Högskolan i Halmstad
Sektionen för Ekonomi & Teknik
Affärsystemsprogrammet inr. företagsekonomi

Användningen av automatiska kontroller i svenska företag

- *att använda sig av ERP-systemets automatiska kontroller för att öka tillförlitligheten i den finansiella rapporteringen*

Uppsats i Företagsekonomi 15hp
Slutseminarium 2012-05-31

Kajsa Jansson 861028
Anton Runesson 860810
Mathias Sunnegård 890429

Handledare: Arne Söderbom
Examinator: Jan-Olof Müller

Förord

Vi vill ta tillfället i akt och tacka alla personer som har gjort den här studien möjlig. Framförallt vill vi tacka vår handledare Arne Söderbom för hans kritiska granskande, samt konstruktiva kommentarer och uppmuntrande ord på vägen. Likaså ett tack till våra opponenter som även de har gett uppmuntran och feedback.

Vi vill även rikta ett stort tack till våra respondenter som har tagit sig tid och engagerat sig i vår uppsats, utan dem hade den här studien aldrig kunnat slutföras. Vi skänker slutligen en varm tanke till Lars Spång vars kaffebryggare har fört den här uppsatsen framåt i svåra tider.

Högskolan i Halmstad den 31 maj 2012

Kajsa Jansson	*Anton Runesson*	*Mathias Sunnegård*

Sammanfattning

Dagens ERP-system ger företagen möjligheten att effektivisera och kostnadsreducera sina processer genom en mängd olika funktioner. Företag sätter idag stor tillit till sina ERP-system. Transaktionerna inom och mellan de olika systemen består av en mängd data som kräver övervakning och kontroll för att reducera riskerna med felaktigheter i den finansiella rapporteringen. En typ av verktyg för detta är automatiserade kontroller, vilka kan vara antingen av förebyggande eller upptäckande karaktär. Syftet med den här studien var att beskriva och analysera hur tre stora, svenska tillverkningsföretag använder sig av automatiska kontroller i sina ERP-system samt att jämföra hur deras syn liknar eller skiljer sig från revisionsbyråerna som dagligen arbetar med att utvärdera tillförlitligheten i den finansiella informationen. För att få en djupare förståelse för ämnet valde vi att göra en kvalitativ studie med en induktiv ansats. I den teoretiska referensramen utvecklar vi de tre huvudbegreppen ERP, automatiska kontroller och riskhantering. Vi har intervjuat tre tillverkande företag samt tre revisionsbyråer vilket gav oss två olika perspektiv på användandet av de automatiska kontrollerna. Samtliga intervjuer spelades in och genomfördes som besöksintervjuer på respondenternas arbetsplats. Resultatet av studien visar att samtliga företag på olika nivåer använder sig av automatiska kontroller. Två av företagen har ett mer avancerat användande medan det tredje ännu befinner sig på en låg nivå. Revisionsbyråerna har ett liknande förhållningssätt som presenteras i den teoretiska referensramen och representerar utopin.

Nyckelbegrepp: ERP, automatiska kontroller, intern kontroll, riskhantering

Abstract

Today's ERP systems provide companies the opportunity to streamline and reduce the cost of their operations through a variety of functions. Companies today put great faith in their ERP systems. The transactions within and between the different systems consist of a collection of data that require monitoring and control to reduce risks of errors in financial reporting. One type of tool is automated controls that can be either preventive or detective. The purpose of this study was to describe and analyze how three large Swedish manufacturing companies make use of automatic controls in their ERP systems and to compare how their views are similar to or different from the accounting firms who work daily to evaluate the reliability of financial information. To get a deeper understanding of the subject, we used a qualitative study with an inductive approach. In the theoretical framework we developed our three main concepts; ERP, automatic controls and risk management. We have interviewed three manufacturing companies and three accounting firms, which gave us two different perspectives on the use of automated controls. All interviews were recorded and were conducted as personal interviews at each respondents' workplace. The results of this study show that all the companies at various levels make use of automatic controls. Two of the companies have a more advanced set of controls while the third is still at a low level. The audit firms have a similar approach as presented in the theoretical framework and represent the utopia that modern business endeavor’s to achieve.

Keywords: ERP, automated controls, internal control, risk management

Förkortningsförteckning

Compliance	Efterlevnad av regler, lagar och policies.
COSO	The Committee of Sponsoring Organizations of the Treadway Commission, organisation för intern kontroll och riskhantering.
ERM	Enterprise Risk Management, metoder och processer för att hantera risker och ta tillvara på möjligheterna att uppnå sina mål.
ERP	Enterprise Resource Planning, ett system som används för att hantera och samordna alla resurser, information och funktioner inom ett företag. Benämns i Sverige ofta som affärsystem.
HR	Human Resources, personalhantering inom företaget.
ITGC	IT General Controls. Generella kontroller inom IT-system.
Koden	Svensk kod för bolagsstyrning, regelsamling för bolagsstyrning som ges ut av Kollegiet.
MRP	Material Requirements Planning, produktionsplanerings- och styrsystem som används för att hantera tillverkningsprocesser.
MRPII	Manufactoring Resource Planning, en metod för effektiv planering av alla resurser i ett tillverkande företag.
SOD	Segregation Of Duties, ett koncept som säkerställer att det krävs fler än en person för att utföra en uppgift. Används för att minska risken för bedrägeri.
SOX	Sarbanes-Oxley Act, lag gällande interna kontroller som måste följas av alla bolag noterade på den amerikanska börsen.

Innehåll

Figurförteckning

1. Inledning

I det här kapitlet kommer läsaren att introduceras för uppsatsens nyckelbegrepp, Enterprise Resource Planning (ERP), automatiska kontroller och riskhantering. Dessutom presenteras en bakgrund av ämnet som är användandet av automatiska kontroller i ERP-system, samt en fördjupad problemdiskussion vilken mynnar ut i uppsatsens problemställning med tillhörande underfråga. Syftet med uppsatsen kommer att klargöras och de avgränsningar som finns inom denna uppsats kommer att beskrivas.

1.1. Problembakgrund

Redovisning syftar till att dokumentera organisationers resurshantering, och revisionens främsta uppgift är att säkra företagets ekonomiska information till marknaden samt ägarna (Deegan & Unerman, 2011). Den finansiella informationen är grunden till de beslut ett företag tar, därmed måste den informationen vara korrekt och ge en rättvisande bild av företagets situation (Daigle, Kizirian och Sneathen, 2005). Att säkerställa den finansiella rapporteringen i dagens tekniskt utvecklade miljö är såväl internt som externt numera ett komplext men inte desto mindre nödvändigt arbete. De senaste åren har betydande ansatser gjorts för att utveckla och effektivisera rapporteringen. Både revisionsbyråer och en hel del företag har investerat i system för att kunna följa upp företagets ekonomiska prestationer (Braun & Davis, 2008). Detta görs genom att verifiera och utreda de manuella och automatiserade kontrollerna som finns inom systemet (Arnslätt & Karlsson, 2010).

I takt med att möjligheterna och nyttan med att använda sig av informationssystem av olika sorter har slagit igenom och utvecklats, är detta numera en självklarhet och ett måste för företag och myndigheter (Hedman, Nilsson & Westelius, 2009). För att bedriva en framgångsrik verksamhet ställer den rådande konkurrensen idag höga krav på användningen av avancerade ERP-system (ibid.). ERP-plattformen ger företag möjligheten att minska sina kostnader, bli mer effektiva och flexibla. Denna ökade funktionalitet ger dock ökade risker, som exempelvis kontrollproblem, vilka måste balanseras med utökade interna kontroller (Turner & Owhoso, 2009).

För riskhantering som kontroll av den finansiella rapporteringens tillförlitlighet och effektivitet samt intern kontroll finns ett antal regelverk, det mest kända är förmodligen Sarbanes-Oxley Act (SOX) Section 404. Regelverket trädde i kraft som gällande lag för alla börsnoterade bolag verkande på den amerikanska marknaden 2004, samt 2006 även för utlandsägda företag som är registrerade på amerikanska börsen (Arnslätt & Karlsson, 2010). Dessa regelverk har lett till ökade kostnader för övervakning och kontroll av den finansiella rapporteringen samt högre kostnader för externa konsulter. De ökade kostnaderna har skapat ett behov av effektivare verktyg för övervakning av verksamhetens processer och transaktioner (Roland, 2007). Svenska företag som ej är noterade på den amerikanska börsen behöver inte följa dessa krav, utan styrs istället av Svensk kod för bolagsstyrning, även kallad Koden. Koden är ett komplement till lagstiftningen och är ett ramverk för självreglering, vilket innebär att Koden är normgivande för god bolagsstyrning i svenska börsföretag och har till syfte att säkerställa att bolagen sköts på ett så tillfredsställande sätt för aktieägare som möjligt (Svensk kod för bolagsstyrning, 2010). Även om kraven på de svenska företagen inte är lika omfattande kan svenska företag likväl ha ett intresse av att med hjälp av automatiska kontroller effektivisera sina processer och skära ned på kostnaderna.

Inom svenska bolag, där kraven på redovisningen av intern kontroll är lägre, har anammandet av automatiserade kontrollverktyg ännu inte haft lika stor genomslagskraft, dock finns intresset för användandet av affärssystemens egna funktioner för att optimera interna kontroller (Niklasson, 2012). Att skapa effektiva kontroller är ingen enkel uppgift och många företag har skapat metoder för att manuellt göra interna tester, något som resulterar i ökande kostnader, ödslade resurser och minskad effektivitet (Roland, 2007). I dagens ERP-system finns det dock möjligheten att automatisera dessa kontroller, och skapa starka affärsfördelar med detta (KPMG, 2010). Att automatisera kontroller av transaktioner och flöden kan enligt Roland (2007) reducera tidsåtgången med 60 till 75 procent.

1.2. Problemdiskussion

Under senare år har frågan om riskhantering, med automatiska kontroller som en stark del av detta, fått ett ökat genomslag. En stor drivkraft bakom detta är de redovisningsskandaler som har drabbat näringslivet både i USA och i europeiska länder, Enron och WorldCom är de två mest omtalade (Bierstaker, Brody och Pacini, 2006). Coderre (2005) påpekar det ökade tryck som finns på ledning och revisorer att leva upp till kraven både från lagar och omvärldens intressen, samt från företagets egna önskemål om effektiva processer och låga kostnader. Hur kan ledningen påverka ett företags efterlevnad av lagar och regler med hjälp av IT?

Ytterligare ett tema är hur begreppen kontroll och risk kan länkas samman. Även om kontroll och risk har två vitt skilda betydelser kan de sägas utgöra de två sidorna på samma mynt. Genom att identifiera brister i företagets kontroll uppmärksammas även potentiella riskområden. Omvänt kan ett företag genom att utvärdera sina risker upptäcka områden som är i behov av nya eller bättre kontroller (Coderre, 2005). Det är en stor utmaning för företag att säkerställa att de befintliga affärsprocesserna utförs till minimal risk i linje med affärssystemets funktionalitet med maximala inslag av automatisering (Bellino, Wells & Hunt, 2007). Ledning och interna revisorer måste sträva efter att skapa, övervaka och förbättra interna kontroller för att skapa större säkerhet genom att förhindra och upptäcka obehöriga transaktioner i systemen (Namiri & Stojanovic, 2007). Hur kan automatiska kontroller integreras i företagens riskhantering för att förbättra den interna kontrollen?

Traditionellt sett har kontroller i redovisningen skett retrospektivt på en cyklisk basis, vilket har renderat i ett begränsat utrymme för utvärdering. Med hjälp av de möjligheter till automatiska kotroller som idag finns att tillgå, kan riskbedömningar och kontroller ske i högre grad och med mer aktuell data, detta tack vare en ökad teknisk utveckling (Coderre, 2005). Företag kan välja att arbeta med automatiska kontroller antingen i förebyggande syfte eller i upptäckande, eller parallellt en kombination av båda sätten (Bierstaker et al., 2006). Hur ser användningen ut i de svenska företagen i vår studie?

Många företag investerar stort i nya affärssystem men fortsätter därefter att arbeta på samma sätt som tidigare med stora inslag av manuella kontroller i sitt arbete med intern kontroll J. Nelling (personlig kommunikation, 18 oktober, 2011). Detta har medfört att vi är intresserade av att undersöka i vilken uträckning svenska företag valt att använda sig av automatiska kontroller i syfte att minimera sina risker och effektivisera sina processer

Vi anser att den svenska forskningen inom det här området är begränsad och hoppas att med den här uppsatsen kunna bidra till att förbättra förståelsen och kunskapen inom den akademiska världen. Uppsatsen ska även vända sig till företag som har ett intresse av arbetet med intern kontroll och riskhantering med inslag av automatiska kontroller.

1.3. Problemformulering

Hur använder sig svenska tillverkande företag av affärssystemens automatiska kontroller för att övervaka sina transaktioner och säkerställa en tillförlitlig finansiell rapportering?

1.4. Syfte

Syftet är att beskriva och analysera hur svenska tillverkande företag använder sig av automatiska kontroller i sina ERP-system för att motverka riskerna med felaktigheter i den finansiella rapporteringen. Med stöd i revisionsbyråernas och storföretagens syn på användningen av automatiska kontroller vill vi undersöka kontrollernas utbredning och betydelse. För att nå en förståelse för hur mycket optimeringen av affärssystemen betyder för företagen kommer vi även undersöka hur engagerade ledningen är i dessa frågor.

1.5. Avgränsningar

Då vi har ett intresse av att undersöka hur stora, svenska tillverkningsföretag arbetar med automatiska kontroller kommer vi att inrikta oss på företag vars interna kontroll inte regleras av SOX-ramverket. Vi kommer att rikta vårt fokus mot större svenska bolag. Årsredovisningslagen definierar ett större företag som ett företag vars andelar, teckningsoptioner eller skuldebrev är upptagna till handel på en reglerad marknad eller en motsvarande marknad utanför Europeiska ekonomiska samarbetsområdet eller uppfyller något av villkoren minst 50 anställda, balansomslutning på mer än 40 miljoner kr eller nettoomsättning på mer än 80 miljoner kr under de senaste två åren (ÅRL 1:a kap, 3§ p.4). För att underlätta jämförelsen mellan företagen har vi valt att enbart rikta in oss på företag som helt eller till viss del använder sig av SAP då de är Europas största affärssystemsleverantör och riktar in sig mot stora företag (Catt, Barbour & Robb, 2008). Vi har valt att begränsa oss geografiskt till södra och västra Sverige, med primärt Malmö och Göteborg som utgångspunkt.

2. Teoretisk referensram

I detta kapitel kommer läsaren att introduceras till de begrepp som är relevanta för uppsatsen. Bakgrunden till affärssystemen kommer att behandlas, likaså kommer olika delar av automatiska kontroller att beskrivas. Slutligen kommer riskhantering och riskrelaterade begrepp tas upp.

2.1. Begreppsutveckling och analysmodell

Vi kommer i vår studie utgå från de tre nyckelbegreppen ERP, automatiska kontroller och riskhantering. Då uppsatsen till stor del inriktar sig på automatiska kontroller i ERP-system kommer referensramen att inledas med en generell introduktion till begreppet ERP. Med dagens ökade IT-integrering i verksamheter har ERP-system kommit att bli mer eller mindre nödvändiga för att företag ska kunna hantera den stora mängd data och transaktioner som är i omlopp och vi kommer att redogöra för de möjligheter till bättre kontroll och processer som Magnusson och Olsson (2008) redovisar. Det ökade informationsflödet erbjuder även nya möjligheter till styrning av verksamheten, i takt med att mängden transaktioner ökar blir även ledningens engagemang allt viktigare för att säkerställa den strategiska nyttan i IT-investeringar. Med hjälp av Neirotti och Paolucci (2007) resonerar vi kring ledningens betydelse för IT.

Automatiska kontroller är verktyg som organisationer kan använda sig av för att skydda sig från bedrägerier och förebygga möjligheten att göra skadliga fel (Kuhn & Sutton, 2010). Det är dessa verktyg vi kommer att fokusera vår studie på. Bierstaker et al. (2006) har forskat kring användingen av förebyggande och upptäckande kontroller. Vi kommer att utveckla dessa begrepp och exemplifiera vilka typer av kontroller som används. Ett begrepp som involverar automatiska kontroller är Segregation of Duties vilket Lightle och Waller Valario (2003) betraktar som ett verktyg som kan hindra användarna från att utföra felaktiga transaktioner i systemet. Vi ska undersöka var våra respondenter använder sig av automatiska kontroller och även på vilken nivå de använder sig av kontrollerna. Som stöd kommer vi att använda oss av Paulk, Curtis, Chrissis och Webers (1993) modell som är ett verktyg för att utvärdera hur väl ett ERP-system utnyttjas.

Vi kommer att knyta samman begreppet automatiska kontroller med riskhantering som två delar i en process för att utveckla och förbättra verksamheten. Behovet av automatiska kontroller i riskhanteringsarbetet utgör en kritisk fråga för företagets ledning. Som en följd av de senaste årens uppmärksammade redovisningsskandaler, bedrägerier och konkurser har kraven för företagens bolagsstyrning och riskhantering ökat. För att stödja företagen i deras arbete har The Committee of Sponsoring Organizations of the Treadway Commission (COSO) utvecklat ramverket Enterprise Risk Management (ERM) med riktlinjer för hur riskhanteringen kan skötas. Vi kommer att resonera kring hur företag kan arbeta med riskhantering och hur automatiska kontroller kan integreras i detta arbete. Som stöd kommer vi bland annat att använda oss av Oringel och Aldhizer (2009) samt Mikes (2009).

Genom att förklara dessa begrepp samt ge en inblick i hur de används och sambandet mellan dem vill vi skapa en förklaring till hur ett företag kan optimera sin verksamhet, förbättra processer samt minimera risken för fel i den finansiella rapporteringen.

2.2. ERP – Affärssystem

2.2.1. Historia och uppkomst

Under 60-talet byggde företagen upp allt större lager för att kunna säkerställa leverans. Detta medförde att dåtidens lagersystem anpassades för att hantera stora lager. Under 70-talet ökade

konkurrensen och företagen blev tvungna att skära ner på sina lager. Detta ledde till att system som gick under namnet material resource planning (MRP) initierades. MRP var ett stort steg framåt för lagerplaneringen, där systemet med stöd av instruktioner om varje produkt hjälper företaget att hålla en optimal lagerstatus (Umble, Haft & Umble, 2003). MRP stärkte även företagens produktionsplanering genom att koppla samman informationen från planeringsprocessen av material och planeringen av produktion (ibid.). Under 80-talet fortsatte utvecklingen av verksamhetsstödjande system och manufactoring resource planning-systemet (MRPII) såg dagens ljus (Magnusson & Olsson, 2008). Dessa system mötte behovet att integrera applikationsprogram för olika affärsfunktioner och processer. Olika applikationer kunde härstamma från en och samma databas vilket gjorde att applikationerna kunde kommunicera och generera uppdaterad information i alla delar av systemet. Under 90-talet bytte programleverantörerna namn på MRPII till ERP då det funktionella innehållet blivit större och bredare (Olhager & Selldin, 2003). Antalet transaktioner ökade i företagen vilket ledde till att systemleverantörer utvecklade moduler där kunderna kunde välja bort de moduler som de inte var i behov av. Denna systemtyp (ERP) kan täcka alla företagens värdeskapande processer med hjälp av en mängd olika moduler som är branschspecifika och går att anpassa efter vad företaget är i behov av (Magnusson & Olsson, 2008). ERP-systemen, som fokuserar på att integrera verksamheten, medför flera olika egenskaper som alla har betydande konsekvenser för företaget:

- **Integration:** ERP-systemets alla delar/moduler är helt integrerade med varandra d.v.s. att de ”pratar” med varandra.
- **Paket:** ERP-system köps in eller leasas i regel av affärssystemsleverantörer och utvecklas inte själva. Detta medför att företagen ofta tvingas anpassa sina processer efter systemet och inte tvärtom och att företagen inte själva kan modifiera systemen (Markus & Tanis, 2000).
- **Utveckling:** ERP-systemen utvecklas ständigt i en snabb takt för att anpassa sig till marknaden. Det som framförallt utvecklas är arkitekturen och funktionaliteten i systemen och idag utvecklas det framförallt mot att webbanpassa systemet (Tarantilis, Kiranoudis & Tehodorakopoulos, 2008).

2.2.2. För- och nackdelar med ERP-system

Det finns ett antal för- och nackdelar som tillkommer med ERP-system. Fördelarna kan vara:

- **Kortare ledtider:** Ett av de stora argumenten för att införskaffa ERP-system. Genom att verksamhetens alla informationsflöden integreras kan företaget förkorta sina ledtider.
- **Effektivare processer:** Företagets processtruktur omarbetas för att passa systemet. Eftersom systemen är standardiserade kan detta leda till att processerna blir effektivare genom att företaget får en strömlinjeformad processtruktur.
- **Bättre kontroll:** Systemen förser ledningen med data och information från hela företaget. Genom att ledningen får all information i realtid underlättas snabba beslut.
- **Ökad datakvalitet:** Genom att inventera systemmiljön får företaget bättre kontroll över sina informationsflöden och processtruktur vilket kan leda till bättre datakvalitet (Magnusson & Olsson, 2008).

