INTERNATIONELLA HANDELSHÖGSKOLAN
HÖGSKOLAN I JÖNKÖPING

Koll på SOX

En fallstudie av implementeringen av SAP GRC Version 10 inom delar av ABB-koncernen

Magisteruppsats inom Företagsekonomi

Författare: Lars Björmsjö 850701

Jacob Öberg 871211

Handledare: Gunnar Rimmel

Jönköping Maj 2012

Magisteruppsats i företagsekonomi inom ramen för Civilekonomprogrammet med företagsekonomisk inriktning vid Internationella Handelshögskolan i Jönköping

Titel	Koll på SOX – En fallstudie av implementeringen av SAP GRC Version 10 inom delar av ABB-koncernen.
Författare	Lars Björmsjö, Jacob Öberg
Handledare	Gunnar Rimmel
Ämnesord	GRC, intern kontroll, SAP, Sarbanes-Oxley Act

Sammanfattning

Bakgrund (och problem): Med de redovisningsskandalerna som skakat den finansiella världen i början av 2000-talet, har lagstiftningen stramats åt för företag för att förhindra att detta inträffar igen. Lagar som SOX ger tydliga direktiv på hur företagen ska stärka sina interna kontroller. Att efterleva SOX är en kostsam historia då, de ställer hårda krav på intern kontroll samt system för att hantera de ökade kontrollerna. Problembakgrunden till denna uppsats bygger på kraven att efterleva SOX och hur ett internationellt företag kan använda sig av ett IT-verktyg som SAP GRC för att klara av de hårdare kraven.

Syfte: Syftet med detta examensarbete är att utföra en fallstudie på hur processen bakom implementeringen av SAP GRC version 10 ser ut i ett multinationellt företag som ABB och vilken roll SOX har i sammanhanget

Avgränsningar: Författarna har valt att avgränsa sig till att enbart titta på implementeringen av SAP GRC, och tittar då inget på andra aktörers liknande produkter. Vidare har författarna valt att bara titta på implementeringen inom det brittiska ABB.

Metod: Studien har ett kvalitativ angreppssätt. Studien är en fallstudie vilket innebär att personlig kontakt i form av telefonintervjuer har varit enda metoden för att samla in data till empirin.

Resultat/Slutsats: Författarnas slutsats av undersökningen fastställs i att SOX har en väldigt viktig roll i implementeringen av SAP GRC, det är anledningen till implementeringen. Vidare har det framkommit att implementeringen är ett väldigt omfattande arbete, som är mycket kostsamt i både monetära mått samt tid. Dock är detta, det mest effektiva och kostnadseffektiva sättet att efterfölja SOX från ett ABB perspektiv

Diskussion: Författarna ser ett par områden för förbättring inom användningen av GRC på ABB för att få ut det mesta av verktyget, samt att effektivera hanteringen av risker. Vidare ser författarna förslag till vidare forskning. I dag finns det ingen direkt forskning på konceptet eller verktyget GRC, författarna finner det intressant om en vetenskapligt grundad definition skulle undersökas.

Master Thesis in Business Administration within the Civilekonomprogram at Jönköping International Business School

Title	Keeping track of SOX – A case study of the implementation of SAP GRC Version 10 in parts of the ABB Group
Authors	Lars Björmsjö, Jacob Öberg
Tutor	Gunnar Rimmel
Subject terms	GRC, internal control, SAP, Sarbanes-Oxley Act

Abstract

Background (and problem): In the reflections of the accountings scandals that occurred in the beginning of this millennium, legislations have tightened to prevent this kind of event to reoccur. Legislations like SOX provide clear directives on how companies should strengthen their internal controls. Compliance with SOX is a costly affair when, they place heavy demands on internal controls and systems to manage the increased controls. Problem discussion to this thesis is based on the requirements to comply with SOX and how an international company can use a tool like SAP GRC to meet the stricter requirements

Purpose: The purpose of this thesis is to conduct a case study on how the process behind the implementation of SAP GRC version 10 looks in a multi-national company such as ABB and the role played by SOX in the implementation process.

Delimitations: The authors have chosen to delimitate thesis merely to look at the implementation of SAP GRC, and do not look at other players at the market, nor their GRC solutions. Furthermore, the authors have chosen to only look at the implementation of SAP GRC at ABB in the United Kingdom.

Method: The study has only a qualitative approach. The study is a case study which means that personal contact in the form of telephone interviews has been the only method to gather data for empirical choose of the authors.

Results and Conclusions: The authors' conclusion of the study acknowledges that SOX has a very important role in the implementation of SAP GRC, and is the main reason for the implementation. Furthermore, it has emerged that the implementation is a very comprehensive work, which is very costly in both monetary and time measures. However the authors have concluded that implementing SAP GRC is the most efficient and cost effective way to comply with SOX from an ABB perspective.

Discussion: According to the authors opinion there are a few areas for improvement in the use of GRC at ABB, in order to get the most out of the tool and to streamline the management of risks. Due to the lack of current research within the field, the authors would find it very interesting if a scientifically based definition of GRC would be investigated.

Förord

Vi vill först och främst tacka respondenterna på ABB i Storbritannien – Julie Haywood, Derek Roberts, Andrew Bainbridge och Anthony Benge för att de tagit sig tid att besvara våra frågor under intervjuerna.

Vi vill också rikta ett tack till Ulf Niklasson och Scott Enerson på PwC Sverige samt till GRC Nordic för att de har ställt upp med material och svarat på våra frågor.

Vi vill även tacka vår handledare Gunnar Rimmel för hans värdefulla hjälp under arbetets gång, för hans åsikter samt vägledning.

Till sist vill vi även tacka vår opponentgrupp för en väl genomförd opponering med bra kritik och många värdefulla åsikter.

Jönköping maj 2012

Lars Björmsjö *Jacob Öberg*

Förkortningar

ADR	American Depository Receipts
COSO	Committee of Sponsoring Organizations of the Treadway Commission
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning (system)
GRC	Governance, Risk Management and Compliance
IC	Internal Control
IS	Information System
LBU	Local Business Unit
NASDAQ	National Association of Securities Dealers Automated Quotation
NYSE	New York Stock Exchange
PCAOB	Public Company Accounting Oversight Board
SEC	Securities and Exchange Commission
SIS	Swedish Standards Institute
SOX	Sarbanes-Oxley Act of 2002

Innehållsförteckning

1 Inledning 1
1.1 Bakgrund 1
1.2 Problemdiskussion 2
1.3 Frågeställning 3
1.4 Syfte 4
1.5 Avgränsningar 4
1.6 Disposition 5

2 Referensram 6
2.1 Introduktion till ABB 6
2.1.1 Asea - Allmänna Svenska Elektriska Aktiebolaget 6
2.1.2 BBC – Brown Boveri et Cie 7
2.1.3 ABB grundas av Asea och BBC 7
2.1.4 ABB:s verksamhet idag 8
2.2 SAP 9
2.3 GRC som koncept 9
2.4 GRC som verktyg 10
2.5 De olika modulerna 10
2.6 Sarbanes-Oxley Act of 2002 11
2.7 Bakgrund till införandet av lagen 11
2.8 Lagens tillkomst och syfte 12
2.9 Myndigheter med ansvar över Sarbanes-Oxley Act 12
2.10 Bolag som omfattas av lagen 13
2.11 Huvuddragen i Sarbanes-Oxley Act 13
2.11.1 Bolagsstyrning 13
2.11.2 Intern kontroll och finansiell rapportering 14
2.12 Fördelar med Sarbanes-Oxley Act 14
2.13 Nackdelar med Sarbanes-Oxley Act 15
2.14 COSO 17
2.15 COSO-Modellen 18
2.15.1 Kontrollmiljö 19
2.15.2 Riskbedömning 19
2.15.3 Kontrollaktiviteter 19
2.15.4 Information och kommunikation 20
2.15.5 Övervakning 20

3 Metod 21
3.1 Val av ämne 21
3.2 Val av företag 21
3.3 Val av respondenter 21
3.4 Val av metod och angreppssätt 22
3.5 Val av referensram 23
3.6 Upplägg och intervjumaterial 23
3.6.1 Genomförande av intervjuer 24
3.6.2 Intervjufrågor 24
3.7 Analys 24
3.8 Validitet och Reliabilitet 25

4 Empiri 26

4.1 GRC definitioner 26
4.2 Vad är målet med GRC? 27
4.3 Kostnadsanalys 28
4.4 Implementeringsarbetet 29
4.4.1 Förarbetet 30
4.4.2 Implementeringsarbetet 32
4.5 Fördelar med den nya versionen 35
4.6 Svårigheter med implementeringen 36
4.7 Hur skulle ABB kunna nyttja GRC på ett djupare plan? 36
5 Analys 37
5.1 Definition av GRC 37
5.2 SOX:s roll i implementeringen av GRC 38
5.3 Implementeringen av GRC 39
6 Slutsats 42
7 Diskussion 44
7.1 Förslag till framtida forskning 45
Litteraturförteckning 46
Bilagor 49

1 Inledning

I det inledande kapitlet beskrivs bakgrund och problemdiskussion som ligger till grund för uppsatsen frågeställningar. Vidare beskrivs uppsatsens syfte samt de avgränsningar som författarna har valt att göra. Kapitlet avslutas med en beskrivning av uppsatsens disposition.

1.1 Bakgrund

Början av 2000-talet var en mörk period på finansmarknaderna runt om i världen. En rad stora och till synes välfungerande bolag ansökte om konkurs, vilket skapade oro och väckte frågor. Det som uppdagades var en rad stora redovisningsskandaler i stora internationella bolag. I USA är två av de mer kända konkurserna när det amerikanska energibolaget Enron och det amerikanska telekombolaget Worldcom ansökte om konkurs under 2001 och 2002 (Moeller, 2004). Den finansiella rapporteringen från dessa bolag visade inte på några större konstigheter men granskningen efter konkurserna har visat en helt annan bild av bolagens egentliga ställning. Företagen hade i sin finansiella rapportering bland annat blåst upp omsättningssiffror, förvandlat förluster till vinster och försummat dokument i syfte att lura marknaden och myndigheter att bolagens ställning var bättre än vad den egentligen var (Svernlöv & Blomberg, 2003).

Vid samma tidpunkt som redovisningsskandalerna sprack den så kallade IT-bubblan. Aktiemarknaden var stark i början av 2000-talet och framför allt IT-sektorn där priset på IT-relaterade aktier blåstes upp högt. När IT-bubblan till sprack blev reaktionerna starka på börser över hela världen. I USA höjdes allt starkare röster för att landets lagstiftning behövde skärpas efter redovisningsskandalerna och den IT-relaterade börskraschen. Förtroendet för finansmarknaden var lågt efter dessa händelser och som en del för att återställa förtroendet för finansmarknaden infördes den amerikanska lagstiftningen Sarbanes-Oxley Act of 2002 (som vidare kommer benämnas SOX i uppsatsen) (Svernlöv & Blomberg, 2003).

Svernlöv och Blomberg (2003) beskriver att huvudsyftet med införandet av SOX handlar om att återställa investerares och andra aktörers förtroende för den amerikanska finansmarknaden. SOX-lagstiftningen reglerar bland annat frågor som rör följande områden: bolagsstyrning, intern kontroll och finansiell rapportering. Intern kontroll är ett av de områden som har stärks i och med införandet av SOX. Sektion 404 i SOX går under namnet *Management Assessment of Internal Controls* och innebörden av sektion är att VD, ekonomichef och övrig ledning på företag har fått ett utökat ansvar för intern kontroll och finansiell planering (SIS, 2012).

SOX-lagstiftningen är utformad på ett sätt som gör att den får ett brett tillämpningsområde. Det som avgör om ett bolag omfattas av lagen är inte vart bolaget har sitt säte utan huruvida bolaget har värdepapper registrerade till försäljning i USA. Detta innebär att lagen får ett extraterritoriellt tillämpningsområde och inte stannar vid USA:s nationsgränser utan påverkar såväl amerikanska som icke-amerikanska bolag (Svernlöv & Blomberg, 2003). SOX påverkar idag ett antal svenska bolag varav ABB är ett av dessa (Dagens Industri, 2012). ABB är ledande inom kraft och automationsteknik och koncernens bolag finns i ett hundratal länder och koncernen har ca 135 000 anställda (ABB, 2012b). Företagets aktie handlas idag på tre börser i världen och en av dessa är börsen i New York. Den 6:e april 2001 introduceras ABB på New York Stock Exchange (ABB, 2010) vilket medför att företaget måste följa SOX.

1.2 Problemdiskussion

Lagstiftare i olika länder har stramat åt lagstiftningen som ett led för att förebygga nya redovisningsskandaler och ett exempel på detta är den amerikanska lagstiftningen SOX. SOX gäller de bolag som är listade på den amerikanska marknaden, och gäller således långt ifrån alla företag. För de företag som är tvingade att följa SOX ligger fokus på företagets interna kontroll, redovisning och bolagsstyrningen. Lagen har både blivit prisad (Palley, 2007) samt hårt kritiserad (Freeman, 2009). En av de stora nackdelarna från ett företags perspektiv är att det är höga kostnader för att utforma och följa SOX. Kostnader som har ökat sedan införandet av SOX är framför allt konsult- och revisionskostnader. Många internationella företag som inte har sitt säte i USA har också fått genomgå stora förändringar och ofta öppna upp egna avdelningar som enbart jobbar med efterlevnad av SOX. Efterlevnad av lagen kostar i genomsnitt $2 300 000 om året för de företag som omfattas av lagen (Freeman, 2009).

