YRKESHÖGSKOLAN NOVIA

Intern kontroll inom Företag X

Ekonomiförvaltning

Johnny Granberg

Examensarbete för Tradenom (YH)-examen

Utbildningsprogrammet för företagsekonomi

Vasa 2017

EXAMENSARBETE

Författare: Johnny Granberg
Utbildning och ort: Företagsekonomi, Vasa
Inriktningsalternativ: Ekonomiförvaltning
Handledare: Anna-Lena Berglund

Titel: Intern kontroll inom Företag X

Datum:1.12.2017 Sidantal: 38 Bilaga 1

Abstrakt

Intresset för den interna kontrollen har hela tiden ökat till följd av olika skandaler inom både den privata och offentliga sektorn. Genom en god intern kontroll ökar organisationerna sina chanser att uppnå sina mål samtidigt som man blir mera effektiva och produktiva. Den interna kontrollen idag är en löpande process som utförs av styrelsen och ledningen såväl som av alla de övriga anställda.

Syftet med arbetet är att reda ut hur den interna kontrollen ser ut idag i Företag X och sedan komma med förbättringspunkter man borde införa. I teoridelen framkommer vad som menas med intern kontroll och arbetet fokuserar främst på en modell, COSO-modellen som är den mest använda modell för intern kontroll. Arbetet tar även upp riskhantering och COSO:s modell för företagsövergripande riskhantering. Den empiriska delen består av en kvalitativ undersökning om hur den interna kontrollen ser ut i Företag X i dagens läge. Undersökningen är gjord med hjälp av en intervju.

Resultatet av arbetet är en checklista med punkter Företag X borde ändra på, men arbetet kan även fungera som en förtydling av vad intern kontroll är och hur man kan undersöka den i ett företag. Slutsatsen är att Företag X har en intern kontroll men att det finns områden företaget kunde göra förbättringar för att uppnå en god intern kontroll.

Språk: svenska Nyckelord: intern kontroll, COSO-modellen, riskhantering

---

OPINNÄYTETYÖ

Tekijä: Johnny Granberg
Koulutus ja paikkakunta: Liiketalous, Vaasa
Suuntautumisvaihtoehto: Taloushallinto
Ohjaaja: Anna-Lena Berglund

Nimike: Yritys X:n sisäinen valvonta

Päivämäärä: 1.12.2017 Sivumäärä: 38 Liitteet: 1

Tiivistelmä

Kiinnostus sisäistä valvontaa kohtaan on jatkuvasti lisääntynyt skandaalien myötä. Skandaaleja on ollut sekä yksityisellä että julkisella sektorilla. Hyvä sisäinen valvonta lisää organisaatioiden mahdollisuuksia saavuttaa tavoitteensa ja samalla hyvä sisäinen valvonta tekee organisaatiosta myös tehokkaamman ja tuottoisamman. Sisäinen valvonta on nykyään jatkuva prosessi, jonka toteutukseen osallistuvat yrityksen hallitus ja johto sekä myös kaikki muut työntekijät.

Opinnäytetyön tavoite on selvittää minkälaista sisäistä valvontaa Yritys X:ssä on ja antaa ehdotuksia, mitä Yritys X voisi tehdä parantaakseen sisäistä valvontaa. Teoriaosassa käydään läpi mitä sisäinen valvonta tarkoittaa. Keskitytään pääasiassa yhteen malliin, COSO-malliin, jotka on eniten käytetty sisäisen valvonnan malli. Lisäksi teoriaosassa käsitellään riskien hallintaa ja COSO:n mallia joka on yrityksen kokonaisvaltaista riskienhallintaa varten.

Empiirinen osa koostuu kvalitatiivisesta tutkimuksesta, jossa selvitetään minkälaista tämänhetkinen sisäinen valvonta on Yritys X:ssä. Tutkimus on tehty haastatteluna.
Opinnäytetyön lopputulos on lista asioista, jotka Yritys X:n tulisi muuttaa, mutta työ voi myös selventää mitä sisäinen valvonta on ja miten sitä voi tutkia. Lopputulos on, että Yritys X:ssä on sisäistä valvontaa, mutta hyvän sisäisen valvonnan saavuttamiseksi joitakin osa-alueita tulisi kehittää.

Kieli: ruotsi Avainsanat: sisäinen valvonta, COSO-malli, riskienhallinta

---

BACHELOR'S THESIS

Author: Johnny Granberg
Degree Programme: Bachelor of Business Administration
Specialization: Financial Administration
Supervisor: Anna-Lena Berglund

Title: Internal Control within Company X

Date:1.12.2017 Number of pages: 38 Appendix: 1

Abstract

The interest in internal control has increased in recent years due to various scandals in both the private and the public sector. Through good internal control, organizations can increase their chances of achieving their goals and at the same time become more efficient and productive. The internal control today is an ongoing process that is carried out by the management, board of directors and all of the employees.

The purpose of the thesis was to analyze what the internal control looks like today in Company X and then come up with points of improvements that should be implemented. The theoretical background showed what is meant by internal control. The thesis focused on primarily one model, the COSO-model which is the most used model for internal control. The thesis also presented risk management and COSO's model for enterprise risk management. The empirical part was based on a qualitative survey of what the internal control looks like in Company X today. The survey was done by means of an interview.

The result of the thesis was a checklist of things Company X should change. The thesis can also serve as an explanation of what internal control is and how to investigate it in a company. The conclusion was that Company X has a working internal control, but there were several areas that the company could improve to achieve a good internal control.

Language: Swedish Key word: internal control, COSO-model, risk management

---

Innehållsförteckning

1 Inledning 1
1.1 Syfte och problemformulering 1
1.2 Avgränsning 2
1.3 Forskningsmetod 2
2 Intern kontroll 3
2.1 Corporate governance 4
2.1.1 Rekommendation 25 – Internkontroll 5
2.1.2 Rekommendation 26 – Riskhantering 5
2.2 COSO-modellen 5
2.2.1 COSO:s ramverk 2013 6
2.2.2 Kontrollmiljö 7
2.2.3 Riskbedömning 9
2.2.4 Kontrollaktiviteter 10
2.2.5 Information & kommunikation 11
2.2.6 Övervakning 12
2.2.7 Olika roller 13
2.2.8 Nyttan med COSO:s ramverk 14
2.3 Värdet av god intern styrning och kontroll 15
2.4 Riskhantering 16
2.4.1 Riskbehandling & riskbedömning 16
2.5 Företagsövergripande riskhantering – Integrerat med strategi och prestanda. 18
2.5.1 COSO ERM 2017 18
2.5.2 Styrelsens och ledningens roll inom företagsövergripande riskhantering 21
2.5.3 Fördelar av företagsövergripande riskhantering 22
3 Empiriska delen 24
3.1 Intern kontroll inom Företag X 24
3.1.1 Kontrollmiljön 25
3.1.2 Riskbedömning 27
3.1.3 Kontrollaktiviteter 29
3.1.4 Information och kommunikation 32
3.1.5 Övervakning och uppföljning 33
3.1.6 Företagsövergripande riskhantering inom Företag X 34
4 Resultat och slutsats 35
4.1 Förslag till vidare forskning 36
5 Validitet och reliabilitet 36

6 Sammanfattning 37
Källförteckning 39
BILAGA

1 Inledning

Till följd av det informationssamhälle vi lever i och hur enkelt det är att få fram information om företag, rapporteras allt flera problem inom både den privata och offentliga sektorn. Till följd av detta har betydelsen för den interna kontrollen inom företag och organistationer ökat väsentligt.

I dagens läge ska den interna kontrollen vara en naturlig del av ett företags verksamhet för att fånga upp fel och brister. Genom att ett företag utformar, använder och följer upp sin interna kontroll kan det öka eller minska risker beroende på om man vill ta större risker eller om man väljer att kontrollera de befintliga riskerna. I dagens turbulenta och komplexa företagsvärld blir ett fungerande system för intern kontroll allt viktigare, då intressenter till en större del har blivit mer beroende av att ett företags system för intern kontroll fungerar. Idag förväntas ett företags ledning och styrelse ha kännedom om vad intern kontroll är samt hur den interna kontrollen fungerar i företaget.

I detta arbete undersökte jag den interna kontrollen inom Företag X som är ett tillverkningsföretag. Jag har även skapat en checklista för hur man kan förbättra den interna kontrollen inom företaget.

Företag X:s vision är att vara deras kunders föredragna partner för alla produkter i deras produktsortiment. För att vara detta är kvaliteten på alla plan inom organisationen väldigt viktig. För att hålla en bra kvalitet på sina produkter krävs också en bra intern kontroll.

1.1 Syfte och problemformulering

Eftersom intern kontroll kan uppfattas på olika sätt av olika personer inom ett företag kan detta leda till missförstånd och problem. Alla kanske inte ens vet vad intern kontroll innebär och hur man inom företaget jobbar på denna. Därför är det viktigt att det finns ett ramverk som fastställer målen samt utformningen av den interna kontrollen inom företaget.

Det finns riktlinjer och rekommendationer på hur den interna kontrollen ska utformas, användas samt uppföljas. Det finns även riktlinjer för vad som kännetecknar en god intern kontroll. Men till hur stor del ett företag väljer att tumma på kontrollen för att nå sina mål är upp till vart och ett. Och i hur stor utsträckning tar Företag X i beaktande den interna kontrollen när man lägger upp sina strategier och när man planerar verksamheten?

Syftet med detta arbete är dels att förklara och reda ut begreppet intern kontroll och ge en grundläggande inblick i ämnet. Men framförallt att kartlägga Företag X:s interna kontroll och ta fram lista med förbättringspunkter som ska kunna förbättra den interna kontrollen inom företaget.

1.2 Avgränsning

Inom intern kontroll finns det flera olika modeller som används. För att avgränsa området kommer detta arbete i huvudsak att fokusera på COSO:s ramverk för intern styrning och kontroll. Detta eftersom det i dagens läge är det mest använda ramverk i världen för intern styrning och kontroll.

Arbetet lyfter även fram riskhantering eftersom det är väldigt integrerat med intern styrning och kontroll. Även här har jag valt att utgå till största del från COSO:s företagsövergripande riskhantering.

Eftersom intern kontroll är ett väldigt brett område och det skulle gå att följa upp det mesta inom ett företag i den empiriska delen, kommer detta arbete begränsa sig till den interna kontrollen inom administrationen i företaget.

1.3 Forskningsmetod

I arbetets empiriska del har jag använt mej av en kvalitativ forskningsmetod. Undersökningen kommer att bestå av en intervju med företagets Business Controller. Frågorna i intervjun är baserade på COSO-modellen och jag har byggt upp intervjun och den empiriska delen utifrån de fem komponenterna i COSO-modellen. Jag har valt en kvalitativ metod för att jag endast har intervjuat en person och för att få så detaljerade och utvecklade svar som möjligt när jag reder ut hur den interna kontrollen ser ut i dagsläget i företaget. Den jag har valt att intervjua är den person som är mest insatt i intern kontroll på företaget och kan ge de grundligaste svaren om den i nuläget.

2 Intern kontroll

Traditionellt sett har man ofta kopplat ihop intern kontroll med endast företagets bokföring samt externa finansiella rapportering. Men i dagens läge har det en mycket vidare innebörd. Intern kontroll syftar idag till hur ett företag följer regler och lagar, om dess rapportering samt redovisning är tillförlitlig och även hur företaget når upp till sina mål man har lagt upp inom verksamheten gällande produktivitet och effektivitet. (Arwinge, 2015 s.13)

Den mest använda definitionen för intern kontroll är COSO:s:

” *Intern styrning och kontroll är en process utförd av en organisations styrelse, ledning och annan personal, utformad för att ge en rimlig försäkran om uppnåendet av mål som rör verksamheten, rapportering och följsamhet gentemot lagar och regler*” (COSO, 2013)

Intern kontroll kostar även för företaget dels i pengar men kan även i vissa fall hämma kreativiteten och innovationen i företaget. Men detta kan läggas i förhållande till att ett effektivt system för intern kontroll hjälper företaget genom att man identifierar risker, värderar risker samt hanterar risker. Detta i sin tur leder till större chans för framgång för företaget. Kontrollen måste alltså placeras dit den behövs för att göra så stor nytta som möjligt, en god och effektiv intern styrning och kontroll leder till att företaget har ett hållbart risktagande. (Arwinge, 2015 s.33)

När det pratas om intern kontroll pratar man ofta om ordning och reda, men detta är inte riktigt sanningen. Man kan säga att intern kontroll har fem kännetecken.