Nackdelar med ERP kan vara:

- **Höga risker:** Att införa ett ERP-system innebär att företaget tar på sig ett stort åtagande och därmed också en stor risk. Det kan utgöras av finansiella risker relaterade till omfattande kostnader och projektrelaterade risker.

- **Strömlinjeformning:** Med strömlinjeformning menas det värde som de interna skillnaderna mellan olika företag inom samma industri skapar. I och med att systemen blir allt mer branschspecifika och likformiga minskar företagens konkurrensfördelar då alla har samma grundsystem.
- **Inlåsningseffekter:** Avtal med en ERP-leverantör kan medföra att kunden blir låst till denna leverantör för en lång framtid (ibid.).

2.2.3. Systemmognad

Systemmognad beskriver olika steg av mognad som ett företag kan gå igenom för att utveckla en grundnivå av kontroll, kvalitet och produktivitet (Debreceny, 2006). Parthasarathy och Ramachandran (2008) och Holland och Light (2001) resonerar kring tre olika nivåer av systemmognad. I den lägsta nivån placeras företag vars systemarbete fokuseras på förvaltandet av befintliga legacy-system och hur ett nytt ERP-system ska införas. På den andra nivån placerar sig företag vars fokus ligger på att integrera och utnyttja funktionerna i ett relativt nytt ERP-system. Hos de företag som placerar sig på den tredje och högsta nivån består system-arbetet av att optimera den strategiska potentialen av ERP-systemet (ibid.).

2.2.4. Ledningens betydelse

För att lyckas med IT-satsningar som kräver stora förändringar i verksamheten och affärerna anser Lundberg (2009) att ledningen måste förstå och stötta projekten till 100 procent. Neirotti och Paolucci (2007) menar att lyckade IT-satsningar inte är slumpmässiga, bakom varje lyckad IT-satsning står en serie av korrekta investeringsbeslut från ledningen. När väl projekten kommit igång minskar ledningens engagemang och de blir allt mindre involverade i projekten. Under projektets gång dyker det ofta upp viktiga vägval där besluten då fattas utan förankring längre ner i organisationen (Lundberg, 2009). Vid en ERP-implementation kan besluten till exempel röra eventuella förändringar eller avvecklingar av produkter som inte stöds av systemet. Om en projektledare eller mellanchef inte är insatt i produkternas strategiska betydelse och fattar dessa beslut riskerar systembytet att generera mer skada än nytta (ibid.).

För att effektivisera organinsationens IT-användning och säkerställa ledningens stöd vid IT-satsningar föreslår Lundberg (2009) och Neirotti och Paolucci (2007) att den bästa lösningen är att involvera en IT-roll i företagsledningen. På det här viset blir IT direkt involverade i beslut som rör företagets strategier och framtid. Det räcker dock inte att enbart representera IT. Rollen ställer krav på kompetens att kunna fatta de rätta besluten och se IT som en del i affärerna istället för en fristående teknisk fråga. En möjlig lösning för företaget är att utse en Chief Information Officer (CIO) som rapporterar direkt till företagsledningen (Lundberg, 2009). I rollen som CIO flyttas enligt Watts och Henderson (2006) fokus från teknik till affärsinriktad utveckling. Genom att kontinuerligt analysera omvärlden mot tekniska risker ligger det ofta i CIO:s ansvar att prestentera nya innovativa tekniker och plattformer för att bemöta dessa. Lundberg (2009) anser att normala arbetsuppgifter för en CIO kan bestå av:

- Företagets övergripande IT-strategi.
- Beredning av IT-frågor ur ett affärs- och verksamhetsperspektiv för att beslut ska kunna fattas av ledningen.
- Att säkerställa företagets långsiktiga IT-utveckling gemensamt med verksamhets-representanter (till exempel processägare, affärsansvariga och produktionsansvariga).
- Att föredra IT-frågor i beslutsgrupper för att tydliggöra kopplingen till företagets övergripande strategi (Lundberg, 2009).

Genom att använda sig av denna roll med rätt mandat och förutsättningar minskar företagen risken att misslyckas med sina IT-projekt. För att vara effektiv behöver rollen som CIO innehas av en IT-ansvarig person som har förankring både inom affär och IT (Lundberg, 2009; Neirotti och Paolucci, 2007).

2.2.5. Interna kontroller i ERP-system

Intern styrning och kontroll är generellt den process som utförs av organisationens styrelse, ledning och annan personal för att ge en rimlig försäkran om att målen uppnås. Målen berör effektivitet och produktivitet i verksamheter, tillförlitlig finansiell rapportering och efterlevnad av lagar och förordningar (COSO, 1992). Den stegrade användningen av ERP-system har gett en kraftigt ökad mängd information att hantera. ERP-system förflyttar även initiering eller godkännande av transaktioner till lägre nivåer i organisationen, och därigenom orsakar ökade kontrollproblem (Turner & Owhoso, 2009). Dagens ERP-system har dock större möjligheter att övervaka interna kontroller än tidigare system haft. Kontrollrapporter kan skapas för att utvärdera ogiltig användning, både i form av standardrapporter och specialiserade rapporter (ibid.). Ledning och interna revisorer måste sträva efter att skapa, övervaka och förbättra interna kontroller för att skapa större säkerhet genom att förhindra och upptäcka obehöriga transaktioner i systemen (Namiri & Stojanovic, 2007).

För kontroll av den finansiella rapporteringens tillförlitlighet och effektivitet, finns ett antal regelverk, det mest kända är förmodligen Sarbanes-Oxley Act (SOX) Section 404 vilket trädde i kraft som gällande lag för alla börsnoterade bolag verksamma på den amerikanska marknaden 2004, samt 2006 även för utlandsägda företag som är registrerade på amerikanska börsen (Arnslätt & Karlsson, 2010). Svenska företag som ej är noterade på den amerikanska börsen behöver inte följa dessa krav, utan styrs istället av Svensk kod för bolagsstyrning. Koden är ett komplement till lagstiftningen och är ett ramverk för självreglering, vilket innebär att Koden är normgivande för god bolagsstyrning i svenska börsföretag och har till syfte att säkerställa att bolagen sköts på ett så tillfredsställande sätt för aktieägare som möjligt (Svensk kod för bolagsstyrning, 2010).

2.3. Automatiska kontroller

Organisationer utsätts ständigt för finansiella utmaningar som exempelvis bedrägerier, felaktigheter i transaktioner och risker med missvisande finansiell information (Coderre, 2005). Kontroller och uppföljning krävs för att säkerställa att den information företaget arbetar med är korrekt, och därmed kan stödja företagets arbete med riskhantering och prestationsoptimeringar (KPMG, 2009). Arbetet med att skapa tillförlitlighet i den finansiella rapporteringen och att efterleva lagar och förordningar benämner COSO som *interna kontroller* (Namiri & Stojanovic, 2007). Processen inom de interna kontrollerna beskriver Namiri och Stojanovic (2007) enligt följande:

”Identifiera alla betydelsefulla konton i företaget. Identifiera vilka affärsprocesser som påverkar dem. Definiera ett antal kontrollmål för varje process som företaget måste följa. Bedöm fortlöpande riskerna för företaget genom identifieringen av kontrollmålen. Utforma och genomför baserat på riskbedömningen ett antal effektiva kontroller i syfte att förhindra eller upptäcka förekomsten av de identifierade riskerna. Kontrollerna måste testas och användas i det dagliga arbetet.” (Namiri & Stojanovic, sid. 1, 2007).

Dessa kontroller görs, trots de högutvecklade system det finns inom dagens näringsliv, många gånger manuellt. Resultatet blir att kostnaderna för arbetskraft blir hög och tid som kunnat användas till att utföra mer värdeadderande aktiviteter uteblir (Hunt & Jackson, 2010). Med hjälp av tillförlitliga systemkontroller blir transaktionerna mer transparenta och en revision på

företaget blir mindre kostsam då revisionskostnaderna minskar, vilket kan ses som en avkastning på en effektiv IT-investering (Daigle, Kizirian & Sneathen, 2005).

2.3.1. Användningsområden för automatiska kontroller

Användningsområdena för automatiska kontroller är många, Coderre (2005) nämner främst finansiella kontroller och säkerhetskontroller. Finansiella kontroller är exempelvis analytiska parametrar vilka läggs in för att undersöka transaktionernas korrekthet. Systemet kan sedan användas för att larma när oegentligheter som dubbla inköp eller ogiltig rabattering görs. Med hjälp av de förprogrammerade parametrarna kan sedan alla inköp testas mot dessa, istället för manuella stickprovskontroller (Coderre, 2005). Automatiska kontroller kan användas för att underhålla och inspektera säkerheten i systemet. Tester huruvida alla användare som rör sig i systemet är giltiga kan göras, likaså kontroller för att validera att systemet är intakt mot hackers. Ett företag kan exempelvis göra matchningar mellan masterdata om de anställda och användandet av login på olika platser för att undersöka om lån av varandras inloggningsuppgifter sker (ibid.). Frekvens och tidpunkterna för säkerhetsrelaterade automatiserade tester kommer helt bero på branschens riskpotential och ledningens synsätt på säkerhetsarbete och företagets säkerhetspolicy (Daigle et al., 2005).

Arbetet med att upptäcka bedrägerier har sedan de stora amerikanska redovisningsskandalerna (Worldcom, Enron, etc.) blivit en viktig fråga för företagsledningen (Bierstaker et al., 2006). Bierstaker, Burnaby och Hass (2004) beskriver hur många företag i arbetet med att motverka bedrägerier har utvecklat procedurer dels för att förebygga bedrägerier innan det händer och dels för att upptäcka bedrägerier efter att det har inträffat. Teknologin har utvecklats och utgör effektiva verktyg för att upptäcka bedrägerier i de finansiella transaktionerna i ERP-systemen. Audit Command Language (ACL) är ett frekvent använt upptäckande verktyg som kan användas för att söka efter trender och anomalier i systemets transaktioner. Fördelen med den här typen av verktyg är att de kan hantera stora mängder data och spåra hur och av vem transaktionen har skapats (ibid.).

Dye (2007) anser att arbetet med att förhindra bedrägerier allt mer rör sig från upptäckande mot förebyggande kontroller. Företagen kan både spara tid och pengar om de väljer att satsa på förebyggande åtgärder istället för att leta efter felaktigheter i efterhand. Som ett led i detta anser Dye (2007) att företagen bör förstärka sina finansiella system, utöka den interna kontrollens omfattning samt kontinuerligt utvärdera, identifiera och åtgärda svagheter i sina system. Bierstaker et al. (2006) anser att företag för att skydda sig mot bedrägerier behöver utveckla metoder som innefattar en mix av förebyggande och upptäckande metoder.

För att uppnå ett effektivt IT-skydd föreslås att företag:

- Utvärderar de finansiella transaktionerna: Konton i redovisningen löper risk att bli manipulerade av de anställda. Konton som har blivit manipulerade kan upptäckas genom dess felaktiga relationer till sina motkonton. Genom att anlita en revisonsfirma som analyserar och spårar transaktionerna kan dessa bedrägerier upptäckas. De kan till exempel använda sig av sampling-tester för att utreda olika konton. Om det exempelvis är möjligt att lägga upp en fiktiv leverantör och göra utbetalningar till denna vet revisorn att risken för bedrägerier existerar och kan utöka kontrollen för leverantörsreskontra (Bierstaker et al., 2006).
- Använder sig av digitala analyser: Baserat på Benford's Law (analyserar sifferordningen i systemets data) kan bedrägliga transaktioner upptäckas då avvikelser från den förväntade sifferordningen upptäcks. Detta kan ske på två sätt. Dels genom att data har lagts till och dels genom att data har tagits bort. Denna teknik används ofta

vid utredningar av skattefusk och fungerar effektivt då människor i regel inte klarar av att manipulera data på ett sätt som uppfyller villkoren i Benford's Law (Ramaswamy & Leavins, 2007).

- Lösenords- och brandväggsskydd: Dessa två tekniker är väl beprövade och utgör ett effektivt skydd mot obehöriga användare i systemen. Lösenorden utgör dock ett omvänt förhållande. Om de byts för ofta och innehåller för långa tecken finns en risk att de anställda skriver ner lösenorden och utsätter organisationen för en risk. Effektivt lösenordsanvändande bör anpassas efter organisationens IT-mognad, inte innehålla för många tecken eller bytas för ofta. Brandväggsskydd används främst för att skydda företaget från intrång via internet. Brandväggen kan skydda och gömma företagets IP-adress för intrång av hackers (Bierstaker et al., 2006).

2.3.2. IT-generella kontroller

Systemkontroller delas in i antingen IT-generella kontroller eller applikationskontroller (Daigle et al., 2005). Information Technology General Controls (ITGC) handlar om grunderna i IT-systemen och tillämpas till alla systemets komponenter, processer och data som finns i en organisation eller systemmiljö. Syftet med dessa kontroller är att garantera en tillförlitlig användning hos applikationer, program, datafiler och databehandling (Bellino et al., 2007). De inkluderar kontrollaspekter som exempelvis Segregation of Duties (SOD), logical access-kontroller och Change Management (Daigle et al., 2005).

Segregation of Duties utgör en viktig del i praktiskt taget alla företags interna kontrollsystem. SOD-kontroller hjälper till att säkerställa att icke behörig personal inte har tillgång till alla aspekter av en transaktion eller affärsprocess och hindrar även personalen från att begå fel eller bedrägerier. Internrevisorer arbetar ofta med att identifiera potentiella SOD-konflikter och göra rekommendationer för att minska risken för att de ska inträffa (Lightle & Waller Vallario, 2003). Logical access handlar i stor utsträckning om användarnamns- och lösenordshantering i systemet och hur dessa ska erbjuda så stor säkerhet som möjligt (ibid.).

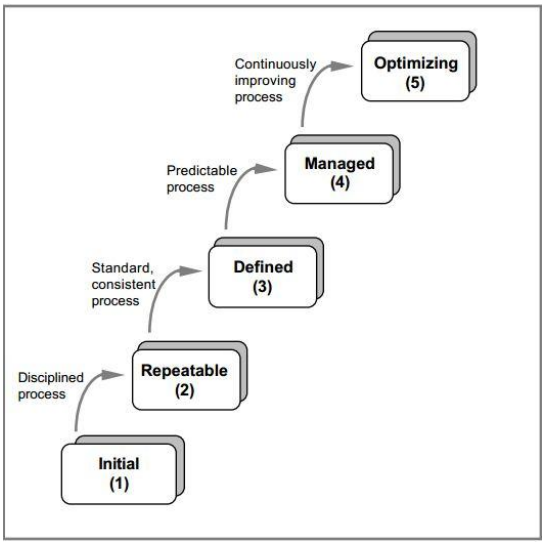
Change Mangagement översätts närmast med ändringshantering. Huvuduppgiften är att dokumentera ändringar i systemen, användartillstånd och godkännande, separation av arbetsuppgifter vid genomförda förändringar, rapportera till ledning, kvalitetskontroll och lämplighetskontroll. Det primära syftet är att säkerställa om företaget har formella change managementprocedurer och om företaget följer instruktionerna när de gör nödvändiga ändringar i sina applikationsprogram (Norman, Payne & Vendrzyk, 2009).

2.3.3. Applikationskontroller

Det främsta syftet med applikationskontroller är att säkerställa realiteten och integriteten i specifika applikationer, exempelvis orderhantering eller leverantörsreskontra (Daigle et al., 2005). Applikationskontroller scannar systemet för att hitta onormala beteenden, det kan exempelvis vara allt från att personalen lägger in fel data till att det sker försök till intrång i systemet (McCollum, 2002). De delar som inkluderas i begreppet är input-kontroller, processkontroller och outputkontroller. Inputkontroller avser de data som förs in i systemet, processkontroller avser datatransformering och outputkontroller arbetar med att säkra att data distribueras till och utnyttjas av användare som har behörighet och används till rätt syften (Daigle et al., 2005). Det kan vara en fördel att använda sig av samma mjukvara som revisorerna då det blir lättare att kontrollera beräkningarna i systemet (Coderre, 1996). Sammantaget ska applikationskontrollerna stödja de finansiella kontrollmålen genom att förhindra eller upptäcka obehöriga transaktioner inom affärsprocesserna (Namiri och Stojanovic, 2007).

2.3.4. Företagens användningsnivåer

Inom IT-ramverket COBIT beskrivs företagets mognadsgrad i systemhanteringen. Det handlar främst om hur bra företaget är på att involvera sina system i processförbättringarna. Nivåerna som beskrivs är icke-existerande (0), initial (1), repeterbar (2), definierad (3), managed (4) samt optimerade (5) och företaget skall sträva mot att optimera sin hantering (Debreceny, 2006). Det är först på de högre nivåerna automatiska kontroller medvetet involveras i arbetet med kontroll och processhantering (Paulk, Curtis, Chrissis & Weber, 1993).



Figur 1, The Five Levels of Software Process Maturity (Paulk, Curtis, Chrissis & Weber, 1993)

På den initiala nivån placerar sig främst företag som inte har en stabil miljö för utveckling och underhåll av systemen. Projekten initieras ofta ad hoc utan ledningens involvering. Företag på denna nivå karaktäriseras av individuellt tänk snarare än organisatoriskt och framgångar beror helt på personerna i projektet. På andra nivån, kallad repeterbar, finns i regel upprättade policies för att genomföra systemprojekten. Företaget ser ofta tillbaka på historiska projekt och använder sig av detta som grund. Den tredje nivån har väl definierade processer, bestående av beredskapsplaner, standardisering, verifiering av arbetet och tydliga mål att uppnå. På den fjärde nivån managed innefattas företag vars IT-resurser är kvantifierbara och förutsägbara då organisationen mäter och följer upp sina prestationer. När fel eller oegentligheter begås kan företaget upptäcka och spåra avvikelsens grund. Högsta nivån benämns optimerad och innebär att arbeta för en ständig förbättring. Förbättringar av IT och verksamhetsprocesser planeras och genomförs som strategiska affärsaktiviteter (Paulk et al., 1993).

För att skapa en bred förståelse för systemen och tillhörande processer är dokumentation centralt. Dokumentationen stödjer företaget i användningen, men skapar också en god grund för IT-revision. Kontroller som är väldokumenterade, lämpligt placerade och fungerar effektivt bidrar till att skapa en större validitet i informationen som skapas (Daigle et al., 2005).

2.4. Riskhantering

De flesta företag har idag upprättat riskhanteringsprogram för att identifiera, bedöma och hantera risker. Samtidigt som teknologin erbjuder nya möjligheter för att integrera verksamheten i olika system medför den även fler risker att hantera (PricewaterhouseCoopers, 2009a). Abrams, von Känel, Müller, Pfitzmann och Ruschka-Taylor (2007) menar att

riskhantering är ett brett begrepp med flera olika definitioner varpå The Committee of Sponsoring Organizations (COSO) i samband med utvecklandet av sitt ramverk för verksamhetsövergripande riskhantering, ERM föreslog en övergripande definition som översatt till svenska blir:

”Övergripande riskhantering (”Enterprise Risk Management”) är en process som påverkas av styrelsen, bolagsledningen och annan personal, etablerat i strategiprocessen och i hela organisationen, utformat för att identifiera potentiella händelser som kan påverka bolaget, och hantera risk inom bolagets riskaptit, för att ge en rimlig försäkran om att bolagets mål uppnås” (Ballou & Heitger, 2005).

Genom att arbeta med en strukturerad riskhantering kan företag uppnå flera fördelar:

- **Affärsmöjligheter fångas upp:** Stora konkurrensfördelar kan uppnås genom att systematiskt analysera potentiella händelser som möjliggör för ledningen att tidigt identifiera och tillvarata affärsmöjligheter ((PricewaterhouseCoopers, 2009b).
- **Kan förutse risker snabbare än konkurrenterna:** Genom att integrera riskhanteringen i hela verksamheten kan företaget snabbare förutse risker än sina konkurrenter och med en bättre riskanalys hantera och exponeras för risker som tidigare avskräckt företaget (Galloway & Funston, 2000).
- **Möjlighet att kvantifiera operationella risker:** Segal (2006) menar att många företag traditionellt arbetar med risker separat och kan inte använda samma approach i hela verksamheten. Genom att implementera ERM och strukturera upp riskhanteringen efter processerna involveras hela verksamhetens nivåer i riskarbetet. Även PricewaterhouseCoopers (2009b) anser att större bolag ofta har flera olika funktioner som arbetar parallellt med riskhantering, till exempel identifikation och rapportering av risk och osäkerhetsfaktorer, arbete med Corporate Social Responsibility och internrevision. Inom dessa områden kan bolagen bli bättre på att integrera de olika funktionerna och arbeta mindre överlappande.