Det faktum att ABB:s aktie handlas på NYSE ligger till grund för detta examensarbete då företaget måste följa SOX. Det finns idag många olika tekniska lösningar för att företag ska kunna efterleva kraven som finns i SOX. Det kan dock vara dyrt för företag att bygga speciella lösningar just för att uppfylla SOX vilket motiverar till att företag försöker integrera kraven som finns i SOX i redan existerande ledningssystem och tekniska plattformar (SIS, 2012). ABB arbetar idag med SAP:s affärssystem samt ett SAP-verktyg vid namn *GRC* för att klara lagkraven relaterade till SOX. GRC står för *Governance, Risk Management and Compliance* och en direktöversättning till svenska är bolagsstyrning, riskhantering och efterlevnad av lagar.

GRC-verktyget erbjuds av flera företag men ABB har valt att använda SAP:s GRC-verktyg för sin verksamhet i bland annat Storbritannien. SAP släppte en ny version av detta verktyg under augus-

ti 2011 (Bjorlin, 2011) som ABB har valt implementera för sina verksamheter i Storbritannien, Norge, Finland samt Sverige under 2012.

GRC är ett verktyg för att integrera de tre koncepten Governance, Risk Management och Compliance i ett företag. Detta innebär i praktiken att GRC är ett verktyg för ha en översyn på behörigheter, segregering av uppgifter, se till att verksamheten följer lagar samt lokaliserar samt minimera företagets risker. Huvudanvändningen till GRC är dock laglydnad. GRC är en produkt som svarar på ökningen av hårdare lagar och regler för företag runt om i världen. Till exempel så används GRC till att säkerhetsställa de interna kontroller som krävs för att följa SOX. (PwC, 2011)

Hur GRC ska användas bestäms dock av kunden, man kan välja och vraka mellan moduler och användningsområden, detta gör det svårt att ge en rak beskrivning på GRC.

GRC-verktyget från SAP är uppbyggt av tre huvudmoduler samt ett antal kompletterande moduler. ABB har valt att implementera två av huvudmodulerna i form av *Access Control* och *Risk management* för att praktisk kunna lösa problemet med att få struktur och ha kontroll på sin interna kontroll. Intern kontroll är ett brett område vilket medför att det kan vara svårt att överblicka allt som det innefattar. För att underlätta förståelsen för intern kontroll har organisationen COSO tagit fram ett ramverk för internkontroll som går under namnet *Internal Control – Integrated Framework*. Ramverket publicerades i september 1992 och i detta presenteras olika verktyg och processer som företag och organisationer kan använda för sin interna kontroll (Moeller, 2004). I ramverket presenteras även en definition av intern kontroll som idag är vedertaget accepterad och används bland annat av myndigheten SEC som är ansvarig för delar av SOX utformning. Moeller (2004) menar även företag idag behöver ha kunskap om COSO:s ramverk för att kunna efterleva delar av SOX-lagstiftningen i form av bland annat sektion 404 som behandlar ledningens ansvar för intern kontroll.

1.3 Frågeställning

Det är med ovanstående bakgrund författarna vill undersöka hur processen av implementeringen och användningen av SAP GRC ser ut i ett multinationellt företag. Detta kommer att vara huvudfråga i uppsatsen. Författarna även valt att inkludera två delfrågor som tar sikte på att undersöka hur viktig roll SOX har bakom implementeringen av GRC samt hur användandet av GRC kan utvecklas. Nedan följer författarnas huvudfråga samt delfrågor.

Huvudfråga

- Hur sker implementeringen av SAP GRC v.10 inom ABB Ltd?

Delfrågor

- Vilken roll har SOX i implementeringen SAP GRC v.10?
- Hur skulle ABB Ltd kunna nyttja GRC på ett djupare plan?

1.4 Syfte

Syftet med detta examensarbete är att utföra en fallstudie på hur processen bakom implementeringen av SAP GRC v.10 ser ut i ett multinationellt företag som ABB och vilken roll SOX har i sammanhanget.

1.5 Avgränsningar

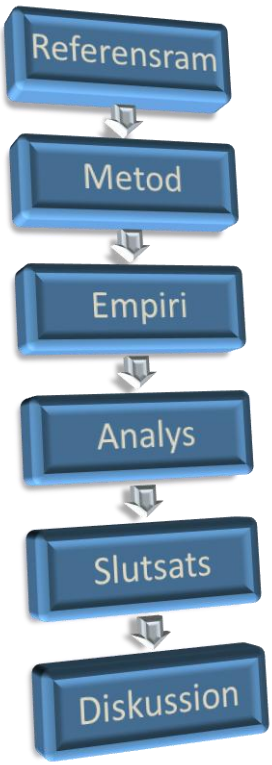
Författarna har i uppsatsen valt att avgränsa sig emot ABB Ltd i Storbritannien (fortsättningsvis i uppsatsen kommer detta förkortas ABB Ltd). Implementeringen av SAP GRC kommer att ske i Storbritannien samt i Norge, Finland och Sverige. På grund av den deadline författarna har, hinner inte implementeringen i de nordiska länderna avslutas vilket innebär att fokus i uppsatsen kommer att enbart vara på ABB Ltd.

Författarna har även valt att avgränsa sig mot att bara undersöka de processer som rör själva implementeringen av GRC, då SAP som är det affärssystem som ABB använder för GRC är av väldig teknisk komplexitet. Då detta är en uppsats på magisternivå inom företagsekonomi, ser författarna ingen anledning att gå in på tekniska specifikationer eller programmering av affärssystemet. Istället kommer fokus att vara på de ekonomiska aspekterna av processerna bakom implementeringen och själva användningen av GRC, samt att undersöka vilken roll SOX har i implementeringen.

På grund av geografisk spridning på uppsatsens respondenter och önskemål från ABB Ltd, har intervjuerna förts via telefon och inte i form av fysiska intervjuer.

Då författarna enbart fokuserar på ABB Ltd och det affärssystem som ABB Ltd använder ser författarna ingen anledning eller vinning på att undersöka vad andra aktörerna erbjuder för GRC applikationer utan det är det en naturlig avgränsning att uppsatsen bara kommer att berör SAPs version av GRC verktyget.

1.6 Disposition



Referensram: Här stipuleras referensramen som skapar den grunden för analys.

Metod: I detta kapitel går författarna igenom metoden för datainsamling till uppsatsen.

Empiri: Här presenteras vilka resultat som framkommit från intervjuer.

Analys: Här kopplas teorin och empirin samman och analyseras.

Slutsats: Här presenteras författarnas slutsatser och reflektioner av analysen.

Diskussion: Här presenterar författarna sina egna åsikter och observationer samt rekommendationer för framtida forskning.

Figur 1. Uppsatsens disposition (Egenarbetad figur)

2 Referensram

Referensramen har till syfte att koppla samman uppsatsen frågeställning med den insamlade empirin. Kapitlet inleds med en kort beskrivning av företaget som används i fallstudien samt det GRC-verktyg som företaget har valt att använda. Den avslutande och största delen av referensramen ägnas åt den lagstiftning som ligger till grund för införandet av GRC-verktyget samt vad innebörden av lagstiftningen är.

2.1 Introduktion till ABB

Asea Brown Boveri (ABB) bildades 1988 när svenska Allmänna Svenska Elektriska Aktiebolaget (Asea) och schweiziska Brown Boveri et Cie (BBC) gick samman. Båda företagen har en lång historia som sträcker sig tillbaka till slutet av 1800-talet (ABB, 2011a).

2.1.1 Asea - Allmänna Svenska Elektriska Aktiebolaget

Aseas historia sträcker sig tillbaka till 1883 då Elektriska Aktiebolaget bildades i Stockholm. Företaget inriktade sin tillverkning på elektriska produkter såsom elektrisk belysning och dynamomaskiner. Elektriska Aktiebolag fortsatte sin verksamhet fram till 1890 då bolagets fusionerades med Wenströms & Granströms Elektriska Kraftbolag. Det nya bolaget fick namnet Allmänna Svenska Elektriska Aktiebolaget och företagets huvudkontor förlades till Västerås. Bolaget valde under senare tid att använda förkortning Asea som företagsnamn (ABB, 2011a).

Asea har varit med och tillverkat många produkter som har fått stor betydelse i samhället. Redan 1889 uppfann Jonas Wenström trefassystemet och detta system omfattade generator, transformator och motor. Några år senare, 1893, byggdes den första längre trefaskraftöverföringen av Asea mellan Hellsjön och Grängesberg. Asea fortsatte att expandera över de kommande decennierna med många nya produkter bland annat inom kraftindustri samt stål- och gruvindustrin. Aseas kunder under denna tid var såväl statliga som privata företag och organisationer (ABB, 2011a).

Asea fick i uppdrag av nuvarande Vattenfall att konstruera den första HVDC-överföringen under 1950-talet mellan Gotland och det svenska fastlandet. HVDC-överföring innebär högspänd likström och är av Aseas innovationer och kan förklaras som kraftöverföring över långa avstånd samt sammankoppling av kraftnät med olika spänningar. HVDC-överföring mellan Gotland och det svenska fastlandet var den första kommersiella i sitt slag och idag finns det ca 100 olika HVDC-system i drift över hela världen varav ABB har levererat ca hälften av dessa (ABB, 2012a).

Industrirobotar är en annan viktig produkt som Asea tillverkar. Den första industriroboten som byggdes av Asea skedde år 1974. Asea fortsatte att göra stora satsningar inom robot- och elektro-

nikområdena under 1980-talet. De stora och långsiktiga satsningarna under lång tid gjorde Asea till en av de tio största koncernerna inom elektroteknik under 1980-talet. (ABB, 2011a).

Aseas produkter har betytt mycket för moderna samhället om man ser till att företagets produkter har använts till elektrifiering av industrin, hemmen och även järnvägsnätet. Företaget har expanderat kraftigt sedan starten 1883 både genom organisk tillväxt och förvärv. Aseas dotterbolag finns över hela världen och majoriteten av företagets omsättning utgjordes under 1980-talet av försäljning med Norden och Europa som bas (ABB, 2011a).

2.1.2 BBC – Brown Boveri et Cie

Brown Boveri et Cie:s historia sträcker sig tillbaka till 1891 då företaget grundades av Charles Brown och Walter Boveri i Baden, Schweiz. Byggnationen av företagets första anläggning påbörjades samma år som företaget grundades och placerades i Oerlikon, Schweiz. Under 1900-talet spelade BBC en viktig roll för elektrifieringen av delar av det europeiska järnvägsnätet. Ett projekt som företaget genomförde på egen hand var att bygga en 20 km lång sträcka åt den statliga schweiziska järnvägen. En annan produkt som företaget var tidigt med att utveckla var ångturbiner och just ångturbiner blev en av de viktigaste produkterna hos BBC. Den schweiziska hemmamarknaden var relativt liten under 1900-talet vilket resulterade i att företaget etablerade dotterbolag i andra länder men företaget hade dock kvar sin tyngdpunkt i Schweiz och Tyskland (ABB, 2011a).

2.1.3 ABB grundas av Asea och BBC

Asea och BBC meddelade den tionde augusti 1987 att de vid årsskiftet skulle bilda ett gemensamt bolag. Det nya bolaget fick namnet ABB Asea Brown Boveri Ltd (ABB) och huvudkontoret placerades i Zürich, Schweiz. Vid bildandet av bolaget delades ägandet i bolaget lika så att Asea ägde hälften och den andra hälften ägdes av BBC. Den 5 januari 1988 påbörjade den nya storkoncernen sin verksamhet och ABB hade då omkring 160 000 anställda över hela världen och cirka 100 miljarder kronor i omsättning (ABB, 2011a).

Vid fusionen mellan Asea och BBC bildades ett av de största företagen i världen inom elektroteknik. ABB fortsatte att expanderade under 1989 genom att förvärva ett 40-tal andra bolag, bland annat köptes kraftöverförings- och kraftdistributionsverksamheterna från Westinghouse Electric Corporation. ABB inleder 1997 arbetet med Industrial IT och projektet syftar till att i realtid knyta ihop produktions- och affärssystem inom ABB. Året efter, 1998, gör ABB sitt största företagsförvärv hittills då man köper Elsag Bailey Process Automation. Motivet bakom förvärvet är att göra ABB marknadsledande inom den globala automationsmarknaden. ABB väljer under

1999 att avyttra delar av sin verksamhet och säljer av sina verksamheter inom kärnkraft, kraftgenerering samt bolagets tågverksamhet. ABB motiverar avyttringarna med att man vill fokusera på att utveckla sin marknadsposition in alternativ energi (ABB, 2011b).

Under det kommande decenniet fortsätter ABB sin omstrukturering. År 2002 säljer företaget av större delen av sin financial service division och under samma år bjuds även divisionen Oil, Gas and Petrochemicals ut till försäljning där delar av divisionen slutligen säljs under 2004. Året innan, 2003, gör ABB en ny strukturförändring då man väljer att effektivisera sin divisionsstruktur. Förändring går ut på att företaget vill fokusera på två områden som är bolagets kärnområden, dessa är Power Technologies och Automation Technologies (ABB, 2011b).

