krav på validitet i substansvärderingen, samt att redovisning och beskattning är nära förbundna. Inom den anglosaxiska traditionen utvecklas däremot revisionen tidigt till ett verktyg för att minska principal-agentproblematiken[2], ett fenomen som uppstår när ägandet i ett företag separeras från den löpande förvaltningen, och revisorernas fokus har i första hand varit att tillfredställa ägarnas informationsbehov, främst angående framtida värdeskapande. (Smith, 2006)

Då globaliseringen tilltagit i omfattning och internationellt verkande företag blir allt vanligare, har krav ställts på harmonisering av redovisnings- och revisionsregler världen över (Förord till Revisionsstandard i Sverige, 2008). Detta bland annat för att underlätta företagens eget rapporteringsarbete i det avseendet att redovisning, och så även revisionskrav, för dotterbolag i olika länder blir enhetliga. Det primära syftet med denna normkonvergens är dock att få till stånd ett regelverk som gör det möjligt för redovisningsanvändare över hela världen att enkelt ta till sig information och kunna göra relevanta jämförelser av företag från olika delar av världen. (Revisorsdirektivet, 2006)

Innehållet i dessa harmoniserade normer har varit präglat av att försöka åtgärda de brister i tidigare redovisningsnormer som uppmärksammades i och med uppdagandet av en rad redovisningsskandaler på senare tid. Bland dessa är de medialt mycket uppmärksammade konkurserna i Enron och Worldcom tydliga exempel på de effekter som bristande intern kontroll kan ge upphov till[3]. (FAR, 2006)

År 2002 godkände till exempel den amerikanska kongressen Sarbanes-Oxley Act[4], en ny lag vars syfte är att öka transparensen i noterade bolag och minska risken för upprepningar av företagsskandaler som exempelvis Enron och Worldcom. Bland annat innebär lagen ökade krav på revisorns oberoende och en noggrannare granskning av företags interna kontroller och rutiner. (FAR, 2006)

Detta ökade fokus på interna kontroller har sedan fått mycket stort utrymme i de internationella standarder som utarbetats, och fortfarande utarbetas, för att återuppbygga förtroendet för både bolags rapportering och revisionsbyråers granskningar (FAR, 2006).

1.5 Teknisk utveckling

Då revisionen är en gammal företeelse, och bolagens karaktär och verksamheter förändrats genom tiderna, har själva revisionsförfarandet tvingats förändras för att även framgent kunna uppfylla de syften revisionen alltjämt har. Ett påtagligt exempel på förändring i hur bolag bedriver sin verksamhet, som inträffat under de senaste årtiondena, är den ökade datoriseringen inom de flesta organisationer. Globaliseringens

[2] Benämning på den informationsasymmetri som uppstår mellan beställaren, principalen, och verkställaren, agenten, när dessa roller är åtskilda. Problematiken uppstår när dessa parters intressen avviker från varandra (Eisenhardt, 1989).

[3] I båda dessa fall handlade det om oriktig redovisning som gjorde det möjligt att dölja stora kostnader och förstora intäkter. Ytterligare en gemensam nämnare var revisionsfirman Arthur Andersen, som hjälpte till att dölja dessa oegentligheter – något som ledde till den anrika firmans undergång.

[4] Se rubrik 4.2.3 Sarbanes-Oxley Act

explosionsartade ökning och den ständigt pågående IT-utvecklingen har för evigt förändrat hur företag världen över interagerar med varandra. (Förord till Revisionsstandard i Sverige, 2008)

Utvecklingen har kommit långt sedan de första datoriserade planerings- och bokföringssystem började användas på 1960-talet. Dessa system sågs i första hand som ett hjälpmedel för verksamheten, och de var inte heller särskilt svåra att kontrollera då andelen automatiska kontroller var låg och all utdata, till exempel fakturaverifikationer, skrevs ut på papper och lagrades i fysisk form. Detta gav revisorn en chans att följa transaktionsspåret och utvärdera IT-miljön, i den mån den ens existerade, utan ingående tekniska kunskaper. Denna möjlighet har dock försvunnit genom utvecklingen av integrerade, helomfattande system för alla delar av företaget, där information lagras digitalt[5] och antalet transaktioner kan uppgå till miljoner. För att effektivisera företagens arbete med dessa enorma datamängder har antalet automatiserade processer ökat, vilket har lett till att de manuella kontrollerna har blivit färre. (Nordin, 2008)

Det som underlättar företagens arbetsgång och rationaliserar deras processer försvårar dock för revisorn att på konventionella sätt ta del av den information de behöver för att kunna göra ett korrekt uttalande i revisionsberättelsen. Olika typer av IT-hjälpmedel, som till exempel datoriserade registeranalyser, har därför introducerats i revisorns verktygslåda, och för att klara av att säkerställa utvärderingen av de risker som förknippas med dagens alltmer komplexa affärs- och informationssystem, har vikten av en mer detaljerad IT-revision ökat. (Nordin, 2008)

1.6 IT-revision

IT-revision är inget tydligt definierat område med ett egenvärde i sig, utan är ett verktyg som har uppstått för att tillfredsställa den finansiella revisionens krav på riskbedömning. På grund av detta skiljer sig IT-revisionens omfattning och genomförande åt mellan olika företag. I små företag klarar den ordinarie revisorn ofta av att bedöma risknivån i systemen, men för mer komplexa system krävs större kompetens, vilket har genererat ett behov av specialiserade IT-revisorer, med ett liknande system för auktorisering som för finansiella revisorer. (Nordin, 2008) Organisationen som ansvarar för detta heter *Information Systems Audit and Control Association (ISACA)* och de erbjuder sina medlemmar bland annat utbildning, kunskapsdelning och tillgång till nätverk av kollegor[6].

Vid en IT-revision av mer komplexa system koncentrerar man sig på två typer av kontroller, dels systemets övergripande funktion och dels hur specifika processer påverkar redovisningen och dess tillförlitlighet. Den övergripande granskningen är fokuserad på hur behörigheter administreras, samt hur tillägg och ändringar av system

[5] Sedan 1999 är det tillåtet för företag att lagra information i digital form. (Bokföringslagen kap 7:1)
[6] Se rubrik 4.5.1 IT-revisorn

och processer hanteras och testas. Detta är en viktig del att förstå för att kunna bedöma riskerna för felaktiga saldon i redovisningen; om andelen användare med högsta behörighet är stor blir risken för fel, både medvetna och omedvetna, mycket större. Man gör också mer specifika granskningar av enskilda saldon och dess underliggande processer för att förstå vilka typer av kontroller som finns, för att på så sätt kunna uttala sig om risken för felaktigheter. (FAR SRS, 2007)

Vilka delar som ska täckas in av en IT-revision, vilka krav som finns på revisorn, samt hur dennes förhållande med en eventuell IT-specialist ska fungera regleras huvudsakligen i tre revisionsstandarder: Revisionsstandard i Sverige (RS) 400, *Riskbedömning och intern kontroll,* RS 401, *Revision i en datoriserad informationssystemmiljö*, samt RS 620, *Användning av en specialist i revisionsarbetet*. Dessa tre standarder är i sin tur svenska anpassningar av motsvarande internationella standarder, *International Standards of Audit (ISA)*, som ges ut av International Federation of Accountants (IFAC[7]). (FAR, 2006)

Generellt för dessa tre standarder är ett centralt krav på revisorns kunskap om, och förståelse av, de interna kontrollsystem, och därmed de IT-system, som används i det reviderade företaget. Dessa krav gäller även om revisorn engagerar en IT-revisor, och då ställs dessutom ytterligare krav på att revisorn ska kunna leda och utvärdera IT-revisorns arbete.

[7] Se rubrik 4.2.1 International Federation of Accountants

2 Problem och syfte

2.1 Problemdiskussion

Två, av varandra oberoende, faktorer ligger till grund för vår problemdiskussion och ämnets aktualitet:

- En förändring i redovisnings- och revisionsnormer, med mycket tydligare fokus på vikten av fungerande interna kontroller, som fått genomslagskraft genom ökad internationalisering och normkonvergens.
- Teknisk utveckling som leder till svårigheter för revisorn att själv utföra de granskningar av interna kontroller som krävs.

Bakom dessa faktorer ligger i grunden även globaliseringen som skapar ett behov av mer avancerade IT-lösningar i och med ständigt växande företag, deras agerande på olika marknader samt allmänt mer komplexa strukturer, och även ett behov av harmonisering av regleringar över landsgränser.

Det är ett obestritt faktum att revisionsprocessen, med anor i 1200-talet, har förändrats över tiden som en naturlig följd av de förändringar som har skett i det reviderade företags verklighet. De senaste decennierna har denna förändring eskalerat än mer genom att de allt mer centrala IT-systemen har utvecklats mycket snabbt, från enkla hjälpmedel för bokföring till komplexa verksamhetsövergripande informationskällor. Ju mer plats och ju större betydelse dessa IT-system får i företagen desto större har behovet av att inkludera dessa i revisionen blivit.

I takt med ständig teknisk utveckling har kraven på revisorns kunskap och förståelse för IT-system således ökat. Till exempel hade revisorn tidigare möjlighet att följa ett fysiskt transaktionsspår för att på så sätt upptäcka eventuella felaktigheter, men i samband med förändringarna av bokföringslagen, som möjliggör för företag att spara data optiskt istället för i fysisk (pappers-)form, måste revisorn klara av att bedöma hur data hanteras av systemet. Till detta ska läggas en mängd inbyggda kontrollmekanismer och automatiska transaktionsprocesser som blivit realitet i och med mer och mer komplexa affärssystem, något som föranlett behovet av en mer detaljerad IT-revision som en del av granskningen av de interna kontrollerna.

Alltsedan de stora bolagsskandalerna i USA i början av 2000-talet har utvecklingen på revisionsområdet gått mot ett allt större fokus på bolagens interna kontrollrutiner. Ett tydligt exempel på detta är den amerikanska Sarbanes-Oxley Act, en reglering som på ett påtagligt sätt influerat den alltmer internationaliserade revisionens utformning när det gäller striktare krav på intern kontroll. Denna internationella normkonvergens tar sig främst uttryck i IFAC:s regeluppsättning ISA, en revisionsstandard som ligger till grund för bland annat svensk reglering på området; RS. I denna reglering föreskrivs revisorns tillvägagångssätt och ansvar gällande just granskning av intern kontroll, och då även specifikt vid IT-revision som en del av den interna kontrollgranskningen.

RS 401 stipulerar till exempel att revisorn ska leda och planera IT-revisionen, men i förekommande komplexa fall tillkalla en specialist; IT-revisorn. Trots denna delegering av utförandet, som regleras i RS 620, är det fortfarande revisorns roll att bedöma revisionsbevisens ändamålsenlighet, samt skaffa sig en insikt om huruvida använda antaganden och metoder är rimliga, baserade på dennes allmänna kunskaper om företaget. Det yttersta ansvaret för att uttalandet i revisionsberättelsen är korrekt ligger alltjämt på revisorn, varför dennes förståelse för IT-revisorns resultat och tillvägagångssätt är centralt.

Den frågeställning som kommer att utgöra grunden för vår studie är således:

> *Har revisorn tillräcklig kunskap och förståelse för att ge IT-revisorn adekvata instruktioner och utvärdera dennes arbete?*

2.2 Syfte

Vi vill med vår frågeställning belysa vikten av att andemeningen i regleringen på området inte går förlorad; revisorns allmänna kunskaper om företaget är av högsta vikt för att IT-revisorn ska kunna planera och genomföra en relevant och ändamålsenlig IT-revision. Detta kräver inte att revisorn har specialistkunskaper om förfarandet, men däremot en god förståelse för resultatet. Vi vill försöka få klarhet i huruvida det föreligger någon diskrepans mellan gällande regler och dess faktiska tillämpning hos Sveriges största revisionsbyråer.

Vi tror att vår undersökning kan vara intressant för normgivare inom revision, till exempel FAR, i deras arbete med att skapa en tidsenlig reglering, med stöd i gällande praxis.

2.3 Avgränsningar

Vi har valt att fokusera vår undersökning på de förhållanden som rör IT-revisioner i större svenska företag och som utförs av någon av de så kallade Big Four-byråerna[8].

[8] Big Four är en benämning av de fyra största revisionsbyråerna i världen och dessa är: Deloitte Touche Tohmatsu, Ernst & Young, KPMG och PriceWaterhouseCoopers.

3 Metod

3.1 Val av uppsatsämne

Genom att skriva en kandidatuppsats om IT-revision lyckades vi på ett bra sätt sammanfoga våra olika framtidsambitioner att arbeta med affärssystem respektive revision. Den avgörande inspirationen bar formen av en platsannons för en tjänst som IT-revisionsmedarbetare hos Deloitte som beskrev vanligt förekommande arbetsuppgifter för denna typ av tjänst. Under vår kandidatkurs i externredovisning hade vi även en gästföreläsare från Ernst & Young som berättade om revisionsprocessens utformning, och även han berörde IT-systemens allt viktigare roll vid revisionen, vilket ytterligare förstärkte känslan av att detta är ett högst aktuellt ämne. Vi anser också att det är spännande att skriva vår uppsats om ett ämne som skiljer sig från de ämnen som traditionellt brukar behandlas i uppsatser inom externredovisning.

3.2 Tillvägagångssätt

Vi inledde vårt arbete med att söka information om hur revisionsprocessen ser ut och vilken roll IT-revisionen spelar i den, vilka syften den fyller, samt hur den är utformad. Vår teoretiska ansats grundas i huvudsak på litteratur som berör revision i traditionell bemärkelse och IT-revisionens del av denna, dock inte dess tillvägagångssätt. Detta beror främst på att de rutiner och metoder som används av IT-revisorer är företagsinterna och därmed inte tillgängliga för allmänheten.

Vi hade stor hjälp av vår handledare Pernilla Rehnberg i detta tidiga skede av arbetet; hennes bakgrund som revisor hos Deloitte, utöver hennes forskartjänst vid Handelshögskolan i Göteborg, gav oss många nyttiga insikter i vad IT-revision faktiskt innebär. Hon var också till stor hjälp i arbetet med att formulera en tydlig och, inte minst, relevant frågeställning. Vi har dock tvingats revidera vår frågeställning under arbetes gång, allt eftersom vi har lärt oss mer, både om revision i allmänhet och om mer specifika detaljer om IT-revision.

För att på bästa sätt svara på vår frågeställning valde vi att göra en fallstudie av revisorer och IT-revisorer hos de så kallade Big Four-byråerna för att undersöka deras attityder och tankar angående IT-revision. Anledningen till att vi valde att intervjua både revisorer och IT-revisorer var att vi ville få en uppfattning om båda sidors syn på kunskap och förståelse. Valet att begränsa studien till personer verksamma vid någon av Big Four-byråerna grundade sig till största delen på att det är dessa byråer som handhar revisionen av den absoluta merparten av Sveriges stora företag, och det är, enligt Pernilla Rehnberg, vid revision av dessa företag som IT-revisorn ofta kopplas in.

För att samla in primärdata genomförde vi personliga intervjuer då vi i första hand var ute efter att undersöka relationen mellan IT-revisorn och revisorn, hur revisionsprocessen påverkas av denna, samt hur normen överensstämmer med praxis.

Vi bestämde oss för att genomföra personliga intervjuer, då vi ansåg att vi var i stort behov av den möjlighet till uppföljning och utveckling som denna intervjuform erbjuder (Lantz, 2007), då vi som tidigare nämnts inledningsvis besvärades av brist på grundläggande information. För att få kontakt med lämpliga respondenter kontaktade vi Big Four-byråernas studentkoordinatorer, som sedan i sin tur tog kontakt med lämpliga medarbetare på deras respektive byrå. Vi sammanställde ett antal frågor som sedan granskades av vår handledare innan de, efter viss revidering, skickades ut till respondenterna i god tid innan intervjuerna. Vår första intervju fick till viss del fungera som pilotstudie då det visade sig att det fanns allvarliga brister i vårt ursprungliga resonemang och de frågor vi hade ställt. Detta berodde främst på att vi inte hade lycktas skapa oss en tillräckligt god uppfattning av revisionsprocessen och IT-revisionens del av denna. Med anledning av detta fick vi lov att återigen revidera våra frågor inför våra resterande intervjuer. Allt eftersom vi genomförde våra intervjuer fann vi ett antal frågeställningar som var de mest centrala i diskussionerna med alla respondenter, och dessa frågor har vi därför använt i sammanställningen av intervjusvaren för att kunna jämföra respondenternas svar. Intervjuerna spelades in för att säkerställa att vi inte missade relevant information och efter att vi sammanställt intervjumaterialet skickades detta tillbaka till respondenterna för att undvika eventuella missförstånd eller misstolkningar.

Empirin inleds med en presentation av revisionsbyråernas organisationsstruktur och arbetssätt, med visst fokus på IT-revisionens del av dessa – baserat på de svar vi har fått under våra intervjuer. Därefter följer en jämförande sammanställning av de två gruppernas attityder angående ett antal övergripande frågor som togs upp vid intervjuerna.

De flesta av våra respondenter har uttryckt en vilja att vara anonyma i så stor utsträckning som möjligt, för att inte skada deras eget eller deras byrås rykte, vilket vi självklart förstår och respekterar. Vi presenterar därför respondenterna endast efter vilken grupp de tillhör, samt en kort meritbeskrivning. Explicita uttalanden knyts heller inte till enskilda respondenter.

