

Intern styrning och kontroll

Malin Sundberg



32:2019

Datum för godkännande: 22.05.2018
Handledare: Christer Kullman

EXAMENSARBETE

Högskolan på Åland

Utbildningsprogram:	Företagsekonomi
Författare:	Malin Sundberg
Arbetets namn:	Intern styrning och kontroll
Handledare:	Christer Kullman
Uppdragsgivare:	-

Abstrakt

Efter flera företagsskandaler som skett runt om i världen har fler fått upp ögonen för intern kontroll. Intern styrning och kontroll är viktigt hos företag för att hålla ordning och reda inom företaget men även för att undvika bedrägerier och fel. COSO:s ramverk om intern styrning och kontroll är det mest använda ramverket idag och består av fem komponenter: Riskbedömning, kontrollmiljö, kontrollaktiviteter, information och kommunikation samt övervakning och uppföljning.

Syftet med det här arbetet är att ge en inblick i vad intern styrning och kontroll är och ta reda på hur ett åländskt företag jobbar med intern styrning och kontroll samt riskhantering.

Arbetet består av en kvalitativ undersökningsmetod och tar upp hur företaget jobbar med de olika komponenterna i COSO-modellen. Det intervjuade företaget kan i det här arbetet anses ha väl fungerande interna kontroller och jobbar med intern styrning och kontroll samt riskhantering dagligen och vill hela tiden förbättra den interna kontrollen.

Nyckelord (sökord)

Intern kontroll, COSO, riskhantering

Högskolans serienummer:	ISSN:	Språk:	Sidantal:
32:2019	1458-1531	Svenska	42 sidor

Inlämningsdatum:	Presentationsdatum:	Datum för godkännande:
09.04.2018	15.05.2018	22.05.2018

DEGREE THESIS

Åland University of Applied Sciences

Study program:	Business administration
Author:	Malin Sundberg
Title:	Internal control
Academic Supervisor:	Christer Kullman
Technical Supervisor:	-

Abstract

Internal control has become an important subject in the world. Internal control is necessary for companies to keep order and to avoid fraud. COSO is the most widely used framework in internal control. The framework consists of five components: control environment, risk assessment, control activities, information and communication and monitoring activities.

The purpose of this degree thesis is to learn more about internal control and to see how an organization on the Åland Islands works with internal control and risk management.

This thesis contains a qualitative investigation, an interview with an anonymous company on the Åland islands. The conclusion of this thesis shows that the interviewed company had a good internal control and works with risk management and internal control on a daily basis and always trying to improve their internal control.

Keywords

Internal control, COSO, risk management

Serial number:	ISSN:	Language:	Number of pages:
32:2019	1458-1531	Swedish	42 pages

Handed in:	Date of presentation:	Approved on:
09.04.2018	15.05.2018	22.05.2018

INNEHÅLLSFÖRTECKNING

1. INLEDNING	6
1.1 Syfte	7
1.2 Problemdiskussion	7
1.3 Avgränsningar	7
1.4 Arbetets disposition	7
2. METOD	9
2.1 Forskningsmetoder	9
2.2 Intervju	9
3. TEORI	11
3.1 Bakgrund	11
3.1.1 Vad är interna kontroller?	11
3.1.2 Corporate governance	12
3.2 COSO:modellen	14
3.2.1 Mål	16
3.2.2 Riskbedömning	17
3.2.3 Styr- och kontrollmiljö	18
3.2.3 Kontrollaktiviteter	20
3.2.5 Information och kommunikation	21
3.2.6 Övervakning och uppföljning	22
3.2.7 Helheten av de 5 komponenterna	24
3.3 Nyttan med interna kontroller	24
3.3.1 Kännetecken på fungerande intern kontroll ur redovisningsperspektiv	26
3.4 Riskhantering	27
3.4.1 COSO ERM - företagsövergripande riskhantering	28
4. EMPIRI	31
4.1 Bakgrund	31
4.1.1 Riskbedömning	32
4.1.2 Kontrollmiljö	32
4.1.3 Kontrollaktiviteter	33
4.1.4 Information och kommunikation	33
4.1.5 Övervakning och uppföljning	34
4.1.6 Företagsövergripande riskhantering	34
5. ANALYS	35
6. SLUTDISKUSSION	38
6.1 Validitet och reliabilitet	39

6.2 Förslag till vidare forskning	39
KÄLLOR	41
BILAGOR	43

1. INLEDNING

Intern kontroll och styrning är idag ett väldigt aktuellt ämne på grund av många stora företagsskandaler som skett runtom i världen. Till exempel under 1980 talet inträffade flera borssskandaler i USA med både bedrägerier och förfalskad finansiell rapportering. Dessa händelser ledde sedan till att COSO skapades - ett ramverk som skulle minska företagsskandalerna. (Wikland, 2014)

Enligt en undersökning Pwc har gjort i Sverige år 2012 så hade drygt vart femte företag blivit utsatt för någon slags form av ekonomisk oegentlighet under de senaste 12 månaderna. Verksamheter som hanterar kontanter, som till exempel affärer eller banker, är mer utsatta för risken än de som inte hanterar kontanter. Dock finns alltid chansen att drabbas ändå. Enligt Arwinge finns det många som tror att det inte kommer hända dem eller att det inte finns några möjligheter att skydda sig mot oegentligheter. (Danielsson, 2012)

Genom både ny lagstiftning och bolagsstyrningskoder som innehåller begreppet intern kontroll, har det också blivit ett mer uppmärksammat ämne. För många är idag interna kontroller ett känt begrepp men det finns fortfarande företagsledare som är obekanta med begreppet enligt Arwinge. Många känner förstås till interna kontroller men har sedan ingen kunskap om de olika komponenterna och principerna. (Arwinge, 2015)

Intern kontroll och styrning kan lätt uppfattas som fler regler och riktlinjer att anpassa sig till men att använda sig av interna kontroller kan tillföra ett stort värde hos organisationer. Att arbeta med intern kontroll och styrning kan skapa en ökad effektivitet, större konkurrenskraft och färre oväntade händelser i organisationen. Nyttan av arbetet med interna kontroller är att det både tar hänsyn till lagkrav men kan även skapa ett bättre resultat för företaget (Arwinge, 2015)

Intern kontroll och internrevision kan ibland förväxlas. Det är två olika saker, dock är intern kontroll viktigt i internrevisorns jobb. Internrevision utgör även en del av företagets internkontrollsystem. Så man kan säga att intern kontroll är en slags revision företaget gör

själv. Intern kontroll fungerar som ett verktyg för företag att vara säkra på att transaktioner dokumenteras på ett pålitligt sätt. Ett väl fungerande internkontrollsystem ska inte låta fel, misstag och bedrägerier få uppstå. (Carrington, 2014)

1.1 Syfte

Syftet med det här arbetet är att ge en inblick i vad intern kontroll och styrning är, ta reda på hur ett åländskt företag arbetar med intern kontroll, vilka risker de anser finns i deras verksamhet och vad de har för åtgärder för att hantera riskerna.

1.2 Problemdiskussion

Interna kontroller har blivit ett mer aktuellt ämne och fler har börjat tänka på interna kontroller. Börsnoterade företag är tvungna att ha fungerande interna kontroller i och med nya lagar. Det finns mycket positivt med interna kontroller men det kan även kosta en del pengar och därför kanske många företag inte tycker det är värt det när de inte är tvungna att ha interna kontroller, dock har de flesta företag någon slags intern kontroll trots att de kanske inte är medvetna om det. Eftersom det på Åland inte finns så många börsnoterade företag som enligt lagar måste ha interna kontroller så tycker jag det är intressant att se hur de icke noterade bolagen ställer sig till interna kontroller och hur de jobbar med dessa.

1.3 Avgränsningar

I de här arbetet har jag valt att avgränsa mig till den interna kontrollen inom den finansiella rapporteringen. Jag har valt att ta upp ramverket COSO i detta arbete, vilket är det mest använda ramverket för intern kontroll. (Widengren & Wendt , 2014) Jag kommer även nämna riskhantering i detta arbete då intern kontroll och riskhantering hör ihop på många plan.

1.4 Arbetets disposition

Arbetet består av sex stycken kapitel. Kapitel ett består av syftet och problemdiskussion. I kapitel två finns en genomgång av vald metod till undersökningen. Kapitel tre består av teorin - först förklaras vad interna kontroller är och corporate governance, sedan förklaras COSO-modellens alla komponenter samt riskhantering. Kapitel fyra består av intervjun med

Företag A, intervjun är upplagd enligt COSO-modellens fem komponenter, i kapitel fyra redovisas hur företaget tillämpar varje komponent i verkligheten. I kapitel fem analyseras svaren från undersökningen och arbetet sammanfattas i kapitel sex.