2.1.4 ABB:s verksamhet idag

ABB är idag ledande inom kraft och automationsteknik. ABB-koncernens bolag finns i ett hundratal länder och koncernen har ca 135 000 anställda. ABB:s verksamhet delas idag in i fem divisioner och nedan följer en beskrivning av de olika divisionerna (ABB, 2012b):

- ”**Power Products** – kraftprodukter – är nyckelkomponenter för överföring och distribution av elektrisk energi. Divisionen har tillverkningsenheter för transformatorer, brytare, mättransformatorer, avledare och annan tillhörande utrustning” (ABB, 2012b).
- ”Divisionen **Power Systems** erbjuder nyckelfärdiga system och tjänster för kraftöverförings- och distributionsnät samt till kraftanläggningar. Ställverkslösningar och stationsautomation är viktiga områden, liksom FACTS (flexibla transmissionssystem för växelström), HVDC samt HVDC Light (högspänd likström) och system för att styra och övervaka nät” (ABB, 2012b).
- **Discrete Automation and Motion** – ”Divisionen erbjuder produkter och lösningar som höjer produktivitet och energieffektivitet. Motorer, generatorer, frekvensomriktare, PLC-enheter (programmable logic controllers) och robotar driver, styr och åstadkommer rörelse i ett stort antal automationsapplikationer” (ABB, 2012b).
- ”Divisionen **Low Voltage Products** tillverkar lågspänningsställverk, lågspänningsbrytare, övervakningsprodukter, kabeltillbehör, skyddskåpor och kabelsystem för att skydda människor, installationer och elektronisk utrustning från elektrisk överbelastning samt produkter och system för maskinsäkerhet” (ABB, 2012b).
- **Process Automation** – ”Divisionen förser kunder med produkter och lösningar för instrumentering, automation och optimering av industriella processer” (ABB, 2012b).

2.2 SAP

SAP AG grundades 1972 i tyska Weinheim utav fem före detta ingenjörer från företaget IBM. Dessa bröt sig loss för att de såg annorlunda på saker gentemot vad IBM gjorde och grunden för SAP AG var lagd. SAP är idag ett av de världsledande företagen inom affärssystem och företagsnamnet är en akronym av de huvudsakliga produkterna (System, Applikationer och Produkter i databehandling (SAP, 2011). Företaget har idag produkter för både medelstora och stora företag samt branschlösningar till de allra största branscherna. SAP har sedan 1972 vuxit ofantligt mycket och är idag arbetsgivare åt över 55 000 människor runt om i världen och finns representerat i cirka 50 länder samt omsätter strax över €14 miljarder. Huvudkontoret ligger idag i Walldorf, Tyskland, en liten stad inte så långt ifrån Frankfurt. (SAP, 2011).

2.3 GRC som koncept

Konceptet bakom GRC är inget nytt då det alltid har varit en viktig grundsten för affärsverksamhet. Att hålla koll på *Governance, Risk Management och Compliance* har företagare gjort under en lång tid. Det som är det nytt med GRC är processerna bakom det hela och hur de integreras in i verksamheten som en helhet istället för att arbeta individuellt med dessa tre områden (Tarantino, 2008).

Att ta fram en vedertaget accepterad definition på GRC är väldigt svårt och experterna är oeniga. Detta eftersom GRC är så anpassningsbart koncept där GRC på företag A jämfört med GRC på företag B kan skilja sig så pass mycket att det inte går ens att jämföra vilket leder till att GRC är väldigt svårdefinierat. Därav har definitionerna på GRC nästan blivit lika många som de bolag som arbetar med GRC. I denna uppsats fokuserar författarna enbart på SAP:s GRC-applikation, men som nämnt tidigare finns ingen exakt definition av GRC, vilket innebär att SAP inte har ensamrätt på detta. Begreppet som sådant är ett paraplybegrep av allt som ingår inom *Governance, Risk Management and Compliance* som ett integrerat koncept. (Tarantino, 2008)

Bakgrunden till uppkomsten av GRC har precis som intern kontroll sin grund i en rad stora externa händelser som har skakat finansvärlden över tid med exempel som Worldcom och Enron. De nämnda händelserna ökade trycket på lagstiftaren att historien inte skulle upprepa sig därför har ny lagstiftning införts däribland SOX. Det är även där GRC tar vid, att följa det exempel vi tidigare använde med SOX är ett mycket stort arbete och kostar mycket pengar såväl som tid. Syftet med GRC är att effektivisera detta arbete, och integrera in det i system. Till lika ska även nämnas att GRC från SAP är även nischat mot branscher som till exempel livsmedel och läkemedelsindustrin där regelverket är om möjligt ännu mer komplicerat och viktigt att efterleva.

2.4 GRC som verktyg

SAP GRC består av tre huvudmoduler och tre moduler som är mer nischade mot specifika branscher eller situationer, vilket gör att de tre sistnämnda inte är passande till alla typer av bolag. Dessa är kopplade till det affärssystem och den databas som ligger i grunden, och integreras mot varandra men fungerar lika bra självständiga (SAP, 2012). Vilka man använder beror på kundens preferenser. De tre huvudmoduler är *SAP GRC Access Control, SAP GRC Process Control* och *SAP GRC Risk management*.

De kompletterande modulerna är *SAP GRC Global trade service, GRC Environment and Safety management* samt *SAP GRC Data privacy* (SAP, 2012). Författarna kommer här nedan ge en kort beskrivning av de olika modulernas syfte.

2.5 De olika modulerna

Access control: Är en modul som styr vem som har tillgång till vilka transaktioner, åtgärder med mera. Modulens syfte är att minimera risken av att någon sitter med uppgifter som kan ge konflikter som kan leda till en risk för stöld, bedrägeri eller komplikationer för företaget. Detta är en övergripande modul som går ner på detaljnivå för att öka segregeringen av uppgifter (SAP, 2012).

Process control: Detta är den huvudsakliga modulen, denna bevakar företagets processer och varnar för eventuella risker och/eller brister i processerna. De risker som undersöks är huruvida processerna överensstämmer med den rådande lagstiftningen, som till exempel SOX men också branschspecifika regler som FDA (Food and Drug Administration) som styr den strikta lagstiftning som gäller för livsmedel och mediciner (SAP, 2012).

Risk management: Denna modul är till för på ett övergripande sätt ha kontrollera företagets huvudsakliga risker utöver segregering av uppgifter samt de risker som finns på individnivå inom företaget. Risk management modulen kollar på de finansiella, operativa samt de juridiska riskerna som företaget utsätts för (SAP, 2012).

Global trade service: Denna modul används för att hålla koll och minimera de risker som finns för företag vars majoritet av kunder och leverantörer finns utanför landet. Modulens syfte är att minimera kostnader för import/export samt minimera de risker som finns vid internationell handel (SAP, 2012).

Environment, Health and Safety management: Detta är SAPs miljömodul, modulen kollar på miljöpåverkan som företaget har och hur denna kan minskas samt att inte skena i väg när det kommer till kostnader (SAP, 2012).

Data privacy: Detta är en modul som är ett samarbete mellan SAP AG och företaget Cisco. Syftet med modulen är att ha koll och kontrollera vem som har tillgång till vilken information. På detta sätt minimera risken att viktig information inte kommer ut till konkurrenter samt att om det inträffar går det lätt att ta reda på vilka som har haft tillgång till informationen och det går då att spåra läckan (SAP, 2012).

2.6 Sarbanes-Oxley Act of 2002

Det har snart gått tio år sedan SOX blev en del av amerikansk lagstiftning. Den 30 juli 2002 skrev USA:s dåvarande president, George W Bush, under lagen vilket innebar att den blev en del av amerikansk federal lag. SOX är uppkallad efter de två huvudsakliga grundarna, senator Paul Sarbanes och kongressledamot Michael G. Oxley och lagstiftningen reglerar bland annat frågor som rör bolagsstyrning, intern kontroll och finansiell rapportering (Svernlöv & Blomberg, 2003).

2.7 Bakgrund till införandet av lagen

Grunden till införandet av SOX kan härledas till en rad internationella redovisningsskandaler i början av 2000-talet. I USA var två av de större skandalerna när det amerikanska energibolaget Enron och telekombolaget Worldcom gick i konkurs. Att ett företag går i konkurs är inte konstigt i sig men i de här fallen var det två tillsynes välfungerande bolag med stabila finanser. Det som uppdagades var att den finansiella rapporteringen från bolagen inte gav en rättvisande bild och i verkligheten var bolagens ställning sämre än vad som angavs i bolagens rapporter. Bolagen hade med sin ekonomiska rapportering och andra åtgärder blåst upp sina omsättningssiffror, förvandlat förluster till vinster och försummat dokument för att lura marknaden och myndigheter (Svernlöv & Blomberg, 2003).

Reaktionerna på redovisningsskandalerna blev stark på börser över hela världen. Vid samma tidpunkt inträffade nya händelser som bidrog till framtagandet av SOX. Aktiemarknaden var stark i början av 2000-talet och en stark marknad var IT-sektorn. Priset på IT-relaterade aktier blåstes upp högt i början av decenniet men till slut brast den så kallade It-bubblan vilket fick stora konsekvenser på börser runt om i världen. Ett exempel på detta är den teknikdominerade Nasdaq-börsen I USA. I början av år 2000 nådde börsen sitt då högsta värde men redan i augusti 2002 hade börsen tappat cirka 80 % av sitt värde. I USA höjdes allt starkare röster på att landets lagstiftning behövde skärpas efter redovisningsskandalerna och den IT-relaterade börskraschen. Förtroendet för finansmarknaden var lågt efter dessa händelser och som en del för att återställa förtroendet för finansmarknaden infördes SOX (Svernlöv & Blomberg, 2003).

2.8 Lagens tillkomst och syfte

Svernlöv och Blomberg (2003) anser att införandet av SOX är den mest betydelse värdepappers-lagstiftningen i USA sedan 1934 (den lag som åsyftas från år 1934 är Securities Exchange Act of 1934). Hela processen kring införandet av SOX skedde mycket snabbt och förenade både demokrater och republikaner i den amerikanska senaten.

Svernlöv och Blomberg (2003) framhåller att huvudsyftet till införandet av SOX handlar om att återställa investerares och andra aktörers förtroende för den amerikanska finansmarknaden. Detta förtroende försvagades rejält efter redovisningsskandalerna och börskraschen. Författarna menar också att lagstiftaren vill öka sin insyn i de publika bolagen. Genom införandet av SOX får de amerikanska myndigheterna en ökad insyn i de bolag som omfattas av lagen. Det som eftersträvas med lagen är att den information som finns i bolagens finansiella rapportering och övriga upplysningar till finansmarknaden ska vara korrekt och stämma överens med verkligheten (Sarbanes-Oxley Act of 2002, 2002)

2.9 Myndigheter med ansvar över Sarbanes-Oxley Act

SOX är en ramlagstiftning vilket innebär regelverket fylls ut genom närmare tillämpningsföreskrifter. Praktiskt fungerar det så att den amerikanska finansinspektionen, the U.S. Securities and Exchange Commission (SEC), har i uppdrag att arbeta fram tillämpningsföreskrifter till bestämmelser i SOX. Detta innebär att SEC:s roll är att arbeta fram ett detaljerade regelverk till större delen av lagen (Svernlöv & Blomberg, 2003).

The Public Company Accounting Oversight Board (PCAOB) bildades som en följd av införandet av SOX. PCAOB är en icke vinstdrivande organisation med huvudsyfte att övervaka revisionen av publika bolag med syfte att stärka förtroendet hos investerare samt hos övriga intressenter att bolagens revisionsrapporter är upprättade korrekt med avseende på information, tillförlitlighet och oberoende. I och med införandet av SOX blir revisorer av publika bolag externt och oberoende själva granskade. Detta är något helt nytt då tidigare lagstiftning inte krävde detta utan yrket kan sägas ha varit självreglerat (PCAOB, 2012).

PCAOB:s styrelse består av fem stycken medlemmar och tillsätts av the Securities and Exchange Commission (SEC) i samråd med andra myndigheter. SEC är tillsynsmyndighet till PCAOB och SEC är även ansvariga för att godkänna PCAOB:s regler, standarder och budget. PCAOB finansieras genom årliga avgifter som betalas av de publika bolagen, mäklare och handlare. De årliga

avgifterna för de publika bolagen beräknas i proportion till bolagens börsvärde. För mäklare och handlare baseras beräkningarna efter företagens nettokapital (PCAOB, 2012).

2.10 Bolag som omfattas av lagen

SOX är skriven på ett sätt som gör att lagen får ett brett tillämpningsområde. Det som avgör om ett bolag omfattas av lagen beror på om bolaget anses som emittent enligt Securities and Exchange Act of 1934 och Securities Act of 1933 (Svernlöv & Blomberg, 2003). Svensk Fondhandlareförening (2011) definierar emittent på följande sätt: ”Den som är utgivare av en Strukturerad Placeringsprodukt och upprättar prospekt samt därmed är betalningsskyldig enligt den Strukturerade Placeringsproduktens villkor”. Begreppet emittent, på engelska *issuer*, innebär att ett bolag har inregistrerade värdepapper i USA eller har lämnat ett prospekt för sina värdepapper. Begreppet värdepapper innefattar aktier och American Depository Receipts (ADR) som kan handlas på amerikanska börser och marknadsplatser. Prospekt innebär att ett företag har initierat ett förfarande för att erbjuda värdepapper i USA. På det sätt som SOX är författad är det avgörande inte huruvida ett bolag har sitt säte i USA eller ej, utan om bolaget faller in under ovanstående kriterier. Detta gör att såväl amerikanska som icke amerikanska företag omfattas av SOX. Några exempel på svenska bolag samt bolag med svensk anknytning som berörs av SOX är ABB, Autoliv, AstraZeneca och Ericsson (Dagens Industri, 2012).

2.11 Huvuddragen i Sarbanes-Oxley Act

SOX innehåller 11 kapitel med totalt 66 sektioner. Lagen har som tidigare nämnt ett brett tillämpningsområde vilket innebär att flera områden tas upp i lagen och även att den berör många olika yrkesgrupper. Lagstiftningen reglerar bland annat frågor som rör bolagsstyrning, intern kontroll och finansiell rapportering. Lagstiftaren har även valt att skärpa påföljderna när bestämmelserna i lagen bryts, exempel på detta är att enskilda företrädare för ett bolag kan riskera dryga penningböter men även fängelsestraff på runt 20 år. (Svernlöv & Blomberg, 2003).