I vår analys tolkar vi våra empiriska resultat, först som en sammanställning av de olika gruppernas attityder och tankar, och sedan sammanbinder vi dem med gällande lagar och regler för att se hur väl norm och verklighet stämmer överens. Slutligen ligger denna analys till grund för vår slutsats.

3.3 Metodval

3.3.1 Datainsamling

Det finns två olika former för datainsamling till en studie: kvalitativ och kvantitativ. Den sistnämnda bygger på insamling av till exempel siffror och utmynnar ofta i en rapport som bygger på olika typer av statistik. En kvalitativ undersökning, däremot, baseras på empirisk data som samlas in från olika typer av källor, såsom böcker eller intervjuer.

Målet med vår uppsats är att jämföra olika praktikers attityder och hur de överensstämmer med gällande regler och praxis, vilket gör en kvalitativ studie till en passande metod. (Ruane, 2006)

3.3.2 Primär- och sekundärdata

I inledningen av vårt arbete förlitade vi oss till stor del på sekundärdata, i form av läroböcker, lagtext och olika typer av revisionsvägledning, för att skriva vårt teoriavsnitt. Den information som vi hämtade från dessa källor användes främst för att förstå vilken roll IT-revisionen förväntas ha i den övergripande revisionen, samt för att förstå hur den har påverkats över tiden och av vad.

Det praktiska arbetet med IT-revision sker ofta enligt internt fastställda rutiner, och med anledning av detta fann vi det svårt att finna relevant information till vårt teoriavsnitt från någon sekundärdatakälla. Vi har försökt avhjälpa denna brist genom att utnyttja ett exempel ur den praktiska vägledning som erbjuds i FAR:s IT-handbok. Vi inleder också vår empiridel med en sammanfattning av respondenternas syn på IT-revisionens genomförande innan vi fortsätter med de övergripande frågeställningarna.

3.4 Intervjumetodik

För att samla in de primärdata vi behöver till vår empiri valde vi att genomföra personliga intervjuer med tre IT-revisorer och tre revisorer. Genom att använda öppna, personliga intervjuer kan en mycket hög flexibilitet uppnås; intressanta idéer kan följas upp och leda till en fördjupad diskussion, frågor kan anpassas under intervjuns gång för att bättre passa respondentens situation och erfarenhet (Lantz, 2007). Det faktum att vi saknade en bra inblick i hur revisionsprocessen ser ut i realiteten, ökade vårt behov av ett öppet utbyte där vi hade möjlighet att, utifrån respondentens upplysningar, bilda oss en uppfattning och följa upp intressanta svar. Dessutom ges intervjuaren en bättre möjlighet att tolka respondentens svar med hjälp av till exempel tonläge och kroppsspråk. Då vår frågeställning främst fokuserar på de inblandade parternas egna erfarenheter är det viktigt att den valda intervjuformen kan fånga upp just dessa. Vi anser att en öppen intervju är väl lämpad för detta ändamål då den erbjuder goda möjligheter att använda sig av en form av så kallad ställföreträdande introspektion för att följa respondentens tankegångar. Detta innebär att man skapar sig en förståelse genom att se på saker utifrån respondentens perspektiv. (Lantz, 2007)

Öppna intervjuformer har två huvudsakliga nackdelar: tidsaspekten och svårigheten att få konsekventa resultat från flera olika respondenter (Lantz, 2007). Tidsaspekten kan dels ta sig uttryck som tidsbrist vid själva intervjutillfället, vilket kan leda till att viktig information utelämnas, men också som ett mycket tidskrävande moment i uppsatsprocessen, då i form av sammanställning av insamlad data. Problemet med inkonsekvent information från de olika respondenterna beror oftast på skillnader i vokabulär och brist på gemensamma definitioner. Vi har vidtagit vissa åtgärder för att minimera dessa potentiellt negativa faktorers påverkan på primärdatainsamlingen, bland annat genom att spela in intervjuerna i sin helhet för att minska problemen

associerade med tidsaspekten. Det faktum att revisionsbranschens arbetsmetoder har mycket tydlig koppling till gemensamma lagar och regler tror vi också kommer att minska inkonsekvensproblematiken.

3.5 Studiens respondenter

Vårt arbete med att finna lämpliga respondenter har underlättats av de stora revisionsbyråernas ambition att, i största möjliga mån, hjälpa studenter komma i kontakt med personer med relevanta erfarenheter. Vad det gäller respondenternas tillförlitlighet underlättas detta av de olika vedertagna certifieringar och auktoriseringar som finns inom branschen, även om vi av respekt för våra respondenters anonymitet har valt att inte ange detta specifikt för respektive respondent. De revisorer vi har intervjuat har alla arbetat på uppdragsledarnivå, något vars vikt kommer att belysas i empiridelen av denna uppsats.

3.6 Validitet och reliabilitet

I detta avsnitt ämnar vi redogöra för vår undersöknings validitet och reliabilitet för att läsaren ska få en uppfattning om vilken giltighet och trovärdighet den information som presenteras har.

3.6.1 Validitet

I uttrycket validitet ryms många olika och ofta komplexa aspekter, man kan bland annat tala om mätningsvaliditet - hur väl anpassat ett visst mått är i förhållande till det som ska mätas - och extern validitet – hur representativa resultaten från urvalet är för den totala populationen (Ruane, 2006).

För att säkerställa mätningsvaliditet kan man bedöma undersökningens innehållsvaliditet, som beskriver passformen mellan nominella och operationella definitioner[9] (Ruane, 2006). Den nominella definitionen i vår undersökning är kravet på revisorns förståelse och kunskap angående IT-revision, såsom den definieras i RS 401 och RS 620. Vi har i vår undersökning valt att ge en övergripande definiering av detta krav: revisorn ska ha tillräcklig kunskap och förståelse för att leda IT-revisionen och kunna ge tydliga instruktioner, men inte nödvändigtvis förstå IT-revisionens tekniska moment. De operationella definitionerna i vår undersökning är de frågor som vi ställde under våra intervjuer för att fastställa revisorernas kunskap och förståelse. Som tidigare nämnts använde vi oss av en mycket öppen intervjuform på grund av vår, på förhand, bristande insikt i revisionsprocessen, vilket självklart har påverkat intervjusvaren; revisorernas förståelse och kunskap har mätts på ett övergripande plan. Vi anser därför att den information som framkommit, trots vår initialt bristande kunskap, har innehållsvaliditet, då det är en bra passform mellan våra nominella och operationella definitioner.

[9] Nominella definitioner: teoretiskt klargörande av olika begrepp. Operationella definitioner: de steg som ingår då man empiriskt dokumenterar ett begrepp.

Som tidigare nämnts, och som namnet antyder, speglar mätningsvaliditet hur väl måttet mäter det som ska mätas; hur väl är frågan utformad. Med extern validitet mäter man istället hur väl undersökningens urval och dess svar är representativa för den totala populationen; att fråga rätt personer. (Ruane, 2006) Som även har nämnts har vi intervjuat anställda hos de så kallade Big Four-byråerna, då de flesta revisionsuppdrag i Sverige som inkluderar en IT-revision av omfattande och komplexa IT-system främst tillfaller dessa byråer. De olika byråerna använder sig av företagsgemensamma arbetsmetoder som ser likadana ut, inte bara för alla svenska kontor utan också i resten av världen. Utifrån detta anser vi att man kan göra antagandet att våra resultat har en hög extern validitet, givet vår studies avgränsningar, trots att vårt begränsade urval inte uppnår någon högre statistisk signifikansnivå.

3.6.2 Reliabilitet

En undersökning med hög reliabilitet ska kunna ge samma resultat varje gång man upprepar den, förutsatt att man inte ändrar någon variabel, och därmed svara på hur väl man har besvarat sin frågeställning. Med anledning av detta är det vanligt att man använder sig av en så kallad ”test-retest-metod” för att bedöma reliabilitetsnivån; metoden går ut på att man helt enkelt upprepar undersökningen och jämför hur väl resultaten korrelerar. (Ruane, 2006) Ett sådant förfarande har dock inte varit möjligt för oss, då det ofta är svårt att få till ens en intervju med rätt respondenter, och vi har istället försökt att minimera denna potentiella risk genom att ställa frågor om ett specifikt problem på flera olika sätt; i litteraturen talar man om användandet av sammansatta mått (Ruane, 2006).

En annan faktor som kan påverka reliabiliteten är skevhet (Ruane, 2006). I vår undersökning har vi stundtals märkt av en viss tendens bland respondenterna att i första hand vilja ge ett passande svar på frågan, snarare än ett korrekt svar. En trolig anledning till detta kan möjligtvis vara att branschen präglas av olika typer av certifieringar och auktoriseringar och att detta gör att respondenterna är måna om sitt anseende.

4 Teori

4.1 Inledning

IT-revisionens omfattning är ett svårdefinierat område; idag används en mängd olika affärssystem på en mängd olika sätt beroende på företagets verksamhet, storlek och komplexitet. Däremot finns det tydligt definierade krav på vilka syften en IT-revision ska uppfylla och dessa baseras till stora delar på de lagar och regler som styr revisionen som helhet. Då de interna kontroller, som IT-revisionen syftar till att analysera, får allt större utrymme i den internationella debatten, och global harmoniseringen av redovisnings- och revisionsstandarder ligger till grund för svensk reglering på området, ämnar vi dela upp detta teorikapitel i följande underkategorier:

- Övergripande internationell reglering.
- Övergripande svensk reglering.
- Revisionsprocessens uppbyggnad, regleringar och standarder.
- IT-revision
- Tidigare forskning

4.2 Övergripande internationell reglering

I detta första avsnitt vill vi ge en bakgrund till de trender som präglar redovisnings- och revisionsregleringens utformning och riktning.

4.2.1 International Federation of Accountants

Sedan grundandet 1977 har den oberoende internationella organisationen för professionella revisorer, IFAC, haft som mål att tillvarata allmänhetens intressen i näringslivet. IFAC representerar över 2,5 miljoner verksamma revisorer, spridda över 123 länder, och verkar genom dessa för införandet av internationellt gemensamma standarder och etiska principer vid revisionen. IFAC har en uttalad strävan att deras revisionsstandarder, ISA, ska bli allmänt accepterade revisionsstandarder i hela världen. Organisationen är oberoende av myndigheter och företag, och övervakas istället av en rad kommittéer som säkerställer att organisationen följer sitt uppdrag. Samarbeten med myndigheter, lagstiftare och auktoriteter på revisionsområdet är dock centrala för att utveckla internationellt accepterade standarder i syfte att bland annat förstärka aktieägares, och övriga bolagsintressenters, insyn i företagen samt öka möjligheterna för rättvisare jämförelser och värderingar av liknande företag i olika länder. Detta fokus på bolagsintressenternas, och allmänhetens, intressen ska enligt IFAC bidra till att öka kvaliteten på de tjänster som revisorskåren tillhandahåller världen över. (www.ifac.org, 2009)

Harmoniseringen av de internationella revisionsregleringarna innefattar gemensamma standarder för kvalitetskontroll, revisorers ansvar och oberoende, revisorers utbildning samt etiska principer för revisorn att verka utifrån. (www.ifac.org, 2009)

Sverige har på eget initiativ infört ISA i sin reglering, i form av RS, och i förekommande fall även gjort vissa tillägg för att kunna applicera standarden på svenska förhållanden (Förord till Revisionsstandard i Sverige, 2008). Samtidigt finns det ett krav från EU, genom det åttonde bolagsrättsliga direktivet, att medlemsländerna ska anamma unionsgemensamma revisionsbestämmelser. Även dessa utgörs av ISA som, enligt direktivet, ska införlivas i nationell lagstiftning allteftersom EU-kommissionen godkänner dess olika beståndsdelar. (Förord till Revisionsstandard i Sverige, 2008)

4.2.2 Åttonde bolagsrättsliga EU-direktivet – Revisorsdirektivet

Från och med 1 juli 2009 ska EU:s åttonde bolagsrättsliga direktiv, det så kallade revisorsdirektivet, ha införlivats i svensk rätt (Prop. 2008/09:135, 2009). Direktivet är resultatet av EU:s ambitioner att harmonisera revisionskraven för liknande företag inom unionen, men också för att skapa ett unionsgemensamt godtagbart minimikrav för företagens finansiella rapportering – minimikrav eftersom medlemsstaterna får ställa kompletterande krav utöver de som reglerats av EU-kommissionen (Brännström, 2006). Harmoniseringen syftar till att underlätta jämförelser av liknande bolag i olika unionsländer genom gemensamma standarder för utformningen av finansiell rapportering, men även för att underlätta för revisorerna i landsöverskridande koncerner där koncernrevisorn hålls ansvarig för revisionen i samtliga länder oavsett vem den utförs av. Harmonisering i sig har dock inget egenvärde så länge kvalitetsaspekten lämnas oberörd, varför EU-kommissionen också lägger stor vikt vid att medlemsländerna ska utveckla och lagstadga egna kvalitetssäkringssystem – detta i enlighet med IFAC:s standarder, men här förstärkt av EU-kommissionens egna kontroller av att dessa system finns och efterlevs. Åttonde direktivet förespråkar även vikten av att ha ett revisionsutskott internt i de bolag som ”är av allmänt intresse”. Revisionsutskottet ska övervaka den finansiella rapporteringen och upprättandet av finansiella rapporter, utvärdera effektiviteten av företagets interna kontrollfunktioner, samt bistå revisorn med underlag vid en revision. Trots att revisionsutskottet i mångt och mycket kan underlätta revisorns jobb är det också utskottets uppgift att granska revisorn och revisionsbolaget med hänseende på oberoende och tillhandahållandet av oförenliga tjänster. (Revisorsdirektivet, 2006)

4.2.3 Sarbanes-Oxley Act

Som en följd av de stora företagsskandalerna som präglade de första åren av 2000-talet, röstade USA:s kongress i juli 2002 igenom The Public Company Accounting Reform and Investor Protection Act of 2002, eller som den också benämns, The Sarbanes-Oxley Act (SOX), efter de två kongressledamöter som skrev lagförslaget. Lagen lade främst fokus på en förbättrad intern kontroll för att förhindra att omfattande företagsbedrägerier som de som skedde i exempelvis Enron och Worldcom inte ska upprepas. Detta ska åstadkommas genom ökad transparens, aktualitet och kvalitet i företagens finansiella rapportering och lagen gäller för alla företag som finns registrerade på någon av de tre amerikanska börserna (New York Stock Exchange, NASDAQ eller American Stock Exchange), även om huvudkontoret är placerat utanför USA. (Merchant & Van der Stede, 2007)

Kravet på förbättrad intern kontroll finns framförallt i den så kallade Section 404 (Avsnitt 404) och har varit föremål för intensiva debatter, främst på grund av de höga kostnader, i första hand för revision, som införandet innebar för de berörda företagen. I avsnittet stipuleras bland annat att företagsledningen ska lämna uppgifter i årsredovisningen om hur väl den interna kontrollen fungerar och att revisorerna ska granska dessa uppgifter. En viktig del i de utökade interna kontrollerna är noggrannare granskningar av företagens IT-system och dess effekter på den finansiella rapporteringen. (Merchant & Van der Stede, 2007)

The Sarbanes-Oxley Acts direkta påverkan på svenska bolag är relativt begränsad och berör främst svenska bolag som är noterade i USA samt svenska dotterbolag till noterade amerikanska bolag. Den indirekta påverkan är däremot mer omfattande; på grund av dagens globaliserade värld förblir få fenomen lokala. Ett exempel på SOX:s påverkan är det krav på revisionsutskott som anges i Svensk kod för bolagsstyrning[10]. Den interna kontrollens ökade betydelse får därför stor betydelse även utanför USA:s gränser, en effekt som dessutom förstärks av en alltmer internationellt homogen redovisnings- och revisionsreglering. (FAR, 2006)

4.3 Övergripande svensk reglering

4.3.1 Aktiebolagslagen

En av de mest påtagliga regleringarna av revisionen, dess delar, och krav på behörighet är Aktiebolagslagens (ABL) nionde kapitel. I detta statueras de krav som finns på företag när det gäller att ha revisor, förse revisorn med information samt låta revisorn genomföra revisionen, men det statueras också krav som revisorn ska uppfylla i form av behörighet och tillvägagångssätt vid revisionen. Revisorn ska till exempel ha den kompetens och insikt som krävs för att kunna göra adekvata bedömningar om de ekonomiska förhållanden som krävs vid en revision. Det finns även strängare krav på att revisorn ska vara auktoriserad eller godkänd revisor som avlagt revisorsexamen, om det reviderade bolaget uppfyller vissa kriterier i form av bland annat antalet anställda och omsättningsstorlek. Till detta ska läggas de generella regler om jäv som gör att revisorn, för att få revidera företaget, inte får vara knuten till det reviderade företaget på något sätt, eller ha personliga intressen som kompromitterar hans eller hennes objektivitet. (Aktiebolagslagen)

För mer ingående regleringar om revisorns kvalifikationer, olika kompetensnivåer och ackrediteringar konsulteras Revisorslagen där även regleringar gällande revisionsbolag står att finna. Fokus ligger på de etiska normer som revisorn väntas upprätthålla, såsom opartiskhet, säkerhet, professionalism och förtroendeskapande, men även de