2.4.1. Enterprise Risk Management

Som en följd av de amerikanska redovisningsskandalerna med bland annat Enron och Worldcom tillkom hårdare lagstiftning för interna kontroller och riskhantering (O’Donell, 2005). Dessa nya regleringar medförde att de flesta företagen helt fick lägga om sitt riskhanteringsarbete och därmed behövde vägledning i hur de skulle upprätta en riskhantering som uppfyllde kraven. För att tillgodose marknadens behov av stöd för dessa nya lagar och regler initierade COSO ett projekt i syfte att utveckla ett ramverk för företagsövergripande riskhantering. Utfallet av arbetet blev ERM som skulle kunna användas av företag som en guide för hur deras övergripande riskhantering kunde utformas. En central del av ramverket inbegriper tillförlitligheten i den finansiella rapporteringen (O’Donell, 2005).

Mikes (2009) nämner fyra typer av riskhantering, som alla arbetar verksamhetsövergripande. *Risk silo management*, inriktar sig främst mot att kvantifiera olika typer av risker. Som exempel nämns den vanligt förekommande metoden *Value-at-risk* vilken Galloway och Funston (2000) definierar som ett statistiskt mått för oförutsägbara förluster inom marknadsandelar, kreditförluster, operationella försluster och försäkringsförluster. Den andra typen av riskhantering, *Integrated risk management* fokuserar enligt Yang (2000) på att aggregera de kvantifierbara riskerna till en total riskestimering. Den tredje riskhanteringstekniken, *Risk-based management* menar Mikes (2009) kännetecknas av ett fokus på intressenterna. Kalkyler för intressenternas värdeskapande upprättas för att länka samman riskhantering och prestationsmätning. Mikes (2009) redogör för en fjärde typ av

verksamhetsövergripande riskhantering, *Holistic risk management* som blev populärt i samband med en ökad efterfrågan av intern kontroll. Under den här kategorin nämns främst COSO:s ramverk ERM. Riskhantering på den här nivån utmärker sig med att involvera risker som inte är kvantifierbara. Som namnet holistic antyder är syftet med dessa metoder att genom en Top-down approach involvera hela verksamheten på alla nivåer i företaget (ibid.).

2.4.2. Riskhantering med inslag av automatiska kontroller

Oringel och Aldhizer (2009) resonerar kring att företagens riskhantering ofta är ineffektiv för att den inte stödjer frekventa utvärderingar av risker som organisationen utsätts för. Genom att använda automatiska kontroller tillsammans med ERM-rapportering får ledningen realtidsuppdateringar om risker, kontroller och bedrägeriförsök. Med hjälp av denna teknik kan kommunikationen med ledningen ske smidigare och arbetet med riskhantering kan ske effektivare genom att risker upptäcks innan de hinner generera materiella förluster (ibid.). Deloitte (2010) anser att automatiska kontroller ska appliceras där verktygen är som effektivast, det vill säga på bolagens operationella nivå. Vendrzyk och Bagranoff (2003) resonerar kring att revisionsbyråerna anser att både finansiell- och IT-revision måste betraktas som en del av riskhanteringen och Daigle et al. (2005) påpekar att väl dokumenterade kontroller minskar omfattningen av IT-revisorernas arbete och kan bidra till lägre revisionskostnader.

Varje företag är dock unikt och i behov av skräddarsydda riskhanteringsrutiner. Det är därför svårt att skapa ett specifikt ramverk som kan användas av alla (Oringel & Aldhizer, 2009).

3. Metod

I metodkapitlet introduceras läsaren för de olika synsätt som tillämpas i vetenskapliga undersökningar samt vilket tillvägagångssätt vi har valt för att samla in data. Undersökningen utfördes som en kvalitativ studie med en induktiv ansats. Empirin har samlats in genom besöksintervjuer hos respondenterna. Läsaren får även ta del av resonemang kring urval, operationalisering, litteratursökning, uppsatsens validitet och reliabilitet.

3.1. Vetenskapligt förhållningsätt - hermeneutik vs. positivism

För att beskriva det övergripande perspektivet som dominerar och bildar en kultur inom ett forskningsområde används ofta termen paradigm. Paradigmet har stor inverkan bland vetenskapsmännen inom det egna området. Det kan liknas med en gemensam grundsyn som påverkar vilka problem, metoder och modeller forskaren väljer att använda. Paradigmen kan därefter brytas ner i olika perspektiv. Två perspektiv som under 1600-1700-talen etablerade sig i Europa var empirismen och rationalismen. Rationalismen, som utgör den kunskapsteoretiska delen söker lösningen i det som förnuftet inser är sant medan empirismen kännetecknas av en övertygelse att observationer av verkligheten utgör ett säkert fundament. Den sanna källan till kunskap utgörs därmed av våra sinneserfarenheter (Wiedersheim-Paul & Eriksson, 2011).

Rationalismen utgör grunderna i det som i vetenskapssamhället kallas positivism. Detta synsätt baseras på experiment, kvantitativ (matematisk, statistisk metod) mätning och logiska resonemang. Antaganden och satser används för att bilda en teori med vars stöd olika hypoteser kan testats. Kritik som riktats mot detta synsätt består främst av att det anses behandla hur saker är nu och därmed inte tar upp kontroversiella områden för att skapa förändringar i samhället. Medan positivismens utgångspunkt är att beskriva och förklara ämnar det hermeneutiska synsättet att utföra kritiska studier i syfte att uppnå en helhetsförståelse, en insikt (ibid.)

Ordet hermeneutik översätts som ”tolkningskonst” eller ”tolkningslära”. När en hermeneutisk metod används är det i syfte att till exempel en forskare vill förstå en annan persons handlingar. Den viktigaste variabeln är språk. Förståelsen blir lidande om det inte finns ett gemensamt språk eller om orden som används av de inblandade har olika betydelse för parterna. Kritik mot hermeneutiken utgörs främst av att tillvägagångssättet bygger på att undersökaren skapar sig en helhetsbild av händelseförlopp för att kunna tolka detta till ett meningsfullt sammanhang. Om det finns underliggande mekanismer och samband hos människorna som dessa är ovetande om men som ändå styr deras handlingar riskerar det hermeneutiska synsättet att inte räcka till (ibid.).

I vår undersökning ämnade vi att få en djupare inblick i hur storföretag på den svenska marknaden med hjälp av automatiska kontroller i affärssystemen övervakar sina transaktioner och minimerar risken för bedrägerier och ineffektiva processer. Vi samlade in data i form av intervjuer som bygger på språklig dialog vilket medförde att vi behövde tolka intervjuobjektens uppfattningar och vår empiri kom därför att baseras på intervjuobjektens subjektiva uppfattningar. För att få en djup förståelse inom ämnet lämpade sig därför ett hermeneutiskt synsätt bäst.

3.2. Val av perspektiv

Vi har valt att tillämpa ett ledningsperspektiv på denna uppsats. Vi har gjort detta val på grunderna att automatiska kontroller är ett ämne som främst berör högre instanser i ett företag och det är ledningsgrupp och interna revisorer som besitter den kunskap om företaget som krävs. Det är även ledningsgruppens ansvar att redovisa företagets effektivitet och lönsamhet inför aktieägare och andra intressenter. Vi har därför valt att söka efter intervjurespondenter vilka har en mer övergripande roll i revisions- och styrningsarbetet för att få deras perspektiv och tolkningar kring intern kontroll.

3.3. Val av strategi

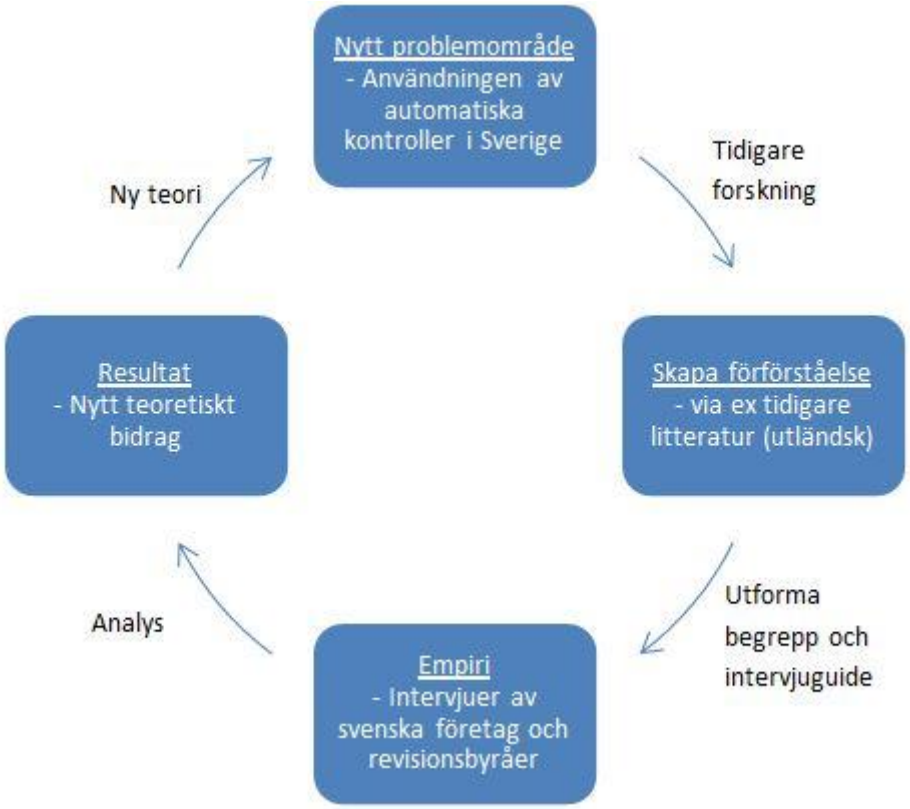
Hur forskaren relaterar teori mot verklighet är ett av de centrala problemen inom det vetenskapliga arbetet. Tre begrepp som behandlar detta är deduktion, induktion och abduktion som alla utgör olika alternativ för hur forskaren kan genomföra sina studier (Patel & Davidsson, 2003).

En forskare som arbetar deduktivt utgår enligt Wiedersheim-Paul och Eriksson (2011) från hypoteser som formas utifrån en teori och utgör testbara påståenden om verkligheten. Resultat uppnås därefter genom logisk slutledning. Alvesson och Sköldberg (2008) anser att den deduktiva ansatsen tenderar att rikta in sig på ett enskilt fall av intresse vilket får konsekvensen att ansatsen kan anses mindre riskfylld. Istället för att söka orsaker till fenomen begränsar sig deduktionen till att enbart fastslå ett fenomens existens (ibid.).

Den induktiva forskningen anser Wiedersheim-Paul och Eriksson (2011) kännetecknas av att forskaren utifrån skilda fenomen ur verkligheten arbetar fram teorier och modeller. Forskningen utförs genom att ett forskningsobjekt studeras utan att undersökningen först har blivit förankrad utifrån en tidigare teori. Forskaren sammanställer därefter sin insamlade empiri och formulerar en teori (ibid.). Alvesson och Sköldberg (2008) menar att induktionen medför ett riskfyllt steg när en samling observationer ska generaliseras till en allmän sanning. Således kan en induktiv slutledning sägas vara svår att applicera på andra situationer än den undersökta.

Patel och Davidsson (2003) redogör även för ett tredje sätt att relatera teori och empiri i vetenskapliga studier. Abduktion benämns som en kombination av induktion och deduktion. Arbetsgången börjar med att forskaren utifrån ett enskilt fall formulerar ett hypotetiskt mönster för att kunna upprätta ett förslag till en teoretisk djupstruktur. Abduktionens belackare anser att ett abduktivt arbetssätt innebär uppenbara risker. Forskare påverkas omedvetet av erfarenheter från tidigare forskning. Med detta i åtanke kan ingen forskning startas förutsättningslöst. En risk som uppkommer är om forskaren väljer sitt studieobjekt baserat på tidigare erfarenheter och formulerar en teori där andra tolkningar är uteslutna (Patel & Davidsson, 2003).

I nedanstående modell gestaltas den grundläggande arbetsgången i vår ansats som vi anser vara induktiv.



Figur 2, Den induktiva ansatsen i vår studie (Egen tolkning)

Då vi ämnade beskriva och analysera hur ett antal svenska storföretag använder sig av de automatiska kontroller som finns att tillgå i deras affärsystem ville vi välja en strategi där vi kunde genomföra empiriska undersökningar utan att vara påverkade av tidigare intryck. För att skapa en förförståelse kring ämnet utformade vi en referensram med teorier inom vårt uppsatsområde. Då mängden forskning inom området är begränsat gick vi in i undersökningsprocessen med ett öppet sinne och en relativt begränsad förförståelse. Vi anser med ovanstående resonemang som stöd att undersökningen stämmer väl överens med en induktiv strategi och valde därför att tillämpa den i uppsatsen. Ansatsen stödjer dessutom syftet att generera ett teoribidrag i ett tidigare outforskat område.

3.4. Val av undersökningsmetod

Ordet kvantitativ kan tolkas som en egenskap eller händelser hos olika mätningar. Variabeln som utgörs av mätvärdena kan även den betecknas som kvantitativ. Modeller som inte kännetecknas av att alla variabler är kvantitativa kallas istället kvalitativa (Wiedersheim-Paul & Eriksson, 2011). I linje med ett hermeneutiskt synsätt kommer studien att genomföras med hjälp av en kvalitativ metod. Jacobsen (2002) anser att en kvalitativ datainsamling fokuserar på att fånga upp ord, i form av texter, meningar och så vidare. Han föreslår även en kvalitativ metod som ett lämpligt val att göra när en djup förståelse för ett mindre antal enheter vill uppnås. Alvesson och Sköldberg (2008) konstaterar att definitionen av en kvalitativ metod inte är självklar. Ett centralt kriterium anses dock vara fokuseringen på en öppen, mångtydig empiri. Att välja en kvalitativ undersökningsmetod blev för oss en självklarhet då vi fokuserade på att få en djupare insikt i några få enheter.

3.5. Datainsamling

3.5.1. Primärdata

Jacobsen (2002) beskriver primärdata som upplysningar direkt från personer, eller grupper av personer. Kravet för att uppgifterna skall klassas som primärdata är att forskaren/undersökaren genom att gå till den primära källan samlar in upplysningarna för första gången. Den här formen av datainsamling lämpar sig särskilt bra för speciella problemställningar. För att samla in primärdata kan forskaren/undersökaren använda metoder som intervju, observation eller frågeformulär (ibid.). Vi har i vår undersökning enbart samlat in primärdata i form av besöksintervjuer på plats hos respondenternas företag. Antalet intervjurespondenter skiljde sig åt på de olika intervjuerna. Även respondenternas befattningar varierade. Under rubriken empiriskt urval diskuterar vi hur dessa faktorer har påverkat resultatet av intervjuerna.

3.6. Utformning av intervjuformulär

Enligt Jacobsen (2002) ska en intervju inledas med en snabb översikt om varför själva undersökningen görs. Vid själva utformingen av frågeformuläret menar Wiedersheim-Paul och Eriksson (2011) att forskaren/undersökaren först behöver bestämma hur formellt formuläret ska vara. Det kan antingen vara formellt för att respondenten ska fylla i svaren själv eller mindre formellt för att användas som ett stöd av undersökaren (ibid.).

I den teoretiska begreppsutvecklingen utvecklade vi ett resonemang kring vilka begrepp som är centrala för uppsatsen. Dessa begrepp, som därefter utvecklades och fördjupades i referensramen, är begreppen som operationaliserats för att utgöra övergripande teman i intervjuguiden. Frågorna har en låg grad av strukturering för att respondenterna inte ska styras för mycket. Med hjälp av detta upplägg kunde respondenterna svara utförligt och även resonera fritt kring våra övergripande teman. De områden som utgör rubrikerna i vårt intervjuformulär är: ERP, automatiska kontroller och riskhantering.

Begreppet ERP delas in i tre undernivåer där vi först behandlade ämnet integrering som enligt Magnusson och Olsson (2008) utgör en av ERP-systemets största fördelar. Underbegreppet systemmognad har sin tyngdpunkt i Ramachandran (2008) och Holland och Lights (2001) resonemang att företags systemmognad kan variera mellan tre nivåer. Det tredje underbegreppet ledningsengagemang grundar sig i Neirotti och Paolucci (2007) och Lundbergs (2009) övertygelser att ledningens engagemang är en viktig framgångsfaktor för lyckade IT-satsningar. Även huvudbegreppet automatiska kontroller består av tre underkategorier. Detta begrepp har vi betraktat som uppsatsens viktigaste och det är här tyngdpunkten i intervjuguiden ligger. Det första underbegreppet, användningsområden grundar sig främst i de tankar Bierstaker et al. (2004) presenterar om förebyggande och upptäckande kontrollers utbredning. Nästa underbegrepp systemkontroller har sin grund i Lightle och Waller Vallarios (2003) resonemang att behörighetshantering och SOD utgör en viktig del av ett företags arbete med automatiska kontroller. Avslutningsvis under begreppet automatiska kontroller har vi utvecklat frågor kring företagens användningsgrad. Med hjälp av den femstegsskala Paulk et al. (1993) har utvecklat har vi tagit fram frågor för att kartlägga på vilken användningsnivå företagen positionerar sig. Det sista huvudbegreppet riskhantering har vi valt att ge lite mindre utrymme än föregående begrepp. Under det första underbegreppet, nivåer har vi utgått från Mikes (2009) resonemang att ett företag bör integrera alla delar av företaget i sin riskhantering. Avslutningsvis tog vi fram frågor för att undersöka hur företagen integrerar sin riskhantering med automatiska kontroller. Temat har sin grund i de tankar O'Donell (2005) har kring ämnet.

Graden av enhetlighet i vad som ska besvaras kan enligt Wiedersheim-Paul och Eriksson (2011) regleras i förväg. Om intervjuaren väljer att skicka frågeformuläret som en enkät tenderar svaren att präglas av större enhetlighet än vid en besöksintervju. Inför intervjuerna valde vi att skicka frågorna till respondenterna i förväg. Då vissa av respondenterna kände sig osäkra på om de var rätt personer att prata med bedömde vi det vara nödvändigt att skicka frågorna i förväg. Flera av respondenterna ställde dessutom som krav att få läsa frågorna innan de ställde upp. Vi är medvetna om att detta innebär att respondenternas svar kan bli mindre spontana och att vi därmed riskerar att gå miste om intressanta synpunkter.

3.6.1. Besöksintervjuer

Den öppna individuella intervjun kännetecknas enligt Jacobsen (2002) av att undersökaren och uppgiftslämnaren för en vanlig dialog. Oftast förekommer det ansikte mot ansikte men kan också förekomma via telefon. Metoden lämpar sig bäst när få enheter ska undersökas, vid intresse av den enskildes egna åsikter och när vi är intresserade av uppgiftslämnarens egna tolkningar av olika fenomen (ibid.). Då vi utförde en kvalitativ studie där vi gick på djupet med ett par enheter anser vi att den öppna individuella intervjun lämpade sig bäst för undersökningsformen. Flera av företagen hade dock önskemål om att representeras av fler än en person. Vi gjorde bedömningen att detta kunde leda till fler relevanta åsikter och välkomnade därför upplägget. I en gruppintervju anser Jacobsen (2002) att undersökaren fungerar som en debattledare eller en ordförande. Vid gruppintervjuer finns risken att en individ är dominant och styr de övriga gruppmedlemmarnas svar (ibid.). Under den intervjun som genomfördes med KPMG:s tre respondenter märkte vi tydligt att den seniora IT-revisorn (X) var den som svarade mest och även fördelade frågor till sina kollegor. Vi är givetvis medvetna om att denna tydliga rollfördelning mellan respondenterna har påverkat svaren under intervjuerna. Att vi fick intervjua tre personer kom även som en överraskning då vi trodde att bara två respondenter skulle närvara. I de övriga två intervjuer som genomfördes i grupp var respondenterna mer synkroniserade i erfarenhet och rang och fungerade därför som ett bra komplement till varandra.

Intervjuer kräver inspelning (ljud eller film) för att andra forskare ska kunna granska det grundläggande materialet (Wiedersheim-Paul & Eriksson, 2011). Jacobsen (2002) anser att inspelning av respondenten kan leda till att denne låser sig och intervjuns resultat påverkas. För att underlätta transkriberingen spelade vi in alla intervjuer. Detta säkerställer även att de citat vi valde att lyfta fram är ordagranna. Ingen av respondenterna sade sig ha några problem med att bli inspelade och godkände att vi spelade in samtalet.

Samtligta intervjuer genomfördes som besöksintervju på respondenternas arbetsplats. Wiedersheim-Paul och Eriksson (2011) menar att besöksintervjuer medför en kontrollerad intervjusituation och en bra möjlighet för intervjuaren att läsa av respondenternas kroppsspråk. Kritik mot besöksintervjuer är att de kan medföra höga kostnader och risk för intervjuareffekten. Då vi ville få en djup förståelse av respondenterna anser vi att det var viktigt att genomföra intervjuerna på plats. Genom att få möjligheten att läsa av respondenternas kroppspråk och skapa en bättre relation anser vi att informationen som vi samlat in blir djupare och mer tillförlitlig än vid telefonintervjuer. Även intervjuareffekten som Wiedersheim-Paul och Eriksson (2011) beskriver som risken att intervjuaren och respondenten påverkar varandra är något vi beaktat vid val av undersökningsmetod. Vi är medvetna om att detta kan ha påverkat utgången av intervjuerna. Vi resonerade i förväg kring hur vi skulle gå tillväga om respondenterna kände sig obekväma med att svara på vissa frågor eller bli publicerade med sitt riktiga namn.