2.11.1 Bolagsstyrning

De företag som omfattas av SOX måste på ett effektivt sätt leva upp till kraven i lagen. Hur företag praktiskt väljer att lösa detta skiljer sig åt och det finns många olika tekniska lösningar för att uppfylla kraven. Det kan dock vara dyrt för företag att bygga speciella lösningar just för att uppfylla SOX vilket motiverar till att företag försöker integrera kraven som finns i SOX i redan existerande ledningssystem och tekniska plattformar (SIS, 2012).

SOX ställer en rad krav på kontroller, säkerhet och rapportering fungerar hos företagen, vilket kräver samverkan mellan stora delar av en organisation. Företag som har ett väl fungerande ledningssystem med etablerade processer har på så sätt en plattform för effektiv bolagsstyrning vilket underlättar för företagen att uppfylla lagkraven. Några viktiga områden som företag arbetar med är riskhantering, intern kontroll och informationssäkerhet (SIS, 2012).

2.11.2 Intern kontroll och finansiell rapportering

Sektion 404 i SOX har fått namnet *Management Assessment of Internal Controls*. Lagtexten i den här sektionen är relativt kort men innebörden av den är mer omfattande. Ramos (2004) beskriver att sektion 404 innebär kortfattat att VD och ekonomichef har ansvar för att utvärdera och rapportera till SEC hur de interna kontrollerna säkerställer den finansiella rapporteringens riktighet. Utöver detta ställs det en rad krav på företagets ledning och externa revisorer. Ledningen är ansvarig för att upprätta och upprätthålla en tillräcklig intern kontroll över finansiell rapportering. Ledningen är även ansvarig för det ramverk som används för att utvärdera hur effektiva kontrollerna är. I de rapporter som framställs måste ledningen skriva ut om eventuella svagheter i sin interna kontroll och dessa rapporter måste läggas fram regelbundet. Ett exempel på vad som måste rapporteras är om förändringar i den interna kontrollen kommer, alternativt, kan materiellt påverka den interna kontrollen över finansiell rapportering. Slutligen har företagets externa revisorer ansvar för att utvärdera hur effektiva de interna kontrollerna över finansiell rapportering är (Ramos, 2004).

Sektion 404 i SOX kan sammanfattas med att företagsledningen har fått ett utökat ansvar över företagens finansiella rapportering, där ledningen bland annat är ansvarig för att upprätthålla rutiner för finansiell rapportering; identifiera processerna för finansiell rapportering samt att redovisningssystemen ska ha hög integritet. För intern kontroll krävs det att företagsledningen utvärderar systemet för intern kontroll och en del av intern kontroll handlar om att företagen behöver ha ett tydligt riskhanteringsprogram för sin verksamhet (SIS, 2012).

2.12 Fördelar med Sarbanes-Oxley Act

Förtroendet för den amerikanska marknaden minskade drastiskt efter en rad redovisningsskandaler i början av 2000-talet samt den IT-relaterade börskrisen som slog till samtidigt. Ett av huvudsyftena med införandet av SOX var att återställa investerares och andra aktörers förtroende för den amerikanska finansmarknaden. Det är även tänkt att lagen ska ha ett avskräckande syfte då påföljderna vid lagbrott har skärpts både i form av dryga penningböter samt långa fängelsestraff. Sedan införandet av SOX har inte några större redovisningsskandaler inträffat i USA och antalet

stämningsansökningar för bedrägerier har även minskar (Prentice, 2007). Detta kan bero på flera olika orsaker men viktig del av SOX-lagstiftningen handlar om säkerställandet av interna kontrollsystem. Med välfungerande interna kontrollsystem finns högre upptäcktsrisk av bedrägerier samt systemen gör det svårare för företag att dölja felaktigheter i sin redovisning. Prentice (2007) menar att införandet av SOX kan ha haft en positiv effekt när det gäller minskade bedrägerier.

Den finansiella rapportering är ett annat område som har stärkts i och med införandet av SOX. Företagsledningen inom företag som berörs av lagstiftningen har fått ett utökat ansvar över den finansiella rapporteringen i form av krav på struktur och rutiner för intern kontroll och finansiell rapportering (SIS, 2012). En parallell kan dras mellan den interna kontrollen och den finansiella rapporteringen, där en väl fungerande intern kontroll validerar riktigheten i de siffror företaget förmedlar då den interna kontrollen verkar som ett skyddsnät för att förhindra bedrägerier. Företagsledningen är även ansvarig för att utvärdera sitt företags kontroller och bedöma dess effektivitet. Tacket, Wolf & Claypool (2006) menar att de interna kontrollerna har fått ett annat bredd och djup sedan införandet av SOX och på så sätt har de interna kontrollerna för finansiell rapportering stärks. Detta styrks även av McCauley Parles, O'Sullivan & Shannon (2007) som beskriver att en majoritet av företagen upplever att deras interna kontroll har tydligt stärkts, alternativt, stärks i och med införandet av SOX. Ytterligare en parallell kan dras mellan intern kontroll och bolagsstyrning. Prentice (2007) beskriver att bolagsstyrning inom amerikanska bolag har förbättrats sedan införandet av SOX.

Kontrollmiljön är en av fem komponenter i COSO:s modell över intern kontroll. Tacket, Wolf & Claypool (2006) beskriver vikten av att ha en fungerande kontrollmiljö och tar upp en rad positiva aspekter som kan uppnås. En fungerande kontrollmiljö sätter den moraliska tonen i en organisation och är en viktig grund. För att detta ska fungera behövs flera olika komponenter i en organisation i form av till exempel inrättandet av hederskodex *(eng. code of ethics)*; en tydlig uppdelning av befogenheter och ansvar samt effektiva mätmetoder. Precht (2005) kan även påvisa att införandet av SOX har gett en tydligare fördelning av roller och ansvar som kan bidra till en lugnare arbetsmiljö och även ge trygghet till de anställda i ett företag.

2.13 Nackdelar med Sarbanes-Oxley Act

Allt sedan införandet av SOX har det diskuterats över hur resurskrävande införandet har varit i form av både tid och pengar. En sektion som ofta nämns för att vara kostsam såväl att implementera som tillämpa är sektion 404 i lagen som behandlar ledningens ansvar och kontroll över den interna kontrollen (Bradford & Brazel, 2007; McCauley, 2007). Tacket, Wolf & Claypool

(2006) påpekar att kostnadsaspekten av sektion 404 kan delas upp i monetära samt icke-monetära kostnader. Båda dessa kostnader uppkommer och måste beaktas vid implementeringen av SOX men svårigheten är att beräkna de kostnader som räknas som icke-monetära och således inte kan mätas i pengar. Monetära kostnader som uppkommer kan vara i form av konsultarvoden och revisionskostnader. De icke-monetära kostnader som uppkommer kan vara i from av logiska brister och kan också bero på en överbelastning av information (*eng. information overload*). En enklare förklaring av icke-monetära kostnader är de svårigheter som uppkommer på grund av lagen men som inte går att mäta i pengar.

De största monetära kostnaderna som uppkommer för att implementera och efterleva SOX är i form av konsultarvoden och revisionskostnader (Tacket, Wolf & Claypool, 2006). En anledning till att just dessa kostnader har ökat markant är den komplexitet som införandet av SOX innebär. De ökade revisionskostnaderna kan härledas till att revisorerna har fått ett utökat ansvar vilket medför utökad granskning (Tacket et. al., 2006). Den utökade granskningen gäller bland annat att revisorerna ska bedöma effektiviteten av det interna kontrollsystemet med avseende på sektion 404 i SOX (Precht, 2005). Att företagens kostnader för konsulttjänster har ökat kan i sin tur härledas till att många företag behöver komplexa affärssystem och verktyg samt andra konsulttjänster för att uppfylla de olika lagkraven (Tacket et. al., 2006). Kostnaden för att efterleva SOX måste vägas mot nyttan och just kostnadsaspekten har lett till att många företag har valt att avregistrera sina värdepapper från amerikanska marknadsplatser (Bradford & Brazel, 2007).

SOX gäller som tidigare beskrivet både för amerikanska som icke-amerikanska bolag. Lagen tar inte sikte på vart ett bolag har sitt säte utan det avgörande är om ett bolag har värdepapper registrerade i USA och om så är fallet måste dessa bolag efterleva SOX och dess tillämpningsföreskrifter. Svernlöv & Blomberg (2003) beskriver att tidigare amerikansk lagstiftning inom området innehöll ofta generella undantag för utländska bolag till skillnad från SOX. Detta innebär att lagen nu får ett extraterritoriellt tillämpningsområde och inte stannar vid USA:s nationsgränser. Detta är något som anses som kontroversiellt och lett till livlig debatt runt om i världen men även inom USA (Svernlöv & Blomberg, 2003). En del av kritiken mot SOX handlar om att det inte tas hänsyn till om de utländska bolagen redan har landspecifika bestämmelser som kan likställas med SOX-lagstiftningen. Att efterleva och rapportera liknande lagstiftning till flera myndigheter kan leda till merarbete för de utländska bolag jämfört med de amerikanska.

2.14 COSO

I lagtexten i SOX benämns att företag ska ha system för intern kontroll. För att förstå och reda ut detta begrepp har organisationen Committee of Sponsoring Organizations of the Treadway Commission (COSO) tagit fram ett koncept för intern kontroll som kan länkas till SOX-lagstiftningen (SIS, 2012).

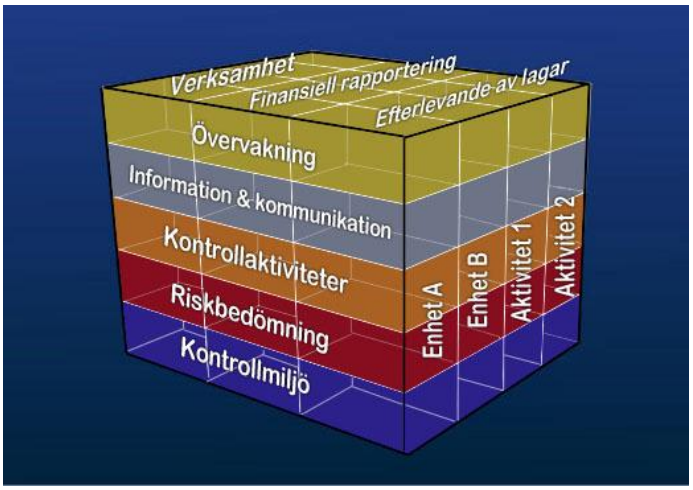
Committee of Sponsoring Organizations of the Treadway Commission bildades 1985 och bildandet av organisationen var ett gemensamt initiativ mellan fem branschorganisationer inom den privata sektorn med representanter från industriföretag, revisionsbyråer, investmentbanker och New York Stock Exchange. COSO bildades för att stödja organisationen National Commission on Fraudulent Financial Reporting och ett av områdena den arbetade med var att studera bakomliggande faktor till bedräglig finansiell rapportering. Organisationen arbetade även med ta fram rekommendationer till företag och deras revisorer, till SEC och liknande myndigheter samt till olika utbildningsinstitutioner (COSO, 2012).

COSO är en oberoende organisation som arbetar med frågor som rör förbättring av ekonomisk rapportering. För att uppnå detta tas flera områden till hjälp såsom affärsetik, interna kontroller och företagsstyrning och ett av syftena med COSO:s arbete är att kvalitén på den ekonomiska rapporteringen kan förbättras genom att bland annat effektivisera intern kontroll och företagsstyrning (SIS, 2012).

En stor del av COSO:s arbeta behandlar intern kontroll och hur den kan förbättras. COSO publicerade 1992 ett ramverk som fick namnet *Internal Control – Integrated Framework*. I ramverket presenterades olika verktyg som företag och organisationer kan använda för att utvärdera sina kontrollsystem för intern kontroll (Ramos, 2008).

2.15 COSO-Modellen

Organisationen COSO gav i september 1992 ut ett ramverk om intern kontroll (Moeller, 2004). I ramverket presenterades en definition av intern kontroll som idag är vedertaget accepterad där ett exempel på detta är att SEC:s definition överensstämmer i stora delar med COSO:s (Ramos, 2004). En skillnad mellan dem är att COSO:s definition är mer generell för intern kontroll och SEC:s tar sikte på intern kontroll över finansiell rapportering. COSO definierar intern kontroll enligt följande:"Internal control is as a process, affected by an entity´s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:



Figur 2. COSO-modellen (Omarbetad från SIS, 2012)

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations (COSO, 1992)"

COSO-modellen är en del av det ramverk organisationen gav ut 1992. Modellen kan både presenteras som en pyramid och som en kub och författarna har här valt beskriva modellen med hjälp av kub-modellen. COSO-modellen kan användas för att utveckla och beskriva definitionen av intern kontroll. Modellens tre huvudsakliga kategorier består av; verksamhet; finansiell rapportering samt efterlevnad av lagar och det är dessa mål organisationen strävar efter att uppnå. Dessa tre kategorier presenteras på den vertikala axeln. Det interna kontrollsystemet presenteras på den horisontella axeln och den tredje dimensionen representerar olika enheter och processer inom organisationen (SIS, 2012).

Det interna kontrollsystemet består av fem huvudsakliga komponenter och under dessa finns en rad principer. Författarna väljer här att beskriva huvuddragen för varje komponent och inte gå in på djupet om varje enskild princip. I COSO:s ramverk beskrivs följande komponenter för att få en effektiv intern styrning och kontroll över finansiell rapportering: kontrollmiljö, riskbedömning, kontrollaktiviteter, information och kommunikation samt övervakning (COSO, 1992).