[10] Se rubrik 4.3.2 Svensk kod för bolagsstyrning

disciplinära åtgärder som blir aktuella om revisorn på något sätt missbrukar sin ställning eller avviker från god sed[11]. (FAR, 2006)

Det framgår i ABL att revisorn ska granska bolagets årsredovisning, bokföring och ledningens förvaltning på ett sådant sätt att revisorn i revisionsberättelsen kan styrka att bolaget agerat i enlighet med god redovisningssed, lagar och regler vid upprättandet av årsredovisningen och i förvaltningen av bolaget. Revisorns uttalande ligger sedan till grund för bedömningen om huruvida ledningen beviljas ansvarsfrihet, i vilken mån resultaträkning och balansräkning kan fastställas samt om föreslagen vinstdisposition är lämplig. Dessutom finns det ett brett ansvar för revisorn att svara på bolagsstämmans frågor, så länge svaren inte väntas skada företaget, och rapportera lagöverträdelser till ansvariga myndigheter. (Aktiebolagslagen)

4.3.2 Svensk kod för bolagsstyrning

Aktiebolagslagen ligger även till grund för utvecklandet av andra normer för kontroll av företag och vägledning vid sådan kontroll. Ett exempel på en central sådan är Svensk kod för bolagsstyrning, vars syfte är att huvudsakligen erbjuda riktlinjer för hur bolag ska styras och skötas för att tillgodose att fokus på ägarnas intresse upprätthålls. Koden gäller för samtliga bolag registrerade på stockholmsbörsen och behandlar generella ansvarsfrågor och rutiner för intern kontroll, något som bland annat underlättar revisorns överblick av kontrollmiljö och kontrollåtgärder vid en analys av interna kontroller[12] i en revision. Det nämns bland annat att styrelsen årligen ska avge en rapport om hur den interna kontrollen gällande finansiell rapportering är organiserad, hur väl den fungerat under innevarande period samt behov för eventuella förändringar. Även arbetet mot revisor, och att internt underlätta för revisorn genom transparens och egen kvalitetssäkring från företagets styrelses sida av de finansiella rapporterna, poängteras, och man anser att ett speciellt revisorsutskott ska tillsättas i bolagsstyrelsen, med ansvar för revisionsfrågor (jfr Revisorsdirektivet och SOX ovan). (Svensk kod för bolagsstyrning, 2008)

4.4 Revisionsprocessen

Vad är revision

En revision ska utmynna i avgörandet om huruvida årsredovisningen har upprättats i enlighet med gällande lagar samt god redovisningssed, fastställandet av balans- och resultaträkning kan säkras, ansvarsfrihet kan beviljas för styrelse och företagsledning samt råda om huruvida vinst kan disponeras på det av ledningen föreslagna sättet (FAR, 2006). Syftet är att tillvarata ägarnas intressen då ägandet och ledandet av bolaget är åtskilt och dessas intressen eventuellt skiljer sig från varandra (Smith, 2006). Det är företagsledningens ansvar att upprätta de finansiella rapporterna och se till att systemen för dessas uppkomst, samt förvaltning av bolaget, fyller de krav som lagar och regler föreskriver för att kunna återspegla en så rättvisande bild av företaget som

[11] Se rubrik 4.4 Revisionsprocessen
[12] Se rubrik 4.4.1 RS 400 Riskbedömning och intern kontroll

möjligt. Revisorns roll är att kvalitetssäkra dessa uttalanden genom att utföra en rad granskningar av företaget, något som sedan ligger till grund för revisorns uttalanden i sin revisionsberättelse. (FAR, 2006)

Förvaltningsrevision och Räkenskapsrevision

Revisionen delas upp i en förvaltningsrevision, där företagsledningens handlande granskas, och en räkenskapsrevision, där presenterade siffror och bokföring granskas. Uppdelningen mellan dessa delar är dock inte så tydlig som det kan förefalla, då de ofta är tätt sammanlänkade. I förvaltningsrevisionen ska revisorn utröna huruvida företagsledningen fullgjort sina plikter eller om de på något sätt försummat de åtaganden som åligger dem i och med deras ställning. Detta kan röra sig om mer eller mindre allvarliga försummelser eller regelöverträdelser och utifrån företeelsens art få reprimander såsom en erinran om att åtgärder bör vidtagas för att åtgärda missförhållandet eller, i de allvarligare fallen, anmälan till åklagare som prövar eventuella lagbrott i domstol. I förvaltningsrevisionen ingår även kontroll av ledningens skapande och upprätthållande av interna kontroller, något som även är en betydande del i räkenskapsrevisionen och således styrker sammanlänkningen av de båda revisionsdelarna. Räkenskapsrevision är uppdelad i tre delar, nämligen revision av bokföringen, årsredovisningen och eventuell koncernredovisning, men fokus i denna uppsats ligger på bokföringen. Då bokföringen ligger till grund för bokslutet, och de uttalanden som bolaget gör i årsredovisningen, är det logiskt att revisorn granskar bolagets löpande bokföringsrutiner för att avgöra om de antaganden och ställningstaganden som presenteras i årsredovisningen är väl underbyggda. (FAR, 2006)

God sed

Uttrycket god sed är frekvent förekommande inom revisionen men ger, beroende på förstavelse till ordet sed, uttryck för olika saker. God redovisningssed är till exempel en vägledning för hur redovisning ska genomföras och presenteras av företag, och alltså något som revisorn ska granska snarare än praktisera. När man talar om god revisorssed syftar man på de yrkesetiska regler, utvecklade av FAR och revisorsnämnden, som en revisor lyder under. (FAR, 2006) Då de yrkesetiska reglerna inte är lagstadgade, utan utvecklade och upprätthållna av Revisorsnämnden, kan tolkningar av dem göras mer dynamiska för att passa sina syften över tiden. Tolkningar av de etiska reglerna görs nämligen av Revisorsnämnden och det säkerställer att de branschgemensamma värderingarna har företräde framför notorisk bokstavstolkning, något som eventuellt skulle vara till förfång för revisorskåren. Ytterst vilar dock alltjämt ansvaret på vad som utgör god sed i de enskilda fallen, på domstolarna. (Prop 2000/01:146, 2001) Till de etiska principerna hör bland annat professionalism och objektivitet, men framförallt att tillämpa god revisionssed. När man talar om god revisionssed menar man det sätt på vilket en revision ska genomföras, tagandes bland annat de båda övriga sederna i beaktande gällande kunskap, erfarenhet och vedertagen

praxis. (FAR, 2006) Inte heller revisionsseden är lagstadgad till sina beståndsdelar, även om lagstiftaren tydligt har påkallat dess användande (Prop 1997/98:99, 1998).

Det är även genom FAR som en branschgemensam kvalitetskontroll upprätthålls, enligt principen om att den som granskar andra själv måste bli granskad för att vara trovärdig. Kvaliteten på revisorns arbete säkerställs genom en god och adekvat utbildning, praktisk erfarenhet, samt granskning och bedömning av utfört arbete av en oberoende part, det vill säga FAR. Värt att nämna är att revisionsbyråerna generellt sett även har interna kontrollsystem där erfarna revisorer kontrollerar att god sed, såväl som ledningens direktiv, följs i hela organisationen. (FAR, 2006)

Revisionsbevis – väsentlighet och risk

För att kunna uttala sig om räkenskapspåståendenas riktighet krävs att revisorn samlar in tillräckliga och ändamålsenliga revisionsbevis som styrker dem. Revisionsbevis utgörs av källdokument och bokföringsmaterial samt annan information eller andra iakttagelser som revisorn dokumenterat vid sin granskning. (RS 500, 2004) Revisionsbevis kan även vara muntliga intervjusvar som revisorn erhållit, och i detta fall är just dokumentationen av dessa av stor vikt för att kunna basera senare bedömningar på (FAR, 2006).

För att kunna säkra tillräckliga revisionsbevis för ett riktigt uttalande i revisionsberättelsen ligger stort fokus på att förstå de risker och förhållanden som råder i det reviderade företaget. Detta speciellt då revisorn omöjligt hinner gå igenom alla transaktioner, processer och saldon och således måste göra väl underbyggda avväganden om vilka aspekter som är av väsentlig betydelse för att ge en rättvisande bild. Att genom erfarenhet, kompetens och förståelse av företaget och dess specifika karaktäristika, avgöra vad som är just väsentligt är något som får stor plats i den inledande planeringsfasen av revisionen. I planeringsfasen, som i sig tar en betydande tidsrymd i anspråk, ska även riskfaktorer bedömas, något som tillsammans med väsentlighetsaspekten ligger till grund för vilka granskningsåtgärder som ska genomföras, i vilken omfattning de ska genomföras samt när man förlägger de olika åtgärderna i tiden. För att samla in revisionsbevis använder sig revisorer bland annat av intervjuer med de anställda på det reviderade företaget, och då främst företagsledningen, men man utvärderar även kommentarer från tidigare års revisionsrapporter eller från branschmedier. Jämförelser med andra bolag i samma bransch och uttalanden från specialister eller revisorer med tidigare erfarenheter av branschen är andra informationskällor som vid sidan om bolagets egna historiska dokumentation kan förstärka revisorns förståelse för bolaget. (FAR, 2006)

Centralt i revisorns arbete är dokumentation av iakttagelser och resultat av de granskningsåtgärder som utförts, allt för att åtgärderna ska kunna utgöra revisionsbevis som kan bedömas i efterhand. Även detaljerad beskrivning av vilka väsentliga åtgärder

revisorn utfört och vilket resultat han eller hon kommit fram till ska framgå av dokumentationen. (FAR, 2006)

Interna kontroller och substansgranskning

Själva granskningen är uppdelad i analys av interna kontroller och substansgranskning. Analysen av de interna kontrollerna ska beröras mer i detalj under nästföljande rubrik, men betyder i stora drag att revisorn granskar de kontrollsystem som ledningen etablerat inom företaget. Syftet med sådana kontroller är bland annat att stärka ledningens kontroll över korrekt information för att optimera ekonomistyrningen, försäkra sig om effektiva processer samt undvika kostsamma fel. Ansvarsfördelning, rapporteringsvanor och inbyggda rutiner för minimering av medvetna och omedvetna fel är exempel på interna kontrollsystem. För att få information om hur dessa kontroller och rutiner fungerar är intervjuer vanliga, men även policy- och styrdokument är möjliga informationskällor. Granskningen av de interna kontrollerna ger således en bild av hur väl företagets presenterade siffror borde överensstämma med verkligheten, men inget företag har kontrollsystem som är 100 % säkra då det sällan är ekonomiskt försvarbart att upprätthålla sådana. Som komplement använder sig därför revisorn av substansgranskningen där enskilda saldons riktighet kontrolleras. Detta sker genom fysisk inventering och kontroll av dokumenterade transaktioner, men även genom analytiska nyckeltalsberäkningar och felsökning vid budgetavvikelser. (FAR, 2006)

Substansgranskning av samtliga saldon och transaktioner är inte ekonomiskt försvarbart och i många fall inte heller tidsmässigt genomförbart, varför urval måste göras av revisorn. Dessa urval bygger i många fall på huruvida de interna kontrollernas karaktär påkallar en substansgranskning av enskilda konton för att säkerställa tillräckliga revisionsbevis, men även slumpmässiga eller systematiska stickprov används. Andelen konton och processer som granskas genom substansgranskning eller analys av interna kontroller beror på revisorns revisionsansats som anpassas utifrån de specifika förutsättningar varje enskilt företag har. Om fokus ligger på de interna kontrollerna behövs färre substansgranskningar göras och tvärtom, men de olika granskningsåtgärderna är inte helt ömsesidigt uteslutande då en viss substansgranskning alltid måste göras. (FAR, 2006) Riktlinjer och vägledning för riskbedömning och analys av intern kontroll regleras i RS 400 Riskbedömning och intern kontroll, vilken, som nämnts ovan, är en svensk översättning av den internationella ISA 400.

4.4.1 RS 400 Riskbedömning och intern kontroll

RS 400 tar sikte på att reglera hur revisorn ska beakta och bedöma den risk som finns för att det reviderade företaget presenterat oriktiga siffror i sin årsredovisning som följd av inneboende felaktigheter i företagets redovisningsprocess. Såväl mänskliga faktorer, såsom felaktiga inmatningar, som felaktiga saldon på grund av programmeringsfel, är exempel på saker man vill upptäcka och åtgärda genom interna kontrollsystem. Även företagets kontrollrutiner när det gäller strukturerandet av de transaktioner som sker

inom företaget, till exempel huruvida fakturering och attestering inte utförs av samma person, är centrala aspekter vid granskningen. RS 400 strukturerar upp tillvägagångssättet för granskning, samt uppdelning och beroende mellan de olika riskaspekterna i ett bolag. (RS 400, 2004)

Övergripande används uttryck som kontrollmiljö och kontrollåtgärder för att beskriva på vilket sätt intern kontroll praktiseras och hur den följs upp. Kontrollmiljön är ledningens övergripande benägenhet att granska och följa upp de siffror och utfall som presenteras i organisationen. I en stark kontrollmiljö läggs stor vikt vid just uppföljning och tydlig ansvarsfördelning, men det i sig räcker inte för att företaget ska sägas ha ett väl fungerande system för intern kontroll. Det krävs också tydliga riktlinjer för hur kontrollerna ska genomföras löpande och vilka moment som ska ingå, så kallade kontrollåtgärder. Till dessa hör till exempel rutiner för inventering, begränsning av fysisk åtkomst till tillgångar och bokföringsmaterial, begränsad tillgång till datasystem, kontroll av bokförda belopp, samt andra åtgärder för att begränsa möjligheter till manipulering av presenterade siffror. (RS 400, 2004)

I RS 400 används samlingsnamnet revisionsrisk för den risk som föreligger för att revisorn gör ett felaktigt uttalande i revisionsberättelsen, en risk vars beståndsdelar utgörs av inneboende risk, kontrollrisk och upptäcktsrisk. Med inneboende risk menas den risk som det specifika företaget utsätts för gällande att eventuella felaktigheter i saldon eller transaktioner överhuvudtaget förekommer och i så fall i vilken utsträckning detta sker. Man bortser i denna del helt ifrån huruvida det finns rutiner för att upptäcka dessa felaktigheter och reglera dem innan siffrorna presenteras, något som istället sägs vara hänförlig till kontrollrisken. Med kontrollrisken menas således risken för att väsentliga fel i saldon eller transaktionsslag inte upptäcks eller rättas i och med företagets egna interna kontrollsystem. Om revisorn upplever att företaget har bristfälliga interna kontroller, tillsammans med hög risk för att företagets presenterade saldon är felaktiga, ska han eller hon göra en utökad substansgranskning för att få tydligare revisionsbevis, på att företaget ändå presenterar rättvisande siffror i årsredovisningen, att basera sina uttalanden i revisionsberättelsen på. Den risk som alltjämt finns att revisorn i sin substansgranskning inte upptäcker de felaktigheter som blir följden av hög såväl inneboende risk som kontrollrisk, kallas upptäcktsrisk. (RS 400, 2004)

Inneboende risk

Revisorn använder sitt professionella omdöme för att bedöma den inneboende risken och fokuserar då på ett antal påverkande faktorer på såväl övergripande årsredovisningsnivå som på detaljerad saldo- och transaktionsnivå (RS 400, 2004).