Jacobsen (2002) menar att anonymitet i studien är något forskaren kommer att behöva ta ställning till. En anonymisering kan skapa en större frihet hos respondenten att svara uppriktigt då graden av känslighet i informationen kan påverka hur utförligt respondenten besvarar frågorna. Om intervjuerna berör känslig information bör undersökaren se till att respondenternas privatliv garanteras (Jacobsen, 2002). Samtliga intervjuer tar upp respondenternas syn på respektive ledningsgruppers engagemang vilket vi anser kan vara ett känsligt ämne att beröra. För att underlätta jämförelse mellan intervjuerna och få ett bättre flyt i analysen bestämde vi oss efter att ett flertal respondenter efterfrågat anonymisering för att anonymisera alla. Vi är medvetna om att valet att anonymisera studiens respondenter påverkar reliabiliteten då respondenternas anonymitet medför att studiens resultat inte kan återskapas med samma respondenter av en annan undersökare. Vi anser dock att anonymiseringen i det stora hela påverkade studien positivt genom att vi då kunde få med samtliga respondenter vi önskade.

Alla respondenter har fått fått möjligheten att läsa igenom empirin innan den publiceras. Vissa av respondenterna har haft synpunkter och förtydliganden på texten och samtliga dessa synpunkter har vi använt för att förbättra validiteten i empirin.

3.7. Urval

3.7.1. Empiriskt urval

För att besvara vår forskningsfråga sökte vi två typer av företag, revisionsbyråer och tillverkande svenska storföretag. Vi intervjuade tre revisionsbyråer vars konsulter dagligen arbetar med att utvärdera stora företags användande av automatiska kontroller. Valet att intervjua revisionsbyråer grundade sig i att samtliga av de revisionsbyråer vi intervjuade på sina hemsidor utgav sig för att arbeta med automatiska kontroller. Att få deras syn på hur svenska storföretag använder sig av automatiska kontroller anser vi tillför uppsatsen ett viktigt perspektiv. Tre av de fyra största revisionsbyråerna har avdelningar som arbetar med dessa frågor i Västsverige. Urvalet föll sig därför naturligt på dessa tre byråer och alla var välvilligt inställda till att delta i undersökningen. Urvalsarbetet med att hitta tre tillverkande företag var desto mer komplext. Då vi tidigare hade avgränsat oss till att söka svenska storföretag som använder sig av ERP-systemet SAP fick vi använda oss av SAP:s svenska användarförenings (SAPSA) register över sina medlemmar. Genom att sortera alla företag efter omsättning, belägenhet och verksamhet kunde vi därefter ringa in ett antal potentiella företag vars storlek och verksamhetsinriktning underlättade möjligheten att jämföra företagen. Vi sorterade bort företag som inte hade sitt huvudkontor i Västsverige eller styrdes av SOX-ramverket. Utifrån dessa urval fick vi en lista på 20 potentiella företag. Dessa företag rangordnades efter omsättning och vi kontaktade alla företag via mail eller telefon. Svarsfrekvensen hos företagen var låg och det var endast tre tillverkande företag som var villiga att delta i undersökningen. Två av företagen, Nibe och Mölnlycke Healthcare omsätter koncernmässigt ungefär lika mycket medan Duni omsätter betydligt mindre än de övriga företagen. Nibe och Duni är börsnoterade aktiebolag medan Mölnlycke Health Care inte finns noterade på någon börs. Vi har tagit i beaktande att skillnader i omsättning och bolagsform kan påverka utfallet av undersökningen.

3.7.2. Urval av personer till öppna intervjuer

Vid valet av lämpliga personer att intervjua påpekar Jacobsen (2002) att urvalet i en kvalitativ undersökning på grund av brist på tid och pengar begränsar antalet enheter som kan intervjuas. Valet av enheter får även stor betydelse för undersökningens tillförlitlighet och trovärdighet. Vid intervjuer måste forskaren/undersökaren vara noggrann med vilka personer som intervjuas. Risken finns att personerna som undersökningen baseras på inte har tillräcklig

kännedom om det vi vill undersöka, ljuger eller på något annat sätt lämnar felaktig information (ibid.). Avsikten med kvalitativa metoder är enligt Jacobsen (2002) att söka efter unika och speciella fenomen som med hjälp av undersökningen ska kunna klarläggas.

I och med utformningen av vår undersökning kunde vi inte göra ett urval som baseras på någon urvalsprocess där respondenterna väljs ut slumpmässigt. Vi valde att aktivt söka oss mot respondenter som är involverade/ansvariga för företagens användning av automatiska kontroller. Att hitta respondenter som befinner sig högt upp i företagets hierarki var för oss viktigt då vi tillämpar ett ledningsperspektiv på uppsatsen. Vilken typ av personer som arbetar med automatiska kontroller varierar från företag till företag. Gemensamt för alla respondenter är att de arbetar på operativ nivå inom IT eller ekonomi. Dunis respondent är chef för systemutvecklarna medan Nibes två respondenter utgjordes av en controller och en redovisningsansvarig. Respondenten från Mölnlycke Healthcare arbetade mellan IT och ekonomi i en nyligen skapad roll för att samordna företagets processer. För att säkerställa att personerna var relevanta för undersökningen skickade vi i förväg ut frågorna för att de potentiella respondenterna skulle kunna göra en bedömning om deras kompetenser lämpade sig för undersökningen. Att hitta lämpliga respondenter hos revisionsbyråerna var en enkel process då vi blev hänvisade till avdelningarna för IT-risker och IT-revision.

3.8. Litteratursökning

Våra kunskaper kring de ämnen som tas upp i denna uppsats var innan starten av uppsatsprocessen begränsade. Litteratursökningen präglades inledningsvis av sökningar på de fyra stora revisionsbyråernas sidor med syfte att ge oss en tydligare bild om ämnets omfattning. Efterföljande litteratursökning kom att fokusera mycket på tidigare uppsatser som skrivits i ämnet. Målet med detta var att leta efter intressanta infallsvinklar och säkerställa att vi inte valde en inriktning som det redan skrivits flertalet uppsatser om.

När vi slutligen bestämde oss för ett syfte och en problemställning inledde vi sökningar i artikeldatabaserna ABI/Inform och Google Scholar. Ur dessa två databaser kunde vi söka fram ett antal vetenskapliga artiklar som användes som stöd för att utveckla den teoretiska referensramen. Det kan påpekas att vi under litteratursökningen kring automatiska kontroller upptäckt att den tillgängliga forskningen är tämligen begränsad till den amerikanska marknaden och saknar kopplingar till den svenska marknadens användning av dessa. Genom att kombinera mestadels journalartiklar med publikationer från revisionsbyråernas hemsida samt utvecklade ramverk från branschrelaterade organisationer som exempelvis COSO har vi skapat en teoretisk utgångspunkt som fungerar som ett stöd till den senare delen av uppsatsen. Vi är medvetna om att desto mindre andel vetenskapliga artiklar vi använder, desto lägre blir tillförlitligheten på referensramen. Vi har i vissa delar av uppsatsen funnit det nödvändigt att främst använda oss av böcker som litteraturkälla. Metodkapitlet grundas på källor i bokform som tagits fram genom sökningar på Högskolebiblioteket i Halmstad. Då vår utbildning inriktar sig mot ERP-system har teoriavsnittet ERP kommit att inbegripa ett par böcker från tidigare kurslitteratur inom ämnet.

3.9. Källkritik

Wiedersheim-Paul och Eriksson (2011) benämner källkritik som en urvalsmetod för den som skriver. En bedömning görs av det material som samlas in, det som inte är bra rensas bort och det som är acceptabelt behålls. Som hjälpmedel för att bedöma källor kan fyra källkritiska kriterier användas:

- **Samtidskrav:** För att förklarara hur samtidskravet uppfylls exemplifierar Wiedersheim-Paul och Eriksson (2011) hur ett statsråd i sina dagliga

dagboksanteckningar återger vad ett annat statsråd sagt till honom vid ett sammanträde. Hade statsrådet däremot återgett händelsen i sina memoarer ett par år senare hade samtidskravet inte uppfyllts.

- **Tendenskritik**: Tillämpas för att besvara vilka egna intressen uppgiftslämnaren har i den här frågan. Genom att hitta två källor med motsatt tendens kan båda användas för att balansera varandra.
- **Beroendekritik**: Det här kriteriet används för att kontrollera huruvida källorna är beroende av varandra, exempelvis om två respondenter återger uppgifter hämtade från samma källa.
- **Äkthet**: Kravet på äkthet har aktualiserats tack vare den ökade användningen av digital information som till exempel internet. En viktig fråga är hur forskaren/undersökaren kan avgöra om en webbplats är vad den utgör sig för (ibid.).

Vi har i uppsatsen varit medvetna om de krav som Wiedersheim-Paul och Eriksson (2011) ställer på källkritik. Vi använde oss till stor del av vetenskapliga artiklar då utbudet av böcker inom ämnet är nästintill obefintligt. Artiklarna kompenserades även av rapporter, så kallade whitepapers från revisionsbyråernas hemsidor vilket kan innebära att deras objektivitet går att ifrågasätta. Mycket av det material som publiceras av revisionsbyråerna har tagits fram i syfte att öka försäljningen av deras tjänster vilket medförde att vi fick granska källorna extra kritiskt. Då uppsatsens giltighet kan bli lidande valde vi att försöka minimera användningen av dessa källor till att fungera som ett stöd åt våra huvudbegrepp.

3.10. Validitet och reliabilitet

Wiedersheim-Paul och Eriksson (2011) definierar begreppet validitet som ett mätinstruments förmåga att mäta det som man avser att det ska mäta. Giltigheten kan delas upp i två olika aspekter: intern och extern giltighet. Enligt Jacobsen (2002) används ofta begreppet bekräftbarhet istället för intern giltighet. Tillvägagångssättet för att pröva bekräftbarheten kan göras genom att fastställa om undersökningen mäter det den ämnar mäta (ibid.). Med extern giltighet syftas till i vilken grad rönen från en undersökning kan generaliseras i andra sammanhang. Kvalitativa metoder har i regel dock inte som avsikt att kunna generaliseraras på större populationer. Syftet är oftast att förstå och fördjupa sig inom olika begrepp genom att utveckla mer generella teorier ur det vi har observerat, läst eller hört (ibid.). I vår undersökning har vi inriktat oss på att undersöka ett fåtal enheter och inser därför att resultatet av vår studie inte kommer att vara generaliserbart på andra företag.

Reliabiliteten är enligt Wiedersheim- Paul och Eriksson (2011) en form av krav som ställs på ett mätinstrument. För att mätinstrumentet ska ha en hög reliabilitet ska det generera tillförlitliga och stabila utslag. Frågor som undersökaren kan ställa sig är om andra undersökare kommit till samma resultat om de använt samma angreppssätt. För att ha hög reliabilitet bör en metod eller angreppssätt därmed vara oberoende av undersökare och undersökta enheter (ibid.). Då vi har spelat in alla intervjuer och dessutom transkriberat ner resultatet har vi arbetat för att öka reliabiliteten i uppsatsen. Eventuell intervjuareffekt samt det faktum att vissa av respondenterna har intervjuats i grupp innebär dock att reliabiliteten i uppsatsen minskar. Valet att anonymisera respondenterna är som tidigare nämnts ytterligare en faktor som påverkar uppsatsens reliabilitet negativt.

3.11. Operationalisering

Under denna rubrik redogör vi för processen från det att intervjuerna utfördes till det att empirin var färdigskriven. Syftet med detta är att tydliggöra för läsaren hur vi har gått tillväga och därmed täcka in faktorer som kan ha påverkat utkomsten av arbetet.

För transkriberingens skull förde vi under intervjuerna stödanteckningar som skulle underlätta arbetet med att föra över materialet till textform. Då tre av intervjuerna genomfördes som gruppintervju var vi noggranna med att notera vem som sa vad. Från transkriberingarna valde vi sedan ut de delar som var relevanta för uppsatsens teman, färgmarkerade och skrev om detta till en empiri som följde begreppsutvecklingens teman. Under intervjuerna kunde diskussionerna ofta falla utanför uppsatsens teman varpå vi fick rensa bort en hel del överflödigt material. För begreppet ERP infogade vi svaren från de frågor som berörde underbegreppen integrering, systemmognad och ledningens engagemang. I begreppet automatiska kontroller förde vi över de svar som föll under kategorierna användningsområden, systemkontroller och användningsgrad. Empirin kring riskhantering kom att involvera begreppen nivåer och kontrollintegrering. För att tydliggöra för läsaren vilka delar vi anser vara viktiga har vi infogat citat där respondenterna belyser ett område på ett tydligt sätt.

4. Empiri

Detta kapitel inleds med en beskrivning av tillvägagångssättet för empirin och är sedan uppdelad utifrån de sex företag som studien innefattar. I varje del presenteras företaget först kortfattat och därefter redovisas resultatet av intervjuerna.

Vid insamlingen av empiri valde vi att intervjua sex olika företag, tre revisionsbyråer, som arbetar med it-revision, samt tre tillverkande företag, som i olika utsträckning använder sig av automatiska kontroller. För att få en god och tydlig struktur på empirin har vi valt att presentera varje tillverkande företag för sig. Den empiriska redovisningen kommer att inledas med de tre revisionsbyråernas redogörelser för att följas av våra tre respondentföretag. Vi inleder med en presentation över respondentens position och ansvarsområden inom företaget för att därefter dela in intervjuerna i våra tre huvudområden ERP, automatiska kontroller och riskhantering. Dessa teman är de mest centrala för vår studie och blir därför en bra grund inför den därpå följande analysen.

4.1. Revisionsbyrån Alfa

Revisionsbyrån som vi väljer att kalla Alfa är både en av världens och Sveriges största aktörer på området och är också den revisionsbyrå som har flest anställda inom sektionen risk och specialiserat redovisningsstöd. Avdelningen är uppdelad i de tre områdena Business Risk Services (BRS), Technology Risk Services (TRS) samt Accounting Consulting Services (ACS). Affärsidén är att granska och ge rådgivning inom interna kontroller, dels genom att hjälpa revisionsdelen inom byrån men också att vara konsult åt kunden i arbetet med styrning och riskhantering. Våra respondenter inom Alfa tituleras riskkonsulter och har varit verksamma inom sitt verksamhetsområde fyra respektive fem år. De kommer i empirin att benämnas som riskkonsult A (verksam fyra år) samt riskkonsult B (verksam fem år).

4.1.1. ERP-system

Revisionsbyrån Alfa är framförallt specialister inom SAP då detta är det största systemet, men de har även kompetenser inom de flesta andra affärssystem. Bitvis kan systemen spela mer eller mindre roll då det är processerna som är fokus många gånger, påpekar riskkonsult A. Deras allmänna uppfattning om hur väl ett företag generellt utnyttjar ERP-systemets olika funktioner är att det beror lite på vilken mognadsgrad företaget har. Faktorer som spelar in är hur väl företaget känner till sina system och förstår vilka möjligheter som finns beskriver riskkonsult B. En del system har väldigt mycket funktioner inbyggda per default medan andra system inte har det. Riskkonsult B ger exemplet att i SAP går det inte att boka in en faktura om inte kredit och debet balanserar

”Det kan vara svårt för företag att veta vilka möjligheter det finns inom systemen. Många har ju ett intresse av att utveckla sin rörelse, men det är lite krävande att ta tag i arbetet med att exempelvis skapa automatiska kontroller” (Riskkonsult B).

4.1.2. Automatiska kontroller

Riskkonsult A beskriver att Alfa har en skala för att bedöma hur företagets interna kontroller ser ut och bedöma hur mogna de är inom detta område. Ett steg i detta är hur mycket de använder sig av automatiska kontroller. På skalan är den högsta graden ”Optimerad”, men merparten av de svenska företagen ligger runt mitten på skalan, vilket innebär att företaget har en del kontroller på plats men det finns utrymme för förbättringar. De företag som lyder under SOX har helt andra krav på sig och med deras arbete hamnar de därmed ofta högre upp på

skalan påpekar riskkonsult B. Riskkonsult A påpekar att skalan de använder sig av handlar just om att komma till en optimerad nivå av användning.

”Det heter optimerat för att företaget måste ta ställning till var ’den gyllene medelvägen’ finns för dem. Det ska vara effektivt, inte outhärdligt att arbeta i systemen och processerna. Det ska vara optimerat, inte totaliserat” (Riskkonsult A).

Kontrollstrukturen kring de automatiska kontrollerna delas enligt riskkonsult B upp i tre delar i en pyramid. I botten finns IT GC, det vill säga IT-generella kontroller. I mellanlagret återfinns process- och applikationskontroller och i toppen finns enhetsnivåkontroller. Riskkonsult A beskriver hur riskonsulterna på revisionsbyrån vid en granskning av systemen och kontrollerna går in och undersöker hur företagets system är uppsatta. Det finns vissa granskningsprogram och verktyg. Konsulterna programmerar även vissa former av scripts vilka kontrollerar olika saker, men de påpekar att det viktigaste när granskningar utförs är att förstå processerna. Det är även så att om de generella IT-kontrollerna inte fungerar måste man arbeta på ett annat sätt i revisionen, exempelvis i form av att utföra mer detaljerad granskning genom att selektera stickprov av manuella bokföringsorders etc. för att på så vis göra en bedömning av bolagets interna kontroll.

Riskkonsult A menar att det finns två typer av fel som kan göras, dels oavsiktliga fel och dels bedrägerier. Arbetar företaget med behörigheter minskar risken för att göra fel, då uppgiften utförs av en person med rätt kompetens inom området. Företag kan ta det ytterligare ett steg och dela upp kritiska arbetsuppgifter på flera personer. Till exempel kan det krävas att två personer godkänner ändringar av kontonummer för kunder. Revisionsbyrån har verktyg för att testa vilka behörigheter som finns och vilka personer som har tillgång till vad.

4.1.3. Riskhantering

Riskkonsult B beskriver hur revisionsbyrån Alfa har förhållningssättet att allt grundar sig i risker. Ska ett företag nå en optimerad nivå av automatiska kontroller måste detta basera sig på en effektiv riskhanteringsprocess, en så kallad risk management-process. Mycket handlar om att se till riskerna i stort och sedan bit för bit bryta ner dem i mindre delar tills konkreta åtgärder kan matchas med de olika riskfaktorerna.

”Man ser till hur farliga riskerna är för företaget och hur stor sannolikhet det är att de ska inträffa, samt vad det kommer få för påverkan på företaget. Man går också med hjälp av revisorn igenom var riskerna med redovisningen finns och fokuserar på de punkterna. Därefter ser man vilka saker som redan finns på plats för att undvika eller minimera riskerna” (Riskkonsult B).

Riskkonsult B betonar även att företaget kan se möjligheterna med riskerna. De menar på att då företaget ser det som är riskfyllt har de också möjligheten att se vilka sätt det finns att genomföra uppgiften bättre på. Vikten av att kontinuerligt arbeta med riskhantering poängteras också, risker är något som förändras och måste omvärderas med viss frekvens. Riskbedömningen kan enligt riskkonsult B på Alfa gärna ske i samband med att företaget sätter sina kort- och långsiktiga mål, och då passa på att diskutera hur riskerna påverkas av detta. Sedan behöver inte hela riskanalysen göras om varje år, men relevanta delar bör ses över.

4.2. Revisionsbyrån Ernst & Young

Ernst & Young är ett globalt företag som är verksamt inom områdena revision, skatt, redovisning och transaktioner. Inom avdelningen Advisory (Rådgivning) finns delen IT Risk and Assurance, med underkategorierna IT Assurance, IT Controls och IT Risk

Transformation. Avdelningen arbetar dels med att stödja den ordinarie revisionsverksamheten med teknisk kompetens och dels direkt gentemot kund genom rådgivning och utvärdering av systemmiljöer och informationssäkerhet. Vår respondent på Ernst & Young har titeln Management konsult inom IT och har arbetat för Ernst & Young cirka fyra år.

4.2.1. ERP-system

Ernst & Young är oberoende från alla typer av systemleverantörer, de ger rådgivning och revisionsstöd till alla ERP-system. Vanligaste systemet beror enligt konsulten på Ernst & Young på företagets storlek, men vanligast bland de större företagen är SAP. Överlag anser konsulten att företagen generellt skulle kunna bli bättre på att använda sig av ERP-systemens funktioner, framförallt utnyttja fler funktioner och använda sig mer av de automatiska kontroller som redan finns inbyggda i systemen och därmed minimera användandet av manuella kontroller. Detta anser han ökar spårbarheten och minimerar risken för fel. Speciellt SAP är byggt för att öka spårbarheten, och har till skillnad från mindre system möjligheten att gå längre tillbaka för att se vem som har utfört vissa ändringar i systemen.