2. METOD

2.1 Forskningsmetoder

Forskning är att hitta ett ämne som intresserar en att fördjupa sig i, meningen med forskningen kan vara att lösa problem eller se samband. Detta görs genom att söka efter ny kunskap eller att använda sig av befintlig kunskap på nya sätt. Det finns två olika metoder att använda sig av, antingen kvantitativ eller kvalitativ metod. (Olsson & Sörensen, 2011)

En kvantitativ undersökning består framförallt av siffror och fokus ligger på mängd, antal och frekvens av variabler som kan analyseras och bearbetas statistiskt. I kvantitativa undersökningar är forskaren objektiv och har ofta en kort eller ingen kontakt alls med respondenten. I dessa undersökningar handlar det ofta om att hitta samband mellan de olika variablerna. Kvantitativa undersökningar kan göras genom enkäter och frågeformulär. (Christensen, Engdahl, Gräås, & Haglund, 2010)

Kvalitativa undersökningar består av ord, text och symboler. Fokus läggs på ordens mening och innebörd, stor vikt läggs på själva helhetsförståelsen och sammanhanget. Beskrivningen av verkligheten genom text och modeller har ett syfte att upptäcka och belysa sammanhang som växt fram. I analys av kvalitativ data är det viktigt att undersökaren har en subjektiv förmåga att se på materialet för att tolka det kvalitativa datamaterialet som det är och inte det som den väntat sig. Kvalitativa undersökningar genomförs ofta genom intervjuer, observationer eller fallstudier (Christensen, Engdahl, Gräås, & Haglund, 2010)

Det här arbetet kommer bestå av en kvalitativ undersökningsmetod då min undersökning går ut på att se hur ett företag arbetar med intern styrning och kontroll och jag vill gå in på djupet och få en förståelse hur teorin fungerar i praktiken och se om det finns några samband.

2.2 Intervju

Beroende på undersökningens problem och syfte kan intervjuer användas som undersökningsmetod. I de undersökningar där meningen är att identifiera och lyfta fram bakomliggande fakta till respondentens syn på det som skall undersökas passar det med intervjuer. När undersökningsområdet är komplext och de målgruppen är högre chefer eller experter kan den personliga kontakten vara avgörande för om respondenten kommer besvara frågorna. Det kan vara svår att använda sig av enkätundersökning när frågorna är många, komplexa eller öppna. Därför är en intervju passlig då undersökaren har möjlighet att ställa följdfrågor och utveckla eller förtydliga svaren.(Christensen, Engdahl, Gräås, & Haglund, 2010)

Det är viktigt att ha syfte och problemområde färdigställt innan undersökningen genomförs för att kunna få ett bra resultat av intervjun. En intervju är en dialog mellan minst två personer och ett samarbetsvilligt klimat behöver skapas för att uppnå bra svar. (Olsson & Sörensen, 2011)

Strukturerade intervjuer innebär att en mängd frågor skall ställas i ordningsföljd. Semistrukturerade intervjuer handlar om att undersökaren har gjort en färdig lista på teman och frågor som kommer ställas under intervjun. Vid ostrukturerade intervjuer finns inte en lista på teman utan det diskuteras fritt, dessa intervjuer används speciellt när området ska undersökas djupare. Sådana här intervjuer används då det inte bara handlar om att ta reda på vad och hur något är på ett sätt utan också varför - de bakomliggande orsakerna. (Christensen, Engdahl, Gräås, & Haglund, 2010)

Arbetet kommer bestå av en semistrukturerad intervju eftersom en rad olika teman med färdiga frågor kommer gås igenom på intervjun men frågorna behöver inte ställas i ordningsföljd och intervjun ska kunna innehålla öppna diskussioner med följdfrågor.

3. TEORI

I teoridelen kommer jag ta upp begreppet intern styrning och kontroll och corporate governance. Bakgrunden till COSO:s modell för intern styrning och kontroll och COSO:s fem komponenter samt företagsövergripande riskhantering som är en stor del av den interna kontrollen. Jag kommer även ta upp värdet företag kan uppleva av intern kontroll.

3.1 Bakgrund

Vad är egentligen intern kontroll och styrning? Intern kontroll och styrning kommer ifrån engelskans Internal control och har tidigare översatts till svenska som endast intern kontroll. Ämnet är mycket bredare än vad som tidigare ansetts, det handlar till stor del hur hela företaget skall styras till lönsamhet och regelefterlevnad samt minska bedrägerier. Allt eftersom företagsbedrägerier och fuskande skett genom åren så har intern kontroll och styrning blivit ett mer känt begrepp mycket tack vare COSO och bolagsstyrningskoder. Det finns flera modeller och ramverk för intern styrning och kontroll såsom Basel för banksektorn, Solvens i försäkringssektorn och comply-or-explain-modellen som är en allmänt accepterad modell som kommer från Storbritannien. (Arwinge, 2015) COSO är det mest kända ramverket inom ämnet och därför har jag valt ta upp just COSO:s modell för intern styrning och kontroll.

3.1.1 Vad är interna kontroller?

Intern styrning och kontroll är en av grundpelarna för att ha en stabil och tillförlitlig verksamhet. De flesta företag har någon slags intern kontroll. Utan någon intern kontroll finns många risker och en osäkerhet finns inom företaget, har till exempel företaget fått betalt från kunder? Finns det pengar på banken och har varor levererats innan betalning sker? Trots att organisationen inte har någon strukturerad linje angående intern kontroll så finns det mer eller mindre användning av interna kontroller i de flesta verksamheter. (Widengren & Wendt, 2014)

Ett internkontrollsystem som är effektivt låter inte fel, misstag och förfalskningar/bedrägerier förekomma inom organisationen. Företagsledningen i sin roll som förvaltare av aktieägarnas kapital och som arbetsgivare för företagets anställda, har huvudansvaret att säkerställa att den interna kontrollen fungerar och att verksamheten drivs på ett bra sätt. (Carrington, 2014)

Interna kontroller anses ofta vara yttre krav för företag att anpassa sig till, det stämmer delvis men fler och fler menar att det även är en framgångsfaktor för företag att implementera interna kontroller i sin verksamhet. (Wikland, 2014)

Så här definierar Arwinge och COSO intern styrning och kontroll:

“Intern kontroll är ett styr- och kontrollsystem som bidrar till att företag och organisationer med rimlig säkerhet når sina målsättningar inom olika områden” (Arwinge 2015)

“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, rapporteringen och följsamhet gentemot lagar och regler” (Carrington, 2014)

Ordning och reda är en förenklad beskrivning av interna kontroller. Genom goda interna kontroller uppnår man ordning och reda i företaget. Enligt Wikland (2014) finns det fem kännetecken för en god intern kontroll:

1. Att lägga upp tydliga mål för företaget och ha konkreta mål kopplat till affärsverksamheten, kunder, marknaden, ägare och så vidare som gör det lättare att fokusera på vad den interna kontrollen ska säkerställa.
2. Hantera de risker som finns så att målen kan uppnås.
3. Det finns många olika risker, därför ska fokus ligga på de största och mest relevanta riskerna som kan leda till att målen ej uppnås.
4. Ledningen i företaget bör vara involverade i arbetet med den interna kontrollen och visa engagemang. Det är en viktig faktor för att arbetet med kontrollen ska bli framgångsrik.
5. Identifiera och hantera riskerna genom olika kontrollåtgärder.

Meningen med interna kontroller är att öka tillförlitligheten och kvalitetssäkra data, detta genom olika sorters kontrollaktiviteter. Ett rätt utformat kontrollsystem leder till att företag kan uppvisa en rättvisande bild av redovisning, att de följer lagar regler och uppnår mål angående effektivitet. Genom att hela tiden följa upp effektiviteten i de interna kontrollsystemen kan ledningen säkerställa att verksamheten i företaget bedrivs korrekt. (Arwinge, 2015)

3.1.2 Corporate governance

Den interna kontrollens ökade betydelse beror mycket på bolagsstyrningens utveckling de senaste 20 åren. Under de senare åren har kraven på bolagsstyrning ökat hos intressenterna. Kraven beror på uppmärksammade problem i företag och ändringar i aktieägarmönster. (Arwinge, 2015)

Det finns ingen direkt definition av begreppet Corporate governance, men översatt till svenska betyder det bolagsstyrning. Värdepappersmarknadsföreningen definierar corporate governance som ett system med vilket företagsverksamheten leds och kontrolleras. (Värdepappersmarknadsföreningen, u.d)

Koden för bolagsstyrning är en samling med 28 stycken rekommendationer som handlar om god förvaltningssed för börsbolag: Dessa rekommendationer kompletterar de skyldigheter som finns i lagstiftningen. År 2015 kom den senaste bolagsstyrningskoden ut, i koden ingår rekommendationer om bolagsstämman, förvaltningsrådet, styrelsen, styrelsens kommitteér, verkställande direktören, den övriga ledningen, belöning, intern övervakning, riskhantering, intern revision, insiderförvaltning och revision. (Värdepappersmarknadsföreningen, u.d)

Meningen med corporate governance är att främja förtroendet på värdepappersmarknaden, att säkerställa att noterade bolags förvaltning är av hög standard, främja kvalitet och internationell jämförbarhet.. Koden ska följas av alla börsnoterade bolag på Nasdaq Helsinki Oy. (Värdepappersmarknadsföreningen, u.d ; Finsk kod för bolagsstyrning,2015) I bolagsstyrningskoden tas intern kontroll och riskhantering upp i rekommendation 25 och 26.