På årsredovisningsnivå bedöms de omständigheter företagsledningen verkar under, och som eventuellt skulle få den att vilja lämna oriktiga uppgifter i årsredovisningen. Revisorn tar hänsyn till bland annat företagsledningens kompetens, branschvana och

integritet, samt de för branschen eller den enskilda organisationen karaktäristiska faktorer som påverkar uppgifterna lämnade i årsredovisningen. Det sistnämnda kan röra sig om mer eller mindre komplicerade relationer till koncernbolag, teknisk utveckling som gör att värden skiftar kraftigt och att man fokuserar på alternativa jämförelseindex, komplicerad kapitalstruktur, samt geografiska skillnader inom företagets verksamhetsområde. (RS 400, 2004)

På saldonivå är det explicita händelser och konton vars överensstämmelse med verkligheten som ska kontrolleras. Det rör sig främst om saldon där värdena i stor utsträckning utgörs av uppskattningar, saldon där man under föregående revision upptäckte felaktigheter som rättades till, men även konton med hög risk för förskingring av tillgångar, samt okonventionella transaktioner, får särskilt stor uppmärksamhet av revisorn. (RS 400, 2004)

Kontrollrisk

Granskning av kontroller tar sikte på att utvärdera företags förmåga att upptäcka och förhindra felaktigheter i redovisningen innan de presenteras. Exempel på åtgärder från revisorns sida är kontroll av de underlag som finns för verifikationer som genomförts, avstämning av konton, och granskning av huruvida det finns rutiner för intern kontroll, i vilken mån de efterlevs och av vem. För att avgöra om kontrollåtgärder tillämpas konsekvent sker förfrågningar inom företaget, men även kompletteringar genom kontroller under året kan vara aktuellt i vissa fall – vanligtvis ger revisorns egna iakttagelser ett starkare revisionsbevis än anställdas utsagor om rutiner. Revisorn ska också ta hänsyn till uttalanden om kontrollåtgärder som gjorts vid tidigare revisioner, men måste för varje ny revision skaffa revisionsbevis som styrker de påståendena man vill göra gällande även under innevarande år. Dessa uttalanden från tidigare år kan ligga till grund för den planering av arbetsgången som revisorn gör gällande granskning av interna kontroller, och visa en viss riktning som revisorn bör gå. Det är dock inte ovanligt att revisorn upptäcker kontrollrisker i och med det allmänna informationsinhämtande han eller hon gör för att skaffa sig en övergripande förståelse för företagets redovisningssystem och de rutiner företaget har vid olika affärshändelser. Företag med hög inneboende risk garderar sig ofta med stark intern kontroll, något som gör att en ensidig bedömning av antingen kontrollrisk eller inneboende risk från revisorns sida kan ge en oriktig bild av revisionsrisken. (RS 400, 2004)

Upptäcktsrisk

Risken att revisorn inte upptäcker eventuella felaktigheter i redovisningen hänger ihop med hur omfattande substansgranskning revisorn gör, något som i sin tur hänger ihop med den bedömda inneboende risken samt kontrollrisken. Vid en upplevt låg inneboende risk, tillsammans med en låg kontrollrisk, kan revisorn vara säkrare på att substansen i de siffror som presenterats av företaget har uppkommit på ett riktigt sätt, att de kontrollerats på ett föredömligt sätt och att de således stämmer bra överens med vad regleringar och god sed kräver. Om granskningen av inneboende risk och interna

kontroller däremot inte ger övertygande revisionsbevis för att revisionsrisken är godtagbart låg ska revisorn göra en grundligare substansgranskning för att på så sätt minska risken för att fel inte upptäcks av revisorn innan han eller hon lämnar sin revisionsberättelse. (RS 400, 2004) Behovet av substansgranskning samt granskning av interna kontroller är dock inte ömsesidigt uteslutande i det hänseendet att den ena inte behövs om den andra ger skäl att anta att ett riktigt uttalande görs i revisionsberättelsen. Tvärtom är de båda mycket tätt sammankopplade och kompletterar varandra snarare än substituerar; viss substansgranskning ska alltid göras på väsentliga saldon oavsett upplevd inneboende risk och kontrollrisk. (FAR, 2006)

Om revisorn upptäckt brister i utformning av redovisningssystem eller interna kontroller ska han eller hon så snart som möjligt påtala detta på en lämplig ansvarsnivå i det reviderade bolaget. I den mån sådana brister påtalas är det viktigt att komma ihåg att de brister som rapporteras endast är relaterade till revisionen och huruvida de påverkar en rättvisande bild av företaget och dess finansiella ställning, och alltså inte har med företagsledningens krav på kontroll att göra (RS 400, 2004). Ett användbart verktyg för företagsledningen, och även för revisorn, är Committee of Sponsoring Organizations of the Treadway Commission (COSO).

4.4.2 COSO

1992 gav COSO ut den första versionen av Internal Control - Integrated Framework, som sedan dess har kommit att betraktas som en mycket användbar standard vid utformningen av god intern kontroll. Medlemmarna av COSO utgörs av en sammanslutning av företag, redovisningsekonomer och revisorer som tillsammans har tagit fram en definition av intern kontroll:

> ”*Intern kontroll är en process som påverkas av styrelsen, bolagsledningen och annan personal, och som utformats för att ge en rimlig försäkran om att bolagets mål uppnås inom följande kategorier:*
>
> - *Ändamålsenlig och effektiv verksamhet.*
> - *Tillförlitlig finansiell rapportering.*
> - *Efterlevnad av tillämpliga lagar och förordningar.”*
>
> (FAR, 2006)

Utöver det tidigare nämnda standardverket Internal Control – Integrated Framework, bör också Internal Control over Financial Reporting - Guidance for Smaller Public Companies nämnas. Detta hjälpmedel publicerades 2006 och är en samling av praktiska exempel och så kallad *best practice*[13], utvecklad som vägledning vid tillämpning av ramverket. (FAR, 2006)

[13] Begreppet beskriver metoder som anses vara särskilt lämliga för att uppnå vissa specifika resultat.

COSO:s betydelse har på senare tid ökat som en följd av de striktare krav på intern kontroll som ställs bland annat i Sarbanes-Oxley Act, i EU:s åttonde direktiv, det så kallade Revisorsdirektivet, och i Svensk kod för bolagsstyrning.

Enligt COSO-definitionen delas den interna kontrollen upp i fem delar:

1. Kontrollmiljö: Avser en sammanfattning av de faktorer som påverkar företagets kontrollmedvetande; vilken struktur och disciplin förmedlas. Det är viktigt att ta hänsyn till hur företagets organisation är uppbyggd, hur ansvar fördelas och hur delaktig företagsledningen och styrelsen är.
2. Riskbedömning: För att upptäcka de väsentliga risker som påverkar den interna kontrollen avseende den finansiella rapporteringen är det viktigt att analysera de olika nivåer där eventuella fel kan uppstå. En kraftansträngning för att identifiera risker för oegentligheter och otillbörligt gynnande av en annan part på företagets bekostnad lyfts också fram. En särskild granskning av redovisningsmässiga bedömningar bör också genomföras, samt en kontroll av hur affärssystemet hanterar transaktionerna. Den information som samlas in vid riskbedömningen ligger sedan till grund för ett antal kontrollmål, vilka används för att stärka räkenskapspåståendena i de finansiella rapporterna.
3. Kontrollaktiviteter: För att upptäcka, förebygga och korrigera de fel som kan uppstå i verksamheten använder man sig av kontrollaktiviteter. I detta moment framhålls vikten av välutvecklade rutiner och styrfunktioner, samt ett välfungerande IT-stöd.
4. Information och kommunikation: I detta steg fokuseras arbetet på att identifiera den information som är viktig för att bibehålla den interna kontrollen avseende den finansiella rapporteringen, och även här framhålls vikten av välfungerande IT-system.
5. Övervakning och uppföljning: För att försäkra sig om en fortsatt god intern kontroll är det viktigt att man kontinuerligt övervakar och följer upp de kontroller som har införts. Det är viktigt att försäkra sig om att de kontroller som används, hur välutformade de än må vara, faktiskt är praktiskt tillämpningsbara. Arbetet med detta kan ske på alla nivåer i företaget, från styrelse och bolagsledning ner till enskilda avdelningar, och kan också, vid behov, genomföras som en särskild granskning.

Det finns mycket tydliga likheter mellan COSO-definitionen och de frågor som behandlas i RS 400, vilket kan ses som ett ytterligare bevis för COSO-definitionens användbarhet. Det bör också tilläggas att de punkter som listas ovan endast ger en kortfattad beskrivning av vad som ryms under respektive punkt. (FAR, 2006)

COSO-definitionen kan antingen användas för att göra en övergripande bedömning av ett företags interna kontroller eller också för att göra en mer noggrann granskning av ett specifikt område inom verksamheten. Figur 4[14] visar hur COSO-definitionen kan

[14] Se rubrik 4.5 IT-revision

anpassas för en genomgång av ett företags IT-säkerhetsarbete (Öhrlings PriceWaterhouseCoopers Gruppen AB, 2006).

4.4.3 RS 401 Revision i en datoriserad informationssystemmiljö

Som en del av analysen av de interna kontrollerna ska revisorn beakta de IT-system som används i det reviderade företaget. Detta kan röra sig om allt från system som har med den operativa driften att göra, som till exempel bokningssystem eller liknande, till affärssystem som är till för att underlätta hantering av bokföring och det ekonomiska rapporteringsarbetet. Även omfattningen av systemen kan variera från att endast fungera som förenkling av enskilda frikopplade processer, till ett omfattande affärssystem där alla företagets processer integreras för att sedan behandlas och bilda rapportunderlag, bas för nyckeltalsberäkningar och/eller strategiframtagning. Alla system i vilka ekonomisk information passerar, och som således sedan kan påverka substansvärderingen, är möjliga objekt för revisorns granskning. Revisorn kan dock omöjligt kontrollera alla system och ska därför bara beakta de system som påverkar väsentliga förhållanden i ett bolags ekonomiska rapportering. (RS 401, 2004)

Revisionens syfte eller beståndsdelar ändras inte på grund av användandet av mer eller mindre komplexa datasystem i det reviderade företaget, tillvägagångssättet för en revisor kan dock skilja sig från de fall där IT-användandet inte är lika utbrett. Revisorn ska skaffa sig tillräcklig kunskap om redovisningssystemen, och de interna kontroller som används i samband med det, för att kunna utvärdera dess påverkan på uppgifterna i årsredovisningen och för att leda revisionsarbetet på ett sådant sätt att tillräckliga kontroller görs för att försäkra sig om att ett rättvisande utlåtande görs i revisionsberättelsen. (RS 401, 2004)

Vid analys av redovisningssystem ska revisorn främst fokusera på sådana processer och steg i databehandlingen som ligger till grund för de väsentligaste punkterna i företagets redovisning. Det gäller speciellt då det rör sig om många inmatningar som sedan var för sig blir svåra att spåra i ett större datasystem, automatiskt genererade saldon eller beräkningar som sker genom att olika program och/eller organisationer är sammankopplade, samt när datasystem tillåts göra värderingar av tillgångar där en subjektiv värdering skulle vara att föredra. Även för en rutinerad revisor är det mycket tidskrävande att genomföra den här typen av kontroller manuellt på alla aktuella konton, varför man i vissa fall kan använda sig av ett datoriserat revisionsprogram som söker i systemen enligt givna parametrar. (RS 401, 2004)

Aspekter som vid revisionen tillkommer i ett mer komplext datoriserat redovisningssystem är bland annat svårigheter att följa så kallade transaktionsspår – vilket innebär att man ska kunna följa en affärstransaktion från dess uppkomst till dess presentation eller påverkan på aktuellt saldo (BFL 5:11) – genom systemets process. Anledningarna till svårigheterna kan vara att spåren bara finns under en kort period eller att systemet utför så många behandlingar och aggregerade beräkningar av olika

siffror att transaktionsspåret aldrig blir helt komplett. Felaktigheter i programmeringen av de stora affärssystemen kan generera konsekvent felaktiga saldon, men i och med komplexiteten av systemen kan det vara svårt att hitta felet då siffrorna flödar genom, och påverkas av, många olika delar av det totala affärssystemet. Bortsett från dessa aspekter av rent tekniska svårigheter och problem finns det också risk för att kontrollåtgärder, som tidigare hindrat att enskilda individer fått för mycket inflytande över enskilda processer, i och med rationaliseringar, som möjliggjorts genom implementeringen av informationsteknologi, samlas hos en person. Detta kan bidra till att färre felaktigheter upptäcks i den finansiella rapporteringen och hanteringen, men också att skrupelfria anställda uppmuntras till bedrägligt beteende då risken för upptäckt minskar. Ansvarsfördelning kan också vara ett problem i de fall datoriserade system genomför en helt automatiserad transaktionsprocess som blir bindande för företaget. (RS 401, 2004)

Användandet av IT-system har dock även fördelar i och med konsekvent behandlande av liknande transaktioner, färre led där mänskliga slarvfel kan uppstå samt genom möjlighet till ökad övervakning från företagsledningens sida genom användandet av analysverktyg och liknande. Det senare är något som ger förutsättningar för upprätthållandet av en stark kontrollmiljö och anses vara en stor fördel. Användandet av ett IT-system ger också, som nämnts ovan, revisorn möjligheter att, genom användandet av speciell programvara för revision av specifika affärssystem, på ett tidseffektivt sätt utföra granskningsåtgärder och få underlag för planering av sin fortsatta revision. I vissa affärssystem kan det för revisorn till och med vara omöjligt att få fram de uppgifter som krävs vid en revision utan användandet av datorstöd. (RS 401, 2004)

Revisorn ska, som nämnts ovan, i och med sitt yrke ha tillräcklig kunskap för att kunna leda och strukturera en revision av IT-systemen i samma utsträckning som i resterande delar av revisionen. Det kan dock finnas fall då det är omöjligt att kräva att revisorn besitter den djupgående kunskap som krävs för att analysera mer avancerade IT-system, och i dessa fall ska revisorn använda sig av en specialist i enlighet med RS 620. (RS 401, 2004)

4.4.4 RS 620 Användning av en specialist i revisionsarbetet

Revisorn har det övergripande ansvaret för att revisionen leder fram till en godtagbart låg revisionsrisk genom säkrandet av adekvata och tillförlitliga revisionsbevis. För att kunna bära detta ansvar och leda arbetet krävs att revisorn besitter en bred kompetens gällande företags affärsförhållanden och de tillvägagångssätt som står till buds för att utvärdera deras redovisning på ett effektivt och strukturerat sätt. På grund av den breda kunskap som krävs för att leda revisionsarbetet kräver regleringen i RS inte att revisorn själv ska ha sådan detaljkunskap om påverkande faktorer som krävs för att bedöma dessa enskilda posters eller faktorers inverkan på företagets rapportering. Aspekter på väsentliga ekonomiska förhållanden kräver ibland kunskaper som ligger utanför redovisning och revision och kan således behöva inhämtas externt från personer med

kompetens utanför revisionsområdet. Det kan till exempel finnas komplicerade juridiska aspekter för vilka revisorn behöver ta hjälp av en jurist, det kan finnas tekniska aspekter som kräver utlåtande av en ingenjör och det kan finnas komplicerade affärssystem som kräver konsulterandet av en IT-revisor. Revisorn ska, trots anlitandet av en specialist, ha tillräcklig kunskap och förståelse för det område inom vilket en specialist används, för att kunna leda revisionsarbetet och säkra tillräckliga revisionsbevis. (RS 620, 2004)

Likaväl som revisorn måste försäkra sig om huruvida revisionsbevis som specialisten presenterar tillgodoser de krav revisorn vill ha uppfyllda, så måste revisorn försäkra sig om att specialisten är kompetent och lämplig för uppgiften. Specialistens professionella meriter och dokumenterade kompetens såväl som eventuella anknytning till det reviderade företaget är aspekter som tas hänsyn till. Om revisorn bedömer att specialistens utlåtande är otillräckliga eller svaga som revisionsbevis på grund av dessa förhållanden kan det vara nödvändigt att ta in synpunkter på området från ytterligare en specialist. I de fall då specialisten är anställd av revisorn, eller jobbar inom samma byrå, är kraven på revisorns kontroll av specialistens kompetens dock avsevärt lägre, då man kan förutsätta att specialisten besitter den kompetens som krävs – arbetet som specialisten utför, och riktigheten i de slutsatser denne drar, måste dock alltjämt beaktas av revisorn. (RS 620, 2004)

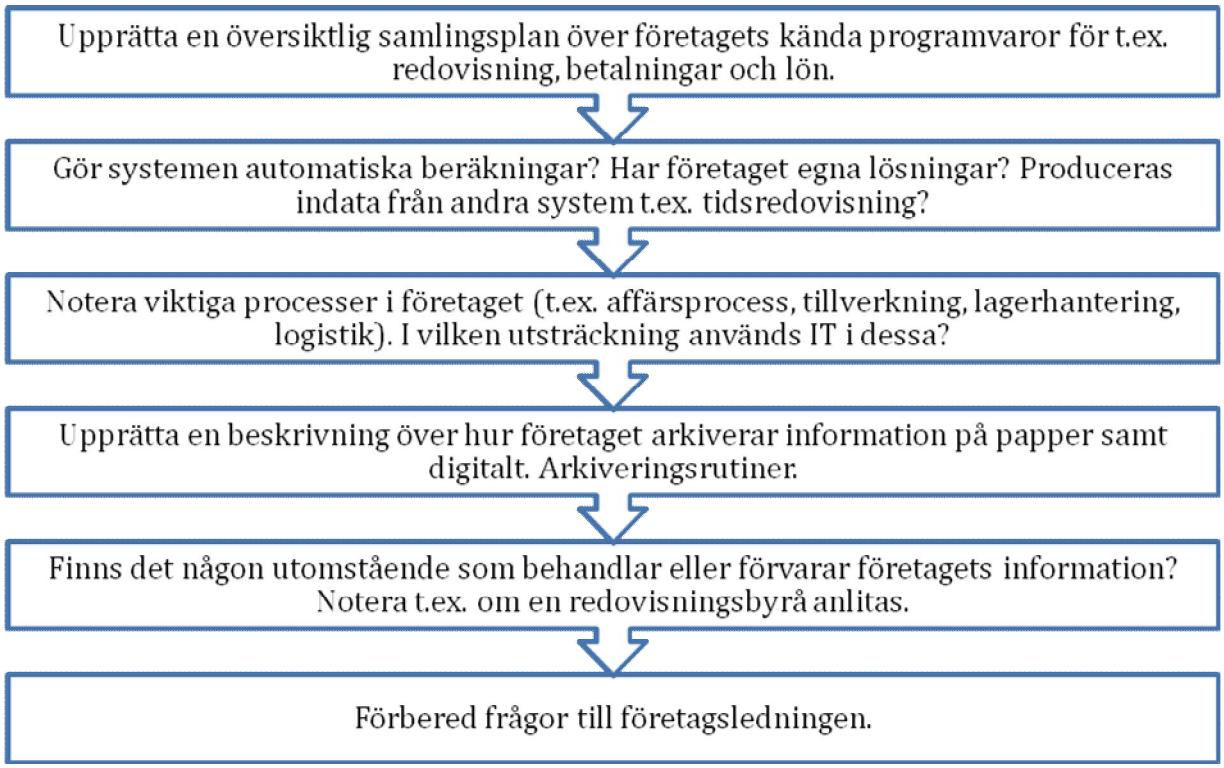
Trots att revisorn inte förväntas ha den detaljkunskap som en specialist har så ska han eller hon ändå, på basis av sin allmänna kunskap om verksamheten och genom jämförelser med egna iakttagelser av de förhållanden som råder där, förstå de metoder och antaganden som specialisten gjort i sitt arbete och avgöra om de är rimliga och ändamålsenliga. I de fall dessa förutsättningar inte specificeras av revisorns instruktioner till specialisten eller i specialistens rapport till revisorn kan detta kräva en elaborerad dialog med specialisten, men även med representanter från företaget samt att revisorn själv granskar de källdata som specialisten utgått ifrån i sitt arbete och jämför specialistens slutsatser med sina egna övergripande dito. (RS 620, 2004)