2.15.1 Kontrollmiljö

Den nedersta komponenten i kuben är kontrollmiljön och Ramos (2004) menar att just kontrollmiljön är grunden för de andra komponenterna i modellen som utgör intern kontroll då kontrollmiljön ger både disciplin och struktur till organisationen. Begreppet kontrollmiljö innefattar den organisationsmiljö där den interna kontrollen ska verka och fungera och områden som räknas in i detta är bland annat organisationens affärsidé, värderingar, ledarskap, verksamhetens art och struktur, mål i form av operativa och strategiska samt utfallet av dessa (SIS, 2012).

2.15.2 Riskbedömning

Hayes, Dassen, Schilder & Wallage (2005) menar att riskbedömning är något som ska göras för alla fem komponenter i modellen, från kontrollmiljö i botten av kuben till övervakning i toppen. Haglund, Sturesson & Svensson (2005) menar att företag kommer alltid att ställas inför risker, interna som externa, vilket gör riskbedömning till ett viktigt område för företag att arbeta med. Externa risker kan utgöras av bland annat finansiella risker, legala risker samt omvärldsrisker medan interna risker inom ett företag kan vara verksamhetsrisker och redovisningsrisker. En risk som både kan vara extern såväl som intern är IT-relaterade risker (Haglund et al, 2005).

Riskbedömning innebär att risker ska identifieras och analyseras som eventuellt kan hindra ett företag eller organisation att uppnå sina mål (SIS, 2012). När detta steg är gjort är det viktigt att arbeta fram hur risker ska hanteras samt eventuellt ta fram förebyggande åtgärder. Haglund et al. (2005) påpekar också att branscher och lagstiftning förändras vilket gör det viktigt att det finns rutiner för hur nya risker ska identifieras och behandlas. Riskbedömning är viktigt för ett företag för att veta hur de ska allokera sina resurser. Genom att kartlägga och analysera externa samt interna risker kan ett företag få fram värdefull information för att på ett effektivt sätt fokusera kontrollprocesser mot områden där risken bedöms högre. Några exempel på konkreta risker kan vara att en obehörig person har möjlighet att beställa varor; att en fakturas uppgifter kan ändras samt att en obehörig person ges möjlighet att attestera (Haglund et al, 2005).

2.15.3 Kontrollaktiviteter

Kontrollaktiviteter är den mittersta komponenten i modellen. Detta område handlar om de kontrollaktiviteter och riktlinjer som är framtagna för att säkerställa att företagsledningens beslut når fram och verkställs. Kontrollaktiviteterna kan ses som de konkreta åtgärder som vidtas för att behandla risk i form av att motverka, alternativt minimera den. Åtgärder tas fram utifrån riskbedömningen och appliceras på företagets kontrollmiljö. Kontrollaktiviteter handlar om delegering, auktorisation och attestregler inom ett företag. Företaget bör ha tydlig dokumentation över an-

svars- och befogenhetsfördelning, regelverk och policys samt tydliga rutinbeskrivningar (SIS, 2012). Några konkreta exempel på kontrollaktiviteter är muntliga och skriftliga godkännande, attestering av fakturor, resultatuppföljning samt kontroll av tillgångar (Haglund, Sturesson & Svensson, 2005).

2.15.4 Information och kommunikation

I ett företag spelar affärssystemet en central roll för intern kontroll och finansiell rapportering med avseende på den information som finns i systemet. Information som hämtas från affärssystemet används för att ta fram en rad olika rapporter såsom verksamhets- och finansiella rapporter men systemet innehåller också information om avvikelser som är viktiga för att kontrollera verksamheten. En grundstomme för den här komponenten är att rätt typ av information identifieras och samlas samt att den kommuniceras till rätt människor i företaget (COSO, 1992). En viktig aspekt att beakta är tid. Information är i många fall kan vara färskvara vilket betyder att rätt information behövs rätt plats vid rätt tillfälle. Detta ställer även krav på att de system som används är aktuella, säkra och att informationen är uppdaterad. Systemen måste vara säkra så att ingen inom företaget får möjlighet att manipulera information (SIS, 2012).

Kommunikation kan delas upp i intern- och extern kommunikation. Den interna kommunikationen är viktig då den skapar förståelse inom företaget om mål, processer och enskilda ansvarsuppgifter. Den externa kommunikationen handlar mer om kommunikation med företagets intressenter angående bland annat finansiell rapportering och om företaget har uppnått sina finansiella mål (COSO, 1992).

2.15.5 Övervakning

Den översta komponenten i modellen är övervakning och syftar till att det interna kontrollsystemet ska kontrolleras och övervakas för att säkerställa dess kvalitet. Det här är en process som handlar om att utvärdera systemets funktion över tid vilket innefattar såväl fortlöpande kontroller som speciella utvärderingar. Ledningen har här det yttersta ansvaret men processen involverar personer inom hela företaget. Eventuella brister som hittas i det interna kontrollsystemet ska rapporteras uppåt i organisationen till dem som är ansvariga för att åtgärder ska kunna vidtas (SIS, 2012).

3 Metod

I metodkapitlet kommer det att beskrivas för läsaren vilka val som har gjorts av författarna, varför dessa val har gjorts samt hur de har påverkat genomförandet och resultatet av uppsatsen. Syftet med kapitlet är att ge läsare en uppfattning om genomförandet av uppsatsen.

3.1 Val av ämne

Intern kontroll är i dag ett viktigare område än någonsin tidigare. Utvecklingen inom området har kommit en lång väg sedan det först kom upp på tapeten i och med den stora börskraschen 1929 (Sennholz, 2000). Det har sedan dess skett en rad stora redovisningsskandaler runt om i världen som har fått uppmärksamhet. I modern tid är två av de mer uppmärksammade redovisningsskandalerna i media och litteratur Enron och Worldcom, två amerikanska bolag som gick i konkurs i början av 2000-talet. Skandaler som dessa har tvingat fram en hårdare lagstiftning om hur bolagen får och ska styras. Detta för att minimera att företagsledningen missköter sig och företagets finanser.

I en tid där de interna kontrollerna blir viktigare och den tekniska utvecklingen går snabbare, är det av författarnas intresse att undersöka hur man med det tekniska kunnande finns idag titta på hur företag kan kombinera redan implementerade affärssystem med interna kontrollerna. Utvecklingen har gått från manuellt kontrollerade och skötta kontroller till ett automatiskt system integrerat i företagets egna affärssystem.

3.2 Val av företag

I detta examensarbete avser författarna att undersöka hur implementeringsprocessen av SAP GRC ser ut och hur verktyget används i ett företag. Författarna hade i ett tidigt skede av uppsatsen, kontakt med ABB i Sverige, vidare gick kontakten mot ABB Ltd istället, då de var i var ansvariga för implementeringen. Efter ett par vändor med kommunikation mellan författarna av uppsatsen och ABB Ltd, fick författarna full access till att utföra fallstudien mot ABB Ltd. Arbetet med uppsatsen har då utvecklats ifrån kommunikationen med ABB Ltd. När kontakt togs var ABB Ltd precis i startgroparna till att påbörja sitt implementeringsarbete.

3.3 Val av respondenter

Författarna har sedan ett tidigt skede haft kontakt med projektledaren för implementeringen av GRC inom ABB, Julie D Haywood. Via henne har författarna fått hjälp att få kontakt med GRC-ansvarige Derek Roberts, Andrew Bainbridge och Anthony Benge. Dessa jobbar på ABB och be-

rörs direkt eller indirekt av GRC i sitt arbete i form av segregering av uppgifter eller uppföljningsarbete av kontroller. Dessa tre personer kommer vara de huvudsakliga respondenterna i detta examensarbete. Författarna har varit i kontakt med dessa personer, då de är få personer med insyn och kunskap om processer och användandet av GRC inom ABB.

Dessutom har kontakt tagits med experter inom området GRC, hos PwC Sverige samt ABB:s tredjepart i implementeringsarbetet, GRC Nordic. Anledningen till kontakten med GRC Nordic har författarna varit i kontakt med då de har jobbat aktivt med implementeringen av GRC hos ABB Ltd genom i stort sett hela processen. Anledningen till kontakten mellan författarna och PwC handlar om att få ett tredje perspektiv på implementeringsarbetet av GRC, med en part som sysslar med detta men inte har en roll i implementeringen hos ABB.

3.4 Val av metod och angreppssätt

Författarna insåg i ett tidigt skede av uppsatsprocessen att det skulle vara mer eller mindre omöjligt att basera uppsatsen på sekundärdata för att kunna besvara frågeställningarna. Att använda årsredovisningen för ABB var helt uteslutet, då dels en sådan rapport inte tar upp någon form av processer, nämner inte känslig information som företaget inte vill ska komma ut och för det tredje nämner inte ens ABB i sin årsredovisning att de använder sig av GRC. Med den frågeställning och den kontakt som hade etablerats med ABB Ltd insåg författarna att de behövde ett angreppssätt som fokuserar på aktuella händelser snarare än ett angreppssätt som fokuserar på historiska händelser. Enligt COSMO tabellen (Yin, 2006, s. 22) finns det tre angreppssätt som kan användas för uppsatsen, det är experiment, undersökning eller fallstudie. Experiment skulle vara väldigt svårt att använda sig av för att besvara frågeställningarna så det ledde till ett omedelbart bortfall. En undersökning skulle vara möjlig men vid en granskning mellan vad som skulle ge en djupare bild av ett ganska avgränsat område så kom författarna fram till att en fallstudie skulle vara det angreppsätt som skulle vara mest optimalt i detta examensarbete. En fallstudie ger författarna en möjlighet att kolla på frågan med utgångspunkten i hur och varför, med förankringen i den aktuella händelsen som i det här fallet är implementeringen av GRC v.10. Dawson (2000) menar att en fallstudie är det optimala valet när det gäller att undersöka processer och förändringsarbeten i en organisation eller ett företag. En fallstudie blir mer en subjektiv undersökning och då man kollar på processer är det svårt att mäta, utan värden man utvinner från intervjuerna i en fallstudie ska istället tolkas enligt Merriam (1994).

En fallstudie betyder i praktiken att författarna har gjort en undersökning av en organisation och en specifik företeelse (Halvorsen, 1992). Författarna har valt att gör göra en fallstudie för att stu-

dera flera aspekter av implementeringen (Halvorsen, 1992). Vid vidare läsning av andra uppsatser med liknade karaktär och metodböcker kunde författarna fastställa att det var intervjufrågor som skulle användas för att få ut det mesta av denna uppsats, den valda metoden intervjufrågor bekräftades vid samtal med uppsatsens handledare på både Internationella Handelshögskolan i Jönköping och på ABB Ltd.

Då författarna undersöker ett mindre avgränsat område med hjälp av intervjuer, är undersökning av kvalitativ karaktär. En kvalitativ undersökning lämpar sig för en undersökning som är av en djupare karaktär, vilket innebär att ett smalt område undersöks djupare (Jacobsen, 2002) och därför har författarna valt detta angreppssätt och metod för uppsatsen.

3.5 Val av referensram

Referensramen för uppsatsen har sin utgångspunkt i SOX. Författarna insåg att det var helt nödvändigt att sätta sig in i SOX för att kunna påbörja ett examensarbete inom intern kontroll. Under förarbete har ett stort informationssökande förts via sökmotorn Google, samt databaser som Business Source Premier och Diva portal. Sökord har varit: GRC, intern kontroll, internkontroll, interna kontroller, internal control, SAP, Sarbanes-Oxley Act samt SOX.

En annan viktig källa för informationssökandet har varit andra uppsatser och avhandlingar inom ämnet och uppsatser som berör ämnet. Dessa uppsatser har författarna funnit via databasen Diva Portal.

Själva utformandet av referensramen har till stor del blivit utvecklad ur lagtexten av SOX, modellen för intern kontroll COSO, samt ur vetenskapliga artiklar som vi har funnit via huvudsakligen Business Source Premier och Google Scholar som behandlar ämnet om SOX eller intern kontroll.

3.6 Upplägg och intervjumaterial

Med tanke på studiens natur har författarna valt att fokusera datainsamlingen via intervjuer och på grund av den stora geografiska skillnaden samt önskemål från ABB att utföra alla intervjuer via telefon. Telefonintervjuer är effektiva eftersom de inte tar lika mycket tid från respondenterna som en fysisk intervju gör, de håller även möjligheterna öppna för följdfrågor. Dock är det ett sämre alternativ än fysiska intervjuer. Då intervjuarna inte kan läsa av kroppsspråk hos respondenterna och inte ger samma möjlighet till fördjupning som en fysisk intervju ger. (Trost, 2005)

Vid samtliga intervjuer har båda författarna varit närvarande för att på bästa sätt få bådas perspektiv och kunna få två synsätt på svaren samt ha olika följdfrågor.

Intervjumaterialet har sedan gått vidare till djupare analys, som hela uppsatsens empiri bygger på samt ställs mot referensramen i uppsatsens analys.

3.6.1 Genomförande av intervjuer

Då alla intervjuer har skötts via telefon har samtalen för smidighetens skull spelats in. Detta för att kunna återges riktigt, exakt samt ligga till grund för transkribering. Författarna har utfört intervjuerna per telefon på uppmaning av ABB Ltd. Författarna har ändå valt att väga fördelarna mot nackdelarna av att utföra intervjuerna via telefon istället för att utföra på plats. Fördelar som hålla kostnader nere och vara effektiva med tiden överväger att en personintervju är en mer kontrollerad intervjusituation och är lämpad för lite mer komplicerade frågor (Langlet & Wärneryd, 1980). För att komma till den slutsats att undersökningen skulle utföras lika väl per telefon som per fysisk intervju.