Rekommendation 25 handlar om intern kontroll. De förklarar i bolagsstyrningskoden att genom att övervaka och styra sin verksamhet kan bolaget uppnå ett gott resultat. Det är styrelsens uppgift att fastställa verksamhetsprinciperna för den interna kontrollen och att bolaget följer upp hur den interna kontrollen och styrningen fungerar. (Finsk kod för bolagsstyrning, 2015)

Dessa verksamhetsprinciper ska sträva efter att uppnå företagets målsättningar. De ska även säkerställa att bolaget följer lagar och bestämmelser. Principerna för den interna kontrollen ska utformas från företaget. Verksamhetsprinciperna ska sedan redovisas i bolagsstyrningsrapporten. (Finsk kod för bolagsstyrning, 2015)

Rekommendation 26 handlar om riskhantering. Meningen med riskhantering är att hitta de risker som skulle kunna påverka affärsverksamheten i bolaget. Dessa risker bör identifieras, bedömas och följas upp. För att uppnå en effektiv riskhantering behöver bolaget ta fram principer för riskhantering och fastställa dessa. (Finsk kod för bolagsstyrning, 2015)

Att ge investerare kännedom om bolagets verksamhetsrisker samt hur dessa hanteras är viktigt i bedömningen av företaget. Därför är det viktigt att ge tillräcklig information om riskhanteringen. Riskhanteringsprinciperna ska redogöras för i bolagsstyrningsrapporten. Även lagstiftningen förutsätter att verksamhetsberättelsen ska innehålla de största riskerna och osäkerhetsmomenten. (Finsk kod för bolagsstyrning, 2015)

3.2 COSO:modellen

Idag finns flera olika ramverk och standarder att välja mellan. Många har försökt definiera begreppet intern kontroll under flera årtionden. COSO skapades efter de börsskandaler som inträffade i början på 1980-talet vilka berodde på bedrägerier och förskönad finansiell rapportering. (Arwinge, 2015 ; Wikland, 2014)

James V. Treadway var initiativtagaren av den kommitté som skapades 1985. I kommittén ingick fem professionella organisationer för controllers, externrevisorer, internrevisorer och andra företagsekonomer. Den kallades då Treadway-kommissionen eller COSO. De

undersökte orsakerna till bedrägerierna som inträffat och kom med en rapport med rekommendationer om åtgärder. COSO skapades alltså för att komma åt bedrägerier och förfalskad finansiell rapportering. (Wikland, 2014) COSO är en förkortning av "The Committee of the Sponsoring Organizations of the Treadway Commission".

Efter den första rapporten som kom 1987 skapades även anvisningar för hur företag ska styra och kontrollera företaget på ett bra sätt samt göra det synligt för de externa intressenterna. Då kom standarden som kallas för COSOs ramverk för intern styrning och kontroll. (Wikland, 2014) De gjorde då klarhet i att interna kontrollens syfte är att bidra till att företag når sina målsättningar inom tre huvudområden: regelefterlevnad, finansiell rapportering samt verksamhetens effektivitet och produktivitet. De delade även in intern kontroll i fem olika delar som tillsammans skulle leda till att målsättningar nås. (Arwinge, 2015)

Efter ramverkets publicering 1992 började det accepteras som standard. Det stora genomslaget för ramverket kom dock tio år senare genom lagen Sarbanes Oxley Act som ändrade mycket i amerikanska börsbolag. Ledning och ekonomichef i bolagen blev ansvariga för den interna styrningen och kontrollen, som skulle leda till korrekt och rättvisande finansiell rapportering. Det var även då COSO fick sitt stora genomslag tillsammans med den rekommenderade standarden för intern styrning och kontroll av den amerikanska finansinspektionen SEC. (Wikland, 2014)

I maj år 2013 släpptes en ny utgåva av COSO ramverket. Ramverket är mer lättillgängligt och har utvecklats för att passa intressenters olika krav. Mycket i det nya ramverket från 2013 är samma som 1992, men Arwinge och Wikland anser att det nya ramverket har bättre struktur och är mer pedagogiskt. Det innehåller 17 principer som har fördelats i fem komponenter: Kontrollmiljö, riskbedömning, kontrollaktiviteter, information och kommunikation samt övervakning och uppföljning. De här komponenterna är utformade att de ska samverka, inom organisationens olika delar samt som en helhet. Meningen med ramverket är att det ska underlätta och upprätthålla arbetet med intern styrning och kontroll. (Arwinge & Wikland, 2013) Nedan kommer jag gå in närmare på de olika komponenterna.

3.2.1 Mål

Mål är inte en av de fem komponenterna i COSOs ramverk. Målen är dock viktiga för utan mål så blir det svårt att hitta riskerna i företaget. Wikland menar att målen kan vara uttalade eller underförstådda men att det är av stor vikt att de finns, ett exempel på det är att ett företag skulle ha som mål att bara finnas - då finns det risker kopplade till målet, alltså att företaget skall upphöra. Därför är det viktigt att först börja diskutera målen och sedan koppla riskerna till målen och ställa sig frågan - Vad skulle kunna hända för att inte målen kommer uppnås? (Wikland, 2014)

Målen ska vara tydligt framlagda, antingen muntligt eller skriftligt, det är viktigt att berörda förstår målen. Så desto tydligare målen är - desto lättare blir det att identifiera riskerna och hitta åtgärder för att minska dem. (Wikland, 2014)

COSO skiljer på olika sorters mål. De finns mål för rapportering och efterlevnad mot lagar och regler. De målen handlar om att följa externa krav och att anpassa verksamheten efter både lagar men även professionella rekommendationer. Målen har alltså att göra med att följa god redovisningssed och att det kan uppvisas en hög kvalitet i bokföringen. Exempel på de målen kan handla om kvartalsrapporter, årsredovisningar och att redovisningsprinciper följs. (Arwinge, 2015; Wikland, 2014)

Verksamhetens mål handlar om företagets effektivitet och produktivitet. Målen kan omfatta omsättning, lönsamhet, kundnöjdhet och utveckling. Dessa mål har inget med externa krav att göra utan målen utformas från företaget. Sådana mål kan vara svårare att uppnå eftersom det kan handla om allt från konkurrenter som tar marknadsandelar till väderförhållanden och konjunkturutveckling som hindrar målen. (Arwinge, 2015; Wikland, 2014)



Figur 1: Att utgå från givna mål (Wikland 2014)

Modellen ovan visar sambandet mellan alla komponenter i COSO-modellen och även hur viktigt det är att ha målen som utgångspunkt för komponenten riskbedömning. Alla dessa komponenter behöver samverka för att uppnå en bra intern styrning och kontroll. Är det en komponent som inte fungerar så kan inte de andra komponenterna heller fungera korrekt. Därför är helheten i COSO modellen viktig. (Wikland, 2014)

3.2.2 Riskbedömning

Alla organisationer utsätts för risker från både internt och externt. COSO definierar risk som möjligheter att negativa händelser kan ske och påverka så att organisationens mål inte uppnås. Risk hanteras enligt COSO-modellen på så sätt att det ska finnas en förståelse för kombinationen mellan sannolikhet och konsekvens. På det sättet ska riskerna sedan hanteras i organisationen och väsentliga risker ska bedömas med hänsyn till sannolikhet och konsekvens. (Committee of Sponsoring Organizations of the Treadway Commission, 2013; Wikland, 2014)

Externa faktorer som kan påverka företaget kan vara lagbaserade faktorer, teknologiska och marknadsmässiga. Interna faktorer kan vara problem med IT och affärssystem, förändringar i ledning och organisation, problem med styrelsens roll och ledning samt kompetensen hos anställda eller inhyrd personal. (Wikland, 2014)

Som jag tagit upp tidigare så är det viktigt att riskerna ska identifieras utifrån målsättningarna men sedan ska man även ta ställning till vilken toleransnivå som finns gentemot riskerna. Riskbedömningen är dock inte bara knutet till målsättningar inom organisationen utan även till risktolerans. Vissa risker kan inte helt undvikas så det kan leda till att man måste acceptera risken eller försöka reducera den. Riskbedömningen ska även uppdateras löpande, det är nödvändigt att vid ändringar i omgivningen, organisationen, affärsmodellen samt vid IT och processer se över riskerna. (Arwinge & Wikland, 2013; Arwinge, 2015)

Riskbedömningen består av fyra principer i COSO modellen:

1. Att precisera målen så tydligt för att kunna identifiera och värdera riskerna som rör målsättningarna.
2. Identifiera risker för att målen inte uppnås i alla nivåer inom organisationens delar som grund för att kunna avgöra hur riskerna ska leda till åtgärder. Det vill säga att man går igenom alla risker för att sedan gå vidare med hur man ska hantera dem.
3. Organisationen bör ta hänsyn till möjligheterna för bedrägerier när riskerna för att målsättningar inte uppnås bedöms. Den här punkten har tagit mer plats i det uppdaterade ramverket år 2013 jämfört med det från 1992 då alla organisationer inte tagit den punkten på tillräckligt allvar.
4. Att identifiera och värdera förändringar i organisationen som kan påverka den interna styrningen och kontrollen. Här ska man ta i beaktande de inträffade, pågående och kommande förändringar i verksamheten och det ska läggas stor vikt vid dessa i riskbedömningen.(Wikland, 2014)

Den tredje punkten i de fyra principerna har fått tagit mer plats i det uppdaterade ramverket på grund av att oegentligheter ökade i amerikanska bolag sedan ramverket från år 1992. Men i och med att denna punkt har markerats extra noga betyder det inte att de andra punkterna skulle ha minskat i betydelse. (Arwinge & Wikland, 2013)

3.2.3 Styr- och kontrollmiljö

Arwinge(2015) anser att kontrollmiljön är den viktigaste komponenten i företagens interna kontroll. Komponenten handlar om att skapa strukturer, roller och ansvar för att följa upp kontroller från styrelsenivå. I kontrollmiljön är ledningens styrande och deras attityder för risker och risktagande viktiga. (Arwinge, 2015) Kontrollmiljön ska ange tonen i organisationen och skapa en medvetenhet hos medarbetarna om betydelsen av styr- och kontrolls signaler. (Wikland, 2014)

Det finns fem principer som förklarar styr- och kontrollmiljön:

1. Organisationen ska visa att den lägger stor vikt vid etiska värden och integritet. Arbetskulturen ska präglas av etiska värden genom att ledningen ska tydliggöra vad som är rätt och fel för att uppnå målsättningar. Det är viktigt att ledningen är ett gott föredöme.
2. Styrelsen fungerar självständigt gentemot ledningen och har som uppgift att övervaka utveckling och resultat i den interna styrningen och kontrollen. Styrelsen kan inte förvänta att ledningen sköter kontrollen - utan de behöver garantera att ledningen faktiskt arbetar med det. Styrelsen kan då ge anvisningar om hur den interna kontrollen ska skötas samt få reda på viktiga förändringar och problem som har upptäckts. Styrelsen har det viktigaste ansvaret i den interna kontrollen för att se till att den faktiskt fungerar genom att definiera roller och ansvar för själva uppföljningen.
3. Ledningens uppgift är att ta fram rapporteringslinjer samt göra en ansvars- och befogenhetsfördelning för att nå målsättningarna, det ska självklart ske under styrelsens tillsyn. Verkställande direktörens uppgift är då att delegera mandat vidare i organisationen - genom fullmakter och attestinstruktioner. De bildas då en struktur i organisationen med ledningen i styrelsen i toppen som övervakar att ledningen delegerar ut ansvar för att skapa en slags infrastruktur som är nödvändig för den interna kontrollens funktion.
4. Organisationen ska visa att den försöker attrahera, utveckla och behålla kompetent personal i enlighet med målen. Kompetenskraven för olika sorters arbetsuppgifter behöver vara kända och följas noggrant vid rekrytering. Det är även viktigt att hänga med i utvecklingen och övervaka ifall en kompetensutveckling kan vara nödvändig.
5. Organisationen kan hålla individen ansvarig för befogenheter den besitter. Ansvar och befogenheter ska göras tydliga inom organisationen så att medarbetare känner till

dessas och vad de har för roll i det hela, samt att de även vet att de kommer följas upp. (Arwinge, 2015; Committee of Sponsoring Organizations of the Treadway Commission, 2013; Wikland, 2014)

3.2.3 Kontrollaktiviteter

Kontrollaktiviteterna är en del av företagets riskbehandling. Tittar man tillbaka har kontrollaktiviteterna tagit störst plats inom intern styrning och kontroll, detta har till viss del bidragit till att företag fokuserat endast på kontrollaktiviteter som checklistor och inte utgått ifrån mål, strategier och risker. Wikland(2014) menar att effektiva kontroller skapas när man matchar kontrollerna mot målen, de viktigaste riskerna och styr- och kontrollmiljön. Ett exempel på det är när företaget går med förlust och deras största risk är konkurs, då ska kontrollaktiviteterna kopplas till detta till exempel genom att särskilt bevaka att företaget får betalt för sålda varor i tid samt att nya och gamla kunder tas väl omhand. (Arwinge, 2015; Wikland, 2014)

Kontrollaktiviteter består av riktlinjer och rutiner som gör att ledningens beslut uppfylls. Kontrollaktiviteterna är en stor mängd olika sorters aktiviteter, COSO anser att de i så hög grad som möjligt ska integreras i verksamheten. Kontrollaktiviteter kan till exempel vara rutiner för godkännande, verifieringar, befogenhetsöverföringar, uppföljningar, kontrollberäkningar och även mer automatiserade kontroller i dagens läge. (Wikland, 2014)

Genom tre stycken principer förklarar COSO kontrollaktiviteternas innebörd:

1. Organisationen behöver välja ut samt utveckla kontrollaktiviteter som ska reducera riskerna relaterade till målsättningarna. Riskerna kan kanske inte reduceras helt, men de ska tas till en nivå som är acceptabel. Kontrollerna ska skapas genom aktiva val och kunna utvecklas, inte bara "göra det som alltid gjorts".
2. De IT-baserade kontrollerna har fått större betydelse inom komponenten kontrollaktiviteter och det ställs större krav på kontroller som berör IT.

Organisationen ska välja ut och utveckla övergripande kontroller gällande IT för att nå målsättningar. COSO betonar särskilt behovet av kontroll över IT som infrastruktur.

3. Sedan ska organisationen genomföra kontrollaktiviteter genom policies, som är riktlinjer och förhållningsregler inom olika områden. De ska göra klart vad som förväntas och se till att policies genomförs. Det är sedan viktigt att de efterlevs och följs upp. (Wikland, 2014)

3.2.5 Information och kommunikation

Kommunikation behövs i organisationen för en fungerande intern styrning och kontroll. Information och kommunikation kan man säga att är en stödjande komponent inom den interna kontrollen. Styrelsen, ledningen och medarbetare behöver kommunicera både internt och externt så att intressenter och aktörer får reda på informationen. Informationen är viktig så att anställda kan sköta arbetsuppgifter och ledningen kan styra verksamheten. (Arwinge, 2015; Wikland, 2014)

Med kommunikation menas dialoger mellan två eller flera personer. För att inte information ska filtreras bort behöver det vara "högt i tak" i företaget och verksamheten. Wikland menar att detta speciellt är viktigt för att kunna föra vidare uppgifter angående avvikelser, felaktigheter, bedrägerier samt inre och yttre hot. Många kan känna att de annars inte vågar vara så kallade "whistleblowers", alltså att lämna känsliga uppgifter, och dessa blir oftast motarbetade eller straffade istället för att belönas. (Wikland, 2014)

När informationen kommuniceras internt på flera nivåer i organisationen - både upp, ner och sidledes i organisationen finns det risker att viktig information faller bort på vägen. COSO påpekar att informationen behöver kunna flöda fritt i en organisation. Informationen och kommunikationen handlar om att försäkra sig att de övriga komponenterna i COSO modellen ska fungera effektivt. (Arwinge & Wikland, 2013; Committee of Sponsoring Organizations of the Treadway Commission, 2013; Wikland, 2014)

Det finns tre principer som förklarar komponenten information och kommunikation:

1. Organisationen ska ta emot eller skapa och använda väsentlig samt kvalitetssäkrad information för att stödja den interna styrningen och kontrollen. Vilket betyder att kraven på information i de övriga komponenterna är klarlagda och att den väsentliga informationen fångas upp.
2. Det är viktigt att informationen når fram till dem som behöver den. Organisationen ska kommunicera informationen internt som ska berätta om mål och ansvar inom den interna styrningen och kontrollen så att anställda, ledningen och styrelsen vet sina ansvarsområden och roller. Det är även till den här principen visselblåsarfunktionen hör, samt att de upprättade kommunikationskanalerna fungerar.
3. Den tredje principen handlar om hur organisationen ska kommunicera med externa parter. Det skall finnas processer upprättade för att kommunicera med organisationens externa intressenter. De externa intressenterna kan vara börsen - för noterade bolag eller tillsynsmyndigheter, men kan även gälla kunder, leverantörer, externrevisorer och ägare. (Wikland, 2014)