I de fall då revisorn inte anser att specialistens slutsatser ger tillräckliga revisionsbevis, eller att de står i strid med andra sådana, ska en fördjupad analys göras av revisorn. Detta kan innebära dialog med företaget, utlåtanden av andra specialister eller en revisionsberättelse som avviker från standardutformningen. (RS 620, 2004)

4.5 IT-revision

IT-revision sker i samband med granskningen av de interna kontrollerna, ett område där IT-lösningarna har fått en ständigt ökande betydelse sedan dessas införande under 1960-talet (Nordin, 2008). Det är dock viktigt att framhålla att IT-revisionen inte är en fristående del av revisionen, utan en integrerad del som används för att säkra tillförlitliga revisionsbevis. I mindre företag klarar revisorn själv av att genomföra den granskning som stipuleras i RS401, men ju större och mer komplexa företag, desto

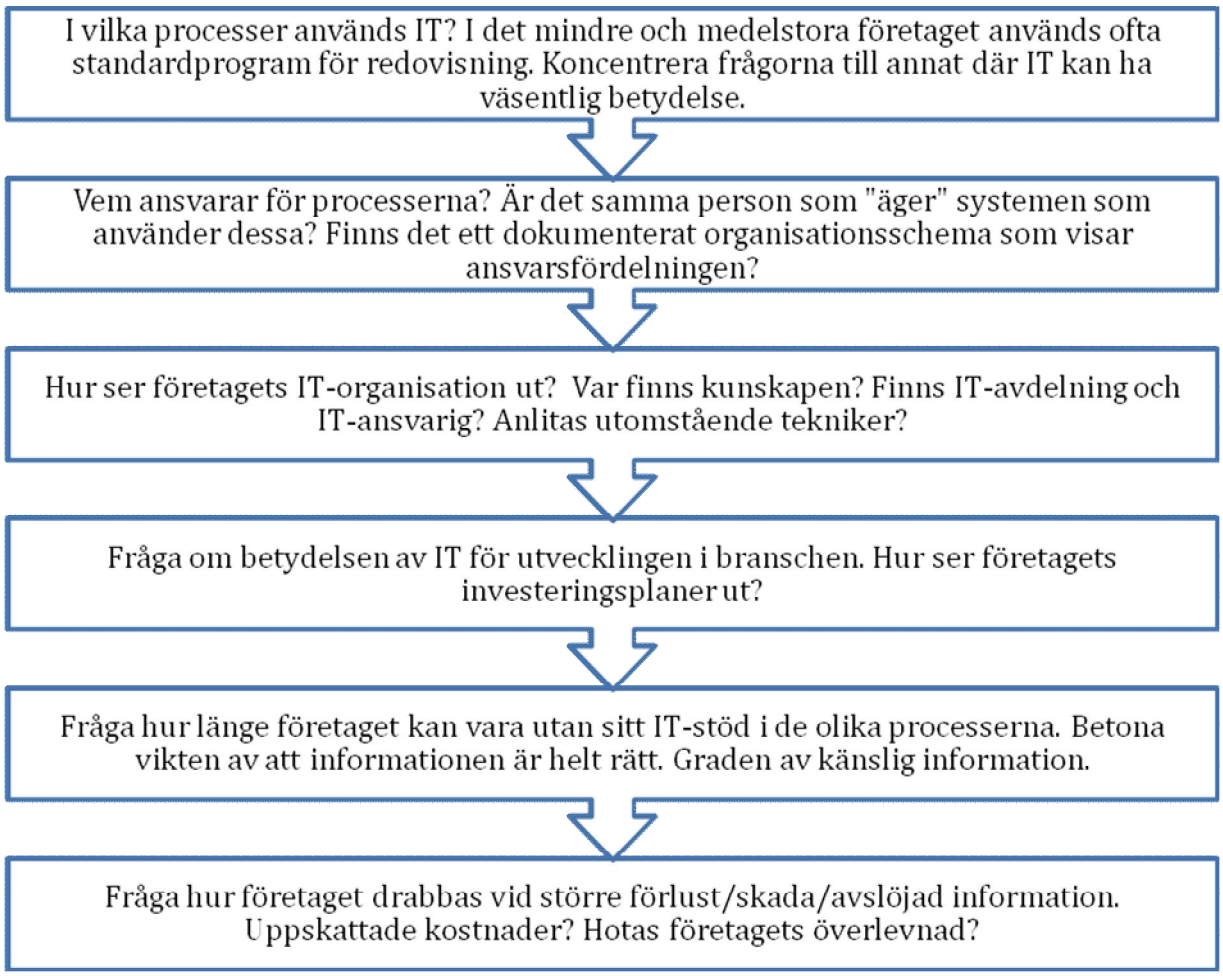
större blir behovet av att ta hjälp av en specialist; IT-revisorn. Figuren nedan visar ett förslag på hur det inledande skedet av en IT-revision kan se ut. (FAR SRS, 2007)



Figur 2 Exempel på arbetsgång vid IT-revision (FAR SRS, 2007)

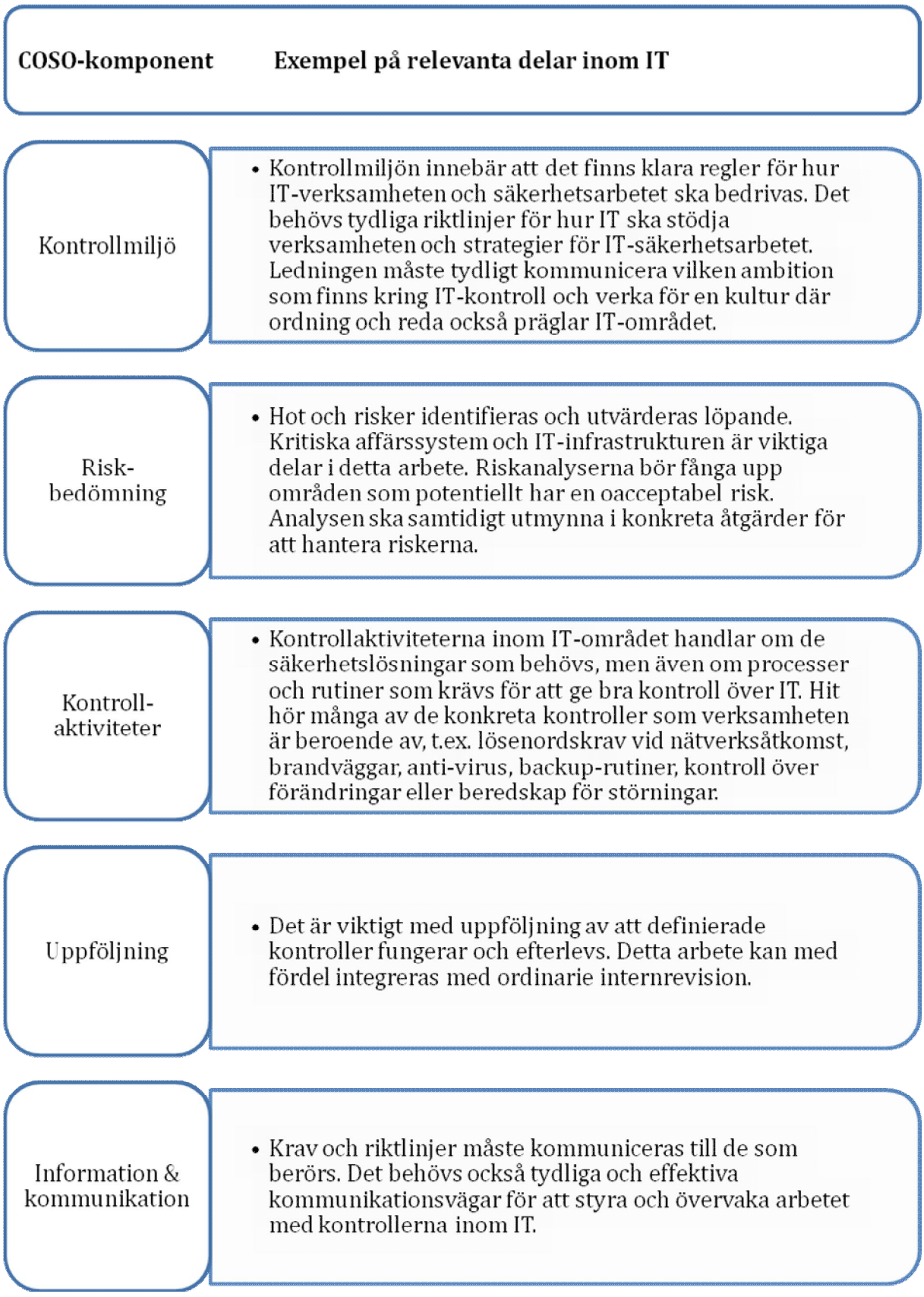
Det förfarande som beskrivs i figuren ovan är utformat för att täcka in de delar som IT-revisionen förväntas granska, men vikten av att genomföra alla dessa steg, som en enhetlig process, är viktigast vid ett nytt uppdrag, då revisorn saknar kunskap om företaget. Vid efterföljande års revisioner räcker det däremot att granska eventuella förändringar, samt tidigare upptäckta riskområden. Ovanstående granskning ska i första hand genomföras av revisorn själv då denne förväntas förstå systemets komplexitet och utifrån detta kunna planera de fortsatta revisionsåtgärderna. Det kan dock redan i detta skede uppstå ett behov av att ta hjälp av en specialist för att förstå en särskilt komplex systemstruktur och en sådan konsultation ska då göras i enlighet med bestämmelserna i RS 620. Momenten som beskrivs i figuren är av sådan art att de bör genomföras i ett mycket tidigt skede av revisionsprocessen, och beroende på tidigare erfarenheter av klienten kan vissa delar genomföras redan innan revisorn träffar företagsledningen. För att utröna vilka potentiella risker som finns i systemet förbereder revisorn, som det anges i figurens sista steg, ett antal frågor till företagsledningen. (FAR SRS, 2007)

En central del av revisorns planeringsarbete baseras på dennes samtal med företagsledningen och deras syn på företagets verksamhet och struktur. För att bedöma företagets behov av IT-stöd i verksamheten är det viktigt att detta berörs i dessa samtal och vi ska återigen använda en figur för att illustrera ett möjligt upplägg. (FAR SRS, 2007)



Figur 3 Exempel på frågor till företagsledning (FAR SRS, 2007)

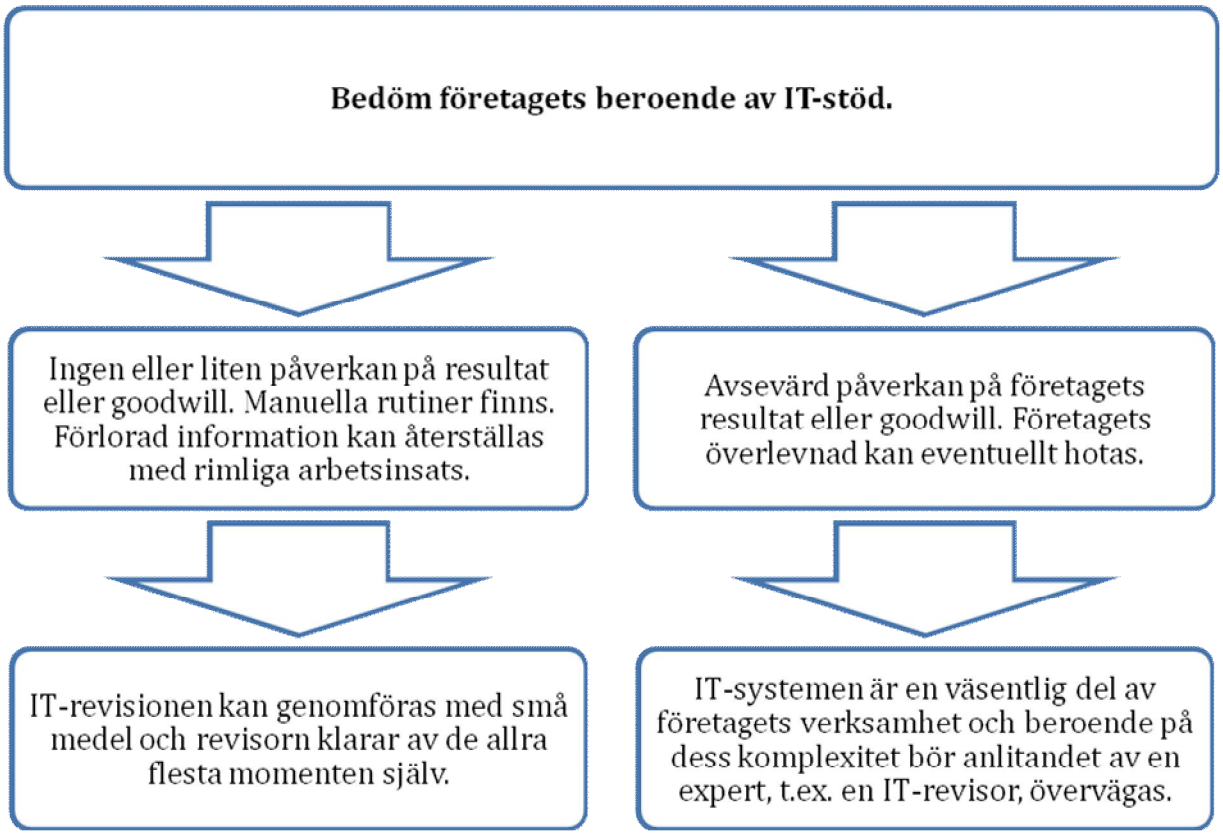
Dessa frågor ska med fördel behandlas av revisorn under samtalen med företagsledningen, för att därefter ligga till grund för dennes revisionsplanering. För att bedöma de potentiella riskerna associerade med IT-systemen kan revisorn till exempel utgå från COSO-definitionen och applicera den på relevanta aspekter av IT-systemmiljön (exempelvis som i figur 4) och sedan utvärdera den information som framkommer i samtalen med företagsledningen (Öhrlings PriceWaterhouseCoopers Gruppen AB, 2006).



Figur 4 Tillämpning av COSO-definitionen på IT-miljön

(Öhrlings PriceWaterhouseCoopers Gruppen AB, 2006)

I samband med revisionsplanering ska revisorn också bedöma vilken fortsatt IT-granskning som bör göras för att kunna säkra tillförlitliga revisionsbevis och om det finns behov av att använda sig av en IT-revisor. Denna bedömning sammanfattas i figur 5. (FAR SRS, 2007)



Figur 5 Exempel på bedömningsgrunder för behovet av IT-revisor (FAR SRS, 2007)

4.5.1 IT-revisorn

För att arbeta som IT-revisor krävs en god förståelse av både ekonomi och IT; trots att vissa moment kan kräva avancerade tekniska kunskaper är grundprincipen vid IT-revision att enbart system och processer som kan ha väsentlig påverkan på företagets räkenskaper ska granskas. Det är därför viktigt att IT-revisorn har goda kunskaper i ekonomi och kan kommunicera med revisorerna och förstå deras utgångspunkt och granskningens mål. Följaktligen är det svårt att definiera en homogen utbildningsbakgrund för IT-revisorer. (Nordin, 2008) Detta är en klar skillnad jämfört med de tydligt definierade krav, på bland annat utbildningens innehåll, som finns för att bli godkänd eller auktoriserad revisor (FAR, 2006). Därmed inte sagt att det inte finns certifieringar för IT-revisorer; de mest meriterande av dessa utfärdas av Information Systems Audit and Control Association (ISACA) (www.isaca.se, 2009).