4.2.2. Automatiska kontroller

Det är framförallt inom de finansiella processerna som automatiska kontroller är vanliga menar IT-managementkonsulten. Det är vanligast inom områden där transaktionsflödena är väldigt stora och frekventa, där pengarna flödar så att säga. Ett annat område som också är lämpligt för automatiserade kontroller är lagerhantering. En bra sammansättning av automatiska kontroller medför en mer tillförlitlig redovisning vilket innebär att revisorn inte behöver göra en lika ingående revison och på så sätt minska revisionskostnaderna. Konsulten beskriver hur konsulterna ibland föreslår en automatisk kontroll istället för en manuell för att skapa bättre legitimitet i sifforna i framtida revisioner.

”Som en del av vår metodik ska vi även granska IT-delen i revisionen, ser man då att det finns väldigt mycket manuell hantering innebär detta att det finns en större risk för felaktigheter i bokföringen” (IT-managementkonsulten).

Processen att granska ett företags automatiska kontroller följer oftast samma mönster. Broberg belyser att först och främst måste de se till företagets IT GC, det vill säga IT-generella kontroller. Fungerande IT Generella Kontroller (ITGC) måste finnas på plats innan det är mening att gå vidare och eventuellt testa applikationskontroller. Fungerande ITGC innebär något förenklat att du vet att alla förändringar som genomförts i systemet blivit godkända, testade och implementerade i enlighet med vad som avsågs när förändringen beställdes. Du vet också att de användare som har behörighet till systemet fått sina behörigheter godkända samt att dessa behörigheter granskas regelbundet.

Segregation of Duties är en viktig del i behörighetshanteringen, menar IT-management-konsulten. Många mindre företag anser dock att det inte är lönsamt att använda sig av SOD då det finns för få personer i flödet. Verksamheten måste kunna fortsätta oavsett om en anställd är frånvarande.

Konsulten vid Ernst & Young påpekar att även om IT GC inte finns på plats kan applikationskontrollerna testas. Det krävs dock många fler exempel, och att dessa inhämtas under utspritt under året. Kan konsulterna inte heller efter detta dra slutsatserna att det går att lita till de här processerna återlämnas beskedet till revisorerna att tillförlitligheten inte kan garanteras och arbetet med revisionskontrollen måste ske manuellt. Detta är enligt managementkonsulten vanligare på mindre företag.

Även grundstrukturen i kontrollerna spelar roll menar IT-managementkonsulten, det finns förebyggande och upptäckande kontroller.

”Förebyggande är ju mycket bättre för då förhindras ju att felet uppstår medan de upptäckande kanske inte upptäcker skadan förrän den redan är skedd, så då får man istället försöka minimera skadan. Därför ska man alltid försöka gå mot förebyggande kontroller i så stor utsträckning som möjligt, det är det som är syftet med automatiska kontroller i helhet” (IT-managementkonsulten).

4.2.3. Riskhantering

Generellt måste arbetet med riskhantering börja från toppen anser konsulten. Det måste vara ledningen som sätter ambitionsnivån och kulturen kring riskhantering.

”Om man arbetar proaktivt med sin riskhantering och kommunicerar ut tankesättet kommer det att genomsyra hela företagets kultur, börjar företaget nerifrån kommer det aldrig få gehör från ledningen och det stödet som krävs” (IT-managementkonsulten).

Ett första steg i riskarbetet menar konsulten kan vara att skapa policys för hur de anställda får använda sina datorer och mobiltelefoner. Ernst & Young kan där gå in och rekommendera och ge vägledning hur företaget ska arbeta med riskhantering på den nivå de befinner sig. Det kan handla om lösenordshantering som ett exempel, eller att företaget ser över sina processer med jämna mellanrum. Införandet av automatiska kontroller bidrar till att företaget minimerar sina risker.

”Det är en naturlig del att få in fler automatiska kontroller för att få ner sin risk inom IT-området, det blir lättare att följa upp och få en bättre överblick över sitt risklandskap” (IT-managementkonsulten).

4.3. Revisionsbyrån KPMG

KPMG är en av världens största revisionsbyråer och bedriver sin verksamhet i 150 länder. Förutom revision erbjuder företaget även tjänster inom skatt och rådgivning. Inom rådgivning har KPMG flera olika specialistavdelningar med personal som har specialiserat sig inom särskilda områden. Specialistavdelningens IT-revisorer arbetar dels tillsammans med revisorerna under revisionsuppdragen och dels som konsulter för externa kunder som inte innefattas i revisionen. Vi har intervjuat tre IT-revisorer vilka vi kommer benämna X, Y samt Z. IT-revisor X har arbetat med IT-revision sedan 1998. IT-revisor Y har arbetat med IT-revision i snart fyra år medan IT-revisor Z är relativt ny i yrket och har arbetat som IT-revisor sedan augusti 2011.

4.3.1. ERP- System

Till vilken grad KPMG:s kunder optimerar användandet av sina affärssystems funktioner menar IT-revisor Z att det beror till stor del på bolagens storlek. Vissa större bolag använder sig av väldigt komplexa affärssystem medan mindre bolag gärna jobbar mer manuellt och inte använder funktionaliteten fullt ut.

”En del företag har mycket större system än vad de behöver egentligen och använder inte all funktionalitet som finns i systemen och en del företag har för små system, men rent generellt brukar företag försöka utnyttja sina system så väl som möjligt” (IT-revisor Y).

Bland KPMG:s stora kunder ser IT-revisor X att funktioner och kapacitet utnyttjas dåligt. Generellt har företagen investerat en mängd olika system och istället för att utvärdera hur dessa skulle kunna användas bättre är bolagen snabba med att köpa in ett nytt system. Vissa företag kan ha en systemflora med hundratals kritiska system. Om ett av dessa system utgörs

av något av de stora ERP-systemen på marknaden anser IT-revisor X att merparten av systemens uppgifter säkerligen hade kunnat lösas i detta system.

Istället för att anpassa ERP-systemet efter verksamhetens informationsbehov använder många bolag istället kringverktyg som till exempel Excel och beslutsstödslösningar där mycket arbete läggs på att föra över data från affärssystemen till dessa. Även dålig kommunikation inom företaget kan vara en orsak till att man väljer att köpa flera system. Till exempel kan marknadsavdelningen vilja ha ett system som är populärt inom marknadsföring även om det befintliga systemet har samma funktioner.

IT-revisor Z upplever att ledningen oftast inte driver frågorna utan skapar istället förutsättningar för att de anställda ska kunna driva frågorna. Att få alla att dra åt samma håll och skapa en brygga mellan IT och verksamhet ser han som en viktig fråga i ledningens arbete med att optimera användandet av affärssystemet.

4.3.2. Automatiska kontroller

I rollen som IT-revisor styrs uppdragen av revisorns behov av specialisthjälp. Innan de automatiska kontrollerna utvärderas finns det en viss arbetsgång som definierar vilka processer som ska undersökas. IT-revisor X förklarar att IT– revisionsprocessen triggas igång när en revisor, efter att ha granskat de konton som ingår i de processer som han/hon anser vara väsentliga för redovisningen i företagen, behöver hjälp av IT-revisorerna att fastställa hur siffrorna kommer in på kontona. Till exempel intäktskonton kan vara oerhört automatiserade i form av att en EDI-order kommer in och rasslar igenom till ett intäktskonto. För att utvärdera tillförlitligheten och riktigheten i det här kontot behöver revisorn stöd och konsultation från en IT-revisor. IT-revisorns uppgift blir därefter att utvärdera de applikationskontroller som är relaterade till processen. Det första IT-revisorn gör är att mappa upp de olika aktiviteterna i processen. Detta görs med en mix av förkunskap om hur olika processer fungerar samt frågeformulär till det berörda företaget. Därefter ringar IT-revisorn tillsammans med företagets personal in de aktiviteter som sker inne i systemet. Med hjälp av dessa aktiviteter ska IT-revisorn därefter identifiera vilka som är kontroller. Ofta är ordinarie aktiviteter i systemet kontroller. Till exempel blir alla order till slut fakturor. Finns det då en statuskontroll som identifierar ofullständiga order kan detta sägas vara en kontroll.

”Typiska automatiska kontroller eller applikationskontroller är logglistor, behörighets-styrning, vem får göra vad, in- och utdatakontroller, intervallkontroller, rimlighetskontroller och larm i systemet” (IT-revisor X).

För att säkerställa kontrollernas effektivitet berättar IT-revisor Y att IT revisorn ofta sitter ner med företagets personal och ber dem skriva in värden i systemet som överstiger de uppsatta kontrollvärdena som ska se till att siffrorna i redovisningen stämmer.

”Det bästa med automatiska kontroller är att om de är utformade på rätt sätt så kommer de att fungera de 365 dagar om året, 24 timmar om dygnet. Om man automatiserar sina kontroller kan man använda människorna till analys och utnyttja sina resurser bättre. Men det krävs en investering för att nå dit” (IT-revisor X).

I bedömningen av om en kontroll är effektiv måste många aspekter beaktas. Dels handlar det om tekniken, men även om hur människorna hanterar tekniken. I vissa fall kan kunden ha för många kontroller vilket i sin tur kan leda till att medarbetarna hittar sätt att kringgå kontrollerna. I ett sådant fall kan det handla om att avråda dem från en för hög säkerhet. Ett exempel kan vara lösenordets utformning i en organisation där personalen inte är mogen att

hantera för långa lösenord som byts med täta mellanrum. I ett extremt fall handlade 30 % av en kunds alla ärenden i supporten om lösenord.

4.3.3. Riskhantering

IT-revisor X menar att deras kunder arbetar med riskhantering på alla nivåer i företaget. Även om de inte använder termen ”riskhantering” arbetas det hela tiden med att analysera marknadens förutsättningar, förändringar på marknaden och arbeta fram strategier för att förekomma dessa förändringar. De delar i riskhanteringen som involverar automatiska kontroller är ofta kopplat till arbetet med den interna kontrollen och att förebygga risken för oegentligheter. I ett företag som har haft problem med att till exempel anställda begår oegentligheter blir möjligheten att använda sig av automatiska kontroller för att täppa igen dessa ”luckor” givetvis en central fråga. Det finns två olika kontrolltyper som används i arbetet med internstyrning och intern kontroll. Förebyggande och upptäckande kontroller fungerar som två byggstenar för att ha en bra styrning och kontroll

”Företagen ska ha en strukturerad riskanalys. Det är A och O. Man utgår från en uppdaterad och dokumenterad riskanalys. Denna analys bör göras minst årligen” (IT-revisor X).

IT-revisor X föreslår en metod med en riskhanteringsprocess som inleds med att skapa en riskanalys. Därefter utvärderar man vilka kontroller man har för att hantera dessa risker. I steg tre funderar man på hur effektivt de här kontrollerna stänger risken. Här kommer man fram till ja eller nej. Om kontrollen inte anses täcka tillräckligt stor del av risken får företaget titta på hur de kan stärka kontrollen och hamna på en risknivå som tolereras av företaget. IT-revisorns roll blir här att granska att kontrollerna är i nivå med de förväntade riskerna.

4.4. Nibe AB

Nibe Industrier AB är ett börsnoterat företag med sitt huvudkontor beläget i Markaryd. Koncernen består av cirka 70 dotterbolag som är resultatet av en strategi att förvärva bolag. Verksamheten består av tillverkning av värmepumpar och är uppbyggt i tre olika segment. Element, Stoves och Energy Systems. 2011 omsatte hela koncernen cirka tio miljarder kronor. Vi har genomfört en intervju med två respondenter från Nibe AB som är det största bolaget inom koncernen och omsatte 2010 cirka 2,65 miljarder kronor. Respondenterna vi har träffat är en controller och en redovisningsansvarig.

4.4.1. ERP-system

Inom koncernen Nibe Industrier berättar controllern att det finns en uppsjö av olika affärssystem. Under de senaste fem åren har Nibe genomgått stora förändringar och tack vare en mängd företagsförvärv växt mycket som företag. De använder sig av en strategi som går ut på att bevara entreprenörsandan i dotterföretagen och vill därför inte påverka hur verksamheten sköts i dessa bolag. Controllern berättar att Nibe AB på sommaren 2009 tog beslutet att fasa ut sitt gamla legacy-system (Styr 400) mot ett affärssystem från SAP. De moduler som används är finans (FICO), Controlling Profitability Analysis (COPA) och till viss del Sales and Distribution (SD). För produktion och inköp använder de sig av ett annat system, Infor XA. Dessutom finns det ytterligare system för CRM, garantiärenden och ett försystem som hanterar leverantörsfakturorna och attesteringen av dessa.

Controllern anser inte att företaget utnyttjar funktionerna i sina affärssystem på ett effektivt sätt. De två mest använda systemen, SAP och XA saknar till stor del integrering mellan varandra. I dagens läge finns det bara kopplingar mellan finansdata, exempelvis försäljningstransaktioner och omsättning, i de olika systemen. De finns dock en ambition att integrera alla transaktioner som sker i XA till SAP:s finansiella modul för att kunna utföra en fullgod resultaträkning utan att behöva bokföra in lagerrapporter manuellt. Controllern ser

stora fördelar med att koppla ihop systemen bättre. En funktion som hon efterfrågar är ett drill down-verktyg där det går att spåra transaktionerna i en faktura ända ner till den inledande ordern. Som det ser ut idag görs många uppgifter manuellt som SAP hade kunnat utföra automatiskt.

”Vi har ett väldigt stort system men använder bara en liten del av det” (Controllern).

Ledningens engagemang i arbetet med optimeringen av affärssystemen är enligt redovisningsansvarig begränsat. Koncernchefen har själv deklarerat att IT inte är en av hans starka sidor. Projekten föds och styrs ofta av projektgrupper som skapas på de olika avdelningarna. Han betonar även att organisationen är uppbyggt på ett platt sätt vilket har sina fördelar och nackdelar.

”Visst kan det emellanåt bli så att inköp hittar på projekt som är bra för dem men som kan haverera hela uppföljningen för oss” (Redovisningsansvarig).

4.4.2. Automatiska kontroller

Redovisningsansvarige berättar att arbetet med kontroller skiljer sig åt både i frekvens och i kvalitet mellan intäkts- och kostnadsredovisningen. Inom intäktsredovisningen sker all fakturering i försystemet vilket innebär att all omsättningsstatistik hamnar där. När all data sedan flyttats över till SAP matchas sifforna och systemet avger signaler om siffrorna inte stämmer och behöver kontrolleras manuellt. Det finns även kontroller att allt som levererats har fakturerats. När en vara har levererats skickas en signal som gör att ordern läggs i en kö redo för att faktureras.

Att arbeta med kreditlimiter ser redovisningsansvarige som ett bra sätt att säkerställa att det som har levererats även kommer att betalas. Det här systemet kan dock kringgås då kreditkontroller och orderläggningen sker i olika system och kreditspärren hindrar inte säljarna från att lägga nya orders. Enligt rutinerna behöver säljaren ringa till företagets controllers för att få ett godkännande att bryta kreditgränsen.

”Under mina tio år har vi peppar, peppar, peppar varit väldigt förskonade från kreditförluster, det är lite det vi lever på” (Redovisningsansvarig).

Om intäktsredovisningens uppgifter känns relativit säkra menar redovisningsansvarig att redovisningen på inköpssidan känns mer osäker. Beställningar av produktionsmaterial utförs i inköpssystemet som dock saknar koppling till systemet för leverantörsfakturor vilket medför att det blir svårare att göra avstämningar. För att komma till bukt med detta problem har redovisningsansvarige det senaste året arbetat mycket med att förbättra denna process. Det genom att använda en modul i inköpssystemet där de prickar av inleveranserna på ett nytt sätt och fyller i inköpsordernummer i fakturasystemet manuellt för att kunna följa upp inköpsorderna i fakturasystemet.

”Det är väl bara till att erkänna till exempel att det kan hända så, att vi idag får ett krav från en leverantör att vi inte har betalat en tre månader gammal faktura, på den sidan har vi lite större osäkerhet” (Redovisningsansvarig).

För att fakturor inte ska komma som en överraskning arbetar Nibe just nu med att alla inköp som görs ska behandlas som inköpsorders så det finns en koppling mellan order och faktura. Andra exempel på kontroller Nibe använder sig av är enligt redovisningsansvarig ett behörighetssystem som reglerar vem som kan attestera vissa fakturor. Om fakturan överskrider ett visst belopp skickas attesteringen automatiskt till medarbetarens chef.

Dotterbolagen på Nibe rapporterar dock inte alla i SAP vilket gör arbetet med att sammanställa koncernredovisningen något mer komplicerat.

För att kontrollera effektiviteten i kontrollerna görs inga specifika tester. Controllern berättar att deras revisionsfirma tidigare år gjorde en kontroll över IT-säkerheten vilket dock inte skett det senaste året. Dessutom finns det en hög tilltro till att IT-avdelningen som kör nattliga körningar med sin erfarenhet märker om det är fel på transaktionerna. Redovisningsansvarig berättar att produktionsplanerings-systemets lagersaldon styr materialinköpen. När systemet signalerar att det behövs till exempel mer plåt finns det ingen uppdaterad kontroll att lagernivåerna i verkligheten stämmer överrens med systemets uppgifter. Ett systematiskt svinn skulle teoretiskt kunna pågå tills den årliga inventeringen.

4.4.3. Riskhantering

Nibe har mer och mer börjat arbeta med en företagsövergripande riskhantering. En kvalitetsgrupp har utsetts som arbetar med detta. Företaget är numera även ISO-certifierat. Controllern beskriver hur kvalitetsgruppen arbetar med att minimera risker i produktionen medan fastighetsavdelningen arbetar med att minska risker för brand och stöld. Det finns dock inget uttalat ramverk som används.

Mycket av controllerns och redovisningsansvariges riskhanteringsarbete berör de finansiella riskerna. Redovisningsansvarige berättar att de via SAP har en direktkoppling till Soliditet som gör kreditbedömningar av alla företag. Om ett företags anseende går från AAA till A kommer det automatiskt in ett alarm med uppgifter om detta i Nibes SAP-system. I ett annat projekt försöker de med hjälp av avancerad kryptering säkerställa att bankfiler som skickas mellan SAP och banken ska vara omöjliga att förändra. Som ett led i att generellt minska sina IT-risker gjordes nyligen en investering i en ny datahall som speglar all data och transaktioner som sker i verksamheten.

Riskhantering är något som sker på alla nivåer i företaget. Controllern berättar att de arbetar mycket med projektgrupper vid produktionsmässiga investeringar. Projektgrupperna ansvarar för att säkerställa att företaget har rätt utrustning. Ledningen och styrelsen engageras enbart om det handlar om godkännande av högre belopp.

4.5. Duni AB

Duni AB är ett svenskt industriföretag som tillverkar och konverterar produkter inom dukning och servering. Verksamheten har sitt ursprung i Billingsfors bruk i Dalsland där den första tillverkningen drog igång redan 1949. Sedan 2007 är företaget noterat på Stockholmsbörsen och huvudkontoret är numera beläget i Malmö. Duni har cirka 2000 anställda utspridda i 17 europeiska länder och omsatte 2011 cirka 3,8 miljarder kronor. Vår respondent har arbetat på Duni de senaste 13 åren. Från att ha arbetat som systemutvecklare är han sedan fem år tillbaka chef för systemutvecklarna. Varannan vecka finns han på plats på huvudkontoret i Malmö och resterande tid arbetar han i Tyskland. Även om systemutvecklingschefen utbildade sig till förvaltningssocionom kom han tidigt i kontakt med IT och har tidigare arbetat som IT-konsult.

4.5.1. ERP-system

Användandet av affärssystem är en aktuell fråga inom Duni. Systemutvecklingschefen berättar att Duni sedan 2002 arbetar med ett strategiprojekt där koncernens olika affärssystem ska fasas ut och ersättas av SAP. Problem som uppstått under vägen har bland annat varit att tvinga de tidigare nästan fristående delarna av företaget att byta från ett system som fungerat väldigt väl. Systemutvecklingschefen menar dock att fördelarna väger över då kommunikation och stöttning inom företaget blivit avsevärt bättre. Funktionsmässigt använder man sig av

modulerna för försäljning, distribution, logistik, vanlig produktion, finans och controlling. Däremot detaljplanering för produktion körs i ett separat SAP- system. Systemet kallas Advanced Planner and Optimizer (APO) och används för lång- och korttidsplanering och även Forecasting inom fabriken. Detta system kommunicerar sedan med SAP-systemets produktionsplaneringsmodul där de grundläggande produktionsorderna skapas och därefter skickas till APO för att förfinas och slutligen skickas tillbaka till produktionsplaneringen. Rent generellt anser systemutvecklingschefen att varje modul inom SAP innehåller en stor mängd möjliga transaktioner då det är framtaget för att passa olika typer av verksamheten.

”SAP:s standardiserade transaktioner är som en motorväg där transaktionerna helst ska flyta på med så få avtagsvägar som möjligt” (Systemutvecklingschefen).

Duni har på grund av att de tidigare använde sig av självständiga system runt om i koncernen hittat egna sätt att arbeta. Även om målet är att verksamhetens transaktioner ska hamna så nära denna motorväg som möjligt menar systemutvecklingschefen att det är svårt att få så få avtagsvägar som möjligt när de gamla affärsprocesserna som växte fram ur andra system ska integreras i SAP:s standardiserade transaktioner.