3.2.6 Övervakning och uppföljning

Uppföljningen och övervakningen hör ihop med kontrollmiljön, eftersom den ska utgå ifrån de roller, ansvar, strukturer och processer som lagts upp inom företagets kontrollmiljö. Uppföljningsområdet har länge varit underutvecklat, då det inte funnits några externa krav på att följa upp kontrollerna och det har ofta tagits för givet att en fungerande intern styrning och kontroll har varit effektiv och inte behöver följas upp. (Arwinge, 2015)

Komponenten övervakning och uppföljning ska bedöma hur den interna styrningen och kontrollen fungerar samt hur effektiv den är. Den interna styrningen och kontrollen kan lätt försämrats och försvagas, därför är övervakningen viktig. Organisationen måste även hålla uppsikt över förändringar i världen eller företaget och anpassa kontrollerna efter dessa. (Arwinge, 2015; Wikland, 2014)

Denna komponent ska användas för att identifiera olika slags avvikelser och brister i den interna kontrollen. Sedan behöver dessa avvikelser och brister kommuniceras vidare till berörda avdelningar. Även styrelsen ska få information om det finns väsentliga brister inom kontrollerna. För en god övervakning menar COSO att organisationen behöver ha löpande uppföljningar, separata utvärderingar och rapportera avvikelser.(Arwinge,2015;Wikland, 2014)

Övervakningen är viktig då företaget i god tid kan korrigera problem i den interna styrningen och kontrollen. Det leder till att informationen blir tillförlitlig och korrekt inför beslutsfattande och företaget kan förbereda finansiella rapporter som är korrekta. Det underlättar även att intyga och berätta om hur effektiv den interna styrningen och kontrollen är i olika rapporter. (Wikland, 2014)

De två sista principerna i COSO modellen handlar om övervakning och uppföljning:

1. Organisation ska välja ut, utveckla och genomföra löpande utvärderingar på att komponenterna i den interna styrningen och kontrollen finns och även fungerar. Det ska finnas både löpande och separata utvärderingar samt blandningar av dessa. Löpande utvärderingar ska integreras i verksamhetsprocesserna och de separata utvärderingarna utföras objektivt - så riskerna att resultatet av uppföljningen inte förskönas eller filtreras.
2. Sedan är det viktigt att utvärdera och kommunicera ut bristerna till berörda i god tid, de berörda har sedan ansvar över att åtgärda bristerna. Även styrelse och ledning ska informeras om det behövs och värdera hur utvärderingarna gått. Ledningen har ansvar över att bristerna faktiskt åtgärdas. (Wikland, 2014)

Wikland(2014) tar upp exempel på övervakande rutiner som COSO rekommenderar:

- Göra periodiska utvärderingar och även testa kontroller genom internrevisionen.
- Att använda sig av löpande övervakningsprogram som finns inbyggda i informationssystemen.
- Att ha en övergripande granskning av kontrollerna, som en normal del av hela processen.
- Analys och uppföljningar av arbetsrapporter eller mätningar som indikerar fel i kontroller.
- Kvalitetsgranskade genomgång av internrevisionen.

3.2.7 Helheten av de 5 komponenterna

De fem komponenterna i COSO-modellen har jag nu gått igenom var för sig. Däremot är det av stor vikt att dessa komponenter samverkar. De ska utformas och användas ihop då de påverkar varandra. Till exempel är kontrollmiljön viktig när riskerna värderas och hanteras, även hur uppföljningen görs har betydelse för hur kontrollaktiviteter utformas och används. De principer som hör till varje komponent behöver fungera för att hela företagets interna kontrollsystem ska vara effektivt. (Arwinge, 2015)

3.3 Nyttan med interna kontroller

Wikland(2014) menar att strängare lagstiftning inte ensamt kan styra utvecklingen av den interna styrningen och kontrollen, utan utvecklingen bör drivas av nyttan med intern styrning och kontroll. Interna kontroller leder till förbättrade beslutsunderlag till ledning och styrelse, mer effektiva processer och en bättre kostnadskontroll. Ett värde uppstår vid god intern styrning och kontroll så som effektivare processer, ökat förtroende från intressenter, nya affärsmöjligheter och bevarat eller ökat anseende. (Widengren & Wendt , 2014)

Den direkta nyttan som uppstår av en bra intern kontroll och styrning är att organisationen kan undvika oväntade händelser med de mål som är uppsatta, bättre rapportering med färre fel och minskad risk för bedrägerier samt följa lagar och regler med mindre risk för lagbrott. Det vill säga att det finns ökade möjligheter att minska händelser som kan skada företaget.

Företag kan genom intern kontroll och styrning mildra händelser som skadar företaget och det kan leda till att lönsamheten ökar, dock ska nyttan av kontrollerna överstiga kostnaderna. Genom den ökade säkerheten inom företaget kan en ökad konkurrenskraft uppstå, jämfört med andra företag som inte satsar lika aktivt på intern kontroll. (Wikland, 2014)

Ytterligare värdeskapande aspekter kan vara möjligheter till förbättrat kreditbetyg hos kreditvärderingsinstitut. De bolag som anses vara välskötta värderas högre än andra bolag. Enligt undersökningar som gjorts i USA visar det att noterade bolag som har en god intern styrning och kontroll värderas avsevärt högre än de bolagen som har svag intern kontroll. (Wikland, 2014)

Enligt en undersökning gjord av PwC(2014) där de har tillfrågat 25 större företag om hur deras företagsledning har upplevt värdet kopplat till deras arbete med intern kontroll. Då förekom 8 värden flest gånger i svaren som är:

1. Bedrägerikontroll
2. Trygghet i korrekt och fullständig finansiell rapportering.
3. Genom klara regler och att ansvarsområdena tydliggjorts skapas en trygghet hos individerna i organisationen.
4. Efterlevnad av lagar och regler, vilket minskar kostnader för böter, juridiska processer och lagöverträdelser.
5. Efterlevnad av mål och strategiska planer.
6. Färre oväntade händelser i företaget, till exempel avvikelser från finansiella och operationella mål.
7. Kunna reagera proaktivt istället för reaktivt, vilket betyder att identifikation av risker sker innan det blir fel.
8. Mer enhetliga och ändamålsenliga processer i verksamheten. (Widengren & Wendt , 2014)

3.3.1 Kännetecknen på fungerande intern kontroll ur redovisningsperspektiv

I och med att mitt syfte är att ta reda på hur god interna kontroller ett företag har med inriktning på de finansiella rapporteringen så tänkte jag även ta upp kännetecknen på goda interna kontroller ur ett redovisningsperspektiv. När revisorn granskar företagets finansiella rapportering väljer den mellan att granska företagets interna kontroller eller substansgranskning. Valet beror på hur tillförlitliga kontrollerna är samt vilken metod som är mest kostnadseffektiv, dock görs oftast en kombination av granskningsmetoderna. (Carrington, 2014)

Det som revisorn i huvudsak granskar är redovisningssystemet och att de kontroller som hör till systemet fungerar. Det som är viktigast för ett välfungerande internkontrollsystem är kompetent och tillförlitlig personal som har en hög integritet. Har ledningen och personalen en hög kompetens och integritet så är de enligt Carrington(2014) kapabla till att hantera risker där övriga delar av internkontrollsystemet påvisar brister. En annan del som är väldigt viktig är att det finns tydligt definierade behörighets och ansvarsområden - så att inte frågor glöms bort och faller "mellan stolarna". Vetskapen om ansvar kan göra att personalen anstränger sig lite extra för att göra ett bra jobb inom sitt ansvarsområde. (Carrington, 2014)

Godkännande och attesteringsrutiner är även viktiga. Det är viktigt att rätt person på rätt nivå fattar besluten, som att köpa in material till en avdelning - bör vara den som har bäst koll på hur mycket material som förbrukas och kan bedöma behovet. Handlar det om att köpa större grejer som en kopianator bör det vara avdelningschefen som godkänner att den får köpas in. För att minska bedrägerier är det inte lämpligt att en person köper in en produkt, betalar fakturan samt registrerar betalningen i redovisningssystemet - då ökar möjligheterna för att personen ska kunna dölja misstag och medvetna bedrägeriförsök. (Carrington, 2014)

För ett fungerande internkontrollsystem bör även företaget ha en god dokumentation - vilket betyder att verifikationer bör vara numrerade och att det inte finns luckor. Det ska även finnas ett underlag till varje verifikation. Godkännande och attesteringar ska det finnas bevis på - en underskrift eller godkännande i ett datorsystem. (Carrington, 2014)

Det är även viktigt att organisationen skyddar och förvarar sina tillgångar i lokaler som är låsta och skyddade mot brand och vattenskador. Att det finns säkerhetskopior på dokumentation, programvaror och att dokumentation i pappersform arkiveras på ett tryggt sätt. Har företaget implementerat dessa komponenter som jag beskrivit ovan har de ett internkontrollsystem som fungerar enligt önskemål från revisorn. (Carrington, 2014)