1. Mycket handlar om frågor för att uppnå sina verksamhetsmål. Alla företag har ju förstås ett vinstmål med verksamheten, men sedan har man även konkreta mål som gäller verksamheten. Dessa kan vara mål om kunder, marknader, personal etc. Här gäller det att ställa sig frågan om alla strävanden i företaget är nödvändiga för att nå målet. Målen ska vara tydliga och ju tydligare de är beskrivna desto lättare är det att fastställa vad den interna kontrollen ska säkerställa.

2. Sedan handlar det om att hantera risker för att målen inte uppnås, alltså saker som hindrar företaget eller organisationen från att uppnå de mål man satt upp. Här avser alltså risk både konsekvensen samt sannolikheten av att målen inte uppnås.

3. Fokus ska ligga på att hantera de viktigaste riskerna för att företaget eller organisationen inte ska uppnå sina mål. Man måste värdera olika risker gentemot varandra för att på så sätt få fram de viktigaste riskerna.

4. Ledningen för verksamheten måste visa sitt stöd för den interna kontrollen för att jobbet ska bli framgångsrikt

5. Man kännetecknar en god intern kontroll av att åtgärder och kontroller införs för att hantera identifierade risker. (Wikland, 2014 s.13)

Ett effektivt system för intern kontroll bidrar till personalens etiska ageranden och minskar möjligheterna till fel. Dock är inte den interna kontrollen alltid så effektiv. Vanliga tecken på en bristande intern kontroll är, ofullständig dokumentation, saknad av skriftlig policy, ofullständig dokumentation gällande arbetsuppgifter, otillräcklig fördelning av arbetsuppgifter, klagomål från kunder och en inaktiv ledning. (Ahokas, 2012 s. 22 – 23)

2.1 Corporate governance

Det finns ingen direkt definition av Corporate Governance. Man kan säga att Corporate governance är ett förvaltnings- och styrningssystem för ett bolag som definierar företagsledningens, alltså styrelsens och ledningens roll men även skyldigheter och förhållande till aktieägarna. Förenklat är det ett system som företagsverksamheten leds och kontrolleras med. (Värdepappersmarknadsföreningen, 2017)

Koden för bolagsstyrning i Finland är en samling av 25 rekommendationer om god förvaltningssed för börsbolag. Denna finns till för att komplettera de skyldigheter som finns lagstadgade och syftet med rekommendationerna är att upprätthålla och främja en hög kvalitet och internationell jämförbarhet i den finländska bolagsstyrningspraxisen. Man strävar efter att harmonisera börsbolagens förfaringssätt och främja öppenhet i fråga om bolagsstyrning och öppenhet. Investerare kan bilda sig en uppfattning om hur bolagsstyrningen är inom börsbolagen eftersom koden för bolagsstyrning förbättrar transparensen inom bolaget. Corporate governance rekommendationerna ger också vissa riktlinjer om bolagets interna kontroll och jag kommer att ta upp mera om dem nedan. (Värdepappersmarknadsföreningen, u.d.)

2.1.1 Rekommendation 25 – Internkontroll

Bolaget ska definiera verksamhetsprinciperna för den interna kontrollen – Styrelsen ska se till att bolaget i fråga dels har fastställt verksamhetsprinciperna för den interna kontrollen samt att bolaget följer upp hur den fungerar. Genom verksamhetsprinciperna för den interna kontrollen strävar man efter att i synnerhet den finansiella rapporteringen förverkligas, men man säkerställer även att bolagets målsättningar gällande strategi, praxis och verksamhet också förverkligas. Genom verksamhetsprinciperna vill man också säkerställa att bolaget följer lagar och regler och verksamhetsprinciperna för den interna kontrollen ska redovisas i bolagsstyrningsrapporten. (Värdepappersmarknadsföreningen, u.d.)

2.1.2 Rekommendation 26 – Riskhantering

Bolaget ska definiera de principer enligt vilka riskhanteringen har organiserats – Riskhanteringen är en del av bolagets styr- och övervakningssystem och finns till för att se till att risker identifieras, bedöms och uppföljs. Principerna för riskhanteringen ska fastställas för att vara effektiv. Det är viktigt för bolaget att ge ut tillräckligt med information gällande risker och riskhanteringen för att man ska kunna bedöma bolaget. Riskhanteringsprinciperna ska redogöras för i bolagsstyrningsrapporten och lagstiftningen kräver att bolagets verksamhetsberättelse ska innehålla en bedömning av de mest betydande riskerna. Bolaget ska dessutom beskriva betydande risker i anknytning till affärsverksamheten på kort sikt i sin regelbundna rapportering. (Värdepappersmarknadsföreningen, u.d.)

2.2 COSO-modellen

Till följd av flertalet stora börsskandaler under 1980-talet skapade man år 1985 en kommitté av fem profesionella organisationer för controllers, internrevisorer, externrevisorer samt andra företagsekonomer. Denna kommitté kallades för Treadway-kommissionen eller COSO. Man undersökte sedan orsakerna till de inträffade bedrägerierna och kom med en rapport 1987 som innehöll flertalet rekommendationer om åtgärder till detta. Rekommendationen innehöll t.ex förslag till lagreglering, krav på extern revisorer samt hur branschorganisationer och börsbolag själva kunde göra. Genom detta uppkom COSO som står för The Committee of the Sponsoring Organizations of the Treadway Commission. (Wikland, 2014 s.57 – 62; COSO, u.d.)

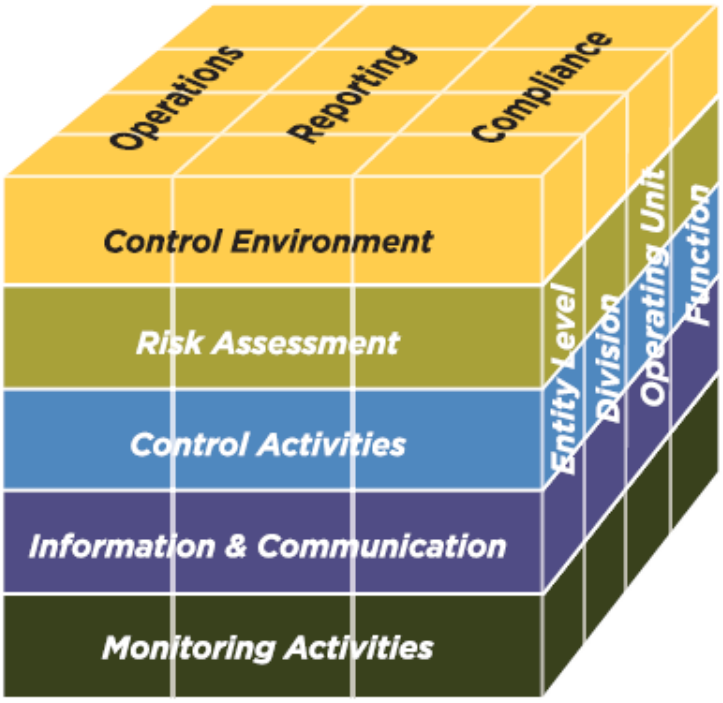
Intern styrning och kontroll betyder olika saker för olika personer och därför uppstår missförstånd mellan dem som arbetar i företag, lagstiftare, myndigheter, samt andra. Därför

valde COSO att skapa ett ramverk för intern styrning och kontroll, man ville etablera en gemensam definition inom området samt skapa en standard som alla företag och organisationer kan använda sig av oberoende om det är små eller stora företag inom den privata eller offentliga sektorn. (Wikland, 2014 s.57 – 62)

2.2.1 COSO:s ramverk 2013

Tjugo år efter det första ramverket COSO gav ut uppdaterades denna. Man reviderade sina standarder och komponenter utifrån erfarenheter och nya förutsättningar för företagen.

COSO-modellen består av fem komponenter, styr- och kontrollmiljö, riskbedömning, kontrollaktiviteter, information och kommunikation, samt övervakning. Dessa i sin tur har en del olika principer som ligger bakom varje komponent. Förutom dessa komponenter och de 17 principerna som ligger bakom varje komponent i COSO-modellen finns det även 87 fokuspunkter som stöd för de 17 principerna. I detta arbete kommer jag inte att gå in på alla de 87 fokuspunkterna utan istället sikta in mej på de huvudsakliga komponenterna samt de principer som ligger bakom dessa. (Wikland, 2014 s.74; Internrevisorerna, 2013)



Figur 1 COSO- modellen

I figur 1 ser man att COSO-modellen är uppbygg som en kub, överst finns de tre huvudsakliga målen för verksamheten, operationella mål, rapporteringsmål och efterlevnad

av lagar och regler. Sedan har man alla fem komponenter som modellen bygger på. På sidan av figuren hittar man organisationens olika delar man kan tillämpa modellen på den kan tillämpas på hela organisationen men även på en enskild funktion. (COSO, 2013; Internrevisorerna, 2013)

Det är av yttersta vikt att alla de fem komponenterna i den interna styrningen och kontrollen samverkar, för att uppnå en god intern styrning och kontroll måste alla fem komponenterna samverka. COSO:s ramverk fungerar som en helhet och komponenterna går väldigt mycket in i varandra, så om en komponent inte fungerar blir det en kedjereaktion som gör att det börjar brista i någon annan komponent också. (Wikland, 2014 s.63)

Utgångspunkten för intern styrning och kontroll är att företaget har satt upp olika mål. Har man inga mål blir t.ex. sökandet efter risker meningslöst. COSO skiljer på olika slags mål för företaget. Man har mål för rapportering och efterlevnad gentemot lagar och regler. Dessa är ganska lika eftersom det är externa krav på företaget som man måste anpassa sina mål till det är t.ex. lagstadgade krav på företaget. Sedan har man mål för verksamheten, vilka baserar sig på effektivitet och produktivitet. Målen för verksamheten lägger man upp internt och det är aldrig riktigt säkert att arbetet för att uppnå dessa mål ger det väntade resultatet mål som dessa kan vara t.ex. vinstmål, mål med personalen och produktionsmål. (Wikland, 2014 s.63)

2.2.2 Kontrollmiljö

Kontrollmiljön är den viktigaste komponenten av de fem. Kontrollmiljön anger tonen i en organisation. Det handlar mycket om att skapa roller och strukturer för den interna kontrollen inom företaget. Den ska skapa en medvetenhet om betydelsen av styr- och kontrollsignaler för medarbetarna inom företaget. Ledningen för företaget ska definiera, begränsa och utkräva ansvar för intern kontroll. Kontrollmiljön ligger som grund för hela företagets interna styrning och kontroll och därför är det så viktigt att man inom företaget förespråkar en sund kontrollmiljö. (COSO, 2013; Wikland, 2014)

Varje komponent i COSO:s ramverk består av olika många principer. Kontrollmiljön bygger på fem principer vilka förklarar innebörden med kontrollmiljön.

1. Organisationen demonstrerar ett engagemang för integritet och etiska värderingar. Ledningen i företaget måste skapa en arbetskultur som baserar sig på etiska värden, där man förklarar vad som är rätt och fel. Framför allt måste ledningen själva fungera som ett omdöme för andra. Ledningen måste skapa en sund riskkultur inom företaget,

detta innebär att man på samtliga nivåer kommunicerar hur viktigt det är att nyckelkontroller utförs. Det här resulterar i att det skapas en konsekvent kontrollkultur genom hela företaget. Företaget kan praktiskt sätta upp en etikpolicy som explicit redogör hur medarbetarna ska förhålla sig till etiska frågor och värderingar.