Utöver har författarna haft uppdelningen under själva intervjun att en av författarna har fört anteckningar över tankar som kommer upp under intervjuerna, samtidigt som den andre författaren då leder samtalen istället.

Intervjuerna har utförts utifrån ett egenskapat frågeformulär för att följa en röd tråd av kontinuitet(BILAGA 1).

3.6.2 Intervjufrågor

Det frågeformulär som har legat i grund för intervjuerna har författarna gemensamt arbetat fram för att uppfylla syftet med uppsatsen. Eftersom majoriteten av respondenterna har engelska som sitt modersmål är frågorna på engelska tillika har intervjuerna genomförts på engelska. Dock med undantaget för intervjuer med respondenter på PwC i Sverige. Vid dessa har bara delar av intervjumaterialet har används (den del som inte är specifik för ABB) och intervjuerna har då genomförts på svenska, med de engelska frågorna som utgångspunkt.

3.7 Analys

I analysdelen knyter författarna samman teoridelen med empiridelen för att kunna drar slutsatser till de frågeställningar som ställs i uppsatsen. Den huvudsakliga informationskälla är intervjuer och det faller då naturligt att det i analysdelen har fokuserats på att analysera den information som har mottagits från respondenterna.

3.8 Validitet och Reliabilitet

Med validitet innebär att studiens giltighets styrks, detta innebär att uppsatsen frågeställningar är de facto det som undersöks under studien. Begreppet reliabilitet menar att den utförda studien är tillförlitlig i utförandet och innehåll. (Jacobsen, 2002)

En stor brist både när det kommer till att utföra detta examensarbete samt att definiera GRC är det finns väldigt lite forskning inom ämnet. Det material som finns tillgängligt är mesta dels från det företag som säljer produkten (SAP) samt konsulter och redovisningsbyråer som tillhanda håller tjänster inom GRC. Detta leder till vinklad information mot den som ger ut den, och är väldigt säljinriktad till varför man ska välja just den aktören vars information du läser.

Det ska dock tilläggas att på grund av att frågeformuläret har används som mall har varit ett standardformulär, och att följdfrågorna varierar beroende på vad respondenten svarar så missas en del av kontinuiteten, vilket ska tilläggas som en brist. Dock har alla samtal spelats in och transkriberats vilket stärker förtroendet på uppsatsens empiri.
På grund av känsligheten av informationen har författarna valt att inte gå ut med några faktiska siffror eller beräkningar och kan därför inte visa på hur ABB förväntas tjäna in investeringen i den nya versionen av GRC.
För att stärka uppsatsen reliabilitet ska det nämnas att en fallstudie inte behöver ha många respondenter, utan det är djupgåendet på en specifik företeelse som undersöks (Halvorsen, 1992). Således är det inget problem för uppsatsens reliabilitet att ha fyra respondet från ABB Ltd.

4 Empiri

I kapitlet presenteras empirin som har samlats in av författarna genom intervjuer. En definition av ämnet och huvudfrågan för uppsatsen ligger som grund för dispositionen av kapitlet. Empirin som presenteras i kapitlet ska i nästa kapitel ställas mot uppsatsens referensram.

Det finns idag inte någon exakt definition av GRC, utan de som finns är ofta individuella eller kopplade till ett företag. I denna del presenteras respondenternas egen definition av GRC, detta ska ligga i grund till hur GRC används och förväntningarna på detta. För att leda in empirin på uppsatsens två huvudsakliga forskningsfrågor börjar denna del av kapitlet med att försöka förklara det huvudsakliga målet med GRC. Vid en hårddragning av respondenternas svar att huvudmålet med GRC är efterlevnad av SOX. Dock ska det noteras att med samtal med GRC Nordic är det i Norden vanligare med företag som har GRC verktyg för den interna kontrollens skull, och inte på grund av SOX då i flesta fall de bolagen i norden inte behöver efterleva den lagstiftningen.

4.1 GRC definitioner

Författarna har i denna del av empirin valt att dela upp våra respondenter i tre grupper för att lättare kunna se skillnader i definitionen av GRC. De tre grupper av respondenter är användare, konsulter och revisorer. Uppsatsens författare att bett respondenterna att med egna ord beskriva vad det tycker att en korrekt definition av GRC och vad som enligt deras åsikter är den viktigaste anledningen till att använda sig av GRC.

Användare: ”Ett automatiserat standardverktyg för att hålla kolla på företagets risker och styrning.” (Derek Roberts, personlig kommunikation, 2012-04-20) Vidare ser han efterlevnad av SOX som den huvudsakliga anledningen till att använda sig av GRC som verktyg.

”Min definition är en påbyggd mjukvara, där ansvarige kollar på förändringar av roller eller påbyggnad av roller och att dessa inte skapar oacceptabla konflikter. Av min åsikt brukar detta vara en ja eller nej fråga. Svaret som brukar komma är antingen ja detta är acceptabelt och förändring sker. Eller nej, vi tillåter inte detta, men i vissa fall kan detta undvikas med att det sätts in en specifik kontroll för den förändringen.” (Andrew Bainbridge, personlig kommunikation, 2012-04-25) Även Andrew ser efterlevnad av SOX som den största anledningen till användning av GRC som verktyg.

Den tredje respondenten på ABB Ltd blev ett bortfall på frågan om definition.

Konsulter: ”Governance = Rätt personer tar rätt beslut. Risk Management = Informera rätt folk om vilka som är de bästa valmöjligheterna. Compliance = Informera rätt personer att de tog rätt beslut” (Matti Halonen, personlig kommunikation, 2012-04-27). Enligt Matti är det skillnad på de olika bolagen som använder sig av GRC som verktyg, Matti som är anställd på GRC Nordic, jobbar mestadels med företag i Skandinavien, de har huvudsak de interna kontrollerna, auktorisering av roller som viktigaste anledning till användning av GRC som verktyg, dock så fort det blir ett Anglosaxiskt land går fokus direkt över till efterlevnad av SOX som den viktigaste anledningen.

Revisorer: ”GRC huvudsakliga mål i min mening, är att minimera risker som finns i vägen för företagets strategi. Oavsett om företagets strategi baseras på finansiella mål eller andra mål som miljömått”. Scott Enerson, personlig kommunikation, 2012-04-13) Scott menar dock på att den viktigaste anledningen till att använda sig av ett GRC verktyg är att stärka de interna kontrollerna och på så sätt förenkla revisionsprocessen.

”GRC kan definieras som organisationens praxis och de olika roller som styrelse och ledande befattningshavare, linjeorganisation och resten av organisationen samspel i förhållande till tillsyn, strategi, riskhantering och strategi utförande avseende efterlevnad av lagar och förordningar och interna policies och förfaranden”. (Ulf Niklasson, personlig kommunikation, 2012-04-02) Enligt Ulf är det dock både SOX och revisionen som är lika starka anledningar till varför ett företag använder sig av ett GRC verktyg, men att detta beror på företaget i sig, vad de har för lagkrav på sig och storleken på verksamheten med mera.

4.2 Vad är målet med GRC?

Det huvudsakliga målet för GRC är uppsatsens respondenter eniga om, målet med GRC är att företaget ska nå sina mål och samtidigt uppfylla SOX under tiden man minimerar sitt företags risker. Då GRC är väldigt brett som koncept och innehåller en väldig massa funktioner blir det väldigt svårt för författarna av uppsatsen att hitta ett mål som är helt enligt med GRC utan att hålla målet väldigt brett.

Målet med *Governance* är inte det samma som för *Risk Management* eller *Compliance*. Utan denna hybrid får då ett annat mål än vad de har individuellt. Från ABB:s perspektiv är det dock målet med implementeringen och användningen av GRC att automatisera så mycket av kontrollerna som möjligt, minska antalet manuella kontroller utan att öka risken för konflikter utan snarare tvärtom, att minska dessa.

Detta går hand i hand med efterlevnad av SOX, så målet kan kallas både externt och internt. Där det externa går ut på att följa SOX och att klara de krav som ställs där. Det interna går då istället

ut på att rätt personer i ABB har tillgång till rätt transaktioner och roller, och där med minimera risken för bedrägeri eller stöld. Ett annat av de viktigaste målen inför implementeringsarbetet av GRC v.10, är det att samma version ska vara identisk över hela regionen som innefattar Storbritannien, Norge, Finland och Sverige, självfallet med undantaget då vissa lagar måste efterlevas i vissa länder men inte i andra. Dock är uppbyggnaden av systemen identiska och roll-systemet är den samma med undantag från Sverige.

4.3 Kostnadsanalys

I en vinstdrivande organisation är självfallet kostnadsaspekten väldigt viktig, och därför ska även kostnadsbilden beräknas. Enligt projektledaren för implementeringsarbetet är det väldigt svårt att räkna på hur mycket man sparar på GRC jämfört med att inte använda sig av GRC. Som tidigare nämnt av författarna i referensramen är kostnaderna för implementering av SOX en väldigt kostsam process. Det är även en väldigt kostsam process med implementering av GRC.

GRC handlar om att förebygga risk, och en risk kostar inget förrän den har inträffat. Därför är de ekonomiska tankegångar som går inför ett sådant implementeringsarbete rent spekulativ och baseras på uppskattningsvärden. Då de använder av ekonomiska siffrorna hämtade från tidigare årsredovisningar och en förutbestämd riskfaktor som visas i procent. En uträkning för detta ser då ut på detta sätt (uträkning fiktiv då ABB inte vill att sådana siffror bli offentliga.)

Att ha en kontroll som ser till att till exempel en anställd inte kan både skicka fakturor samtidigt som denne person kan utföra kreditfakturor. Kostnaden för att säkerhetsställa en sådan kontroll kostar inget utöver implementeringskostnaden för GRC. Däremot om dessa kontroller inte kan säkerhetsställas, att inte någon utfärdar kreditfakturor för egen vinning finns det en risk som kan bli en kostnad i mångmiljon belopp för företaget.

Denna beräknas på ABB Ltd:s genomsnittliga omsättning multiplicerat med en förutbestämd riskfaktor.

Att till exempel, en genomsnittlig årlig omsättning på £5 000 000 000 och en riskfaktor på att någon kommer begå bedrägeri utan att bli upptäckt är 0,1 %. Då är den uppskattade förtjänsten av en sådan kontroll är: £5 000 000 000 x 0,1% = £5 000 000.

Trots en liten procentsats så blir summan av risken väldigt hög. Som sagt är detta dock bara eventualiteter och ingen faktiskt besparing, utan minimering av risken att förlora de £5 000 000.

Faktiska besparingar som implementeringen innefattar är dock kopplat till automatiseringen och därför minskning av arbetade timmar med manuella kontroller. Det har tidigare har suttit perso-

ner och identifierat konflikter manuellt. Detta är ett väldigt omfattande arbete då konflikterna som uppstår mellan roller och transaktioner är i tusental. Det går då att beräkna hur många arbetstimmar som tidigare har gått åt att lokalisera dessa konflikter. Detta sker per automatik i GRC-verktyget vilket ledar till att arbetsbördan i tid blir lika med noll.

Uträkningen blir då antalet arbetstimmar som har tidigare gått åt konfliktlokalisering, multiplicerat med antal personer som jobbar med konfliktlokaliseringen multiplicerat med genomsnittlig förtjänst per timme. Till exempel: 52h x 4 personer x £1 000 = £208 000 i kostnadsbesparingar.

Från ett koncernperspektiv ser ABB också eventuella besparingar i kontorsutrymme, men dessa är spekulationer och skulle detta genera en kostnadsbesparing så är det av en lägre summa och har därför inte legat till grund för beräkningar inför implementering.

Vilka summor detta gäller går inte ABB ut med till författarna, dock i samtal med projektledaren kan författarna uttala sig om att investeringen kommer vara mer eller mindre självfinansierande under en ca treårs period.

Den beräknade ekonomiska livslängden på denna investering går dock inte i dagsläget att förutspå, då ABB kommer vid ett senare skede implementera en nyare version. Detta kommer att bero på när uppdatering av v.10 kommer eller när nästa version blir tillgänglig. Detta ligger utanför ABB:s område, och ABB kommer istället att ta ställning till detta beslut längre fram i tiden. När författarna i samband med ABB diskuterar SAP AG:s tidigare affärscykler så kan det antas att en uppdaterad v.10 är att vänta inom loppet av något år, samt att en ny version kan antas komma inom en tre till femårs period.

4.4 Implementeringsarbetet

Implementeringsarbetets processer går att dela upp i två delar, dessa delar är förarbetet vilket är den del av arbetet som sker innan den faktiska implementeringen av mjukvaran av de två modulerna Access Control och Riskmanagement.

I första delen, har själva förarbetet har skötts från ABB Ltd och inga andra parter har varit inblandade. I den andra delen av arbetet, implementeringen så har på grund av brist på intern kompetens inom GRC, har GRC Nordic, en tredjepart nischad mot GRC, kopplats in för att sköta de tekniska bitarna av implementeringen.

Implementeringen består av totalt nio faser innan implementeringen sätt i bruk och ”go live”, dessa faser är ABB Ltd:s egna och beskrivs nedan.