3.4 Riskhantering

Interna kontroller och risk går hand i hand och intern kontroll är en del av företags riskbehandligssystem. Genom att använda, utforma och följa upp intern kontroll kan företagen välja att öka eller minska sina risker. Därför har COSO även skapat ett ramverk för företagsövergripande riskhantering som benämns COSO ERM, där ERM står för enterprise risk management. (Arwinge, 2015; Wikland, 2014)

Risk handlar om sannolikheten att något kommer inträffa, men även konsekvensen av att något inträffar. Risken är som jag nämnt tidigare knutet till företags mål, finns det inte några mål då kan man säga att det inte finns några risker. Därför är det viktigt att hos företaget först diskutera målen innan de diskuterar riskerna. Oftast pratas det om risker som oönskade händelser men det finns även risk kopplat till önskade händelser som då handlar om att ta risker för att nå ett mål. Ett exempel på det, som är en affärsrisk, är att ett företag vill ta sig in på en ny marknad där de skulle kunna uppnå en hög lönsamhet, men satsningen är dyr och risken finns att den kommer misslyckas, så är man beredd att ta den risken? (Wikland, 2014)

Det finns flera olika typer av riskbehandling och hur de olika riskerna kan hanteras. Riskerna kan helt *undvikas* vilket oftast görs när kontrollkostnaderna överstiger nyttan. Dessa risker kan vara att undvika att sälja produkter i ett visst land, undvika en viss produkt eller ta bort en målsättning för företaget. Företaget kan välja att *reducera* risken, vilket är den vanligaste riskbehandlingsmetoden. Intern kontroll används vid denna riskbehandlingstyp för att reducera att den upptäckta risken kommer ske eller mildra effekten av den. Ledningen behöver dock bedöma om kostnaden överstiger nyttan. En annan möjlighet är att *dela* risken om kostnaden för riskreducering är för stor. Delning av risken kan vara till exempel att

företaget tecknar en försäkring, utkontraktering eller olika former av hedging. Dock är det svårt att göra sig av med hela risken. Slutligen kan företaget välja att *acceptera* risken. Det görs oftast vid alldagliga risker där kostnaderna för kontrollåtgärder skulle vara orimliga och företaget får då stå ut med mindre incidenter och förluster. (Arwinge, 2015)

Ofta läggs fokus på att försöka reducera och minimera risker. Arwinge menar att för lite risktagande dock kan skapa ett stillastående, minskad innovationsförmåga och även minskad intjäning - däremot kan för mycket risktagande liknas vid spelande och då kan något oönskat hända förr eller senare. Det är därför viktigt att lägga ett tak och golv för vilka risker som kan tolereras och vilka risker som bör undvikas. Det kan även förklaras med begreppet riskaptit. Riskaptit handlar om att det läggs en accepterad nivå för risker för att kunna bestämma vilka risker som man tänker acceptera och vilka som behöver åtgärdas. Riskaptit definieras ofta som total mängd risk ett företag är villig att ta för att uppnå sina mål. (Arwinge, 2015)

3.4.1 COSO ERM - företagsövergripande riskhantering

Intresset för riskhantering har ökat och fler företag väljer att lägga fokus på det. Det har funnits ett behov av ett ramverk för att identifiera, värdera och hantera risker. Därför tog COSO initiativ år 2001 till att skapa ett ramverk tillsammans med PwC som skulle kunna användas av företagsledningar för att utvärdera samt förbättra företagets övergripande riskhantering. Ramverket för riskhantering ska inte ersätta ramverket för intern styrning och kontroll, utan meningen är att det ska ge ett mer djupgående fokus på riskhantering och integreras med den interna styrningen och kontrollen. Det svåraste hos företagets ledning är att bestämma hur mycket risk som kan accepteras - COSO ERM ska göra det lättare att möta de här utmaningarna. (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

Företagsövergripande riskhantering ska ge ledningen en möjlighet att effektivt kunna hantera osäkerhet med risker och möjligheter samt kunna öka möjligheter att skapa ett värde. Ledningen måste bestämma hur mycket osäkerhet som kan accepteras för att kunna öka värdet för intressenterna, då organisationen finns till för att skapa ett värde för dess intressenter. Ett maximalt värde uppnås när ledningen har som mål att uppnå en bra balans

mellan tillväxt, vinstmål och riskerna relaterade till det. Resurserna ska även användas effektivt och produktivt för att nå företagets mål. (Committee of Sponsoring Organizations of the Treadway Commission, 2004)



Figur 2: Enterprise risk management (The Committee of Sponsoring Organizations of the Treadway Commission, 2017)

COSO:s ramverk för företagsövergripande riskhantering består av fem stycken komponenter och tjugo principer. Modellen ovanför visar hur komponenterna ska samverka för att uppnå effektiv riskhantering. Nedan tar jag upp de fem komponenterna men jag kommer inte gå in närmare på principerna som hör till varje komponent.

1. **Styrning och kultur:** Med styrning menas att tonen i organisationen ska lägga stor vikt på riskhantering samt att det är viktigt att det finns ett tillsynsansvar över riskhanteringen. Kultur består av etiska värden, önskade beteenden samt en förståelse för risker inom organisationen.
2. **Strategi och mål:** COSO ERM, strategi och målsättning samverkar i en strategiplaneringsprocess. Riskaptiten används vid företagets strategi, affärsmålen sätter strategin i verket och används sedan som underlag för att bedöma, identifiera och åtgärda risker.

- 3. Hantering av riskerna:** Risker som kan påverka strategin och företagets målsättning måste identifieras och utvärderas. Riskerna ska sedan bedömas enligt riskaptit - vilka risker kan tas och vilka risker behöver åtgärdas eller helt undvikas. Organisation väljer hur den hanterar riskerna och rapporterar sedan riskerna till intressenterna - till exempel aktieägarna.
- 4. Granskning och revidering:** Genom att granska företaget kan de få se hur effektivt den företagsövergripande riskhanteringen fungerar i längden och vad för ändringar som kan behövas göras.
- 5. Information, kommunikation och rapportering:** Det är viktigt att nödvändig information delas både från interna och externa källor inom hela organisationen.
(Committee of Sponsoring Organizations of the Treadway commission, 2017)

4. EMPIRI

Företaget jag valt att intervjua är ett större företag på Åland och har i genomsnitt ca. 250 anställda. Intervjun genomfördes över telefon då det inte fanns möjlighet och träffas personligen. Hela intervjun tog lite över en halvtimme för att få svar på alla frågor och det fanns även möjlighet att ställa följdfrågor och utrymme för diskussion fanns. Jag fick även ta del av företagets dokument angående intern kontroll och riskhantering. Även företagets årsberättelse och hemsida har granskats.

4.1 Bakgrund

Företaget som intervjuats anser att den interna kontrollen fungerar bra inom företaget och är nöjda med hur den interna kontrollen ser ut idag. De arbetar medvetet med intern kontroll och anser att den interna kontrollen är väldigt nödvändig i företaget och de upplever en nytta av kontrollen. Den interna kontrollen är viktigt för att företaget ska fungera och att de anställda ska känna sig trygga i arbetet med tydliga riktlinjer hur de ska utföra sitt arbete. Företaget har inte upplevt några direkta nackdelar utan anser att det är viktigt att fokus läggs på rätt saker, som att till exempel inte titta på för små saker där åtgärderna inte ger ett tillräckligt stort värde. Istället försöker de lägga fokus på mer väsentliga brister som finns inom organisationen.

De arbetar kontinuerligt med att försöka upptäcka väsentliga brister eller fel och försöker åtgärda dem så fort de kan. Företaget har använt sig av COSO modellen och försöker följa de fem komponenterna och de har upplevt att COSO-modellen och dess komponenter fungerar bra i praktiken.

Företaget jobbar med mål på ekonomisidan som att leverera tillförlitlig finansiell rapportering och att självklart följa lagar och regler, men har även mål i den operativa verksamheten att åstadkomma effektivitet och där har de även mätbara mål som de sedan kan följa upp där även medarbetarna kan få ta del av resultatet.

4.1.1 Riskbedömning

Riskerna sammanställs varje månad och analyseras hur de skulle kunna påverka verksamheten och sannolikheten att de inträffar. Vad skulle det kosta företaget ifall risken skulle inträffa? Dessa risker rankas och rapporteras sedan till styrelsen på möten där de tar ställning till hur de ska gå vidare med riskhanteringen. Styrelsen har det största ansvaret över företags riskhantering och de väsentliga riskerna ska direkt rapporteras till dem.

Bedrägerier är en sådan risk som alltid finns med i rapporten. Dock anser de att de har bra kontroller för att upptäcka stölder och andra oegentligheter, men förstås så kan små stölder vara svårare att upptäcka.

4.1.2 Kontrollmiljö

Styrelsen och ledningen har månadsvisa möten där de har en agenda med underlag som de går igenom. På mötena diskuteras affärsverksamheten, risker samt åtgärder för att reducera riskerna. Upptäcks det något som inte är som det ska, så ska den som har ansvaret över den berörda avdelningen följa upp det och åtgärda bristen. Månatligen tar VD:n fram styrelserapporter som innehåller finansiell information och aktuella frågor angående verksamheten och vad som sker i omvärlden.