2. Styrelsen visar självständighet gentemot ledningen och övervakar utvecklingen samt resultaten av den interna kontrollen. Detta innebär att det är styrelsen som har det absoluta ansvaret för företaget. Styrelsen måste övervaka så att ledningen jobbar på den interna kontrollen. Detta kräver att styrelsen delar upp roller och ansvar för uppföljning av den interna kontrollen inom organisationen.

3. Ledingen etablerar, med översyn av styrelsen, strukturer, rapporteringslinjer och lämpliga befogenhets- och ansvarsfördelningar i strävan mot företagets mål. Ledningen ska alltså dela upp ansvaret och ge mandat åt medarbetarna. Att ge mandat åt lägre nivåer inom organisationen är ett måste. Det mesta beslutsfattandet görs på lägre nivåer och därför måste man ha mandat att kunna göra sitt jobb på bästa sätt. Men det är även viktigt att ledningen tänker igenom vad som kan gå fel när man ger generösare mandat åt flera medarbetare.

4. Organisationen visar ett engagemang att attrahera, utveckla samt behålla kompetenta individer i enlighet med deras mål. Detta innebär att kompetenskraven ska vara kända för olika arbetsuppgifter och de ska följas vid varje rekrytering. I den allt mera kunskapsbaserade ekonomin ska företaget också se till att utbilda och träna sina anställda så de hänger med i utvecklingen. För att den interna styrningen och kontrollen ska vara effektiv krävs det tydliga kompetenskrav med krav på prestationer och färdigheter och att dessa utvärderas i relation till de uppsatta målen för företaget och individen.

5. Organisationen håller individen ansvarig för deras ansvarsroller i den interna kontrollen i strävan mot målen. Ansvarsrollerna i företaget måste vara tydliga och klarlagda, varje medarbetare ska veta vad deras roll är och vad som krävs av dem, de måste också veta att det följs upp. (Arwinge, 2015 s.87 – 100; Wikland, 2014 s.66 – 68; COSO, 2013)

2.2.3 Riskbedömning

Den andra komponenten i COSO:s ramverk är riskbedömning, som även kallas kärnan i intern styrning och kontroll. Inom COSO ligger fokusen inom riskbedömningen på att ledningens och personalens förståelse och användning av riskbegreppet, den kombinerade effekten av konsekvens och sannolikhet. Detta för att därefter kunna hantera de största riskerna inom företaget. Riskbedömningen ska liksom nästan allt annat inom intern styrning och kontroll vara en integrerad process som sker löpande genom hela organisationen.(COSO, 2013; Wikland, 2014 s. 65)

Som utgångspunkt för riskbedömningen inom COSO har man målen för verksamheten och hur man ska uppnå dessa. Utifrån detta identifierar man risker och bedömer vilka som är allvarliga och vilka som kan vara acceptabla. För att detta ska fungera måste målen vara tydligt angivna. Faktorer som kan leda till att målen inte uppnås kan vara både externa t.ex. lagar och regler och teknologi. De kan även vara interna t.ex. generationsväxlingar, driftsstopp inom IT-system, brist på kompetents inom företaget. (Arwinge, 2015 s.103; Wikland, 2014 s. 65 – 66)

Inom komponenten riskbedömning finns det några saker som COSO speciellt lyfter fram. En risk i sig att uppmärksamma inom organisationen är om sambandet mellan hela organisationens mål och målen på de lägre nivåerna är oklara. Riskbilden inom företaget måste hela tiden omprövas till följd av att förutsättningarna för organisationen ständigt förändras och då ändras också riskbilden. Om mål formulerats som kraftigt höjer ambitionsnivån på verksamheten kan det innebära ökade risker. Om man inte har uttalat något specifikt mål för verksamheten kan det innebära att målet är att fortsätta som hittills. Till ett sådant mål är också risker knutna, t.ex om en konkurrent tar fram väsentligt bättre produkter kan ett sådant ”lågprofilmål” vara förenat med stora risker. (Wikland, 2014 s.65 – 66)

Precis som för de alla andra komponenterna inom COSO:s ramverk har finns det även principer som är kopplade till riskbedömningen, de är fyra stycken.

1. Organisationen specificerar mål med en tillräckligt tydligt för att möjliggöra identifiering och bedömning av risker som är relaterade till målen.

2. Organisationen identifierar risker för att målen för organisationen inte ska uppnås och analyserar risker som en grund för att bestämma hur riskerna ska hanteras. Man

ska alltså ha en fullständig riskinventering först för att sedan kunna gå vidare till hur de ska hanteras.

3. Organisationen bedömer risken för bedrägeri när man gör sin bedömning för riskerna att inte uppnå sina mål.

4. Organisationen identifierar och bedömer förändringar som signifikant kunde påverka systemet för intern kontroll. Man måste ta i beaktande inträffade, pågående och kommande förändringar när man gör sin riskbedömning. (Wikland, 2014 s.65 – 66; Committee of Sponsoring Organizations of the Tradeway Comission, 2013)

2.2.4 Kontrollaktiviteter

Kontrollaktiviteter hör till företagets riskbehandling, många har ofta stirrat sig blinda på olika kontrollaktiviteter såsom checklistor osv, vilket har lett till att det påverkat organisationen negativt. Kontrollaktiviteter är rutiner och riktlinjer som ska leda till att ledningens beslut förverkligas. (Wikland, 2014)

Kontrollaktiviteterna ska så långt som möjligt vara integrerade i verksamheten. De ska inte upplevas som något som gör att arbetet tar längre tid med påföljd att man lämnar dem i skymundan till slutet på arbetsdagen eller veckan. Kontrollaktiviteter kan t.ex. vara verifieringar, godkännanden, kontrollräkningar m.m. För att skapa riktigt effektiva kontrollaktiviteter ska man matcha dem mot verksamhetens mål, de viktigaste riskerna samt kontrollmiljön. (Wikland, 2014)

Kontrollaktivitets komponenten består av tre principer.

1. Organisationen väljer ut och utvecklar kontrollaktiviteter som bidrar till att minska riskerna för att inte uppnå målen till en acceptabel nivå. COSO nämner specifikt att kontrollaktiviteterna ska vara resultatet av aktiva val och föremål för utveckling, de ska inte vara sådana som man tycker att man alltid har gjort inom företaget.

2. Organisationen väljer ut och utvecklar generella kontroller över teknologin för att uppnåendet av sina mål. I dagens läge är IT en enorm del av företagens verksamhet, därför har COSO betonat vikten av att ha kontroll över IT som infrastruktur.

3. Organisationen genomför kontrollaktiviteter genom riktlinjer och polycies som fastställer vad som förväntas och procedurer som ser till att riktlinjerna följs. COSO betraktar riktlinjer och regler som kontrollaktiviteter inom ett företag. Men att bara

införa riktlinjer räcker inte. Man måste även se till att de efterföljs. (Wikland, 2014 s. 68 – 69; Committee of Sponsoring Organizations of the Tradeway Comission, 2013)

2.2.5 Information & kommunikation

Information och kommunikation är den stödjande komponenten inom intern styrning och kontroll. Information och kommunikation är en viktig del av ett fungerande företag, information håller ihop företaget och gör så de anställda kan göra sina arbetsuppgifter, ledningen kan styra och driva företaget samt gör så den interna styrningen och kontrollen kan fungera. (Arwinge, 2015 s.135)

Informationen i en organisation måste kunna flöda fritt genom hela organisationen, både uppåt och nedåt. Om informationen passerar fler än tre hierarkiska nivåer inom en organisation finns det stor risk att en del värdefull information filtreras bort under vägens gång. För att minska den bortfiltrerade informationen måste man inom företaget se till att det är högt i tak och att alla medarbetare känner att man vågar komma fram med känslig information utan att bli motarbetad. (Wikland, 2014 s.69)

Komponenten information och kommunikation består av tre principer, vilka är:

1. Organisationen erhåller eller genererar och använder relevant kvalitetssäkrad information för att stödja den fungerande interna kontrollen. Det gäller att kraven på information från de andra komponenterna är klara men även att man kan fånga upp informationen som behövs. Informationen bör vara kvalitetssäkrad, informationen ska gå att nå för den som behöver den, data ska vara tillförlitlig och korrekt, data ska hämtas tillräckligt ofta och den ska skyddas efter behov, den ska även finnas tillgänglig när den behövs.

2. Organisationen kommunicerar information internt, inklusive mål och ansvar för intern styrning och kontroll, som är nödvändiga för att stödja den fungerande interna kontrollen. Detta innebär att alla anställda ska få den information de behöver, så man vet sina ansvarsområden och roller. Styrelsen ska se till att man vet sitt ansvar och därefter kommunicera det vidare till VD:n som i sin tur kommunicerar vidare. Styrelsen ska även få den information man behöver. Hit hör också att det finns en visslarfunktion vid sidan av de övriga kommunikationskanalerna och att den

fungerar. En visslarfunktion är en neutral, öppen och säker kanal för den som misstänker missförhållanden inom organisationen.

3. Organisationen kommunicerar med externa parter om frågor som påverkar den fungerande interna kontrollen. Det innebär att företaget måste ha en process upprättad för att kommunicera med externa intressenter t.ex med börsen, myndigheter, underleverantörer och kunder. (Wikland, 2014 s.70; Committee of Sponsoring Organizations of the Tradeway Comission, 2013)

2.2.6 Övervakning

När organisationen lyckats skapa en god intern styrning och kontroll måste de se till att den övervakas så den inte försämras men även så man kan utveckla den. COSO lyfter fram tre saker som betecknar en bra övervakning; löpande uppföljning, separata utvärderingar och rapportering av avvikelser. Attityden till övervakning och uppföljning av intern kontroll härstammar från kontrollmiljön och anger tonen vid toppen Därifrån måste organisationen se till att alla vet sina roller och ansvar och på så sätt bildar detta basen i övervakningen. (Arwinge, 2015 s.147 – 148)

Övervakningen är den komponent som har störst förbättringspotential i COSO:s ramverk. Det finns otaliga sätt att övervaka den interna styrningen och kontrollen och det utvecklas hela tiden nya system och övervaknings rutiner. Övervakande rutiner inom företaget kan vara t.ex.

- Inbyggda och integrerade övervakningsprogram i företagets informationssystem.
- Regelbundna tester och utvärderingar av kontroller genom internrevision.
- Som en del av processen övergripande granskning av kontroller.
- Utvärderingar av styrelsen och ledningen i frågor som gäller klimatet inom organisationen och hur effektiva deras övervakande funktioner är. (Wikland, 2014)

Komponenten övervakning bygger i sin tur på två principer.

1. Organisationen väljer, utvecklar och utför löpande och separata utvärderingar för att säkerställa att komponenterna i den interna kontrollen finns och är fungerande. De uppföljningar eller utvärderingar som är löpande ska vara integrerade i verksamhetsprocesserna och beroende på hur snabbt verksamhetsprocesserna

förändras påverkas även valet av blandningen och omfattningen av utvärderingarna. Det ska även finnas objektiva separata utvärderingar för att på så sätt minska riskerna med att resultaten filtreras eller friseras.

2. Organisationen utvärderar och kommunicerar brister inom den interna kontrollen i god tid för de parter som berörs och är ansvariga för att ta korrigerande åtgärder. De parter som berörs inkluderar även styrelsen och ledningen. Detta innebär att när man hittar brister måste man kommunicera detta till dem som berörs så de kan vidta åtgärder och sedan ska även styrelsen och ledningen övervaka så dessa brister åtgärdas.

Det är övervakningen som knyter ihop alla komponenter så att de bildar ett fungerande system för intern styrning och kontroll. Genom att ha en bra övervakning kan organisationen i tid identifiera problem i den interna kontrollen och sedan åtgärda dessa. (Wikland, 2014 s 70 – 72; COSO, 2013)

2.2.7 Olika roller

COSO betonar flertalet gånger vikten av att alla i organisationen vet sina roller och ansvarsområden. Därför lyfter jag här fram roller och uppgifter för de som har störst del i en organisations interna styrning och kontroll.