4.4.1 Förarbetet

I själva förarbetet har huvudsakligen allt arbete skötts från Storbritannien, med undantag för ett par småsaker har skötts från de lokala kontoren, så som undersöka de lokala riskerna, samt allokera monetära medel för investeringen. Detta är till skillnad från själva implementeringsarbetet som har skötts på nationell nivå i samarbete med den tredjeparten GRC Nordic. Vid samtal av GRC Nordic är implementeringsarbetet på ABB väldigt olikt det arbete som de har utfört åt andra kunder. GRC Nordic menar på att implementeringen av version 10 hos ABB från deras perspektiv är ett renodlat IT-projekt, då allt arbete med risker och segregering av uppgifter sker internt på ABB, till skillnad från andra kunder som GRC Nordic jobbar med utformning av riskmatris och segregeringsmatris. Anledningen till detta är det faktum att implementeringen av GRC v.10 är ny för ABB, så är inte verktyget GRC det. Det finns sedan tidigare riskmatris och segregeringsmatris, mer om detta tar författarna upp i stycken nedan.

Fas 1. Vid första fasen i implementeringsprocessen krävs det ett gediget förarbete angående vilken leverantör man ska använda sig av för att kunna maximera sin nytta av GRC kopplat till det ERP-system som företaget har som grund. För ABB som redan har ett ERP-system från SAP (ECC 6) med en Oracle databas i grunden. Vid implementeringsprocessens start körde ABB Ltd redan en äldre GRC applikation i form av v.5.2. Förarbetet för ABB handlade snarare om huruvida uppdateringen av GRC skulle bli till den uppdaterade versionen av den applikation de redan körde, i så fall den uppdaterade v.5.3 som byggde vidare på v.5.2. Alternativt skulle ABB uppdatera till den helt nya versionen, då detta implementeringsarbete ska se över hela regionen (Storbritannien, Norge, Finland och Sverige).

De skandinaviska länderna hade inte tidigare använt sig av någon GRC-applikation tidigare, utan hade tidigare använt sig av manuella kontroller i ett så kallat spreadsheet. Därför behövdes det en lösning som skulle passa alla regionens länder, som standardlösning. Dock skulle de olika ländernas nationella lagkrav variera.

Enligt GRC-ansvarig för ABB Ltd, var v.10 den version av GRC som var mest lämpad för en sådan process och ABB valde då att väja den senaste versionen, v.10.

Fas 2: Eftersom implementeringsarbete skulle vara ett omfattande arbete samt väldigt kostsamt, var det då viktigt att länderna i regionen var insatta i vad som skulle ske och krävas av dem. Vad det kommer att kosta samt att se till att de likvida medlen finns för processen. Detta skötes från England i samarbete med intern kontrollsansvarig i varje land i regionen. När de likvida medlen var säkrade, samt att det fanns en förståelse ute bland de andra ansvariga av intern kontroll inne-

förstådda på vad GRC var och vad det skulle innebära för deras organisation kunde man då gå vidare till nästa fas.

Fas3: Nästa steg var att bestämma varifrån implementeringsarbetet skulle börja. Det är ett omfattande jobb att implementera GRC, detta måste då ske stegvis och ett land i taget. Projektgruppen i England utvärderade då kunskap och erfarenhet av de olika ländernas GRC arbete inom regionen. Det var bara två länder som tidigare hade kört någon form av GRC. Detta var Storbritannien som körde v.5.2 och Schweiz som körde v.5.3. De andra länderna i regionen har bara tidigare kört ett spreadsheet och skött det som GRC gör manuellt istället. Så utgångspunkten för detta omfattande implementeringsarbete skulle bli antingen Storbritannien eller Schweiz. Schweiz hade tidigare jobbat lite mer omfattande med GRC och har två stycken heltidsanställda som bara jobbar med arbetet med GRC till skillnad från Storbritannien som inte hade arbetat lika intensivt med GRC och ansvarig för GRC är en IS security and Compliance manager. Var tjänsten bara består till en del av GRC-arbete.

ABB Ltd valde att utgå ifrån Schweiz som en modell för detta implementeringsarbete, då det här ABB:s huvudkontor ligger och det är detta kontor som har använts sig längst av GRC-verktyg, och därför har den bäst utarbetade grunden i hela koncernen. Detta följdes sedan av en implementering i Storbritannien, Norge, Finland och slutligen kommer implementeringsarbetet ske i Sverige i maj 2012. Eftersom målsättningen med implementeringsarbetet av GRC var att samma applikation skulle köras över hela regionen, var det också viktigt att alla ländernas GRC applikationer skulle vara kopplade till samma servrar. ABB har vad de kallar deras strategiska datacenter nere i Eigen, Tyskland. Vilket också skulle ligga som bas för alla länderna i regionens applikationer.

Fas 4: Efter att ha utvärderat den interna kompetensen blev det tydligt att för att kunna sköta detta implementeringsarbete så smidigt som möjligt, behövdes det en tredjepart som skulle jobba med det praktiska arbetet med att implementera applikationen. Det skulle krävas hög kompetens, kompetens som ABB själva saknade inom området för att kunna sköttas så felfritt som möjligt. ABB tog då in offerter från totalt fyra bolag som jobbar med konsulttjänster inom SAP och/eller GRC. När offerterna hade kommit in, började då arbetet med vilken tredjepart ABB skulle välja.

Pris ställdes mot erfarenheter och meriter. Vilken tredjepart ABB skulle välja var väldigt viktigt, inte bara för att det skulle bli kostnadseffektivt och rätt från början, men också på grund av omfattningen i arbetet. Implementeringen skulle ske över hela regionen och det var därför väldigt viktigt att den tredjepart ABB skulle välja skulle klara av ett så omfattande arbete samt kunna prestera väl under tiden de gör detta. I slutändan valde ABB ett konsultbolag i Finland som job-

bar med affärssystemet SAP men är huvudsakligen ett konslutbolag inom GRC. Detta bolag är GRC Nordic.

4.4.2 Implementeringsarbetet

Fas 5: I fas fem börjar det tekniska arbetet med implementeringen, denna fas kallas Risk containing och i denna fas utvecklar ABB en riskmatris och ett riskramverk för att undersöka vilka risker det finns för företaget och vilka risker man är ute efter att åtgärda med GRC verktyget.

I själva riskmatrisen undersökes ett antal faktorer, dels går man igenom riskgrupperna. Dessa riskgrupper har olika hög sannolikhet att inträffa, samt att de har olika konsekvenser för företaget, i form av kostnader och skadat varumärke. Meningen med fasen är att skapa medvetenheten om riskerna i företaget och hur de ska kunna elimineras med hjälp av GRC. I samförstånd med GRC applikationen utarbetas de kontroller som kommer att laddas upp i applikationen.

ABB använder sig av en standard-riskmatris som från början kommer från SAP. Denna har blivit uppdaterad via huvudkontoret i Schweiz för att anpassas till klimatet och riskerna som finns inom koncernen. Eftersom olika regler och kulturer finns inom de olika länderna, så utvecklas ofta den redan uppdaterade riskmatrisen för att passa landet i frågan.

ABB Ltd är av den meningen att standardmatrisen från ABB inte innehåller tillräckligt många risker, så har de då valt att utveckla matrisen något och införa fler risker och framför allt kolla på segregeringen av uppgifter (Access Control) vilket är den huvudsakliga interna kontrollen som GRC används för inom ABB Ltd.

Fas 6: När riskerna har blivit undersökta och fastställda är nästa steg att lägga in dessa i systemet, så i detta steg implementeras *mitigation of controls,* vilket är de interna kontrollerna som ska hålla koll på att transaktionerna sköts korrekt och att det inte finns några uppenbara fel och brister. Detta är en av de svåraste faserna i implementeringsarbetet, då det är oerhört omfattande kontroller som ska laddas upp i applikationen och detta arbete är något som tar väldigt lång tid och kräver kunskap i företagets risker och kontroller. Som GRC-applikationen ser ut i dagsläget, är detta den en av två delar som fortfarande sköts manuellt av de som jobbar med interna kontroller. Kontrollerna förs manuellt in i applikationen, för att minska risken att onödiga kontroller går in i systemet. Detta kräver en stor kunskap om såväl företagets risker som tidigare kontroller. Detta har varit den stora bristen i implementeringsarbetet i Finland till exempel, då ansvarig för interna kontroller är ny på jobbet och har inte den insyn som de andra intern kontrollansvariga i regionen.

Fas 7: I fas sju utarbetats berhörighetskonceptet och i denna fas kollar man på det viktigaste som finns i SAP GRC Access Control. Själva behörigheterna och rollerna som hela system från grunden bygger på. Behörigheten handlar om vilka transaktioner en anställd har behörighet att utföra ifrån sin roll. Rollen kan förklaras som den position på företaget den anställde har, till exempel är controller en roll. Behörigheten för controller X, kan då vara vad han eller hon har rätt att utföra från ett finansiellt perspektiv. En controller ska till exempel inte ha möjlighet att ta betalt från kunder eller kunna utföra kreditfakturor.

Detta är också en av de lite mer komplicerade faserna. Detta arbete måste ske manuellt och kan ske från två förhållningssätt. Det kan antingen vara *role-based* vilket innebär att behörighetskonceptet utgår från rollen. Till exempel behöver en controller kunna göra viss transaktioner och behöver vissa behörigheter. Detta ger ett mer konsekvent system där det är lättare att tilldela nya roller till personer som byter jobb eller kommer in nya i företaget. Det är lättare att hålla koll på roller och behörigheter.

Den andra inriktningen som kan användas för behörighetskoncepten är *user-based*, till skillnad från *role-based* utgår detta ifrån individen som sitter på en viss position. När behörighetskonceptet bestämts så kollar man på till exempel Herr X. Herr X har tjänsten som controller, men hjälper även till med lite andra saker, därför behöver han ha dessa behörigheter och rätt till att göra dessa transaktioner. När Herr X byter jobb eller position och Fru Y istället tar över hans tidigare position ska arbete göras om och man utgår från vilka behörigheter hon behöver som person, och dessa kan vara helt annorlunda gentemot vad Herr X hade.

Det senare sättet att förhålla sig till behörighetskonceptet hittas endast i Sverige, och kan knytas samman med den svenska arbetsmarknadskulturen. I resten av regionen så använder de nationella kontoren sig av *role-based* förhållningssätt och det är det författarna utav uppsatsen kommer att fokusera på.

Nytt för den nya versionen jämfört med den äldre är simuleringsmöjligheterna. När behörighetskoncepten tidigare var bestämda behövde de ansvariga kontrollera varje roll manuellt. Detta för att de inte skulle vara i konflikt med andra roller, eller att transaktionerna som var kopplade till en roll inte var i konflikt med varandra. Detta arbete var väldigt omfattande tidigare då varje roll har ett x antal transaktioner som han/hon kan utföra att kontroller alla roller och transaktioner blir då oerhört kostsamt i tid. I v.10 kan de ansvariga nu istället ladda upp de olika behörighetskoncepten och testa dessa emot varandra utan att föra i dem i systemet. Detta går betydligt snabbare än i den tidigare versionen och enligt GRC-ansvarig i Storbritannien är en av de största vinsterna

med att implementera den nya versionen istället för en uppdatering av den gamla. Själva arbetet med behörighetskonceptet sker utav GRC-ansvarig i respektive land.

Fas 8: Detta är implementeringsarbetets sista fas innan systemet ska *go live* och börjar brukas. Denna fas kallas för *previsoning* fasen. *Previsoning* är när man delar ut behörigheten till personer och efterföljer naturligt fasen där behörigheterna bestäms. I denna fas implementeras de testade behörigheterna och laddas upp i systemet för att kunna verkställas.

Det är i denna fas applikationer gör själ för sitt namn *Access Control.* Det är här dörrar öppnas och dörrar stängs till förmån för att minimera riskerna för stöld, bedrägeri och finansiella misstag genom att införa kontrollen av segregering av uppgifter. Huvudsakligen är dock GRC ett verktyg som ska fungera internt, eftersom det som sker under det löpande arbetet samt av intern personal och ledning. Samtidigt som den huvudsakliga anledningen till varför ABB ens avvänder det är externa skäl, då man på grund av sin marknadsnotering i USA är skyldiga att efterleva SOX.

Fas 9: Detta är den sista och *go live* fasen, när hela projektet sjösätts och denna ser lite olika ut inom regionen beroende på vilken erfarenhet man har av GRC på nationell nivå. De Skandinaviska länderna som tidigare inte har jobbat med GRC kommer en stor del av den femte fasen bestå utav utbildning av personal inom den nya systemmiljön som är skapad. Medan i Storbritannien som har tidigare erfarenhet kommer inte utbildning ta lika mycket utrymme utan det handlar snare om att förmedla de nya förändringar som har kommit i v.10.

Det skiljer sig dessutom förhållandevis mycket i design och layout av den nya versionen och det kommer krävas ett tag även för de lite mer erfarna att anpassa sig till den nya versionen. När utbildning och inlärningsfasen är över kommer GRC applikation kopplas samman till det ERP-system som ABB bygger på. I ABB Ltd:s fall deras ECC6 plattform och de ansvariga kommer då börja testa kontrollerna i applikationen mot det som är rapporterat i ERP-systemet.

Här börjar även utvecklingen av *workflows*. Vilket är en av de fundamentala byggstenarna för att nytta GRC snabbt och effektivt. Ett *workflow* är en förutbestämd handling som en person med behörighet för detta kan utföra, ett *workflow* fungerar på det sätt att det sätter igång en kedjeeffekt.

Ett workflow kan vara helt administrativt, helt finansiellt, eller en hybrid där emellan. Ett bra exempel att beskriva vad ett *workflow* kan användas till för att skapa kedjeeffekter är sjukanmälan av en anställd. Denne person ringer till sin chef för att anmäla sig sjuk och kommer inte kunna ta sig till jobbet. Dennes chef lägger då in ett *workflow* på en sjukanmälan på denna person. *Workflows* startar då en kedjeeffekt av allt som berörs av att denne person är sjuk. Finns det någon arbetssyssla som måste skötas trots sjukdom? Då skickas det ut förfrågan till någon annan som har en

liknande tjänst om att detta behöver göras, personer som berörs av den sjuka personens arbete blir varnade via systemet att denne person är borta för dagen och så vidare.