Systemutvecklingschefen menar att ledningens engagemang för affärssystemsprojekten kan anses bristfälligt då lednigen inte är särskilt intresserade av projekten i sig, utan snarare av projektets resultat.

”Min chef som är CIO, sitter inte heller i företagsledningen vilket är ett kvitto på att företagsledningen i sig inte är så inriktade på IT. Det är inte så uttalat att IT är en strategisk del av verksamheten. Däremot är IT en strategisk del i att supporta verksamheten” (Systemutvecklingschefen).

Att inte integrera IT och mangagement i ledningen tror systemutvecklingschefen leder till sämre kommunikation och fördröjningar då alla processförändringar mer eller mindre är beroende av IT-stöd.

4.5.2. Automatiska kontroller

Under införandefasen har det generellt inte lagts något större fokus på automatiska kontroller. Systemutvecklingschefen menar att fokus istället har legat på att matcha systemet mot verksamhetens processer. Till viss del anser systemutvecklingschefen att de automatiska kontrollerna har behandlats i och med det grundläggande arbetet med att fastställa behörigheterna i systemet. De olika användarrollerna begränsar vad en användare får lov att göra i systemet. Det främsta syftet med detta är att personer som saknar specifik kompetens på så sätt inte riskerar att göra fel. Arbetet med att fastställa dessa roller har under projektets gång blivit mer och mer avancerat. För varje delprojekt som görs försöker man förfina detta moment och på senare år har användarrollerna kompletterats för att integrera de olika delarna av verksamheten där personen i fråga är anställd. Som exempel nämner systemutvecklingschefen att en kundservicemedarbetare som lägger in order i systemet inte kan lägga order för fler enheter än den som medarbetaren arbetar i. En medarbetare i Sverige kan således aldrig lägga in en order för en enhet i till exempel Holland eller Tyskland. Även inom ekonomiavdelningen gäller liknande regler. Anställda inom ett land ska inte kunna ha tillgång till redovisningen och flödet för andra länder.

Systemutvecklingschefen anser att det omfattande arbetet med behörigheter fungerar väl för Duni.

”Även om personalen till en början kunde irritera sig på begränsningarna i systemet har de flesta ändrat uppfattning när de inser att en reducerad användarroll leder till mindre risk för att bli ansvarig för fel som råkar begås i delar av systemet där en anställd egentligen inte borde befinna sig” (Systemutvecklingschefen).

Även revisorerna har granskat dessa lösningar och anser att det ökar tillförlitligheten inom transaktionerna som sker i systemet. Systemmässigt paketeras alla transaktioner i systemet och kan sedan filtreras ut på de olika användarrollerna. Detta medför att vid företagsförvärv finns alla business-roller i färdiga paket som sedan kan filtreras ut på verksamheten. Systemutvecklingschefen diskuterar även betydelse av Change management. Han beskriver dels att det berör de rutiner som finns för att dokumentera och ändra i systemet, dels även det organisatoriska värdet. Där handlar det om att skapa en beredskap inför en förändring och kunna motivera och engagera ledning och de anställda som berörs.

På en lägre nivå kan automatiska kontroller identifieras i arbetet med leverantörsreskontra. Det finns till exempel regler som styr vilka konton en viss typ av faktura kan bokas på. Systemutvecklingschefen resonerar kring att de automatiska kontroller kanske snarare kan ses som automatiska sättningar, det vill säga att saker och ting konteras automatiskt. Exempel på hur det kan gå till är när statusen på en order ändras mellan produktion och lager och ordern automatiskt konteras och bokas enligt en tidigare definierad sättning.

Systemutvecklingschefen menar att Duni har valt att vända på de automatiska kontrollerna. Istället för att kontrollera sina transaktioner i efterhand arbetar man mer förebyggande istället. Det är exempelvis inte möjligt att boka felaktiga momssatser tack vare förutbestämda villkor som är anpassade efter innehållet på fakturan. Rent generellt menar systemutvecklingschefen att användandet av automatiska kontroller främst involverar finans- och säljrutiner. Inom fakturering bygger den automatiska kontrollen på leveransen. Själva processen bygger på att ett flöde med flera nya dokument skapas mellan transaktionerna. En order blir ett leveransdokument till lagret som sedan rullar vidare i processen där det till slut inte är möjligt att fakturera något som inte har levererats tack vare dessa förutbestämda sättningar.

Sett till framtiden för de automatiska kontrollerna menar systemutvecklingschefen att det är en fråga som inte diskuteras i stor utsträckning. Dunis IT-filosofi handlar snarare om att de satsar på att göra rätt från början. Istället för att arbeta med automatiska kontroller vill man till exempel arbeta med automatiska bokningar. Mer fokus ligger på att förebygga än att kontrollera i efterhand. Det här tillvägagångssättet har även uppskattats av företagets revisorer. Systemutvecklingschefen poängterar dock att det är svårt att helt utesluta de automatiska kontrollerna då företaget måste kontrollera transaktioner som går mellan systemen och modulerna. Dessa transaktioner övervakas genom alarmsystem snarare än övervakningssystem och om de uppsatta regelverken bryts flaggar systemet om detta och en medarbetare följer upp transaktionen.

”All form av skräp i systemet hamnar förr eller senare hos finans, vilket leder till att det viktigaste stället att upprätta automatiska kontroller inte är hos finans, utan tidigare i kedjan. Detta görs genom att till exempel arbeta med behörigheter och sätta upp kontroller av ordertyper och villkor som ska uppfyllas innan ordern får fortsätta i flödet” (Systemutvecklingschefen).

Sammanfattningsvis menar systemutvecklingschefen att varje avsteg från systemets standard ökar risken för att andra standardfunktioner inte längre går att tillämpa. Automatiska kontroller är en term som de flesta användarna inte känner till då det är väl integrerat i deras arbetsrutiner.

4.5.3. Riskhantering

Systemutvecklingschefen berättar att den övergripande riskhanteringen formellt inte styrs via något ramverk utan har växt fram genom olika praxis och erfarenheter i företaget. Ledningens riskhanteringsarbete består i och med att företaget är börsnoterat främst av framtagandet av rutiner som säkerställer att information inte kan läcka ut inför boksluten. Detta styrs inte bara systemmässigt utan det finns klara regler över vad de anställda inte får lov att prata om inför boksluten.

”Till varje möjlighet en användare har att utföra en uppgift i systemet kopplas en risk” (Systemutvecklingschefen).

Här gäller det att noggrant kartlägga vilka kompetenser personalen har för att genom tilldelning av rätt behörigheter minimera riskerna. Systemmässigt arbetar man främst med dessa behörighetsfrågor för att minimera riskerna som organisationen exponeras för.

Som ett annat exempel på riskförberedande arbete nämner systemutvecklingschefen en tydlig satsning mot utbildning. IT-avdelningen har ingen befogenhet att hindra användarna från att utföra vissa transaktioner. Medan processägarna styr vilka befogenheter medarbetarna ska besitta försöker IT-avdelningen snarare identifiera och informera medarbetarna om systemnära transaktioner som kan påverka hela systemet om någon ändrar i dem. På IT-avdelningens finns den uttalade policyn att de inte godkänner några transaktioner till användare som kan vara störande för systemet. De arbetar även rent generellt med att rekommendera olika rollfördelningsprofiler åt processägarna baserat på vad medarbetare bör få ha tillgång till i systemet eller inte. Systemutvecklingschefen menar att all riskhantering är kopplat till behörighetssystemet och på det viset involveras i arbetet med automatiska kontroller och sättningar.

4.6. Mölnlycke Health Care

Mölnlycke Healthcare är ett svenskägt företag som ägnar sig åt tillverkning av engångsprodukter för operation och sårbehandling. Företaget bedriver verksamhet i 30 länder och har sitt huvudkontor beläget i Göteborg. De senaste fem åren har bolaget expanderat kraftig och 2011 nådde omsättningen över 1014 MEUR. Vår respondent arbetar som Finance Process och Systems Manager. Då företaget verkar i många länder arbetar processamordnaren, som vi valt att benämna respondenten, med att samordna alla finansprocesser i bolaget.

4.6.1. ERP-system

Mölnlycke använder sig i första hand av SAP som affärssystem för verksamheten, men kompletterar även med ett BI-system från Cognos med delarna Cognos Planning samt Cognos Control för planering och rapportering. Processamordnaren förklarar hur den gemensamma systemstrukturen gör att de kan arbeta med liknande processer och sprida kunskapen genom organisationen. Även om valet av produktionssystem skiljer sig mellan tillverkningsenheterna sker all inrapportering genom SAP. Processamordnaren påpekar att oavsett om ett företag kör olika system eller samma system genom hela verksamheten så måste ändå viss integrering ske.

Processamordnaren är av den meningen att Mölnlycke är bra på att utnyttja de olika systemen, mycket på grund av att de i starten med stöd av deras tidigare ägare kunde ta fram nya processer som passade systemen. SAP implementerades precis när Mölnlycke blev egen verksamhet och hade då inga arv från gamla system att ta hänsyn till och kunde då, speciellt inom ekonomidelarna, ta mycket av arbetssättet. Systemen utvärderas inte så mycket, processamordnaren beskriver att företaget snarare börjar i andra ändan och ser till vad

processen kräver. Utifrån det kontrollerar de hur stödet för just detta ser ut i SAP först, för att sedan i andra hand söka en annan lösning.

Processamordnaren anser att ledningen är engagerad i företagets IT-frågor och att det faktum att hennes tjänst nyligen har tillkommit är ett bevis på detta. Tidigare fanns företagets CIO med i ledningsgruppen men har nu ersatts av en CFO med IT-ansvar. Då Mölnlycke verkar i en bransch med överlag hårda compliance-krav är det enligt processamordnaren viktigt att ha tillförlitliga system.

4.6.2. Automatiska kontroller

På grund av Mölnlyckes stora tillväxt under de senaste åren har numera företaget bolag på geografiskt större avstånd och fler anställda. Processamordnaren beskriver hur företaget, för att kunna arbeta i samma processer och ha ett gemensamt lärande, är beroende av att systemen ser ut på samma sätt, först då kan de börja arbeta med att förbättra sina processer. Målet är att de processer som redan finns i ekonomisystemen ska följas, det är viktigt att föra kunskapen om processerna vidare. Skillnader i processerna kan exempelvis ge utslag i den finansiella rapporteringen.

Mölnlycke har en grundstruktur för den finansiella rapporteringen som processamordnaren beskriver som något av en automatisk kontroll i sig. I och med att de har en kontoplan vilken är central för alla bolagen måste rapporteringen ske likformigt.

”I och med att bokföringen sker enligt samma principer för alla blir det mycket lättare att granska. Vi har gemensamma sättningar för alla bolagen och det är väldigt lätt att se om ett bolag inte jobbar på det sättet som de ska” (Processamordnaren).

Enligt processamordnaren arbetar de mycket med automatiska kontroller delar där företaget styrs av legala krav, det vill säga fakturering och orderhantering. En del är fakturagodkännande vilken har en process där det alltid krävs två personers godkännande för att fakturan ska kunna lämnas iväg till betalning. Inom detta ryms även en sättning för vilken limit varje ansvarig har befogenhet att signera. Processamordnaren beskriver hur systemet begränsar möjligheten till att göra utbetalningar till okända konton. Den ansvarige för utbetalning av fakturorna kan aldrig vara ansvarig för uppläggningen av masterdata om leverantören, vilket inbegriper kontonummer för utbetalningar, utan detta måste ske genom två olika anställda. Inom produktionen arbetar företaget med automatiska kontroller för bland annat forecasting. Prognoserna på beräknad försäljning kommande 24 månader är integrerade med produktions-planeringsmodulen. Detta för att säkerställa att produktionen är i relation till den prognosticerade försäljningen, vilken kan gå ner ändå på artikelnivå.

De automatiska kontrollerna testas inte på årlig basis eller med någon annan frekvens, enligt processamordnaren. Däremot genomgår de mycket tester innan de implementeras och vid eventuella förändringar, både i testmiljö och i produktionsmiljö. Behörigheterna ses dock över varje år, framförallt för att anställda byter tjänst och inte skall få för breda behörighetsområden.

”När man byter personer så måste man uppdatera tabeller, och då måste de testas om. Vi har bra kontroll, som dock alltid kan bli bättre. Vi har dels en kvalitetsfunktion som går in och gör interna revisioner och dels externa revisorer som går in och kontrollerar” (Processamordnaren).

Processamordnaren redogör för hur ett projekt med att skaffa sig bättre kontroll över behörigheterna ligger i fokus just nu. Mölnlycke vill konkretisera de tidigare ganska vida

behörigheterna för de anställda och begränsa vem som får se och göra olika saker. Det har varit ett stort arbete med att förbättra de roller som finns, man har utgått ifrån de behörighetsroller som finns i SAP och sedan anpassat dem efter Mölnlyckes arbetssätt. Hon reflekterar kring hur det skiljer sig mellan företagets mindre och större bolag, att de mindre bolagen måste kunna ha en lite flexiblare hantering för att skapa en bra process och att man då istället arbetar med mer sidoprocesser och interna kontroller i efterhand.

”Det går alltid att ha mer kontroll. Det handlar dock om en avvägning, hur mycket kontroll bygger vi in i systemen och hur mycket granskningar väljer vi att göra i efterhand. Vad är kostnaden för detta? Man kan alltid bygga in hur mycket kontroller som helst, men ger det mervärde?” (Processamordnaren).

4.6.3. Riskhantering

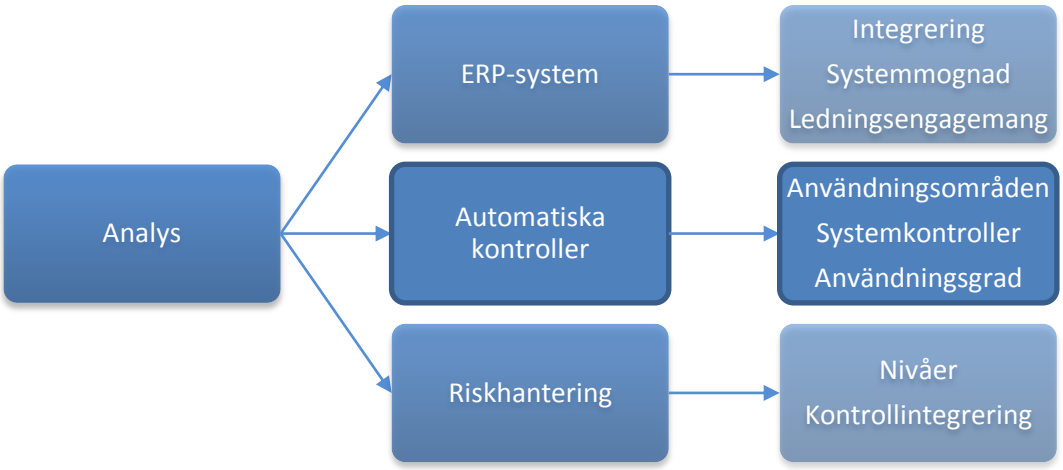
Inom Mölnlycke finns det ett utarbetat ramverk för riskhantering och de identifierar och följer upp sina risker inom alla de olika bolagen. Varje enhet får identifiera vad deras risker är, vilka sedan rapporteras till deras ansvarige för risk management. Inför varje budgetprocess stäms riskerna av så att det finns en koppling till budgeteringen. Processamordnaren beskriver hur arbetet med detta också numera är ett aktuellt område med mer fokus på. Hon poängterar den kopplingen som finns mellan de identifierade riskerna och forecasting/budgetering. Genom att löpande kontrollera att den prognostiserade försäljningen är i relation till tillverkningen minimeras risken att binda likvida medel och stå med onödigt stora lager. Automatiska kontroller betraktas som en viktig del av riskhanteringen i och med deras betydelse för att skapa ett säkert flöde och säkerställa att all finansiell data från de olika bolagen är enhetlig och korrekt.

5. Analys

Kapitlet inleds med en beskrivning av analysens upplägg och tillvägagångssätt. Utifrån de tre kategorier som valts, kommer vi koppla samma intervjuer från empirin med tidigare teorier och studier. Genom detta kan vi få en bild av vilka likheter och skillnader som finns, samt jämföra företagens förhållningssätt till automatiserade kontroller och riskhantering.

För att skapa en bra struktur och en överblick kommer analysen delas upp i de tre centrala begrepp vi tidigare har använt oss av i den teoretiska referensramen och den empiriska studien; *ERP-system*, *automatiska kontroller* och *riskhantering*. Med utgångspunkt i den teoretiska referensramen kommer vi att tolka vårt insamlade empiriska material. Under respektive begrepp diskuterar vi revisionsbyråernas syn på ämnet och huruvida det skiljer sig från eller liknar de responderade företagens olika tankar kring ämnena.

Vi kommer i vår analys använda oss av en analysmodell, se figur 3. Inom begreppet ERP-system kommer vi att analysera respondenternas syn på sin integrering och systemmognad i deras system. Integreringen berör bland annat hur respondenterna ser på användandet av kringverktyg i sina system eller att använda sig enbart av SAP. Med systemmognad menar vi i vilken utsträckning de använders sig av systemets delar och hur länge systemet har funnits på plats. Vi jämför även hur de ser på graden av ledningsengagemang inom IT och effekten av detta. Därefter tas analysen vidare till respondenternas automatiska kontroller, vilket är området vi kommer att lägga mest fokus på. Vi reflekterar dels kring inom vilka områden de väljer att använda sig av automatiserade kontroller samt i vilken grad de utnyttjar dem. Inom systemkontroller analyserar vi vilken struktur företagen har på utvärderingen av sina kontroller. Begreppen IT-generella kontroller och applikationskontroller är i fokus här. Vi jämför sedan respondenternas användningsgrad med hjälp av systemmognadsmodellen av Paulk et al. (1993). Till sist diskuterar vi respondenternas riskhantering i form av de olika ramverk och förhållningssätt det finns till detta. På vilka nivåer i organisationen väljer företaget att arbeta med riskhantering? Vi redogör även för hur respondenterna integrerar automtiska kontroller inom sina ERP-system för att minimera sina risker.



Figur 3, Analysmodell

5.1. ERP-system

Genom att använda sig av ERP-system kan företag uppnå effektivare processer, bättre kontroll och ökad datakvalité vilket kan optimera affärsverksamheten (Magnusson & Olsson, 2008). Även revisonsbyråerna anser att genom att utnyttja sitt ERP-system bättre kan dessa

effekter lättare uppnås (IT-revisor X, KPMG & riskkonsult B, Alfa). Många bolag använder sig dock av externa system för att utföra vissa moment vilka även hade kunnat utföras av de existerande ERP-systemen (IT-revisor X, KPMG). Detta är något som syns tydligt hos Nibe där de trots sitt SAP-system använder sig av flera olika kringverktyg för bland annat produktionsplanering och leverantörsreskontra. Duni och Mölnlycke har däremot valt att försöka begränsa användingen av extra system. Duni är mitt under ett pågående centraliseringsprojekt där de har valt att implementera SAP i hela koncernen. Hos Mölnlycke har man implementerat SAP i hela koncernen. De har en uttalad strategi att försöka integrera alla verksamhetens delar i SAP. Om detta inte är möjligt överväger de andra system. Magnusson och Olsson (2008) anser även de att ett företags processtruktur bör omarbetas för att passa systemet, detta kan leda till att processerna blir effektivare.

”SAP:s standardiserade transaktioner är som en motorväg där transaktionerna helst ska flyta på med så få avtagsvägar som möjligt” (Systemutvecklingschefen, Duni).

Riskkonsult B på Alfa belyser att utnyttjandegraden av sitt ERP-system har en direkt relation till vilken mognadsgrad företaget har. Parthasarathy och Ramachandran (2008) presenterar ett verktyg för att utvärdera företags systemmognad. På den lägsta nivån befinner sig företag vars fokus ligger på att förvalta befintliga system och planera hur ett nytt ERP-system ska kunna införas. På nästa nivå finns de företag som fokuserar på att förbättra integration och funktionaliteter i ett relativt nytt system. På Nibe har de nyligen infört SAP men använder sig även av ett flertal gamla system. För tillfället är systemen dåligt integrerade och de arbetar aktivt med att förbättra integrationen. Även Duni positionerar sig på det här steget då de är i ett systemskifte som förväntas öka integrationen och förbättra processerna. Verktygets högsta nivå innefattar företag vars fokus ligger på att optimera den strategiska potentialen av ERP-systemet. Mölnlycke, vilka har använt sig av SAP under flera år är det företag som fokuserar mest på att optimera ERP-användningen genom att samordna och standardisera alla koncernens processer. Processamordnaren på Mölnlycke beskriver också arbetet med att använda funktionaliteten i ERP-systemet till prognosförbättrande arbete, ytterligare ett steg i optimeringen. Att utnyttja sina system är dock ett komplicerat arbete, riskkonsult Y på Alfa påpekar att det är svårt att veta vilka möjligheter systemen kan erbjuda. Det kräver tid och resurser att ta tag i detta arbete.