- **Ledningen**: Den verkställande direktören för organisationen har det yttersta ansvaret för systemet intern styrning och kontroll. Det är VD:n som verkligen sätter tonen i toppen på en organisation och det är det viktigaste för en god kontrollmiljö. Den verkställande direktören kan göra detta genom att visa ledarskap och fastställa riktlinjer för de högre cheferna och granska hur de styr och kontrollerar verksamheten. Ekonomichefen har ofta en större roll att övervaka och verkställa kontroller genom hela organisationen. Ofta har även organisationens controller en betydande roll för den interna styrningen och kontrollen.

- **Styrelsen**: Det är styrelsen som ska vaka över att ledningen följer styrelsens riktlinjer och råd. Styrelsen kan göra detta genom att t.ex. ställa frågor till ledningen om hur det går med den interna kontrollen och om det finns något system. Det finns en risk att ledningen utövar för stor makt och kör över kontroller och struntar i att föra fram information från underordnande, detta måste styrelsen vara uppmärksamma på.

Slutligen är det styrelsen som har huvudansvaret för den interna styrningen och kontrollen.

- **Internrevisionen**: Internrevisorer har en roll som oberoende granskare av organisationen. De ska utvärdera hur effektiva kontrollsystemen är och bidra till den löpande effektiviteten. Internrevisorerna har direkt kontakt med styrelsen och ledningen och de har en viktig roll som övervakare av den interna kontrollen.

- **Övrig personal**: Hela personalen inom en organisation berörs av intern styrning och kontroll. Alla har sitt ansvar att förmedla information, avvikande från uppförandekoderna och andra problem som uppkommer inom organisationen till ledningen. Det ska även finnas kanaler för visselblåsare så att inga problem filtreras bort före de har hunnit fram till ledningen. (Internrevisorerna, 2013)

2.2.8 Nyttan med COSO:s ramverk

COSO:s ramverk ger flera fördelar för en organisation, dessa sammanfattas i fyra punkter i boken, Intern styrning och kontroll – Torbjörn Wikland.

1. En bra start för att förbättra den interna kontrollen är att dela upp behovet av intern kontroll i de fem komponenterna. Detta pekar ut fem nyckelområden att arbeta med. Komponenterna bör ses som en kedja och dessutom förtydligas de fem komponenterna med både principer och fokuspunkter.

2. Fungerar som ett verktyg för ledningen. COSO betonar att ju mera ledningen styr arbetet med intern kontroll och använder sig av resultaten från den löpande interna styrningen och kontrollen, desto mera nytta får man.

3. En markering att intern styrning och kontroll är uppbyggt av människor i sitt arbete och sina roller är en viktig del för att förstå vad som verkligen får den interna styrningen och kontrollen att fungera. COSO betonar flertalet gånger att kontrollmiljön har en central roll bland de fem komponenterna. Genom COSO:s syn på detta har även synen på kontroll utvidgats ordentligt. Detta har i sin tur lett till att betydelsen av preventiva kontroller lyfts fram samt att synsättet med mjuka och hårda kontroller kommit fram. Med hjäp av detta får man en mer övergripande bild av styrsignaler och hur de håller ihop och utvecklar organisationen.

4. Intern styrning och kontroll är väldigt riskbaserad, och COSO:s ramverk poängterar att riskmedvetenhet måste genomsyra allt arbete med den interna styrningen och kontrollen. Tidigare har man granskat kontroller i gigantiska och dyra projekt men sedan COSO:s ramverk kom ändrade de till stor del. Inom COSO:s ramverk ger man riskbedömningen en framträdande plats, genom detta kan man avgränsa och vägleda vilka kontroller som behöver granskas. (Wikland, 2014 s.79 – 81)

2.3 Värdet av god intern styrning och kontroll

Nu har vi gått igenom vad intern styrning och kontroll är och hur COSO:s ramverk är uppbyggt och hur det fungerar. Men vad är då nyttan med att ha en så kallad god intern styrning och kontroll?

Värdet från en god intern styrning och kontroll är att man får en flexibel och väl skyddad organisation som har möjligheter och strukturerade angreppssätt för att skapa nya konkurrensfördelar. Genom en god intern styrning och kontroll får organisationen också effektivare processer, nya affärsmöjligheter, ett bättre anseende och framförallt ett ökat förtroende från intressenter. Intern kontroll handlar mycket om att vidga sina vyer så man hittar både risker och nya affärsmöjligheter på ställen man inte tidigare har letat. Genom detta ökar man sitt förtroende och upptäcker nya marknadspotentialer som i slutändan kan ge värde från en ökad lönsamhet. PwC räknar upp åtta konkreta värden man har fått fram i en undersökning av 25 svenska bolag, dessa är:

1. Bedrägerikontroll.
2. Trygghet i korrekt och fullständig finansiell rapportering.
3. Klara regler och tydliga ansvarsområden ger trygghet för individer och organisationen.
4. Minimerar kostnader för böter, lagöverträdelser och juridiska processer till följd av en bättre efterlevnad av lagar och regler.
5. Bekräftelse av efterlevnad av strategiska planer och mål.
6. Minskar antalet negativa överraskningar i form av avvikelser från finansiella och operationella mål.

7. Identifiering av risker innan faktiska brister möjliggör ett proaktivt agerande iställe för reaktivt.

8. Mer enhetliga och ändamålsenliga processer i verksamheten, leder till bättre effektivitet. (PwC, 2014)

2.4 Riskhantering

Intern styrning och kontroll står i en nära relation till risk och riskhantering. Intern styrning och kontroll är i dagens läge en del av ett företags riskbehandlingssystem och kan användas för att öka och minska risk inom olika områden. Begreppet risk utgår från sannolikheten att något ska inträffa, men nu har man även med konsekvenserna av att något inträffar. Risk är alltså den samlade bedömningen av sannolikheten för en oönskad händelse och konsekvensen om denna händelse ska inträffa.

Ett företags riskhantering är en process som bedrivs av företagets styrelse, ledning och annan personal, tillämpad i en strategisk miljö och över hela företaget. Den är utformad för att identifiera potentiella händelser som kan påverka företaget, och för att hantera risker så de ligger inom företagets riskaptit och ska samtidigt ge en rimlig försäkran om uppnåendet av enhetens mål.

Utgångspunkten för företagets riskhantering är målen man har lagt upp inom företaget. Målen kan vara underförstådda eller uttalade men de måste likväl finnas. Om företaget inte har ett konkret mål har inte heller ordet risk någon meningsfull innebörd kopplat till företaget. Att då börja diskutera och arbeta med risker är helt bakvänt. (Arwinge, 2015; Wikland, 2014 s. 21 – 24)

2.4.1 Riskbehandling & riskbedömning

Den företagsövergripande riskhanteringen inom en organisation, var den interna styrningen och kontrollen ingår som en komponent syftar på att skapa enighet mellan preferenser för risk, organisatorisk handling samt strategi. Företagsövergripande riskhantering syftar även på att skapa en enighet mellan den önskade risknivån och den faktiska risknivån, detta genom att implementera kostnadseffektiva riskbehandlingar.

Tidigare har det kommit fram att man måste utgå från sina mål när man behandlar risker och värderar dem, men man ska även värdera riskerna i förhållandet till andra risker, och till slut för att få ett riktigt grepp om vilka risker man måste skydda sig mot måste man skaffa sig en

bild av vilka som är accepterade risker utifrån organisationens perspektiv. Man ska alltså se till företagets så kallade riskaptit, vilket innebär att man bedömer den mängd risk organisationen är villig att ta i syfte för att uppnå sina mål.

Till följd av hur organisationer utformar och använder intern kontroll är det många som tyvärr bara fokuserar på att avgränsa risktagandet uppåt, man reducerar alltså nedsidan av risken genom att kontrollera allt som kan gå fel. Men risktagande och även kontroll handlar om uppsidan av risken. Riskhanteringen ska skapa värde genom att man tar till vara på möjligheter. Man ska alltså ange gränser för risktagande både uppåt och neråt, för liten risk skapar stagnation och hämmar innovationsförmågan men med för mycket risk blir det lätt att man ”gamblar”. Tar man för stora risker och chansar för mycket har man snabbt förbrukat organisationens riskkapacitet, vilket är den totala förmåga organisationen har för att absorbera risk. Riskkapaciteten för organisationen handlar mycket om deras finansiella situation, om man har tillräckligt med kapital för att absorbera risken eller ej. (Arwinge, 2015; Wikland, 2014 s.26 – 29)

Det finns olika typer av riskbehandling och dessa baserar sig på hur man som företag bedömer risken.

- Undvika: Om organisationen anser att kontrollkostnaden överstiger nyttan, oftast när man anser att risken är för stor kan man välja att undvika risken. Man kan göra detta genom att t.ex. undvika att vara aktivt i ett visst land eller undvika vissa produkter.

- Reducera: Den vanligaste riskbehandlingen är att reducera risken, ofta genom en god intern styrning och kontroll. Man använder den interna styrningen och kontrollen för att minska sannolikheten att risken materialiseras samt att mildra effekten av den.

- Dela: Ifall kostnaden för att reducera risken är för stor kan man välja att dela risken. Detta gör man via t.ex försäkring och utkontraktering. Dock kvarstår ofta det formella ansvaret för risken så man får inte bort hela risken.

- Acceptera: Om organisationen anser att risken är tolererbar så väljer man att acceptera risken. Det handlar ofta om vardagliga risker var kostnaden för kontrollåtgärder skulle vara allt för hög (Arwinge, 2015)

2.5 Företagsövergripande riskhantering – Integrerat med strategi och prestanda.

2004 publicerade COSO sitt första ramverk om företagsövergripande riskhantering, under det senaste decenniet har detta ramverk blivit brett accepterat av organisationer i hur man ska hantera risker. Under denna period har dock affärsvärlden ändrat, riskernas komplexitet har ändrat, det har kommit fram nya risker och styrelser och ledningar har förbättrat deras förståelse och översikt av risker och begärt ett förbättrat ramverk.

År 2017 publicerade COSO sitt uppdaterade ramverk för företagsövergripande riskhantering, Enterprise Risk Management – Integrating with Strategy and Performance. Det nya ramverket betonar vikten av att överväga risker i strategi processen och vid prestandan. Rapporten är uppdelad i två delar, den första ger ett perspektiv på nuvarande och utvecklande koncept och tillämpningar av företagsövergripande riskhantering. Den andra delen består av själva ramverket som har gått från att vara 8 komponenter till att nu vara fem komponenter, vilka har tjugo bakomliggande principer. (Committee of Sponsoring Organizations of the Tradeway Comission, 2017)

Man har även simplifierat definitionen av företagsövergripande riskhantering till;

” The culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value” (COSO Advisory Council Outreach Material, 2017)

2.5.1 COSO ERM 2017

Det nya ramverket förtydligar vikten av företagsövergripande riskhantering vid organisationens strategiska planering och förankrar det genom hela organisationen, eftersom risk påverkar och anpassar strategin och prestandan för alla avdelningar och funktioner. Det nya ramverket består alltså av fem komponenter och 20 bakomliggande principer och jag kommer nu redogöra för alla komponenter och deras principer. COSO har också tagit fram en ny matris som visuellt visar uppbyggnaden av den företagsövergripande riskhanteringen och dens integration i strategi planeringen. (Committee of Sponsoring Organizations of the Tradeway Comission, 2017)

Figur 2: COSO ERM

1. Styrning och kultur – Styrningen sätter organisationens ton, och förstärker vikten av, samt upprättar tillsynsansvar för den företagsövergripande riskhanteringen. Kultur avser etiska värden, önskat beteende och förståelse av risk i organisationen. Komponenten har fem bakomliggande principer.