ISACA

Grunden för det som idag är ISACA lades redan 1967, då ett antal personer som arbetade med kontroll och revision av datasystem insåg vikten av en centraliserad informationskälla för att hantera de allt viktigare datasystemen. Idag har organisationen

över 86 000 medlemmar i hela världen, varav 557 stycken i Sverige, och dess syfte är att ”vara en heltäckande intresseorganisation för styrning, säkerhet, kvalitet, revision och kontroll inom IS/IT-området. Föreningen ska verka för medlemmarnas kompetensutveckling och för ett aktivt erfarenhetsutbyte mellan kollegor över hela världen.”. (www.isaca.se, 2009)

En viktig del av ISACA:s verksamhet är certifiering av personer som arbetar med kontroll, styrning och säkerhet för IT-system och de erbjuder tre olika titlar: CISA, CISM och CGEIT. Av dessa tre är det främst CISA (Certified Information Systems Auditor) som är relevant för IT-revisorn. (www.isaca.se, 2009)

CISA

Sedan 1978 har titeln CISA delats ut av ISACA till personer med minst fem års arbetslivserfarenhet inom IT-revision eller IT-säkerhet och uppnått minst 75 % rätta svar på ett certifieringsprov, bestående av 200 flervalsfrågor. Certifieringen är den enda i sitt slag och för att behålla sin titel krävs det att man är fortsatt aktiv och ständigt vidareutbildar sig. Detta är en viktig anledning till att CISA idag är en globalt erkänd certifiering med hög status och dess betydelse ökar ständigt, inte minst i Sverige. (www.isaca.se, 2009)

4.6 Tidigare forskning

I en magisteruppsats från Högskolan i Gävle, daterad 2008, har Anna-Carin Nordin undersökt hur revisorers arbete har förändrats till följd av företagens ökade nyttjande av IT-lösningar. Hon har bland annat undersökt behovet av specialiserade IT-revisorer, vad som menas med att vara IT-revisor, samt vilken del IT-revisionen spelar i den traditionella revisionen. Hennes uppsats har ett något mer tekniskt fokus än vår och hennes empiri bygger på intervjuer med 4 revisorer som företrädesvis arbetar med de IT-relaterade delarna av revisionen, men ingen av dem är auktoriserad IT-revisor enligt exempelvis CISA. För att säkerställa IT-revisionens riktighet använder de sig av olika typer av standardiserade ramverk, främst ISO-17799 och COBIT[15]. (Nordin, 2008)

Hennes respondenter menar samstämmigt att IT-revisionen i de flesta fall utförs av revisorn själv, och att behovet av en IT-revisor främst uppkommer vid stora och komplexa system, ofta hos internationella företag. De betonar dock att utveckling går mot ett allt större behov av IT-revisorer, då det blir allt svårare för revisorer med traditionell ekonomibakgrund att utföra de granskningar som behövs. Ytterligare en aspekt som de anser kommer leda till större efterfrågan på IT-revisorer är införandet av Sarbanes-Oxley Act och dess ökade krav på intern kontroll. (Nordin, 2008).

[15] Allmänt accepterade ramverk för att säkerställa en tillförlitlig IT-revision. (Nordin, 2008)

5 Empiri

5.1 Inledning

Då vi intervjuat både Revisorer och IT-revisorer kommer empiridelen inledas med en förklaring av gemensamma begrepp och strukturer för att sedan fortsätta med en jämförelse av de två olika respondentgruppernas syn på en rad frågeställningar. Dessa frågeställningar grundas i den reglering som finns på området, såsom den beskrivs i teoridelen ovan, och svaren tjänar till att belysa de olika respondentgruppernas syn på praxis.

5.2 Byråernas metodiker och organisationsstruktur

Samtliga respondenter har varit eniga om vikten av deras byråers interna metodik för hur arbetet planeras och utförs. Dessa metodiker och arbetssätt är företagsinterna, ej publicerade och därför nästintill omöjliga att studera för en utomstående. Genom våra intervjuer har vi dock fått en viss insikt i hur de är utformade och hur de påverkar det dagliga arbetet. Vi har också fått en viss förståelse för hur organisationerna är utformade; hur ansvarsförhållandena ser ut och hur arbetet leds och kontrolleras.

Arbetssätten hos de olika byråerna, som våra respondenter representerar, uppvisar stora likheter avseende sättet på vilket arbetet organiseras. För varje uppdrag finns en påskrivande revisor, vanligtvis någon av byråns partners, och en uppdragsledare (nedan enbart benämnd revisor), som sköter det operativa arbetet. Till sin hjälp har uppdragsledaren ett antal medarbetare, dessa utgörs främst av revisorer men i förekommande fall även av andra kompetensgrupper som kan behövas beroende på företagets verksamhet och särart. IT-revisorerna faller, tillsammans med exempelvis skatte- eller affärsjurister, under denna sistnämnda grupp. Dessa specialister är i sin tur organiserade i självständiga avdelningar, vanligtvis med en partner som ytterst ansvarig. En viktig del av byråernas kvalitetssäkring är den kontinuerliga kontroll som finns inbyggd i denna hierarkiska konstruktion.

Den andra, och allra viktigaste, delen av kvalitetssäkringen är användandet av byråernas globalt utvecklade revisionsmetodiker, som är utformade för att överensstämma med gällande lagar och regler. Tack vare det faktum att alla kontor använder sig av samma metodik kan medarbetare på alla nivåer i företaget, från de påskrivande revisorerna och nedåt, vara förvissade om att deras underlydandes arbete har utförts på korrekt och tillförlitligt sätt. Med forskningsterminologi skulle man kunna tala om en mycket hög reliabilitet; metodiken har utformats, utvärderats och utvecklats för att leverera så tydliga och konsekventa svar som möjligt. Utöver den direkta kopplingen till lagar och regler som finns inbyggd i metodiken, tas även hänsyn till andra viktiga standarder och praxis. Ett tydligt exempel på detta är COSO-definitionens tydliga påverkan på revisionsprocessen, något som flera av respondenterna också lyfte fram.

5.3 Intervjusammanställning

Presentationen av respondentgruppernas uppfattningar utgörs generellt av den aggregerade uppfattningen inom respektive grupp, detta för att beskriva den konsensus som vi ändå upplevt föreligger mellan de enskilda respondenterna inom de båda grupperna. Jämförelsen mellan de båda grupperna är intressant då de lagar som ligger till grund för interaktionen dem emellan tar sikte på de olika roller som finns och vilket ansvar som ligger på vilken part.

Med revisor menas nedan den revisor som är ansvarig för revisionsuppdraget, även kallad teamledare, gruppledare och uppdragsledare

Var och när i revisionsprocessen kommer IT-revisorn in?

Revisorer

Bland revisorerna gick åsikterna något isär angående i vilket skede IT-revisorn blir aktuell att engagera. Generellt för revisorsgruppen är dock att de lägger stort fokus på att revisorn själv ska vara tillräckligt kompetent för att kunna analysera IT-systemen och avgöra var eventuella risker skulle kunna föreligga. IT-revisorn används sedan, enligt en av revisorerna, endast då revisorn själv har identifierat riskerna i systemet, samt väsentligheten av dessa, men inte besitter tillräcklig kompetens för att fullt ut kunna analysera om risken är ett reellt hot eller om man har ett fullgott skydd mot denna risk. Detta innebär också att IT-revisorn, enligt samma revisor, vanligen engageras först efter att revisorn avslutat planeringsfasen av revisionen. Övriga revisorer menar att IT-revisorn kopplas in direkt då revisorn konstaterat att affärssystemen är av komplex karaktär, något som enligt dem uppenbarar sig mycket tidigt i kontakterna med företaget och alltså betyder att IT-revisorn medverkar i planeringsfasen.

IT-revisorer

Den allmänna uppfattningen bland de IT-revisorer vi intervjuat var att de är med mycket tidigt i de bolag där det överhuvudtaget är aktuellt för revisorn att ta hjälp av IT-revisorer. Huruvida det är aktuellt eller inte är något som, enligt IT-revisorerna, görs uppenbart för revisorn efter en första kontakt med företaget då revisorn skapar sig en övergripande förståelse för företaget och förstår vilken roll IT-systemen spelar. En av IT-revisorerna menar att han dessutom hjälper till med kartläggning av bolaget med avseende på IT-strukturen, något som alltså innebär att revisorn inte gör denna kartläggning utan endast bedömer behovet av en sådan.

Utsträckningen i vilken IT-revisorn medverkar i planeringsfasen är, enligt en av IT-revisorerna, avhängig den enskilda revisorns förståelse för IT, en förståelse som varierar med ålder och erfarenhet. I vissa fall är alltså IT-revisorn med från början och gör bedömningar om affärssystemsfunktioners påverkan är väsentliga och medför risk. I andra fall har revisorn själv gjort bedömningar om vad som är väsentligt och var risk

kan föreligga, analysen av systemen delegeras sedan i förekommande fall vidare till en IT-revisor.

Vilken roll spelar IT-revisorn i revisionsprocessen?

Revisorer

Revisorerna menar att IT-revisorn främst är ett verktyg för att säkerställa tillräckliga revisionsbevis för bolagets räkenskapspåståenden, men två av revisorerna understryker också att de ser IT-revisorn som ett stöd för att skapa förståelse för IT-systemet vid revisorns egna övergripande bedömningar av systemet. En av revisorerna påpekar att det ofta handlar om att göra en tillräckligt noggrann, men samtidigt kostnadseffektiv, revision och att det då är mer ekonomiskt försvarbart att låta en IT-revisor granska de IT-baserade kontrollerna än att revisorn själv ska lägga tid på att skaffa revisionsbevis genom substansgranskning.

Två av revisorerna menar också att det kan ha sina fördelar att en IT-revisor sköter kommunikationen med företags IT-avdelning då de kommunicerar mer på lika villkor i och med en gemensam vokabulär. Den rent kommunikativa aspekten underlättas än mer av att IT-revisorn på ett tydligare sätt kan förstå, och förmedla erkännandet av, det arbete IT-avdelningen gjort, menar revisorerna som påpekar att deras eventuellt begränsade förståelse för enskilda IT-lösningars effekter kan göra dem mindre benägna att uppmuntra positiva initiativ från företagens IT-avdelningar.

IT-revisorer

Gemensamt för samtliga IT-revisorer är att de ser sig som en integrerad del av teamet, snarare än en extern resurs, vid revisionen. Det finns dock lite olika bilder av IT-revisorns roll och ansvar inom teamet. En av IT-revisorerna menar att han är en självklar del av teamet och direkt får ansvar för alla IT-relaterade kontrollgranskningar, samt genomför dessa. Denna IT-revisor påpekar också att han stöttar revisorn i väsentlighetsbedömningen i de fall IT-systemen spelar in i denna. De andra två menar att integrationen med revisionsteamet baseras på uppdragets storlek; i mindre uppdrag används IT-revisorn endast som en resurs medan han i större uppdrag blir en mer integrerad del i likhet med den första IT-revisorns syn. I de fall de hämtas in som resurs görs oftast bara små riktade insatser där IT-revisorn själv inte tillåts analysera systemen så djupt som denne många gånger skulle vilja, väsentlighetsbedömningen har i dessa lägen alltså redan gjorts av revisorn, påpekar en av IT-revisorerna.

Även om revisorerna hävdar att de i regel inte initialt låter IT-revisorn analysera de interna kontrollerna i hela IT-systemet, hävdar IT-revisorerna att de i förekommande fall kan gå igenom i stort sett hela systemet i de fall revisorn behöver hjälp med att bilda sig en förståelse för systemet. Dessa påståenden kan verka motstridiga, men skapandet av en övergripande förståelse kräver inte samma detaljerade analys som en granskning av de interna kontrollerna gör. Åtminstone två av IT-revisorerna menar att de vid större uppdrag nästan uteslutande gör dessa analyser för att bidra till revisorns förståelse, och

att de sedan ligger till grund för IT-revisorns rekommendationer till revisorn avseende var fokus av kontrollerna bör ligga.

Hur leder revisorn IT-granskningsprocessen?

Revisorer

Samtliga revisorer är av uppfattningen att de styr IT-revisorerna mot områden som revisorerna uppfattat som väsentliga. Konsensus råder, som nämnts ovan, mellan revisorerna om att man inte släpper IT-revisorn fri att själv analysera och bedöma risker i hela företagets IT-system, detta främst då det skulle kunna resultera i evighetsuppdrag och behandlande av oväsentliga detaljer. En av revisorerna menar till och med att det ofta rör sig om explicita kontoanalyser där IT-revisorn ges i uppdrag att samla in tillräckliga revisionsbevis för att kunna styrka redovisningspåståenden om enskilda saldon gjorda av företaget. De andra två menar dock att det kan röra sig om mer generella områden som de, genom dialog med IT-revisorn, identifierar som viktiga att analysera.

Gemensamt för samtliga revisorer är att de, efter att ha instruerat IT-revisorn om var fokus ska ligga och vilka revisionsbevis de vill ha, mer eller mindre släpper IT-revisorn fri att välja tillvägagångssätt i sina granskningar. Rent praktiskt betyder detta, enligt revisorerna, inte att det är upp till IT-revisorn att efter egen skön välja fritt hur han ska samla in information och analysera IT-systemen, utan snarare att han själv gör bedömningen om vilka till buds stående verktyg som lämpar sig bäst i det enskilda fallet. Verktygen i detta fall utgörs av revisionsbyråernas interna arbetsmetodiker som utvecklats för att uppnå ett fullgott resultat, samt upprättats i överensstämmelse med gällande lagar och regler, praxis och seder. Anledningen till att revisorn lämnar det upp till IT-revisorn att avgöra vilken metod av dessa som lämpar sig bäst är att revisorn säger sig vara trygg i byråns, och i detta fall IT-revisionsavdelningens, egna tillvägagångssätt och interna kvalitetssäkringar, samt att revisorn ibland inte själv besitter den detaljkunskap som krävs för att avgöra vilken metod som bör användas.

Eventuella problem av teknisk karaktär, det vill säga som har med IT-revisorns verktyg att göra, förväntar sig revisorn att IT-revisorn ska lösa internt inom sin avdelning, och eventuellt genom konsultationer högre upp i den interna hierarkin och/eller globalt inom byrån. Problem som är av fysisk karaktär, och alltså har med inhämtandet av material att göra, förväntas dock lyftas till revisorn och kan leda till att denne genomför ytterligare granskningar inom sitt kompetensområde för att försäkra sig om tillräckliga revisionsbevis.

IT-revisorer

Beroende på IT-revisorernas svar om när de kommer in i processen och vilken roll de spelar blir deras svar lite olika. I de fall då IT-revisorn är med redan i planeringsstadiet, och identifierar väsentliga områden för granskning, upplever de att en mer jämlik diskussion mellan revisor och IT-revisor leder fram till IT-revisorns

uppdragsbeskrivning, medan de i andra fall blir styrda av revisorn mot specifika mål som denne identifierat.

Revisorn styr även IT-revisorn genom tilldelning av viss andel av total revisionsbudget – och därmed tid till IT-revisorns förfogande – något som kan innebära att IT-revisorn själv får göra vissa avvägningar i sin granskningsinsats då det sällan finns utrymme för extensiva kontroller av alla potentiella riskområden. Denna något friare styrning används, enligt en IT-revisor, främst vid mindre uppdrag där resurserna är mer begränsade och avvägningar får större vikt. Samma IT-revisor menar att man vid större och mer komplexa uppdrag istället lyder under strängare krav där omfattningen på granskningen i högre grad är kontrollerad och uppstyrd. Kontrollen är då bunden till olika, mer omfattande, handlingsmallar där vissa moment ska genomföras. IT-revisorn menar dock att han i dessa fall är mer delaktig i avgörandet av omfattningen av granskningen eftersom revisorn i högre grad konsulterar IT-revisorn när det rör sig om komplexa IT-system och dess påverkan på redovisningspåståendena.

Vid större och mer komplicerade uppdrag konsulteras, som nämnts ovan, ofta IT-revisorn tidigt och lämnar en rekommendation till revisorn om var granskningar bör göras. Utifrån dessa rekommendationer, och den övergripande förståelse som revisorn får i och med IT-revisorns analys, tar revisorn sedan beslut om vilka instruktioner han ska ge IT-revisorn. Revisorn väger in sina egna iakttagelser och kan, utifrån sin övergripande förståelse och insikt i företaget som helhet, i vissa fall styra om IT-revisorns fokus till andra delar än de föreslagna.

Samtliga IT-revisorer påpekar också att de, även i de fall då revisorn vill ha revisionsbevis för ett explicit redovisningspåstående, gör en mer omfattande analys av IT-systemet för att förstå de olika applikationernas interaktion med varandra och de riskmoment som uppstår där.

Vilket inflytande har IT-revisorn över utformningen av IT-granskningen?

Revisorer

Det går inte att komma ifrån att revisorn har det övergripande ansvaret för att riktiga uttalanden görs i revisionsberättelsen, och detta är även något som samtliga revisorer i undersökningen anger som skäl till den generella bild av vem som gör bedömningar om IT-granskningens utformning. Alla väsentlighetsbedömningar anses nämligen göras av revisorn baserat på dennes allmänna kunskap och förståelse om företags och branschers karaktär i allmänhet, och det enskilda företagets utformning i synnerhet. Detta är en kunskap och förståelse vars grund ligger i den erfarenhet revisorn samlar på sig under sin yrkesverksamma karriär, gällande företag och branscher i allmänhet, och genom samtal och analys i det enskilda bolagets fall. Utifrån denna kunskap gör revisorn bedömningar om vilken revisionsansats denne vill ta – tonvikt på substansgranskning eller granskning av interna kontroller – och detta ligger i sin tur till grund för IT-

revisorns eventuella inblandning. Revisorn förväntas alltså identifiera de risker som finns i enskilda bolag och styra IT-revisorn mot dessa i sina instruktioner.

Två av revisorerna menade att de även styrde IT-revisorns fokus och djup genom att tilldela IT-revisorn en viss del av den totala revisionsbudgeten utifrån vilken IT-revisorn sedan planerar sitt arbete. Om IT-revisorn i sina granskningar skulle hitta fler aspekter som denne finner relevanta att granska ytterligare vid revisionen ska detta enligt samtliga revisorer diskuteras med revisorn som, baserat på sin övergripande förståelse, avgör om det är av väsentlig betydelse eller ej. Samtliga revisorer understryker att det sker en dialog, men revisorns bedömningar, både under planeringsfasen och löpande efter IT-revisorns analyser, är de som gäller i slutändan.