En viktig del i optimeringen av ERP-systemet är ledningens engagemang. Lyckade IT-satsningar beror inte på slumpen, Neirotti och Paolucci (2007) menar att en rad korrekta investeringsbeslut av ledningen är grunden till framgång. En vanlig orsak till misslyckade ERP-implementationer kan enligt Lundberg (2009) vara att projektledare och mellanchefer under projektets gång tvingas fatta strategiska beslut bortom deras kompetenser. Att engagera sig i ERP-systemets utveckling ser inte ledningen på Nibe som sin starkaste sida. Reovisningsansvarig beskriver att IT-projekten initieras och underhålls av projektgrupper på avdelningsnivå. Emellanåt kan dock projekt med kortsiktig vinning få negativa effekter.

”Visst kan det emellanåt bli så att inköp hittar på projekt som är bra för dem men som kan haverera hela uppföljningen för oss” (Redovisningsansvarig, Nibe).

På Mölnlycke finns det i ledningen en stor medvetenhet om IT:s betydelse för organisationen. Processamordnaren menar att ett bevis på detta är att den tjänst hon innehar överhuvudtaget har skapats. Dock har företaget ersatt en tidigare CIO genom att flytta dennes arbetsuppgifter till CFO:n. En CIO är däremot tillsatt på Duni. Denna person finns dock inte representerad i företagsledningen, vilket systemutvecklingschefen anser vara ett tecken på att ledningen inte är särskilt IT-inriktade. Däremot ses IT som en viktig del i att supporta verksamheten. Lundberg (2009) påtalar vikten av att tillsätta en CIO för att säkerställa företagets långsiktiga

IT-utveckling. IT-revisor Z på KPMG upplever att ledningens uppgift bör vara att skapa en brygga mellan IT och verksamheten, på detta sätt ges de anställda förutsättningarna att driva IT-frågor. Om företaget har verksamhet i flera olika länder anser riskkonsult B vid Alfa att IT-frågor bör ligga i ledningens intresse då framgångsrika lösningar kan appliceras i hela koncernen.

5.2. Automatiska kontroller

5.2.1. Användningsområden

Automatiska kontroller har många olika användningsområden, Coderre (2005) nämner två centrala kategorier. Finansiella kontroller berör transaktionernas korrekthet och säkerhetskontroller innefattar alla former av intern och extern säkerhetshantering av systemen. IT-managementkonsulten från Ernst & Young har åsikten att automatiska kontroller förekommer främst inom de finansiella delarna av verksamheten då dessa inbegriper de transaktionstätaste processerna.

”Typiska automatiska kontroller eller applikationskontroller är logglistor, behörighets-styrning, vem får göra vad, in- och utdatakontroller, intervallkontroller, rimlighetskontroller och larm i systemet” (IT-revisor X, KPMG).

För att motverka bedrägerier beskriver Bierstaker et al. (2004) hur företag i detta arbete kan använda sig antingen av förebyggande eller upptäckande kontroller. Dye (2007) menar på att trenden rör sig alltmer mot förebyggande kontroller då företagen kan spara både tid och pengar på att upptäcka problemen innan de uppstår. Även revisionsbyråerna ser stora fördelar i att arbeta med en mer förebyggande kontrollstruktur. IT-managementkonsulten på Ernst & Young anser att förebyggande kontroller speglar själva syftet med automatiska kontroller och bidrar till att fel kan upptäckas redan innan skadan är skedd.

Det syns tydligt att även de tillverkande företagen har strategier för huruvida de vill arbeta med förebyggande eller upptäckande kontroller. På Duni råder en tydlig dominans av förebyggande kontroller, systemutvecklingschefen nämner som exempel att förutbestämda villkor vid bokningen av en faktura reducerar möjligheterna för att det ska uppstå fel senare i flödet. Trots den stora tilltron till förebyggande kontroller menar systemutvecklingschefen även att det är svårt att klara sig utan upptäckande kontroller. Med tanke på det stora antalet transaktioner som rör sig mellan modulerna krävs det även ett övervakningssystem som larmar ifall de uppsatta regelverken bryts.

”All form av skräp i systemet hamnar förr eller senare hos finans, vilket leder till att det viktigaste stället att upprätta automatiska kontroller inte är hos finans, utan tidigare i kedjan. Detta görs genom att till exempel arbeta med behörigheter och sätta upp kontroller av ordertyper och villkor som ska uppfyllas innan ordern får fortsätta i flödet” (Systemutvecklingschefen, Duni).

Mölnlyckes kontrollflora utmärks även den av en dominans av förebyggande kontroller. I dagsläget arbetar de på ett projekt för att förbättra kontrollen över behörigheterna, vilket enligt processamordnaren ska leda till en begränsning av vem som får lov att göra vad i systemet. Då Mölnlyckes dotterbolag skiljer sig i storlek och komplexitet menar processamordnaren dock att det är oundvikligt att utesluta de upptäckande kontrollerna då vissa av de mindre företagen kräver ett mer flexibelt arbetssätt varpå kontroller istället får genomföras i efterhand. Även Bierstaker et al. (2006) förespråkar att en effektiv kontrollsturktur bör innehålla både förebyggande och upptäckande kontroller. Den största anledningen till behovet av upptäckande kontroller är risken att anställda manipulerar konton i

redovisningen som bara kan upptäckas om dessa i efterhand utvärderas och matchas mot varandra (ibid.). Inom Nibe går det att identifiera en förebyggande strategi kring kontrollerna, vilket inte minst visar sig i säljprocessen där orders kan stoppas om kunden inte bedöms vara kapabel att betala fakturan. Denna kontroll fungerar dock informativt och kan enkelt kringgås av säljarna. Även på inköpssidan finns det inslag av förebyggande kontroller, fakturor som överskrider ett visst belopp skickas automatiskt till en chef för attestering. Upptäckande kontroller förekommer till viss del hos Nibe. Redovisningsansvarige berättar att faktureringsdata flyttas från ett försystem till SAP och om transaktionerna innehåller fel larmar systemet och en manuell uppföljning sker. Den här typen av kontroller är dock sällsynt hos Nibe då flera kringsystem inte är integrerade till SAP och överflyttning av data sker manuellt vilket kan leda till att fel värde skrivs in utan att upptäckas.

5.2.2. Systemkontroller

De två grundstenarna inom systemkontroller är IT-generella kontroller och applikations-kontroller (Daigle et al., 2005). Detta är också grunderna i revisionsbyråernas granskningar. Från både Alfa, Ernst & Young och KPMG beskrivs hur en IT-revision tar sin början i de IT-generella kontrollerna. IT-managementkonsulten på Ernst & Young påpekar att när ett företag har god hantering av de förändringar som sker i systemet, det så kallade Change management, ökar tillförlitligheten och ger tillit till applikationskontrollerna. Skillnaden mellan företagen i studien är tydlig inom detta område. Nibe hyser stor tilltro till att IT-avdelningen upptäcker fel genom sin erfarenhet medan Duni och Mölnlycke har mer utvecklade handlingsplaner för ändringshantering. Dunis systemutvecklingschef lägger ytterligare en betydelse i begreppet Change management. Han framhäver även det organisatoriska värdet av begreppet när han ska sälja in en förändring för ledning och personal som berörs av ändringarna.

En stor del i de IT-generella kontrollerna är behörighetshanteringen, kallat Segregation of Duties. Lightle och Waller Vallario (2003) menar på att SOD utgör en viktig del i princip alla företags interna kontrollsystem. Systemutvecklingschefen på Duni menar till och med att SOD är en av de viktigaste delarna inom automatiska kontroller. Han beskriver det arbete som skett med att fastställa behörigheterna i systemet som grundläggande och en grund för alla vidare processer. Då detta varit fokus hos företaget under längre tid har de ett mer utvecklat ramverk för SOD än de båda andra företagen. Mölnlycke arbetar med att utveckla sin behörighetshantering. Från att vara ganska vida har de precis som Duni utgått från behörigheterna som finns fördefinierade i SAP och anpassat dessa. Nibe använder sig av behörigheteter inom fakturahanteringen där det regleras vem som kan attestera vad och är det företag i studien som utnyttjar SOD minst. Revisionsbyrån Alfa menar att med hjälp av SOD kan risken för fel blir mindre, rätt person genomför då uppgiften och skapar tillförlitligare transaktioner vilket revisionsbyrån med hjälp av ett verktyg kan utvärdera. Lightle och Waller Vallario (2003) beskriver hur företagen själva, med hjälp av internrevisorer arbetar med att identifiera potentiella SOD-konflikter och göra rekommendationer till företagen hur dessa kan minskas.

Applikationskontrollerna är de kontroller som automatiskt körs i de olika applikationerna (Daigle et al., 2005). Under begreppet inkluderas de tre kontrolltyperna inputkontroller, processkontroller och outputkontroller. Inputkontrollerna som kontrollerar vad som förs in i systemet är den typen av kontroller som respondenterna främst använder sig av. På Duni bygger order till faktureringensprocessen på ett flöde där det hela tiden skapas nya dokument mellan transaktionerna. En order kan inte faktureras förrän den har levererats. När leveransen bekräftats skapas ett nytt transaktionsdokument som är redo för att faktureras, vilket medför att olevererade order inte kan bli fakturerade av misstag. Inputkontroller ser vi även i stor

utsträckning hos samtliga respondenter i form av grundstrukturen i den finansiella rapporteringen. De olika bolagen i Nibe rapporterar dock inte i samma system, vilket försvårar uppföljningen. Duni och Mölnlycke arbetar mycket med att begränsa möjligheterna till felaktiga inmatningar snarare än att använda sig av uppföljande kontroller. Även Namiri och Stojanovic (2007) lyfter fram syftet att förhindra och upptäcka obehöriga transaktioner med applikationskontrollerna. Processamordnaren på Mölnlycke beskriver hur redovisningen ska ske likformigt i hela koncernen.

”I och med att bokföringen sker enligt samma principer för alla blir det mycket lättare att granska. Vi har gemensamma sättningar för alla bolagen och det är väldigt lätt att se om ett bolag inte jobbar på det sätt som de ska” (Processamornaren, Mölnlycke).

5.2.3. Användningsgrad

Mognadsgraden inom interna kontroller handlar främst om hur bra företaget är på att involvera sina system i processförbättringarna (Debreceny, 2006). Revisionsbyråerna är alla noga med att betona vikten av att förstå processerna i företaget för att kunna skapa effektiva kontroller. Riskkonsult A på Alfa menar också att det är viktigt för företaget att känna till sina system och förstå vilka möjligheter som finns. Även processamordnaren på Mölnlycke beskriver arbetet med att utnyttja sina system vid att man utgår från vad processen kräver och efter det utvärderar SAP:s möjligheter att stödja denna process. Paulk et al. (1993) menar att ett företag befinner sig på någon av de fem nivåerna mellan initierad och optimerad gällande användningen av sina system för att optimera verksamheten. På den lägsta nivån karaktäriseras företagen av individtänk före organisatoriskt tänk. Redovisningsansvarig på Nibe redogör för hur projekt inom företaget föds och drivs på avdelningsnivå, vilket kan leda till suboptimering. Paulk et al. (1993) menar vidare att projektens framgång är helt beroende av de involverade personernas kompetens. Nibe gör inga tester av sina kontroller utan har en stark tilltro till att IT-avdelningen med hjälp av sin erfarenhet upptäcker felaktigheter.

På den repeterbara nivån har företaget oftast upprättat policies och tar lärdom av tidigare projekt (Paulk et al., 1993). Duni driver sedan tio år tillbaka ett implementeringsprojekt där SAP införs efterhand i alla koncernens bolag. Genom att ta lärdom av varje delprojekt menar systemutvecklingschefen att kontroller och behörigheter kan utvecklas för varje nytt projekt. Tredje nivån i femstegsmodellen inbegriper väl definierade processer, standardisering av systemen samt en tydlig strategisk riktning (Paulk et al., 1993). Både respondenterna på Duni och Mölnlycke poängterar vikten av att använda sig av systemens standardiserade lösningar för att skapa en organisatorisk konsekvens. Processamordnaren på Mölnlycke talar om fördelen med ett enhetligt systemanvändande i hela organisationen och hur de då kan utveckla sina processer. Målet är att genom väldokumenterade processer sprida företagets vision om ett effektivt och enhetligt arbetsätt vilket i sin tur kan underlätta kontroller av transaktioner. På fjärde nivån beskriver Paulk et al. (1993) att företaget enkelt kan upptäcka och spåra avvikelser i transaktionerna.

Revisionsbyrån Alfa har utvecklat en modell för att bedöma mognadsnivån i deras kunders systemanvändning och interna kontroller. Modellen har många gemensamma nämnare med femstegsmodellen Paulk et al. (1993) förespråkar. En parameter i denna modell är användningen av automatiska kontroller. Riskkonsult A på Alfa menar att de flesta av deras kunder som inte styrs av SOX hamnar någonstans på mitten av skalan, det vill säga att det finns en hel del kontroller på plats men det finns även mycket att förbättra.

”Det heter optimerat för att företaget måste ta ställning till var ’den gyllene medelvägen’ finns för dem. Det ska vara effektivt, inte outhärdligt att arbeta i systemen och processerna. Det ska vara optimerat, inte totaliserat” (Riskkonsult A, Alfa).

5.3. Riskhantering

Företagsövergripande riskhantering är en central del i det strategiska arbetet och Mikes (2009) beskriver att syftet är att involvera hela verksamheten på alla nivåer i företaget. Dock måste initiativet komma ifrån ledningen i en top-down-process (ibid.). Samma tankar har IT-managementkonsulten på Ernst & Young, han påpekar att det måste vara ledningen som sätter ambitionsnivån och hela kulturen kring riskhanteringen. Företagen i studien har olika syn på riskhanteringen. På Mölnlycke har ledningen tillsatt en riskmanager som har ansvaret för den övergripande riskhanteringen. Processamordnaren beskriver hur de själva har utarbetat ett ramverk för riskhantering där riskmanagern är centralt placerad. Nibe har inte samma ledningsengagemang men har istället tillsatta projektgrupper vilka arbetar med företagsövergripande riskhantering. Controllern exemplifierar att det kan röra sig om produktionsmiljön med dess inbegripna risker. Ledningen blir involverad främst då det rör sig om att godkänna investeringar av större belopp som berör riskhanteringsarbetet. Duni har enligt systemutvecklingschefen inte något ramverk de följer utan använder sig av praxis och erfarenheter. Han menar att de arbetar på riskhantering generellt genom företaget, på hans nivå exemplifieras detta av behörighetshanteringen.

Riskhantering handlar om att kunna förutse och hantera risker, men även att kunna se möjligheterna med desamma. En bättre riskanalys kan enligt Galloway och Funston (2000) göra att företaget kan hantera och exponera sig för risker de tidigare undvikit. Riskkonsult B på Alfa diskuterar även möjligheterna med risker och menar med detta att då företaget ser det riskfyllda kan de även se möjligheten till att utföra en uppgift på ett bättre sätt. Systemutvecklingschefen på Duni uttrycker en mer försiktig bild och hävdar att till varje möjlighet en användare har att utföra en uppgift i systemet kopplas det en risk.

Integreringen av automatiska kontroller inom riskhanteringen appliceras enligt Deloitte (2010) lämpligast där de gör störst nytta, på bolagens operationella nivå. IT-managementkonsulten på Ernst & Young påpekar hur det ska vara en naturlig del för företaget att få in fler automatiska kontroller i riskhanteringsarbetet, och menar att det blir lättare att följa upp och få en bättre överblick över sitt risklandskap. En gemensam nämnare hos både revisionsbyråerna och företagen är fokuseringen på den finansiella tillförlitligheten. Validiteten i den finansiella rapporteringen utgör en av fyra hörnstenar inom ramverket ERM (O’Donell, 2005). Processamordnaren på Mölnlycke uttrycker vikten av att ha korrekt finansiell information, och hon påpekar kopplingen som finns mellan riskerna och budgeteringen/forecastingen. Med hjälp av automatiska kontroller i riskhanteringen kan Mölnlycke minimera lager och kapitalbindning. Även controllern på Nibe anser att mycket av riskhanteringsarbetet berör de finansiella riskerna. Automatiska kontroller gällande sina kunders kreditvärdighet och soliditet är ett exempel på detta.

Oringel & Aldhizer (2009) betonar att varje företag är unikt och behöver skräddarsydda riskhanteringsrutiner, det är svårt att skapa ett ramverk som kan användas av alla. Duni arbetar även manuellt med att identifiera risker i systemet genom att leta efter systemnära transaktioner som bör exkluderas från rollfördelningsprofilerna. Systemutvecklingschefen menar på att all riskhantering är kopplad till behörighetssystemet och att detta spelar en central roll i arbetet med automatiska kontroller och sättningar.

5.4. Resultat av analys

Respondenterna i vår studie har alla olika förhållningssätt till automatiska kontroller och riskhantering. Revisionsbyråerna representerar utopin och vägen dit, då de har den specialiserade kunskapen om hur en optimerad användning ser ut och hur ett företag ska arbeta för att nå sitt mål. Gentemot den teoretiska referensramen är revisionsbyråernas tankar kring hur användingen av automatiska kontroller bör se ut gemensamma i många frågor.

Att ledningen har en inverkan på användningen av affärssystem och automatiska kontroller råder det inga tvivel om. De företag som har en IT-engagerad ledning har även kommit längre i arbetet med automatiska kontroller.

Gemensamt för alla bolagen är att de i olika former använder sig av automatiserade kontroller vilka är väl integrerade i deras arbetsrutiner. Företagen i vår studie är alla på olika nivåer i utvecklingen av de automatiserade kontrollerna. Mölnlycke driver aktivt ett projekt för att utveckla sina processer och arbeta på ett mer standardiserat sätt. Duni är likaså måna om att ha likartade processer inom hela koncernen. Nibe prioriterar däremot möjligheten för dotterbolagen att ha ett stort handlingsutrymme för att behålla entreprenörsandan. Beroende på sin situation har företagen olika strategier för hur de använder sig av automatiska kontroller. Företagen skiljer sig i uppdelningen mellan förebyggande och upptäckande kontroller. Två av företagen strävar i större utsträckning mot att ha förebyggande medan det tredje företaget för tillfället håller på att utveckla upptäckande kontroller.

Både företagen och revisionsbyråerna anser att behörighetshanteringen är en viktig del i processen med att skapa en säker och tillförlitlig finansiell information. Att arbeta med SOD begränsar medarbetarnas möjligheter att av misstag eller med uppsåt manipulera transaktioner. Samtliga företag använder sig främst av automatiserade kontroller inom de finansiella områdena, vilket även respondenterna från revisionsbyråerna uttrycker är vanligast förekommande. Revisionsbyråerna betonar alla i olika ordalag att företagen måste söka efter ”den gyllene medelvägen” när det gäller intern kontroll, systemet de arbetar i bör både vara effektivt och kontrollerat för företaget.

Huvudbegrepp och underbegrepp	Nibe AB	Duni AB	Mölnlycke Health Care AB
ERP-system			
Integrering	Låg integrering SAP	Hög integrering SAP	Hög integrering SAP
Systemmognad	Lägre nivå, nyligen implementerat SAP till fåtal dotterbolag	Medelnivå, implementerar sedan tio år SAP i alla bolag	Medel/hög nivå, använder sig av SAP i alla bolag, samordnar koncernens processer
Ledningsengagemang	Ej aktivt engagerade i IT-frågor, arbetar i avdelningsprojekt	CIO är ej med i ledningsgruppen, IT ses som ett viktigt stöd för verksamheten	Tillsatt processamordnare, är aktivt engagerade i IT-frågor

Automatiska kontroller			
Användningsområden	Upptäckande kontroller	Förebyggande kontroller, upptäckande kontroller i mindre skala	Främst förebyggande men även upptäckande
Systemkontroller	Svag behörighets-hantering som försvåras av bred systemflora	Använder sig i stor utsträckning av behörigheter/SOD	Strävar mot bättre behörighetshantering
Användningsgrad	Initial	Repeterbar/definierad	Definierad/managed
Riskhantering			
Nivåer	På projektnivå, kan vara suboptimerande	Generellt hela företaget	Riskmanager som samlar information från alla enheter
Kontrollintegrering	Finansiella kopplingar som ex. kreditbedömningar	Framförallt en stark behörighetshantering	Även kopplat till budgetering och lagerplanering

6. Slutdiskussion

För att besvara vår problemställning, kommer vi i detta kapitel presentera de slutsatser vi drar av analysens resultat. Vi kommer att föra en diskussion kring ämnet och avsluta med de viktigaste bidragen samt förslag till fortsatt forskning.

Syftet med uppsatsen var att beskriva och analysera hur svenska tillverkande företag använder sig av automatiska kontroller i sina affärssystem för att motverka riskerna med felaktigheter i den finansiella rapporteringen. Vi har tagit avstamp främst i de tillverkande företagens syn men har även tagit del av revisionsbyråernas åsikter kring de automatiska kontrollerna. För att nå en förståelse för hur mycket optimeringen av affärssystemen betyder för företagen har vi även undersökt hur engagerade ledningen är i dessa frågor. Med ursprung i dessa tankar har vi ställt upp följande problemformulering och underfråga:

Hur använder sig svenska tillverkande företag av affärssystemens automatiska kontroller för att övervaka sina transaktioner och säkerställa en tillförlitlig finansiell rapportering?