   Den första är att styrelsen utövar riskövervakning – Styrelsen övervakar strategin och utövar ansvar för styrning för att stödja ledningen i uppnåendet av strategi och affärsmål. Den andra principen är att man ska upprätta operativa strukturer – Organisationen etablerar operativa strukturer i strävan efter strategi och affärsmål. Sedan ska man även definiera önskad kultur – Organisationen definierar det önskade beteendet som karakteriserar enhetens önskade kultur. Den fjärde principen för denna komponent är att organisationen visar ett åtagande gentemot kärnvärdena – Organisationen visar upp ett åtagande och engagemang till enhetens kärnvärden. Den femte och sista principen är att organisationen attraherar, utvecklar och behåller kompetenta individer – Organisationen är engagerade i att bygga mänskligt kapital i linje med strategi och affärsmålen. (Committee of Sponsoring Organizations of the Tradeway Comission, 2017)

2. Strategi- och målsättning – Företagsövergripande riskhantering, strategi och målsättning fungerar tillsammans i strategiplanerings processen. Riskaptiten är etablerad och i linje med strategin; affärsmålen sätter strategin i verket medan den tjänar som underlag för identifieringen, bedömningen och åtgärdningen av risker.

Komponenten strategi och målsättning har fyra bakomliggande principer. Först ska organisationen analysera affärskontext – Organisationen beaktar potentiella effekter av affärskontext och riskprofil. Den andra principen är att organisationen Definierar riskaptit – Organisationen definierar riskaptit i sammanhang med att skapa, bevara och realisera värde. Sedan ska organisationen utvärdera alternativa strategier – Organisationen utvärderar alternativa strategier och potentiell inverkan på riskprofilen. Slutligen ska man formulera affärsmålen – Organisationen beaktar risk vid etableringen av affärsmål på olika nivåer som star I linje med och stöder strategin. (Committee of Sponsoring Organizations of the Tradeway Comission, 2017)

3. Prestanda – Risker som kan påverka uppnåendet av strategi och affärsmålen måste identifieras och bedömas. Risker prioriteras beroende på omfattning och svårighetsgrad i kontexten av riskaptiten. Organisationen väljer sedan riskåtgärder och tar en portföljvy av den mängd risk den har antagit. Resultaten av denna process blir rapporterade till nyckel riskintressenter.

   Den första av de fem principerna som komponenten prestanda bygger på är, organisationen identifierar risk – Organisationen identifierar risk som påverkar prestandan av strategi och affärsmål. Den andra principen är att organisationen bedömer riskens allvar – Organisationen bedömer allvarligheten av risken. Seden ska organisationen prioritera risker – Organisationen prioriterar risken som grund för att välja åtgärder till risker. Som fjärde princip fungerar att man implementerar riskåtgärder – Organisationen identifierar och väljer åtgärder för risker. Slutligen ska organisationen utveckla portföljvy –organisationen utvecklar och utvärderar en portföljvy av risker. (Committee of Sponsoring Organizations of the Tradeway Comission, 2017)

4. Granskning och revidering – Genom att granska en enhets prestanda kan en organisation överväga hur väl den företagsövergripande riskhanteringens komponenter fungerar över tid och i ljuset av väsentliga förändringar och vilka ändringar som behövs.

   Komponenten granskning och revidering har tre principer och dessa är att organisationen; bedömer väsentlig förändring – Organisationen identifierar och bedömer förändringar som väsentligen kan påverka strategi- och affärsmålen. Granskar risk och prestanda – Organisationen granskar enhetens prestanda och beaktar risk. Eftersträvar förbättring av den företagsövergripande riskhanteringen –

Organisationen eftersträvar förbättring av den företagsövergripande riskhanteringen. (Committee of Sponsoring Organizations of the Tradeway Comission, 2017)

5. Information, kommunikation och rapportering – Företagsövergripande riskhantering kräver en kontinuerlig process av att erhålla och dela nödvändig information, från både interna och externa källor som strömmar upp, ner och över hela organisationen.

   Information och kommunikation har tre bakomliggande principer de är att organisationen; Utnyttjar informationssystem – Organisationen utnyttjar enhetens informations- och teknologisystem för att stödja den företagsövergripande riskhanteringen. Kommunicerar riskinformation – Organisationen använder kommunikationskanaler för att stödja den företagsövergripande riskhanteringen. Rapporterar om risk, kultur och prestanda – Organisationen rapporterar om risk, kultur och prestanda på flera nivåer över hela enheten. (Committee of Sponsoring Organizations of the Tradeway Comission, 2017)

2.5.2 Styrelsens och ledningens roll inom företagsövergripande riskhantering

Det är ledningen som har det övergripande ansvaret för att hantera risken för organisationen, men det är också viktigt för ledningen att gå längre än så, att förbättra dialogen med styrelsen och intressenter om att använda företagsövergripande riskhantering för att få konkurrensfördelar gentemot andra. Detta görs genom att integrera företagsövergripande riskhanteringen i valet och utvecklandet av strategin.

Genom denna process kommer ledningen att få en bättre förståelse för hur beaktandet av risk kan påverka valet av strategi. Företagsövergripande riskhantering berikar ledningens dialog genom att ge ett bättre perspektiv på styrkor och svagheter i en strategi när förhållandena förändras, och hur bra en strategi passar organisationens mission och vision. Det gör det möjligt för ledningen att känna sig mer säker på att de har undersökt alternativa strategier och tagit i beaktande input från de som kommer att implementera strategin i organisationen.

Styrelser förväntas allt mera fungera som övervakare och att ha översyn över den företagsövergripande riskhanteringen. I styrelsens riskövervaknings roll kan det ingå att granska, utmana och instämma med ledningen i frågor om t.ex. den föreslagna strategin och riskaptiten, signifikanta affärsbeslut, anpassning av strategin till organisationens kärnvärden, mission och vision. Styrelsen ska övervaka godkännande av ledningsincitament och

ersättningar samt delta i investerar- och intressentrelationer. (Committee of Sponsoring Organizations of the Tradeway Comission, 2017)

2.5.3 Fördelar av företagsövergripande riskhantering

Syftet med COSO:s ramverk om företagsövergripande riskhantering är att skydda och förbättra värdet gentemot intressenter. Den underliggande filosofin var att värdet maximeras när ledningen sätter strategi och mål för att få en optimal balans mellan tillväxt och avkastningen från målen och de relaterade riskerna, och att effektivt utnyttja resurser i strävan mot organisationens mål.

Alla organisationer behöver lägga upp sin strategi och regelbundet anpassa den för att alltid vara medveten om de ständigt föränderliga möjligheterna till att skapa värde och de utmaningar som uppstår i strävan efter det värdet. För att göra det behöver de, bästa möjliga ramar för att optimera strategin och prestandan. Det är här den företagsövergripande riskhanteringen kommer väl till pass. Organisationer som har integrerat företagsövergripande riskhantering genom hela organisationen kan få många fördelar. Dessa fördelar är:

- Ökar utbudet av möjligheter – Genom att överväga alla möjligheter, både positiva och negativa aspekter av risk kan ledningen identifiera nya möjligheter unika utmaningar i samband med de nuvarande möjligheterna.

- Identifierar och hanterar risker över hela enheten – Varje enhet står inför flertalet risker som kan påverka många delar av organisationen. Ibland kan risken härstamma från en del av enheten men påverka en annan del. Följaktligen identifierar ledningen och hanterar dessa enheters omfattande risker för att upprätthålla och förbättra prestandan.

- Ökar positiva resultat och fördelar samtidigt som negativa överraskningar reduceras – Företagsövergripande riskhantering tillåter enheter att förbättra deras förmåga att identifiera risker och etablera lämpliga åtgärder, vilket minskar överraskningar och relaterade kostnader eller förluster, samtidigt som man drar nytta av fördelaktiga utvecklingar.

- Reducerar prestationsvariabiliteten – För vissa är inte utmaningen med överraskningar och förluster så överhängande, utan den största utmaningen är variationen i prestandan. Att prestera över schemat eller utöver förväntningarna kan orsaka lika mycket oro som att inte prestera i tid och att inte nå upp till förväntningarna. Företagsövergripande riskhantering tillåter organisationer att förutse risker som skulle påverka prestationen, detta gör det möjligt för dem att sätta in de åtgärder som behövs för att minimera störningar och maximera möjligheter.

- Förbättrar resursutnyttjande – Varje risk kan betraktas som en begäran av resurser. Att få robust information om risker ger ledningen möjligheten att bedöma det övergripande resursbehovet, prioritera resursplaceringen samt att förbättra resursfördelningen.

- Förbättrar företagets motståndskraft – Ett företags medel- och långsiktiga lönsamhet beror på företagets förmåga att förutse och reagera på förändringar, inte bara för att överleva utan också för att utvecklas och frodas. Detta är delvis möjligt genom en effektiv företagsövergripande riskhantering. Det blir allt viktigare allteftersom takten av förändring och affärskomplexiteten ökar.

Dessa fördelar markerar det faktum att risk inte bör ses enbart som en potentiell begränsning eller utmaning mot att fastställa och genomföra en strategi. Man bör istället se det som att förändringen som ligger till grund för risk och åtgärderna mot risken ger strategiska möjligheter och viktiga differentierande funktioner för företaget. (Committee of Sponsoring Organizations of the Tradeway Comission, 2017)

3 Empiriska delen

I den empiriska delen undersöker jag hur den intern kontrollen ser ut just nu i Företag X, för att sedan analysera den mot teori delen och komma med förbättringspunkter som företaget kan göra för att förbättra den interna kontrollen.

Uppbyggnaden av den empiriska delen består av COSO-modellens fem komponenter, jag kommer i tur och ordning att reda ut hur de olika komponenterna fungerar i företaget just nu och hur man kan förbättra dem. Undersökningen har alltså utgjorts av en intervju med företagets Business Controller. Jag har genom några frågor för varje komponent tagit reda på hur den interna kontrollen ser ut just nu. Den empiriska delen är uppbyggd som COSO-modellens komponenter där jag först redogör för hur den interna kontrollen ser ut i dagsläget och sedan binder det till teorin och hur man kan förbättra vissa delar. Till slut kommer resultatet bli en checklista med saker som bör ändras och förbättras inom den interna kontrollen.

3.1 Intern kontroll inom Företag X

Huvudmålet med den interna kontrollen inom Företag X på administrationssidan är att minimera farliga kombinationer t.ex. att samma person inte ska kunna öppna en leverantör, lägga in bankdetaljer, göra inköp, granska och godkänna fakturor. Man arbetar inte med någon speciell modell för den interna kontrollen utan man lyssnar på revisorn och vad denna säger att borde åtgärdas och arbetar kontinuerligt med att förbättra den interna kontrollen på detta sätt. Revisorns roll har genom åren till viss del varit att styra företaget mot ett tänkande hur man kan förebygga farliga kombinationer.

En sak som framkommit tydligt i teorin är att det är av yttersta vikt att företaget har tydliga mål och att de finns tillgängliga för alla, både för den interna kontrollen och för riskhanteringen.

Företag X har tydligt uppsatta och nedskrivna mål som alla i personalen har tillgång till. Man har t.ex. KPI och PI som står för Key Performance Indicators och Performance Indicators. KPI följs på gruppnivå och här hittar man mål som leveranssäkerhet, yield, kassaflöde, underliggande EBITDA och fasta kostnader.

En gång i kvartalet har man informationstillfälle för hela personalen där man går igenom alla dessa mål och hur man har uppnått dem. Sedan går man även igenom dem inom

ledningsgruppen för företaget och därefter kommunicerar förmännen för de olika avdelningarna detta neråt i företaget.

För att bättre illustrera hur man uppnått målen använder man sig av trafikljusens färger, alltså grönt om de har uppnåtts, gult om de ligger på gränsen och rött om de inte har uppnåtts. Här är nyckeln att speciellt de som ligger på gult och rött måste kommuniceras neråt och man måste lösa hur man ska uppnå dessa. I figur 3 kan man se hur KPI och trafikljus färgerna ser ut.