I företaget har de en arbetsordning för styrelse och ledning. Varje år fastställs ledningsgruppens olika ansvarsområden och befogenheter av styrelsen. De anställda har olika fastställda befogenheter om vem som ska/kan, till exempel skriva avtal med nya kunder, anställa ny personal och göra inköp. Medarbetarna känner till arbetet med intern kontroll beroende på vilken avdelning de jobbar på och vilka kontroller de påverkas av och arbetar med.

De anställda känner väl till sina ansvarsområden och roller inom företaget. När de anställs får de en lista över deras befattning med en arbetsbeskrivning vad som förväntas av dem och vad deras arbetsuppgifter är. Dessa går de sedan igenom vid utvecklingssamtalen som sker årligen och bedömer sedan medarbetaren från dessa punkter, vad de gör bra och var de kan

utvecklas. Även genom deras kommunikationssystem så kan de anställda ta del av sina medarbetares arbetsuppgifter och då få en kännedom vad allas olika arbetsuppgifter är.

Företaget arbetar med de anställdas trivsel och erbjuder utbildningar och friskvård. Även personalfrågor är viktiga för företaget. De jobbar även mycket med hållbarhetsredovisning där satsningar på bättre intern kommunikation gjorts.

4.1.3 Kontrollaktiviteter

De mesta av företagets kontrollaktiviteter integreras i deras bokföringssystem. Mycket som sker inom andra avdelningar av företaget som registreras i affärssystem går automatiskt till redovisningssystemet så att de inte uppstår fel på vägen. De har även controllers som följer upp att siffrorna blir rätt. I redovisningssystemet kan företaget följa upp verksamheten i sina olika affärsområden men de kan även följa upp de olika avdelningarna och speciella kunder inom affärsområdena.

Avstämningar sker månadsvis vid månadsbokslut. Då stäms redovisningen av mot företagets bankkonto och de ser om det stämmer, även balanskonton, resultat och marginaler granskas månadsvis för hela företaget av ekonomiavdelningen. Kundreskontra stäms av veckovis då de har mycket kunder som de fakturerar och påminnelser skickas ut två gånger innan de går till inkasso.

Leverantörsfakturer skickas ut för attest i ett fakturahanteringsprogram och följer en attestkedja och konteras innan de slutgodkänns - belopp högre än 5000 euro ska alltid slutgodkännas av ekonomichefen.

4.1.4 Information och kommunikation

Företaget kommunicerar med personalen genom ett system som kallas Workplace - som är en slags motsvarighet till Facebook men företaget äger själv all information som delas där, det är även ett slutet system så att endast de som är anställda på företaget har tillträde dit. Där delas information som medarbetarna bör känna till, även livesändningar med personalinfo läggs upp där så de som inte kan delta på plats även kan ta del av informationen. Annars har

företaget även ett intranät som de använder och en websida som då mer riktar sig till kunderna.

Styrelsen och ledningsgruppen håller möten kontinuerligt. Affärsområdena har även egna möten där de följer upp verksamheten inom sitt affärsområde och förmedlar även informationen vidare till medarbetarna. Även uppföljning av avdelningsmål görs vid berörda avdelningar. De vill vara öppna med vad som händer och diskuteras inom företaget så att de anställda ska känna sig delaktiga.

Vid rapportering av oegentligheter har de ingen direkt whistleblower-funktion utan upptäcker de anställda något så ska de prata med sin närmsta chef. Vilket de flesta inom företaget borde känna sig bekväma med.

4.1.5 Övervakning och uppföljning

Företaget har ingen formell uppföljning av den interna kontrollen. De jobbar kontinuerligt med att förbättra sig så ifall de upptäcker någon väsentlig risk försöker de reducera den genom att till exempel bygga om funktionen i deras IT och affärssystem så att felen inte uppstår eller arbeta med rutiner och checklistor.

4.1.6 Företagsövergripande riskhantering

Företaget arbetar med riskhantering och har en riskhanteringspolicy där de har principer om hur de ska arbeta med riskhantering och vilka som ansvarar över de olika delarna i riskhanteringsprocessen. Riskhanteringen är viktig i beslutsfattandet men även i den dagliga verksamheten. Vid affärsbeslut ses risken över och anses risken vara för stor fattas beslutet att undvika risken.

5. ANALYS

Att definiera tydliga mål är grundpelaren i arbetet med intern kontroll, det är viktigt att utgå från målen för att kunna definiera riskerna. COSO skiljer på olika sorters mål inom verksamheten som produktivitet och effektivitet samt mål för rapportering och efterlevnad mot lagar (Wikland, 2014) Företaget som har intervjuats har tydliga mål angående effektivitet, produktivitet och regelefterlevnad och utgår från dessa mål i sitt arbete med den interna kontrollen. De har som mål att redovisningen ska följa regler och lagar samt verksamhetsmål som de kan följa upp via nyckelindikatorer. Även mål sätts upp för de anställda på de olika avdelningarna som även följs upp och presenteras.

COSO betonar att det ska finnas en förståelse mellan sanning och konsekvens vid risker. Genom de sambanden skall sedan riskerna bedömas och väsentliga risker ska sedan åtgärdas. Eftersom alla risker inte kan åtgärdas är det viktigt att lägga upp en risktolerans där det bestäms vilka risker som ska åtgärdas, undvikas eller accepteras. (Committee of Sponsoring Organizations of the Treadway Commission, 2013; Wikland, 2014) Ledningen i det intervjuade företaget tar månatligen fram risker och tittar på sannolikhet och konsekvens samt rangordnar dessa risker innan de rapporteras till styrelsen, som sedan får besluta vilka åtgärder som behöver göras. De fokuserar främst på väsentliga risker i företaget. Wikland (2014) menar att punkten angående bedrägerier i COSO-modellen har tagit mer plats i det uppdaterade ramverket då den ofta inte tagits på allvar. Det intervjuade företaget har alltid risken för bedrägerier med i sin månatliga riskrapport.

Arwinge(2015) anser att kontrollmiljön är den viktigaste komponenten i COSO:s ramverk. Det handlar om att skapa strukturer, roller och ansvar. Ledningens styrande och deras attityder gentemot risker och risktagande är viktig. Styrelsen ska övervaka ledningens arbete med intern kontroll och ledningen ska rapportera direkt till styrelsen. Ansvar och befogenheter ska göras tydliga inom organisationen. (Wikland, 2014) Det intervjuade företaget har en arbetsordning för styrelse och ledning och ansvarsområden fastställs varje år.

Medarbetarna har olika befogenheter om vem som har tillgång till att till exempel skriva avtal med nya kunder. De anställda får god information om sina ansvarsområden och vad som förväntas av dem.

Med kontrollaktiviteter menas riktlinjer och rutiner som skapar effektiva kontroller som matchas mot målen, riskerna och kontrollmiljön (Wikland, 2014). Carrington(2014) menar att godkännande och attesteringsrutiner är viktiga för att uppnå god intern kontroll, han anser även att arbetsuppgifter ska delas upp på flera personer för att undvika misstag och medvetna bedrägeriförsök. Eftersom det intervjuade företaget jobbar mycket med olika kunder är det viktigt att de följer upp faktureringen och att kunderna betalar fakturor för att företaget ska få in sina pengar och nå sina verksamhetsmål. Detta görs veckovis och påminnelser skickas ut. För att undvika misstag eller bedrägeriförsök vid leverantörsfaktureror följer de en attestkedja där flera personer behöver granska och godkänna fakturan innan utbetalning sker, vid större belopp behöver även ekonomichefen godkänna fakturan.

Information och kommunikation fungerar som en stödjande komponent inom den interna kontrollen. COSO betonar att det är viktigt att informationen får flöda fritt inom organisationen. Det är av stor vikt att information når fram till de som behöver den. Styrelse, ledning och medarbetarna behöver kommunicera både internt och externt. (Wikland, 2014) Företaget som intervjuats använder sig av ett kommunikationssystem där information delas till de anställda och även livesändningar görs av personalinformationstillfällen så att alla medarbetare som inte är på plats kan följa med och ta del av information. För kunder och andra externa intressenter har de en hemsida där information delas

I komponenten övervakning och uppföljning bedöms den interna kontrollens funktion och effektivitet. Den interna kontrollen kan lätt försämrats och försvagas och därför är det viktigt att den övervakas och följs upp. Arwinge(2015) och Wikland (2014) menar att det är viktigt att hålla uppsikt på förändringar i världen eller i företaget och anpassa kontrollerna efter dem. Övervakning är viktigt för att företaget ska ha möjlighet att i god tid korrigera problemet i kontrollen och löpande utvärderingar ska göras för att bevisa att den interna kontrollen fungerar (Wikland, 2014). Uppföljning görs löpande hos det intervjuade företaget, upptäcker

de brister i sitt internkontrollsystem åtgärdas det så att felen inte uppstår. Annars finns det inte direkt någon formell övervakning eller uppföljning inom företaget.