Som nämnts i föregående frågeställning har revisorn inget inflytande över hur IT-revisorn går tillväga under den faktiska granskningen, något som härrör i revisorns brist på detaljkunskap på området men även på en tilltro till IT-revisorsavdelningens interna metoder och kontroller.

IT-revisorer

Den IT-revisor som tidigare uttalat att han på ett mer påtagligt sätt medverkar till och med innan planeringsfasen, och därmed i den övergripande kartläggningen av bolaget, upplever att han har stort inflytande över de väsentlighetsbedömningar som görs. Generellt sett beror IT-revisorns medverkan i bedömningarna på huruvida det är första gången man reviderar bolaget och i vilken utsträckning man har tidigare erfarenheter av bolagets karaktär och kontrollstruktur. Två av IT-revisorerna menar att de nästan alltid ombeds göra en övergripande analys av IT-strukturen i de fall den upplevs som något komplex och man inte har reviderat företaget tidigare. Den rapport av analysen som IT-revisorn sedan presenterar för revisorn ligger sedan till grund för diskussion dem emellan gällande vad som kan utgöra risker och i vilka fall de har väsentlig påverkan på redovisningen.

En IT-revisor menar att det är han som, mer eller mindre ensam, identifierar väsentliga risker i den IT-baserade kontrollsystemen som sedan granskas och avrapporteras till revisorn. Grundinställningen hos de två andra IT-revisorerna är dock att det alltjämt förs en dialog med revisorn utifrån den rekommendation som de lämnar i sin rapport, men att de får stort gehör för sina bedömningar då de trots allt förväntas ha en djupare förståelse för systemen än revisorn. De upplever också att de dessutom delar revisorns förståelse för vad som kan vara relevant att beakta då de flesta IT-revisorer har en bakgrund inom finansiell revision. Även om så inte skulle vara fallet menar en IT-revisor att erfarenhet som just IT-revisor gör att man lärt sig vad revisorn brukar fokusera på och därmed kan göra goda väsentlighetsbedömningar även utan ekonomisk bakgrund.

I förlängningen, menar en IT-revisor, att det, i alla fall när det rör sig om mindre uppdrag, beror på revisorns erfarenhet av IT vem som styr IT-revisionens innehåll. Det

faktiska tillvägagångssättet av IT-revisionen bestäms, enligt samtliga IT-revisorer, uteslutande av dem själva inom ramen för revisionsbyråns metodik för IT-revision. Det är de som behärskar verktygen och förstår dessas passande tillämpning, och det finns således ingen anledning för revisorn att detaljstyra vilka metoder som används, enligt IT-revisorerna.

Hur skapar sig revisorn tillräcklig förståelse för att kunna utvärdera IT-revisorns arbete?

Revisorer

Revisorerna är alla överens om att de mycket sällan ifrågasätter de metoder som IT-revisorn använder sig av, eller de antaganden som IT-revisorn gjort i sitt arbete. Fokus för revisorn ligger nästan uteslutande på resultatet av IT-revisorns granskningar och man litar på att de metoder som använts är hämtade ur byråns interna IT-revisionsmetodik. Denna metodik upplevs av samtliga revisorer som innehållandes strikta tillvägagångssätt och noggranna vägledningar för rättvisa övervägningar av IT-revisorn, och är baserad på lagar och god sed. Revisorerna har fullt förtroende för den ofta globalt utvecklade metodiken, då den är ett resultat av byråns samlade kompetens och erfarenhet.

Bedömningen om huruvida IT-revisorns antaganden har varit rimliga, med hänseende på byråns interna metodik, överlämnar revisorn sedan åt IT-revisionsavdelningens egna interna kontroller av arbetsmetoder och ansvarsfördelning. Som förklaring till detta hävdar en av revisorerna att dessa bedömningar av gjorda antaganden med fördel bör göras av experter inom IT-revision, snarare än av revisorn själv som kanske inte fullt ut kan avgöra huruvida arbetsgången och antagandena faktiskt har varit ändamålsenliga eller ej. Det handlar här om att den som är bäst lämpad att göra bedömningen bör göra den, och att denna auktoritet således inte behöver ifrågasättas av revisorn.

IT-revisorer

Konsensus råder även bland IT-revisorerna om att den interna revisionsmetodiken spelar en avgörande roll i revisorns förståelse för det arbete IT-revisorn utför. De tre IT-revisorerna har dock alla lite olika syn på revisorns förståelse, och i vilken utsträckning revisorn aktivt söker sin förståelse eller passivt litar på att IT-revisionsavdelningens egna kvalitetskontroller fungerar.

En av IT-revisorerna understryker att förståelsen för hans arbete varierar beroende på revisorns allmänna förståelse för IT; vissa revisorer är generellt mycket insatta och förstår på egen hand de antaganden som gjorts och de metoder som valts, medan andra i större utsträckning förlitar sig på att den interna metodiken försäkrar att rätt avvägningar har gjorts. En annan av IT-revisorerna lyfter fram att vissa revisorer skapar sin förståelse av metoderna genom en kombination av de rapporter som IT-revisorn lämnar och en dialog mellan parterna om innehållets innebörd. Den tredje IT-revisorn antydde att det fanns en så stark tilltro till byråns interna metodik att revisorn

överhuvudtaget mycket sällan, om ens någonsin, tyckte sig behöva bedöma IT-revisorns antaganden och metoder.

Mycket handlade även enligt IT-revisorerna om att metodiken är så utförligt formulerad, och baseras på gällande lagar och beprövade metoder, att det, i kombination med ansvarsfördelning och interna kvalitetskontroller, verkar räcka för att revisorn ska anse sig vara säker på att IT-revisorns metoder och antaganden är adekvata. En förutsättning för detta är att revisorn är mycket insatt i revisionsbolagets revisionsmetodik – något som samtliga IT-revisorer anser som självklart att revisorn är.

Hur skapar sig revisorn en förståelse för IT-revisionens resultat?

Här behandlar vi både revisorns och påskrivande revisors förståelse. Detta då revisorns förståelse är av vikt eftersom han eller hon vanligen kommunicerar IT-revisionens resultat till både företag och påskrivande revisor, medan påskrivande revisors förståelse är av vikt då det är han eller hon som bär det yttersta ansvaret för ett rättvisande uttalande i revisionsberättelsen.

Revisorer

Revisorns förståelse av IT-revisorns arbete grundar sig på den rapport IT-revisorn lämnar efter utförd granskning av de interna kontrollerna. Alla revisorer understryker att en dialog utifrån rapporten är central för revisorns förståelse för IT-revisorns arbete, men en av revisorerna menar att denna kommunikation görs mer eller mindre ingående beroende på huruvida IT-revisorns slutsatser skiljer sig från de resultat revisorn själv kommit fram till angående samma räkenskapsposter. I de fall det råder samstämmighet finns det enligt revisorn ingen anledning att ifrågasätta IT-revisorns resultat, medan man lyfter IT-revisorns resultat till diskussion i de fall då de avviker från revisorns. På detta sätt gör man en sammantagen bedömning för varje enskilt räkenskapspåstående tills man säkrat tillräckliga revisionsbevis för att kunna göra ett rättvisande uttalande i revisionsberättelsen.

Den rapport som IT-revisorn lämnar in hänger således inte i luften såtillvida att den är ett statiskt dokument som bara accepteras av revisorn. Två av revisorerna förtydligar också de skillnader i rapporteringsvägar, och rapporternas form, som uppstår beroende på uppdragens storlek. Vid mindre uppdrag bifogar revisorn IT-revisorns rapport till den revisionsrapport som lämnas till påskrivande revisor. Vid revisorns genomgång med påskrivande revisor utelämnas ofta tekniska aspekter som kanske varit aktuella vid revisorns diskussion med IT-revisorn, och på så sätt filtreras informationen genom hierarkin för att alla berörda parter ska kunna tillgodogöra sig resultatet på en lämplig förståelsenivå, baserat på respektive nivås informationsbehov. Om det är ett större revisionsuppdrag så lämnar revisorn en sammanfattning av väsentliga delar i IT-revisorns rapport i sin revisionsrapport till påskrivande revisor, men i dessa fall närvarar ofta ansvarig IT-revisor vid avrapporteringen till påskrivande revisor så att

denne kan ställa eventuella frågor direkt till den som är mest insatt i de IT-kontroller som gjorts, IT-revisorn.

IT-revisorer

Även bland IT-revisorerna lyfts deras rapport fram som central för revisorns förståelse av deras resultat, men här också, i förekommande fall, i kombination med vikten av standardiserade utformningar av rapporterna. Denna utformning är dessutom skapad i enlighet med byråns metodik för att tolkningarna av IT-revisorns presenterade resultat ska vara konsekventa. Förutsatt att IT-revisorns rapport är upprättad enligt den interna revisionsmetodiken, vilket den uteslutande är, finns det alltså vägledning för revisorn om hur han ska tolka det som står i rapporten.

Detta gäller, enligt en av IT-revisorerna, i synnerhet vid större uppdrag då arbetsgången är mycket tydligt definierad och resultaten tar stöd i strikta vedertagna processer, varför man mycket sällan som revisor behöver tvivla på utfallet. Samma IT-revisor säger också att den beskrivning av sitt arbete som han lämnar till revisorn underlättar revisorns förståelse och att den också, rent hypotetiskt, skulle kunna ligga till grund för revisorns synpunkter på vad som har gjorts, eller vad som behöver göras ytterligare. Några sådana synpunkter hade han dock aldrig varit med om, då revisorn aldrig uttryckt tvivel över det resultat som presenterats.

Generellt anser IT-revisorerna att påskrivande revisor har mycket stor förståelse för generella risker i enskilda företag och på basis av detta kan ha en övergripande förståelse för IT-revisorernas presenterade resultat. I de fall han eller hon söker en djupare förståelse hämtas den nerifrån i hierarkin, dock inte nödvändigtvis från IT-revisorn då påskrivande revisor främst kommunicerar med revisorn när denne avrapporterar revisionen. Revisorn har ofta bildat sig en bra förståelse genom IT-revisorns rapport och dialog med denne, något som är nödvändigt, enligt en av IT-revisorerna, då det ofta är revisorn som kommunicerar IT-revisorns resultat även till det reviderade bolagets representanter. Överlag är dialog och avstämningsmöten mellan IT-revisorn och revisorn ett vanligt komplement till den rapport av sina granskningsåtgärder och resultat som IT-revisorn lämnar.

6 Analys

6.1 Inledning

Nyckeln till att kunna besvara vår frågeställning är att först definiera revisorns kunskap och förståelse. För att lyckas med detta har vi genomfört intervjuer och samlat in de empiriska resultat som presenterades i föregående avsnitt. Det som återstår innan vi kan försöka svara på vår frågeställning och dra några slutsatser är att analysera våra empiriska data, för att på så sätt definiera revisorns kunskap och förståelse.

6.2 Revisorns kunskap och förståelse

Vårt försök att fastställa revisorns kunskap och förståelse har gjorts på ett mycket översiktligt plan och är av kvalitativ, snarare än kvantitativ, natur. Analysen kommer därför att bygga på en sammanställning av de empiriska data som vi har samlat in, uppdelat på tre övergripande kategorier:

- Planering
- Ledning
- Utvärdering

Planering

I regleringen, här främst i form av RS 400, poängteras vikten av revisorns förståelse för redovisningssystem och system för intern kontroll; till exempel förmågan att utvärdera ett affärssystems struktur och dess möjliga risker. Denna förståelse krävs för att revisorn, i sin planering, ska kunna välja en lämplig revisionsansats. Detta krav på förståelse och kompetens är något som också har framhållits av revisorerna bland våra respondenter som något självklart i deras arbete, och finns inte förståelsen ska revisorn inte åta sig uppdraget. Revisorns förståelse för det enskilda företagets redovisningssystem, och de risker som är förknippade med detta, baseras på den generella förståelsen revisorn har av företaget och dess miljö. I praktiken är det däremot föga sannolikt, menar IT-revisorerna, att revisorn besitter den detaljkunskap om IT-system som i vissa fall krävs för att skaffa sig en välnyanserad bild för den fortsatta planeringen. De framhåller också det naturliga i att deras specialistkompetens tas i anspråk så tidigt som möjligt i processen för att hantera uppdrag så effektivt som möjligt.

Värt att framhålla är att IT-revisorns inblandning i planeringsfasen, och i förekommande fall även innan denna, beror på det reviderade företagets storlek och komplexiteten i de använda IT-systemen. Revisorns inställning är att han själv, så långt det är möjligt, ska genomföra all analys av bolaget och dess IT-struktur, samt identifiera de risker som finns däri. Denna inställning bottnar i revisorns historiska ansvar för utformning och planering av revisionsinsatsen. Detta har dock blivit en allt svårare uppgift för revisorn; systemens omfattning och komplexitet har ökat enormt och antalet transaktioner likaså, och därmed krävs en annan kompetens än den som revisorer normalt besitter.

Vi kan alltså konstatera att revisorn, särskilt i större, komplexa uppdrag, förlitar sig på IT-revisorernas assistans för att bilda sig en uppfattning om hur det fortsatta arbetet bör utformas och att den kunskap och förståelse som är relevant i dessa sammanhang är förmågan att avgöra de IT-relaterade riskernas väsentlighet i revisionen som helhet.

Ledning

Det är viktigt att poängtera att samspelet mellan revisorn och IT-revisorn är dynamiskt, snarare än statiskt. Utifrån vad respektive part finner i sina granskningar, förs en dialog om hur problem ska bemötas och risker bedömas. Våra respondenter är samstämmiga i denna beskrivning, men de betonar också faktumet att det är revisorns bedömning som är den avgörande. Återigen utgår revisorn ifrån sin allmänna kunskap och förståelse för att avgöra risker och väsentlighet utifrån den information som framkommer i och med IT-granskningen, samt dess del i den totala revisionen. Däremot överlåts det operativa ansvaret för valet av metoder och genomförandet av IT-granskningen till IT-revisorn, som genom sin större tekniska kompetens är bättre lämpad för detta.

De revisorer vi talat med är mycket tydliga med att de på intet sätt känner ett behov av att utvärdera de metoder och verktyg som IT-revisorn använder, då dennes metoder, liksom revisorns, är en del av byråns arbetsmetodik. Följaktligen har de inte större anledning att betvivla de metoder som IT-revisorn använder än de har av att betvivla de metoder som de själva använder sig av dagligen. De berättar också att ett vanligt verktyg för att styra IT-revisorns granskning är mängden tilldelad tid i den budget som upprättas för varje uppdrag, för att på så sätt begränsa och koncentrera granskningen till de mest väsentliga områdena.

Utvärdering

När man i lagen nämner revisorns förståelse och förmåga att utvärdera IT-revisorns arbete görs ingen skillnad i om det är påskrivande revisor eller arbetsledaren man menar. I realiteten krävs också, som nämnts ovan, att både påskrivande revisor och arbetsledande revisor kan utvärdera IT-revisorns arbete och resultat, men de gör det på olika sätt.

När det gäller att utvärdera IT-revisorns arbete är revisorns förståelse för de tekniska tillvägagångssätten underordnad dennes kunskap om byråns interna revisionsmetodik. Är revisorn väl insatt i byråns metodik och hyser tillit till byråns, och då i synnerhet IT-avdelningens, inbyggda kontrollmekanismer, behöver han själv aldrig bilda sig en djupare förståelse för enskilda detaljer. Anledningen till detta är att revisorn vet att de metoder som används, i form av IT-revisionsmetodiken, är baserade på byråns samlade kompetens och erfarenhet på området. Detta gäller i synnerhet påskrivande revisor då dennes kunskap och förståelse förväntas vara mycket omfattande, men inte nödvändigtvis på detaljnivå. Således är det endast det aggregerade resultatet av IT-revisionen – som en del av granskningen av de interna kontrollerna – och dess påverkan på revisionen som helhet, som är av vikt för påskrivande revisor. Arbetsledande revisor

har ett något större behov av detaljerad information, och förståelsen för denna, då det oftast är han eller hon som kommunicerar IT-revisorns arbete med företaget och påskrivande revisor.

De tillvägagångssätt som IT-revisorn använt sig av placeras, i och med dennes rapporter, in i den metodikstruktur som revisorn har mycket god kännedom om och därför kan tillgodogöra sig arbetsgången utifrån. Då förståelsen för IT-revisorns metoder och antaganden trots allt varierar från revisor till revisor, utgör IT-revisorns avrapportering en möjlighet för revisorn att ställa frågor och be IT-revisorn förklara sina tillvägagångssätt i den mån revisorn känner ett behov av detta. Detsamma gäller även för påskrivande revisor när arbetsledande revisor rapporterar till denne. Ytterligare en faktor som underlättar revisorns förståelse är det faktum att IT-riskerna beskrivs med en terminologi som är konsekvent med den som används för övriga granskningar; ett tydligt exempel på revisionsmetodikens betydelse för revisorns förståelse.

6.3 Norm och praxis

Baserat på revisorns förståelse såsom den beskrivs ovan, inser man tämligen obesvärat att den inte ser ut på det sätt som regleringen på området stipulerar. Förståelsen som revisorn besitter är alltjämt en förståelse för generella samband och risker, en förståelse som skapats genom erfarenhet och studier av de enskilda bolagen, men ytterst sällan en sådan förståelse för explicita delar av det arbete som utförs av IT-revisorn som kommer till uttryck i regleringen på området.