Generellt sett har man en bra syn på den interna kontrollen, huvudpunkten låg på att minimera farliga kombinationer vilket i mångt och mycket är vad den interna kontrollen ska gå ut på. Man kunde jobba mera med att få den interna kontrollen som en process som genomsyrar hela företaget. Den interna kontrollen ska vara en process som styrelsen, ledningen och övrig personal jobbar med för att uppnå målen med verksamheten, rapporteringen och efterlevnaden av lagar och regler.

Man kunde undersöka möjligheten med att anställa en internrevisor som skulle ansvara helt och hållet för den interna kontrollen. Just nu använder man sig till stor del av den externa revisorn för råd om intern kontroll, och denna kanske inte har tid att till fullo kolla den interna kontrollen hela tiden. Här måste företaget naturligtvis väga nytta mot kostnad, väger nyttan mera än kostnaden så kan man göra det, om den inte gör det borde man avstå. Arbetet med den interna kontrollen skulle troligtvis underlättas mycket om man bestämde sig för att följa en viss modell för intern kontroll. Detta ger en bättre överblick i hur man uppnår en god intern styrning och kontroll och det blir lättare för de som är ansvariga för den interna kontrollen.

Företaget har bra uppsatta mål för verksamheten och de finns tillgängliga på intranätet för alla anställda. Sedan gäller det för var och en av de anställda att man bekantar sig med målen. Att man även har kvartalsvisa informationstillfällen där man går igenom uppnåendet av dessa mål är i ljuset av intern kontroll väldigt bra. Dessutom går man igenom hur man uppfyller målen på gruppnivå på morgonmöten som hålls antingen en gång i vecka eller varje dag.

3.1.1 Kontrollmiljön

Kontrollmiljön är den viktigaste komponenten inom intern kontroll och den anger tonen för hela kontroll arbetet. Ledningen inom företaget försöker att alltid föregå med gott exempel

och genom detta ge en god ton för den interna kontrollen. Det är såklart alltid lättare att säga hur man borde göra saker än att faktiskt få det implementerat, man möter på motstånd och personalen kan undra om det faktiskt är nödvändigt att göra vissa saker.

Inom Företag X känner iallafall ekonomiavdelningen till innebörden med den interna kontrollen, man är medvetna om att det kan krävas lite extra arbete som ibland kan kännas lite onödigt men som i slutändan är väldigt viktigt för företaget. Det finns vissa uppdelningar av ansvars och befogenhetsroller uppgjorda men de är inte riktigt fullständiga.

Just nu arbetar man med att upprätta riktlinjer om vem som får godkänna räkningar och för hur mycket, det har tidigare inte funnits ett tydligt dokument där det står att t.ex person X har 20000€. Man lägger även upp riktlinjer för hur person X ska gå tillväga om det kommer en faktura på mera än 20000€. Detta vill man ha utskrivet på ett dokument så det finns svart på vitt. Det finns från tidigare vissa gränser när det gäller investeringar för vissa personer i företaget men inget dokument där man har med alla.

Utbildning av personalen är en stor del av kontrollmiljön och Företag X erbjuder inte riktigt tillräckligt med utbildning och man har inte riktigt har tagit sig tid att internt utbilda personalen på en tillräcklig nivå. Det har inte riktigt hunnits med i dagens läge att fundera ut hur man internt kunde utbilda de anställda.

När det gäller kontrollmiljön så är en viktig del att ledningen föregår med gott exempel och på så sätt sätter en god ton i företaget. Det verkar som ledningen i Företag X gör detta och man försöker få detta att avspegla sig neråt till resten av de anställda. I intervjun nämndes det att man kan möta på motstånd av de anställda och de kan undra om det faktiskt är så viktigt att göra olika kontroller som tar tid. Här gäller det för företaget att förklara tydligt vikten av en god intern kontroll och få de olika momenten så integrerade i arbetet som möjligt. De olika kontrollaktiviteterna ska vara så integrerade i det dagliga arbetet att det inte känns extra tungt och jobbigt för de anställda när de måste göra något extra.

Genom att ha tydliga och nedskrivna riktlinjer om de anställdas ansvarsområden eliminerar man problemet med att någon inte skulle veta sitt ansvarsområde. På det här viset kan även företaget kräva ansvar av den anställda att den personens uppgifter blir skötta. Här arbetar företaget just nu med att tydliggöra vem som får godkänna fakturor och för vilka belopp.

Att attrahera, behålla och utveckla personal är en viktig del inom kontrollmiljön, här har Företag X en del att se över. De anställda borde erbjudas tillräcklig utbildning, detta hjälper företaget i det långa loppet och gör det mera konkurrenskraftigt. Att utbilda sin personal gör

att de hela tiden hänger med i den konstant utvecklande ekonomin just nu. Företaget behöver inte direkt skicka iväg personalen på dyra skolningar man kan börja med att internt utbilda hela grupper för att sedan skicka utvalda på fördjupade skolningar och de i sin tur kan förmedla detta vidare till resten av gruppen. Att hålla en hög kompetens på de anställda borde vara av yttersta vikt för företaget.

3.1.2 Riskbedömning

Det finns ett särskilt tillvägagångssätt för riskbedömning inom företaget och på detta vis identifierar, bedömer och hanterar man risker. Man använder sig t.ex. av risklappar där personalen får lämna in lappar om man har upptäckt något som kan vara en risk. Om det är en allvarlig risk, en noll-olycka eller en olycka som har resulterat i sjukfrånvaro så graderas denna med en skala där man bedömer sannolikheten för risken samt hur allvarlig risken är. Sedan multiplicerar man sannolikhetstalet och allvarlighetstalet med varandra för att få fram den totala risken.

Man gör egentligen någon form av riskbedömning med allt som görs, t.ex. när man skaffar nya linjer och när man skapar nya procedurer. Riskbedömningen förekommer dock främst i produktionen och mera sällan inom administrationen. Det förekommer såklart till en viss del t.ex. vid remburs affärer, vid nya kunder. Inom företaget har man mycket nickel och priset på nickeln skyddar man med olika derivatinstrument, man köper och säljer nickeltermins affärer beroende på om den börjar skena iväg allt för högt.

En hörnsten i riskbedömningen är målen med verksamheten om det finns tydligt uppsatta mål, för annars är det svårt att ha en riskbedömning om man inte vet vad som ska skyddas. Som tidigare framkom finns det tydliga mål med verksamheten man har både KPI och PI. Hur detta ser ut illustreras i bild 3.

KPI	2014 (Actual)	2015 (Actual)	2016 (Forecast)	2017 BUDGET	Budget-Forecast 2016 Diff	Budget 2017 vs 2015 Diff
Safety LTI (YTD)	8,7	5,6	0	0	0	-6
Underlying EBITDA (TEUR)	11 272	9129	6855	9 366	2 511	237
Cash Flow from operations (TEUR)	8233	7860	960	4 716	3 756	-3 144
Safety Hours / working hours	1,1 %	1,3 %	1,3 %	1,3 %	0,0 %	0,0 %
Energy consumption MWh/ton	0,77	0,77	0,79	0,78	-0,01	0,01
Yield standard	91,9 %	92,5 %	91,9 %	92,5 %	0,6 %	0,0 %
Yield special	77,7 %	77,6 %	82,0 %	85,0 %	3,0 %	7,4 %
Yield Slice	96,0 %	96,2 %	95,1 %	96,0 %	0,9 %	-0,2 %
Cost of scrap (eur/ prod kg), excl Slice		0,065	0,062	0,059	-0,003	-0,006
Delivery performance on day	46,0 %	62,8 %	79,0 %	92,5 %	13,5 %	29,7 %
Delivery performance on day excl cust. reasons	46,0 %	62,8 %	82,0 %	95,0 %	13,0 %	32,2 %
Availability of AA items		74,0 %	75,0 %	95,0 %	20,0 %	21,0 %
Availability of A items		75,0 %	70,0 %	85,0 %	15,0 %	10,0 %
Availability of AA items		92,0 %	85,0 %	95,0 %	10,0 %	3,0 %
Availability of A items		86,0 %	80,0 %	85,0 %	5,0 %	-1,0 %
Inventory ton (tons - CAP)		n/a	9600	10100	500	
Inventory ton (tons - CAP)		n/a	1050	1000	-50	
Fixed costs (excl depr & allocations)	15 435	16010	15130	14 800	-330	-1 210
% Alien RM sourcing (ton)		0,8 %	8,0 %	8,0 %	0,0 %	7,2 %
Growth (tons)		-6	566	3 089	3 089	3 645
Growth (tons)		231	43	39	39	56
Order Intake Contribution (QV TEUR)		25638	25547	26 066	519	428
Sold tons per person , including produced KP	156	159	171	192	21	33

Figur 3 Key Performance Indicators - Företag X

I figur 3 ser man tydligt hur företaget har lagt upp sina mål med verksamheten, här hittar man t.ex leveranssäkerhet, yield, säkerhet osv. färgerna på kolumnen till höger illustrerar om man har uppnått målen eller inte, där grönt innebär att man har uppnått dem och rött är att man inte uppnått dem och gult att man ligger på gränsen för att uppnå dem.

När det kommer till risken för bedrägeri så litar man på sin personal men man har såklart olika kontrollfunktioner som ska fungera som en avskräckare, personalen vet att det finns t.ex. loggar och att det bara är vissa som kan lägga in kontonummer för kunder och leverantörer osv. Så man anser att man ganska fort skulle märka om det förekommer bedrägeri inom företaget.

Företaget anser att risken är större för externt bedrägeri och man nämner att banken brukar skicka varningar och frågor hur man hanterar externt bedrägeri. I dagens läge förekommer det mera och mera bluffakturor och de blir allt mera sofistikerade. Man kontrollerar alltid fakturor som ser konstiga ut och väcker extra uppmärksamhet, man identifierar en större risk för bluffakturor under sommaren när det är sommarpraktikanter som inte är lika vana och kanske inte känner till de olika leverantörerna lika bra som den ordinarie personalen.

Inom företaget jobbar man tydligt med riskbedömning och den finns som en naturlig process inom det dagliga arbetet. Man använder sig av risklappar där man bedömer sannolikheten och konsekvensen av risken vilket gör det hela väldigt tydligt. Det förekommer dock oftast olika säkerhetsrisker på dessa risklappar, man kunde utforma ett liknande system när man bedömer risker på t.ex marknaden. Överlag kunde företaget göra upp tydliga modeller för alla sorters riskbedömning även risken för bedrägeri.

En sak som har framkommit flera gånger i detta arbete och som framkommer konstant i teorin om intern kontroll är vikten av uppsatta mål. Företag X har en väldigt tydlig bild av deras mål med verksamheten, och som teorin betonade är det dessa man själva kan påverka till största del. Att ha tydligt uppsatta mål är viktigt för att man ska kunna bedöma risker som kan påverka företagets möjlighet att uppnå dessa mål.

Företag X har även bedömt risken för bedrägeri på ett gott sätt och försöker hela tiden göra det så svårt som möjligt att utföra någon sorts bedrägeri.

3.1.3 Kontrollaktiviteter

När det kommer till kontrollaktiviteter så är en vanlig aktivitet den att det ska finnas en granskare och en godkännare av fakturor och denna får inte vara samma person. Denna aktivitet använder sig Företag X av också. Däremot har man inom inköp av olika mindre saker inte just nu den bästa kontrollen. Man har en inköpare och en inköpschef som kopplas in när det handlar om större inköp. Men sedan kan t.ex. produktionsingenjörer köpa in sådant man anser att behövs. I sådana fall är de också de som granskar fakturan och sedan deras förman som godkänner fakturan.

Man jobbar även på att få klara riktlinjer för vilka personer som får godkänna fakturor till olika belopp. Det svåra här är hur man ska få en balanserad gräns på beloppen olika personer har rätt att godkänna. Lägger man för hög gräns styr man för mycket arbete åt de som har rätten att godkänna de högre summorna, lägger man för låg så har kanske fel person möjlighet att godkänna för stor summa och hela kontrollaktiviteten undermineras. En annan aspekt man bör ta i beaktande är vilken person man ger befogenheterna till, det finns mera och mindre ansvarsfulla personer och det gäller att man inte ger för stora befogenheter till en som inte tar sitt ansvar.