Denna analys av företagets arbete med intern kontroll kan påvisa att det finns samband med teorin och praktiken. Det kan anses att företaget har en god intern kontroll i denna undersökning och de arbetar med de olika komponenterna i COSO-modellen. Den del som kan anses bristfällig är komponenten övervakning och uppföljning. Arwinge (2015) menar att den komponenten länge varit underutvecklad och att det tas för givet att en fungerande intern kontroll är effektiv och inte behöver följas upp. Företaget skulle kunna följa upp kontrollerna mer speciellt vid förändringar inom organisationen eller i omvärlden så att kontrollerna kan åtgärdas innan fel uppstår. Detta är förstås en kostnadsfråga för företaget och det måste ses över om nyttan överväger kostnaderna.

6. SLUTDISKUSSION

Syftet med det här arbetet var att ge en inblick i vad intern styrning och kontroll är samt att ta reda hur ett åländskt företag arbetar med intern kontroll och hur de hanterar risker. Jag har genom teorin gått igenom bakgrunden till intern styrning och kontroll samt COSO:s ramverks fem komponenter.

I detta arbete har jag fått reda på att medvetenheten och arbetet med intern kontroll och riskhantering är stor inom det företaget som intervjuats. De har lagt ner mycket arbete för att kunna ha en bra intern kontroll inom företaget, då de ansåg att det var väldigt viktigt för deras dagliga arbete och att företaget inte skulle fungera lika effektivt utan kontrollerna. Det intervjuade företaget tillämpar COSO:s modell för intern styrning och kontroll och de ansåg att modellen fungerade bra i praktiken. Mer fokus hade lagts på vissa komponenter men alla komponenter finns medräknade vilket är viktigt då komponenter ska samverka för att uppnå en effektiv intern kontroll.

Interna kontroller kostar pengar och därför måste en övervägning göras om värdet av kontrollen överstiger kostnaderna. Det är viktigt att fokus läggs på de mest väsentliga riskerna inom organisationen. Det intervjuade företaget har valt att ranka riskerna de upptäckt inom företaget och sedan görs avvägningar vilka risker som behöver åtgärdas och är mest väsentliga.

Jag upplevde att företaget hade ett bra tänkande när det gäller intern kontroll, de hade ett tankesätt att de hela tiden vill förbättra sig. De insåg att det inte går att undvika alla risker och därför åtgärdades de mest väsentliga riskerna och lade mer energi på dem istället för att börja fundera på mindre risker som inte skulle vara lika förödande för företaget, om de skulle inträffa. Förbättringar kan alltid göras på de olika komponenterna men då behöver det avgöras om värdet överstiger kostnaderna. Sett till teorin så följer företaget den på ett bra sätt och de har ett väl fungerande internkontrollsystem.

Syftet för det här arbetet tycker jag att uppnåtts då jag har tagit upp den viktigaste teorin inom ämnet och även fått reda på hur ett företag tillämpar teorin i praktiken. Intern kontroll är en viktig faktor i företags arbete att nå sina mål och att undvika oförutsedda händelser som påverkar företaget negativt.

6.1 Reliabilitet och validitet

Med reliabilitet menas att samma resultat ska kunna uppstå vid nya undersökningar med samma mätinstrument. Vid en hög reliabilitet ska alltså likande resultat kunna uppnås vid en undersökning vid ett nytt tillfälle. (Olsson & Sörensen, 2011)

Att ha en hög validitet är lika viktigt som att ha en hög reliabilitet. Validitet handlar om att det ska finnas ett samband mellan verkligheten och tolkningen. Tolkningen ska vara förankrad i empirin oavsett synen på verkligheten. (Olsson & Sörensen, 2011)

Jag anser att reliabiliteten är hög i detta arbete, skulle samma undersökning göras igen så skulle samma resultat kunna uppnås men jag anser att det finns brister. I och med att det är en kvalitativ undersökning som genomfördes genom en telefonintervju skulle kanske en personlig intervju ge mer djupgående svar. Under intervjun märkte jag även att frågorna kunde ställts annorlunda och att de kunde bearbetats och gjorts tydligare för att få bättre svar. Angående validiteten tycker jag att samband finns mellan verkligheten och tolkningen.

I detta arbete har jag huvudsakligen använt mig av Wiklands(2014) samt Arwinges(2015) böcker om intern styrning och kontroll vilket kan göra att detta arbete speglas mycket av deras åsikter angående ämnet och andra viktiga synvinklar kan ha missats.

6.2 Förslag till vidare forskning

I detta arbetet har fokus legat på COSO:s ramverk för intern styrning och kontroll och hur ett åländskt företag arbetar med interna kontroller. Förslag till vidare forskning skulle vara att intervjua ett börsnoterat bolag och se hur de arbetar med intern kontroll och hur de ser på finsk kod för bolagsstyrning. Även att göra en kvantitativ undersökning och se på åländska

företags syn på intern kontroll skulle vara intressant och om det finns några samband beroende på verksamhetsområde eller bransch.

KÄLLOR

Arwinge , O. (2015). *En introduktion till intern styrning och kontroll*. Stockholm: Sanoma Utbildning.

Arwinge, O., & Wikland, T. (2013). Utvecklingen av intern styrning och kontroll - reflektioner utifrån uppdaterat ramverk. *Balans*.

Carrington, T. (2014). *Revision*. Stockholm: Liber AB.

Christensen , L., Engdahl, N., Gräås, C., & Haglund, L. (2010). *Marknadsundersökning, en handbok*. Lund: Studentlitteratur AB.

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Företagsövergripande riskhantering - sammanhållet ramverk*. Hämtat från <https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Swedish.pdf>

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal Control - Integrated Framework Executive Summary*. Hämtat från <https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf>

Committee of Sponsoring Organizations of the Treadway commission. (Juni 2017). *Enterprise Risk Management Integrating with Strategy and Performance*. Hämtat från <https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>

Danielsson, C. (2012). Oegentligheter inom företag. *Balans*, ss. 18-20.

Olsson , H., & Sörensen, S. (2011). *Forskningsprocessen*. Stockholm: Liber AB.

Widengren, G., & Wendt, J. (2014). *Vad är värdet av intern kontroll?* Hämtat från PwC:
<https://www.pwc.se/sv/pdf-reports/vad-ar-vardet-av-intern-kontroll.pdf>

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

Värdepappersmarknadsföreningen. (2015). *Finsk kod för bolagsstyrning*. Hämtat från
<https://kauppakamari.fi/wp-content/uploads/2012/04/hallinnointikoodi-2015sve.pdf>

Värdepappersmarknadsföreningen. (u.d.). *Vad är corporate governance?*. Hämtat från
<https://cgfinland2.fi/sv/vad-ar-corporate-governance/vad-ar-corporate-governance/>

BILAGOR

Intervjufrågor

Hur anser ni att den interna kontrollen fungerar inom ert företag idag och arbetar ni aktivt med den interna kontrollen? Följer ni någon speciell modell för intern kontroll? T.ex. COSO-modellen

Mål:

- Har ni tydliga mål med verksamheten? Kommuniserar ni ut det till medarbetarna så även de känner till alla mål?
- Vilka är era mål?

Riskbedömning:

- Var har ni för risker i verksamheten och hur identifierar och bedömer ni dessa risker?
- Hur ser ni på risken för bedrägerier inom företaget och hur sker arbetet för att stoppa eventuella bedrägerier?
- Uppdateras riskbedömningen kontinuerligt? T.ex. vid förändringar i organisationen, omvärlden osv.

Kontrollmiljö:

- Finns det en medvetenhet hos medarbetarna om interna kontroller?
- Hur arbetar styrelsen och ledningen med den interna kontrollen?
- Har ledningen gjort upp ansvar- och befogenhetsfördelningar bland medarbetarna?

Kontrollaktiviteter:

- Vad har ni för kontrollaktiviteter för att minska riskerna? Kan ni ge exempel.
- Har ni mycket automatiserade kontroller i IT och affärssystemen?

Information och kommunikation:

- Förmedlas information om den interna kontrollen till medarbetarna?
- Vad använder ni er av för kommunikationskanaler? Fungerar kommunikationen bra i företaget?
- Känner medarbetarna till sina ansvarsområden och roller?
- Vet de anställda vem de ska rapportera oegentligheter till om de skulle upptäcka något?

Övervakning och uppföljning:

- Följer ni upp/utvärderar hur den interna kontrollen fungerar?
- Övervakar styrelsen och ledningen den interna kontrollen?

Har ni upplevt någon nytta av den interna kontrollen, kan ni ge exempel?

Tycker ni nyttan överväger kostnaderna för den interna kontrollen?

Upplever ni några nackdelar med intern kontroll?

Hur arbetar ni med riskhantering?