Enligt RS 400 ska revisorn ta hänsyn till IT-miljön när han utformar sina granskningsåtgärder, något som onekligen kräver en förståelse för dessa system i enlighet med vad som beskrivs i RS 401. Där ställs tydliga krav på revisorns förståelse för IT-systemens påverkan för bedömningen av inneboende risk och kontrollrisk, i synnerhet i de fall då revisorn ska leda en eventuell IT-revisor, i enlighet med RS 620, och således också kunna utvärdera denna specialists resultat.

Redan i första läget kan revisorns kunskaper vara för knappa för att han eller hon ensam ska kunna tillgodogöra sig alla aspekter i företagets IT-system för att kunna beakta dem i sin planering av revisionen – något som avhjälps genom konsultation av en IT-revisor. I andra läget handlar det om att ha en tillräckligt god förståelse för vad som bör granskas för att kunna leda den specialist som ska utföra granskningen, en förståelse som revisorn på ett generellt plan besitter. När det gäller att explicit styra IT-revisorn i vilken sorts granskning denne bör genomföra är revisorn av naturliga skäl utlämnad till IT-revisorns kompetens på området. Detta medför dock enligt regleringen i RS 620 att revisorn ska bedöma IT-revisorns arbete baserat på en förståelse för de antaganden och metoder som IT-revisorn använt. Även här upplever vi, med stöd i empirin, att revisorns kunskap är begränsad. I det här fallet är anledningen dock att revisorn inte söker den information som krävs för bedömningen av IT-revisorns metoder på grund av att metodernas lämplighet och utförandets kvalitet bedöms på ett sätt som anses bättre

lämpat – av en auktoritet inom IT-revisionsavdelningen, på basis av den interna metodiken. I det sista läget handlar det om att utvärdera det resultat IT-revisorn presenterat, något som grundar sig i att förstå de metoder som IT-revisorn använt men som också kräver förståelse för hur resultatet ska tolkas. Här begränsas revisorn av tekniska aspekter och eventuellt brist på gemensam vokabulär, något som överbryggas i och med användande av konsekventa terminologier i och med användandet av byråernas interna metodik som revisorn är mycket väl förtrogen med.

6.4 Koppling till tidigare forskning

Anna-Carin Nordins studie av IT-revisionens del av den traditionella revisionen och behovet av en IT-revisor erbjuder ytterligare empiriskt stöd på några punkter, men avviker också på en viktig punkt.

Nordin har, liksom vi, funnit att IT-revisorns kompetens oftast åberopas i samband med revisioner av stora företag med komplexa IT-system och att revisioner av detta slag ständigt ökar i betydelse, inte minst på grund av den påverkan som Sarbanes-Oxley Act innebär. Det finns dock en viktig skillnad i beskrivningen av hur IT-revisionen utförs; Nordins respondenter säger sig använda olika typer av allmänna ramverk, medan samtliga våra respondenter framhåller användandet av deras byråers interna metodiker.

7 Slutsats

Nedan presenteras de slutsatser vi dragit utifrån vår övergripande frågeställning;

> *Har revisorn tillräcklig kunskap och förståelse för att ge IT-revisorn adekvata instruktioner och utvärdera dennes arbete?*

Vi anser oss ha funnit empiriska bevis för att det föreligger en diskrepans mellan den kunskap och förståelse som stipuleras i regleringen och den kunskap och förståelse som revisorn de facto besitter. Det krav på revisorns systemförståelse och förmåga att bedöma IT-revisorns antaganden, metoder och resultat, som vi anser finns i RS, uppfylls inte av denne på en teknisk nivå, utan med hjälp av övergripande kunskap och förståelse.

För att besvara vår frågeställning måste man dock fråga sig huruvida det är relevant att revisorn faktiskt har en teknisk förståelse för att kunna ge IT-revisorn adekvata instruktioner och tolka dennes resultat. Det är vår övertygelse att så inte är fallet då vi menar att kravet på den enskilde revisorns djupare förståelse blir överflödigt i och med att byråns arbetssätt, ansvarsfördelning, samt dess kvalitetssäkringssystem ger möjligheter till kontroll och utvärdering som vida överstiger den som skulle vara möjlig om allt sådant ansvar vilade på en ansvarig revisor.

Det är därför vår åsikt att den praxis som, i olika utföranden, används inom Big Four-byråerna idag på alla sätt motsvarar de kvalitetskrav på revisorn som anges i regleringen – trots det faktum att man i praktiken har överfört revisorns reglerade kompetenskrav på byråns metodik och system för intern kontroll. Det är i det här sammanhanget viktigt att komma ihåg att revisorns kompetens inte har degenererats med tiden, snarare tvärtom, men att kraven på denne har ökat i och med den tekniska utvecklingen.

Kravet på revisorns förståelse av redovisningssystemen var rimligt när de fortfarande var relativt okomplicerade och revisorn utförde alla kontroller mer eller mindre på egen hand. Det finns dock ingen rimlighet i att kräva revisorns förståelse och medvetenhet om alla detaljer som dessa system är uppbyggda av idag.

Slutsatsen blir således att revisorn har tillräcklig kunskap och förståelse för att ge IT-revisorn adekvata instruktioner och utvärdera dennes arbete, men att tillräcklig i det här fallet innebär ett betydligt lägre krav på kunskap och förståelse än det som stipuleras i regleringen. Kunskaps- och förståelsegapet mellan norm och praxis överbryggas av byråns interna metodik och system för interna kontroller, ansvarsfördelning samt kvalitetssäkring.

7.1 Fortsatt forskning

Vi har i vår studie behandlat revisorernas kunskap och förståelse utifrån ett kvalitativt perspektiv; vi har utgått från våra respondenters personliga erfarenheter och försökt bilda oss en övergripande uppfattning om revisorers kunskapsnivå. Målet med vår studie har dock inte varit att exakt fastställa revisorernas kunskapsnivå, utan snarare bedöma om den är tillräcklig i relation till gällande reglering. Således bör en kvantitativt inriktad studie, med syfte att kartlägga och gradera revisorernas kunskap och förståelse, vara intressant. Förslagsvis bör begreppen kunskap och förståelse tydligt definieras, gärna med hjälp av normgivare och/eller IT-revisorer, och den fortsatta studien ha formen av en enkätundersökning eller strukturerade intervjuer.

Ytterligare ett område av intresse kan tänkas vara att undersöka hur arbetet på mindre revisionsbyråer, som inte har egna IT-revisorer, förhåller sig till regleringen.

8 Källförteckning

8.1 Böcker

FAR. (2003). *FARs Revisionsbok 2004.* Stockholm: FAR Förlag AB.

FAR. (2006). *Revision - En praktisk beskrivning.* Stockholm: FAR Förlag AB.

FAR SRS. (2007). *IT-handbok - Vägledning för revision.* Stockholm: FAR SRS Förlag AB.

Lantz, A. (2007). *Intervjumetodik.* Lund: Studentlitteratur AB.

Merchant, K. A., & Van der Stede, W. A. (2007). *Management Control Systems.* Harlow: Pearson Education Limited.

Ruane, J. M. (2006). *A och O i samhällsvetenskaplig forskning.* Lund: Studentlitteratur AB.

Smith, D. (2006). *Redovisningens språk.* Lund: Studentlitteratur AB.

8.2 Artiklar

Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review. *Academy of Management Review* , s. 57-74.

Öhrlings PriceWaterhouseCoopers Gruppen AB. (2006). Intern kontroll över IT – nya förväntningar och utmaningar – en introduktion för styrelse och ledning. Stockholm: Öhrlings PriceWaterhouseCoopers Gruppen AB.

8.3 Databasartiklar

RS 400 Riskbedömning och intern kontroll. (2004). *FAR Komplett* . Stockholm: FAR SRS Förlag.

RS 401 Revision i en datoriserad informationssystemmiljö. (2004). *FAR Komplett* . Stockholm: FAR SRS Förlag AB.

RS 500 Revisionsbevis. (2004). *FAR Komplett* . Stockholm: FAR SRS Förlag AB.

RS 620 Användning av en specialist i revisionsarbetet. (2004). *FAR Komplett* . Stockholm: FAR SRS Förlag AB.

Förord till Revisionsstandard i Sverige. (December 2008). *FAR Komplett* . Stockholm: FAR SRS Förlag AB.

Brännström, D. (2006). Kommentar om Direktiv om lagstadgad revision av årsbokslut och sammanställd redovisning. *FAR Komplett* . Stockholm: FAR SRS Förlag AB.

8.4 Uppsatser

Nordin, A.-C. (2008). *IT-revision - En ny del i den traditionella revisionen.* Institutionen för ekonomi. Gävle: Högskolan i Gävle.

8.5 Webbplatser och webbdokument

Facts about IFAC. (2009). Hämtat från IFAC.org: http://web.ifac.org/download/Facts_About_IFAC.pdf den 13 Maj 2009

Om FAR SRS; Historik. (2009). Hämtat från FARSRS.se: http://www.farsrs.se/portal/page?_pageid=33,38321&_dad=portal&_schema=PORTAL den 28 April 2009

Mer om CISA CISM. (2009). (I. S. Chapter, Producent) Hämtat från ISACA.se: http://www.isaca.se/extra/pod/?id=16&module_instance=1&action=pod_show&navid=16 den 9 Maj 2009

Om ISACA. (2009). (I. S. Chapter, Producent) Hämtat från ISACA.se: http://www.isaca.se/extra/pod/?id=9&module_instance=1&action=pod_show&navid=9 den 9 Maj 2009

8.6 Lagar, propositioner och EU-direktiv

Aktiebolagslagen.

Bokföringslagen.

Direktiv om lagstadgad revision av årsbokslut och sammanställd redovisning, 2006/43/EG (den 17 Maj 2006).

Prop 1997/98:99 Aktiebolagets organisation (den 26 Februari 1998).

Prop 2000/01:146 Oberoende, ägande och tillsyn i revisionsverksamhet (den 14 Juni 2001).

Prop. 2008/09:135 Revisionsutskott m.m. – genomförande av 2006 års revisorsdirektiv (den 12 Februari 2009).

8.7 Övrigt

Svensk kod för bolagsstyrning. (den 1 Juli 2008). Stockholm: Kollegiet för svensk bolagsstyrning.

8.8 Intervjuer

IT-revisor 1. (den 11 Maj 2009). IT-revisor, 4 års erfarenhet. (S. Dolck, & N. Roos, Intervjuare)

IT-revisor 2. (den 12 Maj 2009). IT-revisor, 3 års erfarenhet. (S. Dolck, & N. Roos, Intervjuare)

IT-revisor 3. (den 15 Maj 2009). IT-revisor, 1,5 års erfarenhet som IT-revisor, ytterligare 7 år övrig erfarenhet. (S. Dolck, & N. Roos, Intervjuare)

Revisor 1. (den 7 Maj 2009). Godkänd revisor, lärare på grundutbildning i revision, 7 års erfarenhet. (S. Dolck, & N. Roos, Intervjuare)

Revisor 2. (den 15 Maj 2009). Auktoriserad revisor, mångårig erfarenhet. (S. Dolck, & N. Roos, Intervjuare)

Revisor 3. (den 15 Maj 2009). Auktoriserad revisor, mångårig erfarenhet. (S. Dolck, & N. Roos, Intervjuare)

8.9 Figurförteckning

Appendix

A1. Intervjufrågor till IT-revisorer

Vad innebär IT-revision, varför görs den?

- o *Vad består IT-revisionen av?*
- o *Finns det obligatoriska protokoll/regleringar och därmed någon typ av harmoniserad standard för IT-revisionen?*
- o *Finns det andra regleringar eller policys som ni följer vid en IT-revision?*
- o *Hur bestäms vilken typ av kontroll som ska göras, är det helt upp till IT-revisorn eller sker detta i samförstånd med revisorn och/eller kunden?*

Finns det olika grader av omfattning av en IT-revision, t.ex. vid större och mer komplexa affärssystem och IT-system överhuvudtaget? Vem/vad avgör omfattningen av IT-revisionen?

- o *Om du som IT-revisor förespråkar en mer omfattande kontroll, får du då gehör för detta hos revisorn?*
- o *Om revisorn förespråkar att en mer omfattande kontroll bör genomföras och du som IT-revisor bedömer att så är inte fallet, tar revisorn hänsyn till detta?*

Hur redovisas resultatet av IT-revisionen för revisorn och hur granskas detta av denne?

- o *Anser du att de krav på revisorns förståelse av IT-revisionen, i frågan om ändamålsenlighet som revisionsbevis i linje med revisionen syfte, som uttrycks i RS 620, tillgodoses i realiteten? Upplever du rent allmänt att revisorerna har tillräckliga kunskaper för att hantera och kritiskt granska IT-revisionens resultat?*
- o *Finns det reglerat hur mycket information och vad för slags information som ska presenteras för revisorn och i vilken form (finns det strukturerade, formaliserade och heltäckande mallar där alla tänkbara aspekter beaktas och värderas utifrån eventuella deskriptiva måttenheter, finns det en enklare rapport med endast en del viktigare aspekter av högre signifikans, eller kan det ske på mycket mer informell basis – lite hårddraget en post-it)?*

A2. Intervjufrågor till revisorer

Vad innebär IT-revision, varför görs den?

- *Hur bestäms vilken typ av kontroll som ska göras, är det helt upp till IT-revisorn eller sker detta i samförstånd med dig som revisor och/eller kunden?*

Finns det olika grader av omfattning av en IT-revision, t.ex. vid större och mer komplexa affärssystem och IT-system överhuvudtaget? Vem/vad avgör omfattningen av IT-revisionen?

- *Skulle du som revisor, i dina instruktioner till en IT-revisor, ta hänsyn till det reviderade bolagets beskaffenhet gällande huruvida IT-lösningar som sådana är centrala för företagets verksamhet (jfr Betsson med stort fokus på IT-lösningar genom sin operationella verksamhet, och Kabe där IT-användandet kanske är mer koncentrerat till affärssystemen – om än komplexa sådana). Blir kontrollen av IT-systemen automatiskt mer väsentliga, och således föremål för en mer omfattande granskning, när de är centrala för verksamheten?*
- *Om IT-revisorn förespråkar en mer omfattande kontroll, får han då gehör för detta hos dig?*
- *Om du som revisor av någon anledning förespråkar att en mer omfattande kontroll bör genomföras och IT-revisorn bedömer att så är inte fallet, tar du då hänsyn till detta och handlar enligt IT-revisorns rekommendation?*

Kontrollerar revisorn IT-revisorns arbete på något sätt för att försäkra sig om ett rättvisande revisionsbevis? (Revisorns förståelse och förmåga att styra specialisten mot revisorns mål)

- *Hur kontrolleras IT-revisionen av dig som revisor?*
- *Anser du att de krav på revisorns förståelse av IT-revisionen, i frågan om ändamålsenlighet som revisionsbevis i linje med revisionen syfte, som uttrycks i RS 620, tillgodoses i realiteten? Upplever du rent allmänt att du som revisor har tillräckliga kunskaper för att hantera och kritiskt granska IT-revisionens resultat?*
- *Känner du som revisor att du behöver ha kunskaper för att kritiskt granska IT-revisorns arbete eller räcker det med dennes expertutlåtande?*
- *I de eventuella fall då du som revisor inte har den explicita kunskapen om IT-systemet som en specialist inom samma firma har, och på grund av detta inte kan avgöra huruvida specialistens antaganden och metoder varit rimliga (i enlighet med RS 620 p 14), händer det då att du tillkallar en annan specialist för att styrka revisionsbevisen (enligt RS 620 p 10) eller litar du på att den första specialisten gör adekvata bedömningar?*

- *I den händelse då du som revisor upptäckt en del osäkerheter/problem i på viss avdelning i det reviderade företaget som IT-revisorn också bedömer i sitt arbete, men som han inte anmärkt på, hur ser förfarandet då ut för att säkerställa revisionsbevisen? (Litar du på IT-revisorns kontroll eller vill du göra en djupare analys? Hur ser en djupare analys eller uppföljning från din sida ut? Finns det möjligheter för dig att lyfta fram sådana explicita kontroller ur IT-revisorns rapporter eller kommer det ett aggregerat utlåtande?)*

Hur redovisas resultatet av IT-revisionen för revisorn?

- *Vilken typ av underlag lämnar IT-revisorn över till dig som revisor och hur stor del av detta används sedan i den slutgiltiga dokumentationen av den utförda revisionen? Tar den sikte på att underlätta för en framtida IT-revisor, och innehåller den därför detaljerad information för denne, eller utformas den som vägledning för revisorn, genom t. ex ett enklare konstaterande om att IT-revision genomförts med ett visst resultat?*
- *Finns det reglerat hur mycket information och vad för slags information som ska presenteras för dig som revisor och i vilken form (finns det strukturerade, formaliserade och heltäckande mallar där alla tänkbara aspekter beaktas och värderas utifrån eventuella deskriptiva måttenheter, finns det en enklare rapport med endast en del viktigare aspekter av högre signifikans, eller kan det ske på mycket mer informell basis – lite hårddraget en post-it)?*
- *Finns det tillfällen då du som revisor skulle vilja ha tydligare, mer omfattande och mer detaljerad information från IT-revisorn? Exempel på sådana tillfällen?*
- *Tycker du att den information som lämnas till dig från en IT-revisor är för detaljerad? Hade det räckt med ett generellt utlåtande?*