Just nu håller företaget på att utveckla en applikation i sitt fakturaprogram där det ska framkomma vem som är kontrollerare av fakturan och vem som är godkännare. Detta för att

säkerställa så det inte är samma person, men även att det följer en rangordning. Det ska vara så att den som är lägre hierarkiskt är granskare och den som är högre är godkännare, man vill alltså förhindra maktmissbruk. Just nu har man tyvärr inte så bra uppföljning på hur gränserna för inköp följs alltså en uppföljning på t.ex om person X har en inköpsgräns på 10000€ att han inte köper in för 15000€ eller ännu mera.

Inom ledningsgruppen har det diskuterats om att man ska börja använda sig av olika stickprover på t.ex betalningar. Man ska ta stickprover på olika betalningar och jämföra kontonumren för att på så sätt se att pengarna faktiskt är på väg till rätt kontonummer och någon inte har lagt i rullning att vissa betalningar far in på fel konto.

En annan kontrollaktivitet man använder sig av är olika spärrar och autentiseringar för att kontrollera vilka personer som rör sig på olika delar av ERP-systemet och för att förhindra att de ska uppstå farliga kombinationer genom att fel personer rör sig på fel ställen inom ERP-systemet. Exempel på detta kan vara att alla inte slipper och inventera, alla slipper inte och öppna kunder, man har även så att inköparen slipper och öppna en leverantör men inköparen slipper inte och lägga in kontonumret till leverantören det måste någon som har hand om godkännade av fakturor göra. Sedan använder man sig även av logger som visar vem som har rört sig på sidan och lagt in t.ex. kontonumret. På det här viset vill man skydda sig mot farliga kombinationer och även avskräcka personer från att ens försöka.

Det finns olika kontroller och riktlinjer för olika delar av administrationen, på försäljningen finns det vissa gränser man får sälja för utan något godkännande uppifrån och till vem man får sälja finns det direktiv om. Inom inköp har man som riktlinje att avdelningen är mera inblandade i större inköp och då har besluten blivit manglade i ledningsgruppen vid flertalet tillfällen och slutligen ger t.ex. VD:n eller produktionschefen godkännande för inköpet. Inköpet har även hand om avtal man skriver på årsbasis t.ex vid transportavtal så finns både logistikchefen och inköpschefen med i processen och där har man riktlinjer för vad priset ska vara.

Företaget försöker också ha manualer och instruktioner för varje avdelning och för olika poster inom företaget så att arbetet ska kunna fortlöpa även om en person skulle vara borta vid sjukdom eller annat. Det kan variera lite från avdelning till avdelning med dessa manualer men iallafall på ekonomisidan har man uppgjort sådana, för att arbetet inte ska stanna av om någon är borta. Det svåraste är kanske att få tillstånd instruktioner om uppgifter som görs endast någon gång i året man kanske inte riktigt kommer ihåg hur man gjorde och man har mycket annat att göra.

Överlag kan man säga att Företag X har en hel del olika kontrollaktiviteter, vissa mera utvecklade och vissa är under utveckling. Företaget borde fokusera på att få en bättre kontroll på inköpen inom företaget, eller närmare bestämt de inköp som inte kräver att inköpschefen är inblandad. Just nu verkar det som att en produktionsingenjör kan beställa det man anser sig behöva utan större frågor och hinder. Sedan ska förstås fakturan godkännas av dennas förman. Men problemet är att köpet redan förverkligats vid denna tidpunkt och man kan inte göra desto mera. Så att få de mindre inköpen under kontroll är en sak företaget verkligen skulle behöva se över. En lösning på detta kan vara att man inom sitt ERP-system skulle fixa så den som ska köpa något lägger in en köpanmodan som sedan måste godkännas av förmannen, först efter detta skulle man göra inköpet och inköpet skulle skötas helt av inköpsavdelningen.

Som det framkom i intervjun håller man på att uppgöra riktlinjer för vem som får godkänna fakturor samt för hur högt belopp. Dessa riktlinjer är otroligt viktiga för den interna kontrollen, det ska finnas tydliga och nedskrivna riktlinjer om vem som har rätten att godkänna fakturor och till vilken summa. Det hjälper både företaget och personalen att detta finns, företaget vet vem man ska hålla ansvarig och de anställda vet exakt vad som krävs av dem.

För att får tydliga gränser som fungerar kan företaget först se över frekvensen av olika stora inköp, och sedan dela upp det i t.ex. tre grupper, små, medelstora och stora inköp. Sedan har man en som godkänner små inköp, en som godkänner medelstora och en som godkänner stora. För att få detta att lyckas krävs det att man backar tillbaka några år och jämför inköpen och därefter sätter gränserna.

Företag X har alltså gränser för hur mycket olika personer får köpa in för, men dessa verkar inte följas upp i tillräcklig grad för att det ska vara under kontroll. Här bör företaget göra så man kan samlar ihop information från alla inköp och sedan kontrollerar för hur mycket olika personer har köpt in för. Det kan göras t.ex månatligen eller kvartalsvis och sedan i slutet av året kan man ha en genomgång med de personer som berörs. Det viktigaste är att det finns någon som helst kontroll på detta, annars fallerar hela konceptet med att ha inköpsgränser.

Man kunde ta hjälp av applikationen man håller på att utveckla just nu där man ska hålla koll på vem som har granskat och godkänt fakturor. Därifrån kunde man samla ihop beloppen för varje person och sätta in gränserna så det syns när en person går över eller börjar ligga väldigt nära sin gräns.

Ett problem för företag är att det under årens lopp har blivit så att det bara är en person som kan sköta en arbetsuppgift. När denna sedan är frånvarande har ingen riktigt koll på hur personen brukar göra. Företag X har iallafall inom ekonomiavdelningen uppgjort bra manualer för de olika arbetsuppgifterna, detta gör det så mycket enklare att fylla in på någons post när denna är borta. Det här är en sak man kontinuerligt måste göra genom hela företaget. Det kommer hela tiden nya moment och de anställda utvecklar hela tiden sitt arbetssätt så därför måste det alltid finnas tydliga nedskriva manualer om hur man sköter andras uppgifter. Ett företag i dagens läge får inte bli lidande av att en person är frånvarande.

3.1.4 Information och kommunikation

Som informationskanaler använder man sig till största delen av intranätet, där får personalen allmän information om vad som händer i företaget och vad som är på agendan. Man har även morgonmöten, vissa avdelningar har varje morgon ett möte på ca 10 min där man går igenom dagliga saker t.ex. hur man uppnår vissa uppsatta mål, om det finns kritiska saker, reklamationer osv. Under dessa möten får personalen ventilera om man har något man funderar på eller förbättrings förslag. Inom administrationen strävar man till att ha dessa möten iallafall en gång i veckan men på flera avdelningar har man detta varje morgon.

Ledningsgruppen har möten kontinuerligt och där lyfter man upp lite större frågor, sedan ska förmännen informera neråt om det finns behov av det. En viktig informationskanal som man lyfter fram är helt vanligt korridorssamtal, det behöver inte alltid vara så formellt. Man får löst mycket genom att bara sätta sig ner och prata en stund och ofta går det snabbare och enklare.

Information om saker som gäller intern kontroll får man fram till stor del genom morgonmöten eller så kallar man till ett större informationsmöte, där man sitter och funderar på hur man ska göra och ställer frågor. Personalen har fått information om sin roll och sitt ansvarsområde inom den interna kontrollen och inom administrationen borde detta vara på klart. För rapportering av oegentligheter eller om man märker att det är något konstigt så finns det en oskriven regel att man meddelar Business Controllern om detta och han i sin tur tar ärendet vidare.

Informationen och kommunikationen inom Företag X verkar flöda bra genom hela organisationen, de anställda har tillgång till intranät, man har veckovisa eller dagliga morgonmöten, man har större informationstillfällen osv. Det verkar också vara ”högt till tak”

när det gäller att ta upp problem och kommunicera sinsemellan om t.ex. oegentligheter eller i allmänhet sådant som gäller företaget och intern kontroll.

Företaget kan införa möten där man diskuterar den intern kontrollen med de anställda, det kan ske på avdelningsnivå och där man skulle gå igenom de anställdas roller och ansvar för den interna kontrollen. I Företag X vet personalen sin roll men för att personalen ska hållas uppdaterade och uppmärksamma kan ett kort möte någon gång i året vara på sin plats.

Däremot borde man uppgöra tydliga tillvägagångssätt för rapportering av oegentligheter. Det räcker inte med en oskriven regel för att det ska anses vara god kontroll. Man kunde göra upp ett tydligt tillvägagångssätt för situationer när man märker olika oegentligheter. Dessa ska finnas tydligt nedskrivna och tillgängliga för alla anställda, då kan inte de anställda skylla på att man inte visste och det fungerar även som en påminnelse för de anställda att hela tiden vara uppmärksamma.

3.1.5 Övervakning och uppföljning

Som övervakning av den interna kontrollen har man inom Företag X t.ex. applikationen inom fakturaprogrammet där man ser vem som har granskat och vem som godkänt fakturan. Tidigare nämndes också att man ska börja använda sig av stickprov om en del av övervakningen, och man använder sig också av begränsningar inom ERP-systemet för att på ett sätt övervaka den interna kontrollen.

Den intervjuade anser att styrelsen och ledningen inte i dagens läge övervakar den interna kontrollen tillräckligt men man jobbar på att bli bättre på det. Man har diskuterat att övervakningen måste bli striktare inom ledningen, och ska försöka få bukt med problemet. Just nu litar man på sina kontroller och att det skulle uppdagas ganska fort om det skulle förekomma några oegentligheter.

Det är upp till styrelsen och ledningen att övervaka den interna kontrollen. Här måste man ständigt följa med utvecklingen och se till att företaget följer uppställda riktlinjer gällande den interna kontrollen. Det ska finnas löpande uppföljning, separata utvärderingar och rapportering av avvikelser inom den interna kontrollen.

Företag X har en del på gång när det kommer till övervakningen. Som det framkommer i intervjun har man applikationen inom fakturaprogrammet, man har loggar i ERP-systemet och man ska börja använda sig av stickprov. Alla dessa är bra övervakningsmetoder och kommer ske löpande genom processen.

Utvärdering av den interna kontrollen har man till synes inte ha tagit upp så mycket just nu. Man måste hela tiden jobba för att utvärdera hur bra de olika kontrollaktiviteterna är och hur den interna kontrollen överlag fungerar. Här hjälper det mycket om man utgår från en modell på hela den interna kontrollen där man på ett strukturerat sätt kan se vad som krävs för en god intern kontroll. Man kan även göra upp någon form av lista där man utvärderar hur den interna kontrollen fungerar och där kan man sedan pricka av vad som fungerar på ett bra sätt och vad som inte gör det.

3.1.6 Företagsövergripande riskhantering inom Företag X

Företaget är noga med riskhantering vid affärsbeslut vid köp av t.ex. köper en ny linje reder man ut om det finns efterfrågan, marknadsrisken, om man har tillräckligt med kontakter för den nya produkten, vad det innebär att skapa det nya kontaktnätverket, finns det kapacitet inom försäljningen för detta och naturligtvis det rent finansiella med investeringen. Bolaget är ett skuldfritt bolag så vid investeringar är man noga med att likviditeten ska vara god inom företaget och att man ska växa organiskt.

När man lägger upp sin strategi beaktar man till viss del också riskhanteringen, man utvärderar risker på marknaden och på de områden man har tänkt växa, risken att man inte hänger med i utvecklingen och konkurrenterna. Man ser även över risken med att man förlorar olika nyckelpersoner inom företaget, och hur man ska hitta kunnig personal när man ska växa. Man bedömer risker från fall till fall och identifierar risker och reder ut hur man ska hantera dessa. Företaget har på det viset inte lagt upp någon riskaptit för företaget utan bedömer sedan risken från fall till fall och hur mycket man är beredd att riskera.