6.1. Slutsatser

Företagen i studien utnyttjar sina ERP-system i olika utsträckning och har diversifierade uppfattningar om hur systemen bäst kan användas. Revisionsbyråerna påpekar att det finns en komplexitet med att utnyttja sina system till fullo, då det är ett tid- och resurskrävande arbete att optimera sitt ERP-system. Magnusson och Olssons (2008) tankar om hur ERP-systemen kan användas till att standardisera och effektivisera ett företags processer styrks av Duni och Mölnlyckes uttalade strategier att integrera alla delar av sin verksamhet i de standardiserade SAP-modulerna. Målet hos båda företagen är att följa SAP:s standardiserade transaktioner och minimera avvikelser från dessa processer. Ett av företagen i studien, Nibe har däremot valt att välja en annan strategi, systemens betydelse har hamnat i skuggan av dotterbolagens behov av handlingsfrihet, vilket medfört en stor systemflora och låg utnyttjandegrad av SAP-systemet. Med hjälp av vår studie kan vi konstatera att arbetet med automatiska kontroller inte tar sin början i själva kontrollerna, utan grundar sig i företagets strategier och processer.

Tidigare studier av Neirotti och Paolucci (2007) visar att lyckade IT-investeringar till stor del beror på ledningens engagemang, vilket även resultatet av vår studie påvisar. Vi har observerat tydliga samband mellan ledningens IT-engagemang och företagets utnyttjande av system där Duni och Mölnlycke utmärker sig med en högre utnyttjandegrad än Nibe. Trots att IT kunde vara starkare representerat i samtliga organisationer betraktar Duni och Mölnlyckes ledningar IT som ett viktigt verktyg för att stödja verksamheten. Detta uttrycks tydligt i deras centraliserande strategiprojekt där SAP används som ett medel för att förbättra processerna och integrera verksamhetens områden. På Nibe initieras integreringsprojekt av ekonomiavdelningen och ur deras synvinkel finns det en strävan efter att uppnå en bättre koppling mellan systemen. Ledningens engagemang i dessa projekt berör endast godkännandet av investeringen.

Paulk et al. (1993) redovisar i sin studie en femstegsmodell för företagens mognadsgrad i systemhanteringen. Vi har i vår analys av företagen noterat hur användningen av automatiska kontroller främst förekommer på skalans högre nivåer i modellen. Detta styrks av revisionsbyråernas uppfattning av vikten att förstå processerna i företaget för att därefter kunna upprätta effektiva kontroller i systemen. Studiens resultat visar att Mölnlycke är det företag som använt sig av SAP längst och dessutom placerar sig högst på skalan. Duni har en liknande systemstrategi men fokuserar för tillfället på att sprida SAP i hela organisationen.

Nibes fokus stämmer väl överens med skalans lägre nivåer där ERP-systemet inte betraktas ur ett koncernmässigt helhetsperspektiv. Vi ser dock inte att något av företagen kan placeras på den optimerade nivån då den förutsätter att IT-förbättringar sker kontinuerligt och betraktas som strategiska affärsaktiviteter. Denna slutsats styrks av revisionsbyråernas uppfattning om att ej SOX-styrda företag oftast hamnar någonstans runt skalans mellersta steg.

I tidigare studier har Dye (2007) dragit slutsatsen att kontroller bör vara av förebyggande karaktär hellre än upptäckande. Bierstaker et al. (2004) är däremot av den mer kompromissande uppfattningen att en effektiv kontrollstruktur bör innehålla både förebyggande och upptäckande kontroller. Resultatet av vår studie visar att kontrollfloran bör anpassas efter företagets IT-struktur. I de fallen företaget har en låg grad av integration i sina moduler är behovet av upptäckande kontroller större då migrerad data måste kontrolleras när den rör sig mellan modulerna. Har företaget en högre integrationsgrad kan de med fördel använda sig av förebyggande kontroller för att minimera tidskrävande uppföljningsarbete. Nibe representerar här det tidigare påståendet medan Duni och Mölnlycke står för det senare. Studiens sammantagna resultat visar på att kontrollerna bör bestå av en mix av både upptäckande och förebyggande kontroller, dock med tyngdpunkten åt de förebyggande. Företagen visar även på olika incitament för att inte exkludera de upptäckande kontrollerna. Det rör sig dels om att kontrollera systemnära transaktioner mellan modulerna, men även att öka flexibiliteten i de mindre dotterbolagen där alltför rigorösa kontroller kan medföra ohållbara arbetssätt. Denna slutsats styrks även av revisionsbyråernas rekommendationer att ett optimerat användande inte ska vara totaliserat.

En stor del av de förebyggande kontrollerna identifierar vi som behörighetshanteringen inom systemet. SAP har en bred uppsättning av fördefinierade roller vilka företagen utnyttjar i varierande grad. Lightle och Waller Vallarios (2003) teori om att SOD utgör en viktig del i princip alla företag kan vi till viss del verifiera. Duni betraktar SOD som en av de viktigaste delarna inom de automatiska kontrollerna där företaget kan begränsa möjligheterna till att felaktigheter uppstår, vilket är en större risk än att bedrägerier utförs av en medarbetare. Revisionsbyråerna menar att SOD säkerställer att uppgifter utförs av en behörig person och därmed ökar tillförlitligheten i redovisningen. Även Mölnlycke ser stora möjligheter med SOD och driver för närvarande ett projekt där syftet är att stärka och förbättra sina behörighetsroller. Nibe fokuserar däremot inte i samma utsträckning på att utveckla sina behörigheter vilket kan tolkas som att användningen av SOD kräver ett visst mått av systemmognad och ett i större utsträckning integrerat system.

Sammanfattningsvis drar vi slutsatsen att all användning av automatiserade kontroller handlar om att utveckla företagets riskhantering. Företagen i studien uttrycker vikten av att ha korrekt finansiell information och att riskhanteringsarbetet också berör de finansiella riskerna. Likt Oringel och Aldhizer (2009) drar även vi slutsatsen att riskhanteringen uppvisar stora skillnader beroende på vilket företag och vilken respondent som studeras. Automatiska kontroller och behörighetshantering är olika sätt att hantera finansiella risker vilket medför att företagen i studien använder sig av olika tekniker i sitt riskhanteringsarbete.

6.2. Studiens bidrag

Resultatet av den här studien grundar sig helt på de företag och respondenter som varit delaktiga. Det går därför inte att påstå att våra slutsatser kan appliceras på andra företag. Däremot hoppas vi att flera företag kan använda vårt resultat för att öka sina kunskaper om automatiska kontroller. Våra bidrag är:

- För att lyckas med automatiska kontroller krävs att kontrollerna ligger i linje med de behov som finns i organisationen. För att utveckla kontrollerna och gå mot en optimerad grad av användning krävs en hög systemmognad.
- För att skapa en god kontrollstruktur krävs ledningens stöd och engagemang i IT-arbetet samt att IT betraktas som ett strategiskt stöd för verksamheten.
- De automatiska kontrollernas utformning beror till stor del på företagets IT-infrastruktur. En bred systemflora kräver mer upptäckande kontroller medan ett i större utsträckning integrerat system kan utnyttja förebyggande kontroller. En kombination av dessa krävs dock för att täcka in hela verksamheten.
- Det finns en större oro för okunskap än bedrägerier bland företagen i studien. Segregation of Duties betraktas av respondenterna som det effektivaste sättet att undvika oavsiktliga fel av medarbetare i den finansiella rapporteringen.

6.3. Förslag till fortsatt forskning

Vi har under intervjuerna med revisionsbyråerna fått en inblick i respondenternas arbetsuppgifter. En intressant aspekt är att samtligas arbetsområden innefattar både revisionsgranskning och även konsultarbete åt kunder som inte innefattas i revisionsuppdragen. Det första arbetsområdet ställer krav på konsulternas oberoende vilket skulle göra det intressant att undersöka hur det fungerar att växla mellan rollen som revisor och konsult. Andra områden som vore intressanta att utforska är:

- Hur kan revisionsbyråerna hjälpa företagen att uppnå den optimerade nivån av användning?
- Kan alla företag nå upp till en optimerad nivå av användningen av automatiska kontroller?

Referenslista

Abrams, C., von Känel, J., Müller, B., Pfitzmann, B., & Ruschka-Taylor, S. (2007). *Optimized Enterprise Risk Management.* Rüschlikon: Zurich Research Laboratory.

Alvesson, M., & Sköldberg, K. (2008). *Tolkning och reflektion- Vetenskapsfilosofi och kvalitativ metod.* Lund: Studentlitteratur AB.

Arnslätt, S., & Karlsson, H. (2010). *IT-revisorns bidrag till IT-styrning - Magisteruppsats.* Lund: Ekonomihögskolan Lunds universitet.

Ballou, B., & Heitger, D. L. (2005). A building-block approach for implementing COSO's Enterprise Risk Management- Integrated Framework. *Management Accounting quarterly, 6*, Sid. 1-11.

Bellino, C., Wells, J., & Hunt, S. (2007). Auditing Application Controls. *Global Technology Audit Guide*, 1-28.

Bierstaker, J. L., Brody, R. G., & Pacini, C. (2006). Accountants' perception regarding fraud detection and prevention methods. *Manegerial Auditing Journal, 21*, 520-535.

Bierstaker, J. L., Burnaby, P., & Hass, S. (2004). Internal auditors' fraud prevention and detection methods. *Internal Auditing, 19*, 37-40.

Braun, R. L., & Davis, H. E. (2003). Computer-assisted audit tools and techniques: analysis and perspectives. *Emerald Managerial Auditing Journal*, Sid. 725-731.

Catt, P. M., Barbour, R. H., & Robb, D. J. (2008). Assessing forecast model performance in an ERP. *Industrial Management & Data Systems, Vol. 108*, Sid. 677-697.

Coderre, D. (1996). Testing Application Controls. *The Internal Auditor, 53*, 18-20.

Coderre, D. (2005). Continuous auditing: Implications for assurance, monotoring and risk assessment. *Global Technology Audit Guide, Vol.10*, Sid. 1-33.

COSO, 1. (u.d.). *http://www.coso.org/IC-IntegratedFramework-summary.htm.* Hämtat den 03 03 2012

COSO, Committee of Sponsoring Organizations of the treadway commisison. (den 01 02 2012). *Committee of Sponsoring Organizations of the treadway commisison*. Hämtat från http://www.coso.org/aboutus.htm.

Daigle, R. J., Kizirian, T., & Sneathen, L. D. (2005). System Controls Reliability and Assessment Effort. *International Journal of Auditing*, Sid. 79-90.

Debreceny, R. S. (2006). Re-engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls. *Proceednings of the 39th Hawaii International Conference on System Sciences*, Sid. 1-10.

Deegan, C., & Unerman, J. (2011). *Financial Accounting Theory.* Berkshire: McGraw-Hill Education.

Deloitte. (2010). *Continuous Monitoring and Continuous Auditing: From Idea To Implementation.* Deloitte Developement LLC.

Dye, K. M. (2007). Corruption and fraud detection by public sector auditors. *EDPACS*, 6-15.

Galloway, D., & Funston, R. (2000). The challenges of enterprise risk management. *Balance Sheet,* 22-25.

Hedman, J., Nilsson, X., & Westelius, F. (2009). *Temperaturen på affärssystem i Sverige.* Lund: Studentlitteratur.

Holland, C., & Light, B. (2001). A Stage Maturity Model for Enterprise Resource Planning Systems Use. *The Database for Advances in Information Systems, Vol. 32*, Sid. 34-45.

Hunt, R., & Jackson, M. (2010). An introduction to continuous controls monitoring. *Computer Fraud & Security*, Sid. 16-19.

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

Kollegiet för svensk bolagsstyrning. (den 1 Februari 2010). Svensk kod för bolagsstyrning. Stockholm.

KPMG. (2009). *IT Audit perspectives on Continuous auditing/Continuous monitoring.* KPMG LLP U.S.

Kuhn, J. J., & Sutton, S. (2010). Continuous auditing in ERP Systems Environments: The Current State and Future Directions. *Journal of Information Systems, Vol.24*, Sid. 91-112.

Lightle, S. S., & Waller Vallario, C. (2003). Segregation of Duties in ERP. *The internal Auditor,* 27-31.

Lundberg, D. (2009). *IT och affärsnytta.* Lund: Studentlitteratur.

Magnusson, J., & Olsson, B. (2008). *Affärssystem.* Studentlitteratur.

Markus, M. L., & Tanis, C. (2000). The Enterprise System Experience- From Adoption to Success. *In Framing the Domains of IT Management: Projecting the Future Through the Past*, 173-207.

McCollum, T. (2002). Applications Control. *The Internal Auditor, 59,* 23-25.

Mikes, A. (2009). Risk management and calculative cultures. *Management accounting research, 20*, 18-40.

Namiri, K., & Stojanovic, N. (2007). *A Formal Approach for Internal Controls Compliance in Business Processes.* 8th workshop in Business Process Modelling.

Neirotti, P., & Paolucci, E. (2007). Assessing the strategic value of Information Technology: An analysis on the insurance sector. *Information & Management, 44*, 568-582.

Niklasson, U . (den 28 Mars 2012). *Erfarenheter från en SAP Process Controls implementation.* SAPSA Vårimpuls - SAP:s svenska användarförening, Malmö.

Norman, C. S., Payne, M. D., & Vendrzyk, V. P. (2009). Assesing Information Technology General Control Risk: An instructional Case. *Issues in Accounting Education, 24*(1), 63-76.

O'Donell, E. (2005). , Enterprise Risk Management: A Systems-Thinking Framework for the Event Identification Phase. *International Journal of Accounting Information Systems*, 177-195.

Olhager, J., & Selldin, E. (2003). Enterprise resource planning survey on Swedish manufacturing systems. *European Journal of Operational Research*, Sid. 365-373.

Oringel, J., & Aldhizer, G. R. (2009). Continuous Auditing and Monitoring- Enhancing the effeicency and effectiveness of auditing and ERM. *Internal Auditing, Septermber-October*, Sid. 17-26.

Parthasarathy, S., & Ramachandran , M. (2008). Requirements Engineering Method and Maturity Model for ERP Projects. *International Journal of Enterprise Information Systems, Vol. 4*, Sid. 1-15.

Patel, R., & Davidsson, B. (2003). *Forskningsmetodikens grunder- att planera,genomföra och rapportera en undersökning.* Lund: Studentlitteratur.

Paulk, M. C., Weber, C. V., Chrissis, M. B., & Curtis, B. (1993). Key Practices of the Capability Maturity Model. *Journal of Software IEEE, Vol. 10*, Sid. 18-27.

PricewaterhouseCoopers. (2009a). *Extending Enterprise Risk Management (ERM) to adress emerging risks.* PricewaterhouseCoopers in collaboration with its partners.

PricewaterhouseCoopers. (2009b). *Styrelsens och bolagsledningens arbete med värdeskapande riskhantering och intern kontroll.* PricewaterhouseCoopers i Sverige AB.

Ramaswamy, V., & Leavins, J. (2007). Continuous auditing, digital analysis and Benford's Law. *Internal Auditing*, 25-31.

Roland, H. (2007). Using automated controls to ensure better, faster, cheaper audits. *Financial executive, November*, Sid. 50-53.

Segal, S. (2006). Value-based enterprise risk management: The key to unlocking ERM potential. *Corporate finance review*, 16-26.

Sevenius, R. (2007). *Bolagsstyrning.* Lund: Studentlitteratur.

Tarantilis, C. D., Kiranoudis, C. T., & Tehodorakopoulos, N. D. (2008). A Webbased ERP-system for Business Services and Supply Chain Management: Application to Real-World Process Scheduling. *European Journal of Operational Research*, Sid. 1310-1326.

Turner, L. D., & Owhoso, V. (2009). Use ERP Internal Control Exception Report and Improve Controls. *Management Accounting Quarterly, Vol 10 Nr. 3*, Sid. 1-15.

Umble, E. J., Haft, R. R., & Umble, M. M. (2003). Enterprise resource planning: Implementation procedures and critical success factors. *European journal of operational research*, 241-257.

Vendrzyk, V. P., & Bagranoff, N. A. (2003). The evolving role of is audit: A field study comparing the perceptions of IS and financial auditors. *Advances in accounting, 20*, 141-163.

Watts, S., & Henderson, J. C. (2006). Innovative IT climates: CIO perspectives. *Journal of Strategic Information Systems, 15*, 125-151.

Wiedersheim-Paul, F., & Eriksson, L. T. (2011). *Att utreda forska och rapportera.* Malmö: Liber AB.

Yang, H. (2000). An integrated risk management method: VaR approach. *Multinational Finance Journal, 4*, 201-219.

Intervjukällor

Tillverkande företag:

Systemutvecklingschef. Duni AB. 2012-03-28
Controller. Nibe AB, 2012-04-04
Redovisningsansvarig. Nibe AB. 2012-04-04
Processamordnare. Mölnlycke Healthcare AB. 2012-04-10

Revisionsbyråer:

IT-managementkonsult. Ernst & Young. 2012-03-16
IT-revisor X. KPMG. 2012-03-29
IT-revisor Y. KPMG. 2012-03-29
IT-revisor Z. KPMG. 2012-03-29
Riskkonsult A. Revisonsbyrån Alfa. 2012-03-29
Riskkonsult B. Revisionsbyrån Alfa. 2012-03-29

Bilaga 1: Intervjuguide – företag

Intervjun kommer vara en del av vår empiri i vår kandidatuppsats kring användandet av automatiska kontroller i affärssystem. Intervjun är uppdelad i fyra teman; bakgrund, ERP-system, automatiska kontroller samt riskhantering. Vi har valt att avgränsa oss till stora svenska företag vilka inte är styrda av SOX. Vi vill på förhand tacka för att ni väljer att medverka!

Bakgrund

1. Berätta lite om er verksamhet.
2. Berätta lite om din arbetslivsbakgrund och nuvarande roll i företaget.

ERP-system

3. Vilket/vilka affärssystem använder ni er av i organisationen?
4. Hur väl tycker du att affärssystemets olika funktioner utnyttjas?
5. Hur gör ni för att utvärdera om ni utnyttjar ert affärssystem till fullo?
6. Hur upplever du att företagets ledning engagerar sig i optimeringen av affärssystemet?

Automatiska kontroller

7. I vilka områden/delar i affärssystemet är det möjligt (alt. lämpligt) att använda sig av automatiska kontroller?
8. Hur mycket använder ni er av automatiska kontroller i affärssystemet?
9. Beskriv tillvägagångssättet när ni utvärderar era automatiska kontroller.
10. Hur testar ni funktionaliteten i de automatiska kontrollerna? Hur ser ni att det är rätt kontroller som görs?

Riskhantering

11. Hur arbetar ni med riskhantering?
12. Arbetar ni efter ett utarbetat ramverk för riskhantering?
13. På vilka nivåer i företaget arbetar ni med riskhantering?
14. Hur kan automatiska kontroller involveras i riskhanteringsarbetet?
15. Vad kan integreringen av automatiska kontroller i ert företags riskhantering innebära?

Bilaga 2: Intervjuguide – revisionsbyrå

Intervjun kommer vara en del av empirin i vår kandidatuppsats kring användandet av automatiska kontroller i affärssystem. Intervjun är uppdelad i fyra teman; bakgrund, ERP-system, automatiska kontroller samt riskhantering. Vi har valt att avgränsa oss till stora svenska företag vilka inte är styrda av SOX. Vi vill på förhand tacka för att ni väljer att medverka!

Bakgrund

1. Berätta lite om er avdelnings verksamhet.
2. Berätta lite om er arbetslivsbakgrund och nuvarande roll i företaget.

ERP-system

3. Vilka affärssystem hjälper ni era kunder med att utvärdera?
4. Hur väl tycker ni överlag att företag utnyttjar sina affärssystems olika funktioner?
5. Hur gör ni för att utvärdera om kunden utnyttjar sitt affärssystem till fullo?
6. Hur upplever ni att företagens ledning engagerar sig i optimeringen av affärssystemet?
7. Hur bör företag generellt arbeta för att utnyttja sina affärssystem bättre?

Automatiska kontroller

8. I vilka områden/delar i affärssystemet är det möjligt (alt. lämpligt) att använda sig av automatiska kontroller?
9. Hur utbrett är användandet av automatiska kontroller bland era kunder (större svenska företag)?
10. Beskriv tillvägagångssättet när ni utvärderar era kunders automatiska kontroller.
11. Hur testar ni funktionaliteten i de automatiska kontrollerna? Hur ser ni att det är rätt kontroller som görs?
12. Hur kan automatiseringen av kontroller påverka kundens processer?

Riskhantering

13. På vilka nivåer i företaget är det mest kritiskt att arbeta med riskhantering?
14. Hur kan ett företag agera för att förbättra sin riskhantering?
15. Hur kan automatiska kontroller involveras i riskhanteringsarbetet?
16. Vad kan integreringen av automatiska kontroller i ett företags riskhantering innebära?