4 Resultat och slutsats

Nu har man i arbetet först kunnat läsa om teorin bakom intern styrning och kontroll och hur COSO-modellen är uppbyggd, sedan hur den interna kontrollen ser ut i dagsläget inom Företag X. Man kan även läsa i slutet av varje underrubrik i kapitel 3 om hur det är kopplat till teorin. Därför kommer jag i denna göra upp en checklista med saker Företag X borde ändra på och fixa till för att ha en god intern styrning och kontroll utgående från COSO-modellen. Detta kommer att fungera som resultatet av min forskning.

☐ Anställ en person som endast arbetar med den interna kontrollen t.ex. internrevisor.
☐ Arbeta utgående från en modell gällande intern styrning och kontroll.
☐ Utbilda personalen, både i större och mindre skala
☐ Skapa en funktion i ERP-systemet så man får lägga in en köpanmodan
☐ Följ upp inköpsgränserna noggrannare
☐ Sätt upp tydliga riktlinjer för vem som granskar och godkänner fakturor samt gränser för hur mycket respektive person får godkänna.
☐ Säkerställa att det finns arbetsmanualer fört det dagliga arbetet på samtliga avdelningar.
☐ Gör upp tydliga, nedskrivna riktlinjer för hur man skall gå tillväga för att rapportera oegentligheter.
☐ Säkerställ att ledningen och styrelsen gör löpande uppföljningar, separata utvärderingar och har en god rapportering av avvikelser inom den interna kontrollen.

- Förtydliga alla de anställdas roller och ansvarsområden inom den interna kontrollen.

När det kommer till punkten att anställa en internrevisor måste man naturligtvis väga nyttan mot kostnaderna. Men om nyttan överstiger kostnaden för en internrevisor är detta en mycket bra förbättring. Överlag anser jag inte att den nuvarande interna kontrollen är så dålig inom Företag X men det finns naturligtvis områden inom den interna kontrollen man kunde förbättra. Genom att förbättra dessa punkter förbättrar man även alla de fem komponenterna som finns i COSO-modellen. Man får en mera transparent och effektiv organisation där de anställda vet vad man ska göra, vet vad intern kontroll är och hur viktigt det är, man hjälper även de anställda att sköta sitt arbete på ett bättre sätt när man tydligt definierar deras ansvar och samtidigt kräver deras ansvar. Man minskar även riskerna för bedrägeri och man minskar framför allt riskerna för att inte uppnå sina uppsatta mål med verksamheten.

4.1 Förslag till vidare forskning

Ämnet intern styrning och kontroll är väldigt brett och man kan göra en undersökning i princip hur stor skala som helst. Så man kunde i en vidare forskning rikta in sig mera på produktionen och den intern kontrollen där, eller välja endast en komponent av COSO-modellen och göra riktigt detaljerade förbättringar inom en viss komponent. Man kunde även börja implementera de åtgärder jag har föreslagit i resultatet och göra en undersökning om hur det blev när de är implementerade i verksamheten.

5 Validitet och reliabilitet

Enligt mig är ämnet väldigt intressant och har blivit mera och mera viktigt för företag under de senaste åren. Intervjun utfördes ansikte mot ansikte med personen i fråga och jag valde att inte inflika några egna synpunkter och kommentarer under intervjun för att inte leda in den intervjuade på sidospår samt att inte försöka få den intervjuade att återspegla mina åsikter. Jag valde även att helt hålla företaget anonymt i detta arbete för att jag ville få så ärliga svar som möjligt på mina frågor, detta nämnde jag också till den intervjuade i början av intervjun så personen i fråga inte behövde oroa sig för att företaget skulle se dåligt ut utåt.

När det kommer till reliabiliteten kan jag konstatera att den kunde ha varit bättre om jag hade intervjuat flera personer på företaget. Visserligen intervjuade jag den person som har mest koll på intern kontroll men man hade kunnat få andra svar på frågor som, om de anställda vet sina roller och ansvarsområden, om de vet vikten av den interna kontrollen osv. En bra kombination för undersökningen skulle ha varit att ha en intervju med samma person för de mera detaljerade frågorna men även att använda sig av enkät för resten av de anställda var man kunde ha ställt mera allmänna frågor om deras syn på intern kontroll. Jag kunde även ha valt att intervjua en person från styrelsen för att få deras perspektiv på den interna kontrollen inom företaget.

6 Sammanfattning

Området intern kontroll är väldigt omfattande och begreppet intern kontroll uppfattas på olika sätt beroende på vem man frågar av. Detta kan skapa problem när det handlar om att sätta mål med den interna kontrollen. Därför är det viktigt att man lägger upp ramar för företagets interna kontroll och tydliggör betydelsen av den samt definierar begreppet intern kontroll.

Den interna kontrollen är en löpande process som genomsyrar hela organisationen och ger en rimlig försäkran om att organisationens uppsatta mål nås. Den interna kontrollen ger organisationen en ökad effektivitet, tillförlitlighet och produktivitet.

Det mest använda ramverket för intern kontroll är COSO:s ramverk för intern kontroll. Den nyaste versionen av ramverket kom 2013 och används idag över hela världen. COSO-modellen bygger på fem samverkande komponenter. Komponenterna är kontrollmiljö, riskbedömning, kontrollaktiviteter, information och kommunikation samt övervakning och uppföljning. Genom att tillämpa detta ramverk inom organisationen och nå en acceptabel nivå på samtliga komponenter ska organisationen få en så kallad god intern kontroll. Förutom de fem komponenterna fastställer också ramverket tre huvudsakliga mål för organisationen, mål med verksamheten, mål med rapporteringen samt efterlevnad av lagar och regler.

2017 gav COSO ut ett nytt ramverk för den företagsövergripande riskhanteringen. Denna gång fokuserade ramverket på att integrera riskhantering med strategin i organisationen. Avsikten med ramverket är inte att ersätta ramverket för intern kontroll utan att integrera de

båda med varandra eftersom riskhantering och intern kontroll går mycket in i varandra och fungerar ihop. Företagsövergripande riskhanteringen består även den av fem komponenter, styrning och kultur, strategi och prestanda målsättning, prestanda, granskning och revidering samt information och kommunikation.

Syftet med arbetet var att reda ut Företag X:s interna kontroll i nuläget och sedan förbättra den utifrån teorin. Den empiriska delen av arbetet undersökte hur den interna kontrollen ser ut i nuläget genom en intervju med företaget Business Controller. Den empiriska delen är uppbyggd efter COSO-modellens fem komponenter och under varje rubrik återges vad som kommit fram i intervjun för just den komponenten och därefter reflekterar jag om vad som kunde ändras och förbättras. Detta för att ge läsaren möjlighet att specifikt läsa om varje komponent samt direkt därefter få läsa reflektionerna.

I den empiriska delen kommer det fram att det finns en del saker Företag X borde ändra på och förbättra för att uppnå en god intern styrning och kontroll men man kan ändå dra slutsatsen att man har en intern kontroll och att personalen förstår innebörden med den vilket är en väldigt viktig del. Inom företaget finns också flera väldigt bra kontrollaktiviteter och man jobbar för att förbättra dem och ta fram nya.

Några saker som företaget måste förbättra är bl.a. att utbilda sin personal till än högre grad än man gör just nu, man måste följa upp inköpsgränserna noggrannare, skapa tydliga riktlinjer om vem som får godkänna fakturor samt för vilket belopp och man måste öka övervakningen av den interna kontrollen från ledningen och styrelsen. Resultatet av undersökningen blev alltså en checklista där företaget har listat tio konkreta punkter man borde förbättra för att få en bättre intern kontroll och på det viset även öka effektiviteten, tillförlitligheten och produktiviteten inom företaget.

Källförteckning

Ahokas, N., 2012. *Yrityksen sisäinen valvonta.* Jyväskylä: Edita Publishing OY.

Arwinge, O., 2015. *En introduktion till intern styrning och kontroll.* Stockholm: Olof Arwinge och Sanoma utbildning AB.

Committee of Sponsoring Organizations of the Tradeway Comission, 2013. *COSO Internal Control - Integrated Framework Principles.* [Online]
Available at: https://www.coso.org/Documents/COSO-ICIF-11x17-Cube-Graphic.pdf
[Använd 30 09 2017].

Committee of Sponsoring Organizations of the Tradeway Comission, 2017. *Enterprise Risk Management Integrating with Strategy and Performance.* [Online]
Available at: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf
[Använd 11 10 2017].

COSO Advisory Council Outreach Material, 2017. *Corporatecompliance.org.* [Online]
Available at:
https://www.corporatecompliance.org/Portals/1/PDF/Resources/past_handouts/euroCEI/2017/602_slides_A4_2.pdf
[Använd 11 10 2017].

COSO, 2013. *Internal Control - Integrated Framework.* [Online]
Available at: https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf
[Använd 09 09 2017].

COSO, u.d. *About us: COSO.* [Online]
Available at: https://www.coso.org/Pages/aboutus.aspx
[Använd 05 09 2017].

Internrevisorerna, 2013. *COSO internal controll - executive summary.* [Online]
Available at: http://www.theiia.se/uploads/intern_styrning_exicutive_summary.pdf
[Använd 16 09 2017].

PwC, G. W. o. J. W. -., 2014. *inyett.se.* [Online]
Available at: https://www.inyett.se/assets/pdf/PwC_VardetAvInternKontroll.pdf
[Använd 16 10 2017].

Wikland, T., 2014. *Intern styrning och kontroll- både lönsamt och säkert.* Stockholm: FAR Akademi AB.

Värdepappersmarknadsföreningen, 2017. *Vad är corporate governance.* [Online]
Available at: https://cgfinland2.fi/sv/vad-ar-corporate-governance/corporate-governance-och-lagstiftningen-i-finland/

Värdepappersmarknadsföreningen, u.d. *Finsk kod för bolagsstyrning 2015.* [Online]
Available at: https://cgfinland2.fi/wp-content/uploads/sites/6/2015/10/hallinnointikoodi-2015sveweb.pdf
[Använd 11 10 2017].

Intervju med Företag X:s Business Controller - 2017

Intervju angående den interna kontrollen inom Företag X

1. Hur skulle du beskriva den interna kontrollen inom Företag X?
2. Arbetar ni efter någon speciell model för intern kontroll?
3. Finns det nedskrivna och tydlogt beskrivna mål med verksamheten, vinstmål, kunder,marknader?

Kontrollmiljö

- Känner personalen till innebörden med intern styrning och kontroll?
- Ger ledningen en god ton för kontrollmiljön?
- Har ledningen gjort upp lämpliga befogenhets- och ansvarsfördelningar?
- Erbjuds utbildningstillfällen för de anställda inom företaget?

Riskbdömning

- Hur identifirerar, bedömmer och hanterar man risker i företaget?
- Har man en löpanande och integrerad riskbedömning?
- Finns det tydligt uppsatta och nedskrivna mål?
- Hur ser man på möjligheten till bedrägeri?

Kontrollaktiviteter

- Använder man sig av granskare och godkännare av fakturor?
- Hur övervakar man inköp? Vem kan köpa, hur mycket, följs det upp tillräckligt?
- Finns det spärrar i ERP systemen som gör att alla inte slipper till alla ställen?
- Finns det riktlinjer för alla procedurer, t.ex transkationer, försäljning, inköp?

Information och kommunikation

- Hurudana kommunikaitonskanaler använder ni er av?
- Hur förmdelas information om intern styrning och kontroll till personalen?
- Vet alla anställda om sin roll och ansvarsområde när det gäller intern kontroll?
- Vet de anställda om vem man ska rapportera till vid oegentligheter?

Övervakning och uppföljning

- Hurudana uppföljning och utvärderings processer har man för den interna kontrollen?
- Övervakar styrelsen och ledningen den interna kontrollen tillräckligt?

Riskhantering

- Hur skulle du beskriva riskhanteringen inom Företag X?
- Hur beaktas risk vid strategiska samt affärsbeslut?
- Har man lagt upp någon riskaptit för företag