Go live: När alla dessa faser hade blivit genomförda var det då dags för ABB att *go live* och börja köra systemet i verkligheten mot de transaktioner, roller, kontroller och konflikter som finns i den vardagliga affärsverksamheten. Arbetet med GRC sker löpande och kan delas upp i två moment: *godkännande* och *kontroll*.

Den *godkännande* delen är delen gällande segregeringen av uppgifter, här sker det manuellt huruvida en person ska ha rätt till en roll eller en transaktion. Denna godkännande del sköts bara av en person och det är GRC ansvarige i England. Den godkännande delen sköts via modullen *Acecess Control* och är den mest grundläggande funktionen.

Kontrollerande delen består av interna kontroller och simulation. Samtidigt som det är här själva förarbetet till hur vidare GRC-ansvarige ska godkänna en roll, person eller en transaktion. Kontrolldelen är den grundläggande delen i risk management-modulen och från den hämtas utdrag som skickas en gång i kvartalet till *Local Business Unit (LBU)* controller som är ansvarig för att signera att kontrollerna som finns styr upp företagets konflikter.

4.5 Fördelar med den nya versionen

En av de viktigaste fördelarna med den nya versionen från ABB:s perspektiv är att den automatiserar fler kontroller än tidigare vilket i det stora loppet gör att arbetsbördan minskar och kontrollerna blir säkrare eftersom de bygger på SAP ECC6 systemet som finns i bakgrunden. I jämförelse med ABB:s tidigare GRC version är den nya betydligt snabbare än den tidigare enligt användarna. Från att någon på *human resources* eller en chef på någon nivå ber GRC-ansvarig om att tilldela någon en ny roll, tills den simuleras för att kolla efter konflikter, för att sedan tilldela rollen om inga konflikter som inte kan hanteras uppstår, kan gå inom loppet av ett par minuter om ingen hänsyn tas till andra arbetsuppgifter.

En annan klar förbättring från den tidigare versionen är att numera kan ABB använda sig av SAP *workflow* även inom GRC-verktyg, detta var inte möjligt i v.5.2 eller v.5.3 vilket går hand i hand med automatiseringen, där mindre handlingar har en större effekt på kontroller och maximerar nyttan av verktyget. En annan fördel som gör v.10 snabbare än de tidigare är att numer finns möjligheten för GRC-ansvarig att köra simuleringar utanför verktyg för att kunna kolla vilka konflikter som uppstå vid tilldelning av en ny roll eller transaktion.

Den huvudsakliga fördelen med v.10 och ett av huvudargumenten till varför v.10 var den som blev vald att implementeras över hela regionen istället för de äldre versioner som använts av Storbritannien och Schweiz, var att v.10 var mer anpassningsbar och lättare att individualisera till varje lands egna lagkrav med mera. Trots detta förblir grundapplikationen den samma rakt igenom regionen.

4.6 Svårigheter med implementeringen

Implementeringsprocessen sett utifrån ABB Ltd:s perspektiv har varit relativt felfri och utan större svårigheter. Dock har det funnit två stycken hinder på vägen som har tagit lite tid och krävts lite extra arbete för att lösa.

Det första problemet i själva implementeringsprocessen berör själva kontrollerna och där de skulle föras in i verktyget. Tidigare version har det varit möjligt att föra in de tidigare kontrollerna via ett så kallat spreadsheet i Excel-format. Detta har blivit bortplockat ur den nya version på grund av risken att felaktiga kontroller kan implementeras från början utan att kontrolleras och det krävs nu istället att dessa kontroller förs in manuellt vilket blev extra jobb som inte var förutspått.

Det andra problemet uppstod när implementeringen var färdig och verktyget testades. ABB lyckades då inte får workflow funktion att funka, vilket i sin tur ledde till att behörigheterna inte funkade som de skulle. Detta var dock bara lite av en barnsjukdom på den nya version och är i dag åtgärdat av SAP.

Dessa problem var dock endast smärre hinder på vägen och ABB Ltd lyckades fortfarande hålla tidsplanen för implementeringen. Implementeringen som projekt är dock inte färdigställt utan det pågår fortfarande arbete i Norge och Finland samt att arbetet med Sverige kommer att påbörjas i början av maj 2012. Projekt kommer inte att anses vara färdigställt förrän alla länderna i regionen har passerat ”go-live”-fasen.

4.7 Hur skulle ABB kunna nyttja GRC på ett djupare plan?

Detta är en av uppsatsens delfrågor, dock utifrån frågans natur har uppsatsens författare insett svårigheten att ta upp frågan i uppsatsens empiri. Då naturen av frågan är subjektiv angående hur författarna ser utvecklingsmöjligheterna hos GRC-verktyget inom ABB. På grund av detta har författarna valt att ta upp den frågan i diskussionen istället, då förbättringsåtgärderna är något som författarna själva ser utifrån att utfört denna fallstudie och kan därför inte knytas samman till referensram.

5 Analys

I detta kapitel av uppsatsen ställer författarna empirin som framkommit ifrån intervjuerna mot uppsatsens referensram. Syftet med analysen är koppla samman dessa för att nästkommande kapitel besvara uppsatsen frågeställningar.

5.1 Definition av GRC

Den genomgående tråden som går att utläsas ur respondenternas egna reflektioner och definitioner, trots att de skiljer sig åt, är att syftet med GRC är styrning av bolaget och stärkandet av intern kontrollen för att förebygga hinder som finns för att nå företagets mål och strategi. Samtidigt är det huvudsakliga målet med GRC är att efterleva SOX-lagstiftningen. Detta går att ställa i perspektiv med vad syftet med SOX är. Enligt Svernlöv & Blomberg (2003) är syftet med lagstiftningen att reglera bland annat frågor kring bolagsstyrning, intern kontroll och finansiell rapportering. I lagtexten finns det stipulerat att företag ska ha ”system för intern kontroll” (Sarbanes-Oxley Act of 2002, 2002). Det är svårt direkt utifrån lagtexten att definiera huruvida GRC går under ”system för intern kontroll”. Utan istället ställs GRC mot det koncept för intern kontroll utvecklat utav COSO, som är länkat till SOX (SIS, 2012).

COSO-modellen kan användas för att definiera intern kontroll och således även GRC. COSO-modellen bygger på ett antal nivåer som används för att definiera intern kontrollens system och för att bedöma huruvida den stämmer in på SOX (SIS, 2012). Dessa nivåer som stipuleras i modellen är:

- Kontrollmiljö
- Riskbedömning
- Kontrollaktiviteter
- Information och kommunikation
- Övervakning

För att bedöma huruvida GRC passar in, ställs GRC mot de olika nivåerna i COSO-modellen. Kontrollmiljön är grundstenen i hela kontrollstrukturen, här går värderingar, företagets strategi och verksamhetsstruktur in (SIS). Enligt en av respondenternas definition av GRC är målet med GRC är eliminera risker som står i vägen för företaget att uppnå sin strategi, oavsett om denna är värdeskapande i monetära mått eller till exempel etiska mått. Kontrollnivå kan då anses vara uppnådd i och med GRC. Vidare menar Hayes, Dassen, Schilder & Wallage (2005) att alla fem nivåerna i modellen ska riskbedömas. Ställt emot GRC så är riskerna i GRC anpassade för hela verk-

samheten i det bolag applikationen implementeras, och kollar på flera nivåer av risker. Vidare menar Haglund et al (2005) att det väldigt viktigt för företaget att ha mål och strategier för att kunna utföra en tillförlitlig riskbedömning av företagets risker. Eftersom lagar och externa förutsättningar ständigt är under förändring måste det finnas tydliga riktlinjer om hur riskbedömningen sker och håller sig ajour.

Kontrollaktiviteterna som beskrivs i COSO-modellen består av de konkreta åtgärder som används för att minska eller att eliminera de risker som företaget tampas med. Enligt COSO-modellen kan detta vara allt från beloppsgränser på inköp till kontroll av tillgångar. GRC har det upplägget att applikationen som sådan själv inte har några implementerade kontroller. Utan de kontroller som är utredda och behövs för ABB är de som ABB själva implementerar. Detta leder till att företaget själva bestämmer hur gedigna de vill att sina kontroller ska vara, kontrollaktiviteterna är då automatiserade och stärks då den mänskliga felfaktorn inte har samma riskmoment. (Haglund et al, 2005)

Informationen och kommunikationen är en av de viktigaste nivåerna i COSO-modellen, då den syftar på informations och affärssystem. En intern kontroll tappar sitt syfte då information eller siffror är felaktiga. Systemet behövs dessutom för att göra informationen kommunicerbar mellan de berörda parterna på företaget. I ABB:s fall använder de sig av en SAP ECC6 plattform som affärssystem, denna grundas på en Oracle-databas vilket gör det möjligt för alla de moduler som är kopplade till plattformen kan kommunicera med varandra, och man kan då komma åt all information från de olika modulerna utan att behöva stänga ner den vederbörande sitter i. Detta gäller självklart också GRC-applikationen som har översikt över alla moduler kopplade till plattformen för att undersöka eventuella konflikter. (Haglund, et al, 2005)

Den sista nivån i COSO modellen berör tillsyn och övervakning, riskerna för ett företag är ständigt under förändring. Detta gör att det är viktigt för att kunna styrka de interna kontrollerna, att de är under kontinuerlig tillsyn, för att ständigt vidimera att kontroller tjänar sitt syfte (COSO, 1992). Detta löser ABB kvartalsvis då LBU controller, går igenom alla kontroller som ABB har aktiva samt gör en tillsyn över alla konflikter som finns med företagets kontroller vid tidpunkt av tillsyn av kontrollerna.

5.2 SOX:s roll i implementeringen av GRC

Det huvudsakliga målet som ligger bakom implementeringen hos ABB är de lagkrav som stipuleras för företag som är registrerade på de amerikanska värdepappersmarknaderna. Det huvudsakliga lagkravet är ramlagen SOX som kom till för att stärka de interna kontrollerna och återvinna

förtroendet hos intressenterna till bolag på de amerikanska marknaderna. För att behöva efterleva SOX räcker det med att bolaget i fråga marknadsförs på en Amerikans värdepappersmarknad, detta innebär att det finns inget krav på att huvudkontoret eller moderbolaget måste vara på Amerikansk mark. (Svernlöv & Blomberg, 2003). På grund av detta är ABB tvingade att efterleva SOX, då de fortfarande säljs och köps på New York Stock Exchange (Dagens Industri, 2012).

I SOX benämns det att företag ska ha ”system för intern kontroll”. För att förstå och reda ut detta begrepp har organisationen Committee of Sponsoring Organizations of the Treadway Commission (COSO) tagit fram ett koncept för intern kontroll som är länkat till SOX (SIS, 2012). Där av har valet blivit att implementera SAP:s verktyg GRC. För att säkerhetsställa de interna kontrollerna på ABB, att uppfylla kraven i SOX. ABB väljer då att implementera detta i rakt led genom hela regionen, med dock ett par mindre skillnader i kultur mellan länderna och deras uppbyggnad av GRC-verktyget för att få en kostnadseffektiv lösning för att efterleva SOX.

5.3 Implementeringen av GRC

Den stora frågan när det kommer till implementeringen av GRC är den samma som alla andra stora investeringar, det handlar om att överväga nyttan med kostnaden, samt kostnaden för att låta bli att implementera det. Freeman (2009) menar att SOX slår väldigt hårt mot de företag som tvingas efterleva lagstiftningen. Då det innebär väldigt höga kostnader för att efterleva lagen i och med ökade revisionskostnader och konsultarvoden för att uppfylla de krav som ställs.

Allt sedan införandet av SOX har det diskuterats över hur resurskrävande införandet har varit både i form av tid samt pengar. SOX består av ett flertal sektioner, men den sektion som ofta nämns för att vara kostsam såväl att implementera som tillämpa är sektion 404 i lagen som behandlar ledningens ansvar och kontroll av den interna kontrollen (Bradford & Brazel, 2007; McCauley, 2007). Sektion 404 är den sektion av lagen som ligger till grund för varför ABB väljer att implementera GRC, då detta går på ett smidigt och effektiv sätt att bygga på det ERP-system som idag redan är aktivt inom ABB-koncernen, för att efterleva de krav på intern kontroll som ställs i sektionen.

Tacket, Wolf & Claypool (2006) påpekar att kostnadsaspekten av sektion 404 kan delas upp i monetära samt icke-monetära kostnader. På grund av omfattningen av implementeringen är den mest omfattande kostnadsaspekten av GRC, de monetära måtten. Tacket, Wolf & Claypool (2006) beskriver monetära kostnader som uppkommer kan vara i form av konsultarvoden och revisionskostnader. Revisionskostnaderna även efter implementeringen av GRC, då revisorerna

ska bedöma effektiviteten av det interna kontrollsystemet med avseende på sektion 404 i SOX (Precht, 2005).

På grund av omfattningen av implementeringen ökar kostnaden av konsultarvoden och investeringen i mjukvara markant samt hårdvara för att klara av den ökning i informationsflöde som implementeringen av GRC innebär. Detta stöds av Tacket et. al (2006) som menar att den absolut största anledningen till ökningen av konsultarvoden är behovet av mycket komplicerade affärssystem som krävs för att uppfylla sektion 404 i SOX.

De icke-monetära kostnader som uppkommer kan vara i from av logiska brister och kan också bero på en överbelastning av information (*eng. information overload*). En enklare förklaring av icke-monetära kostnader är de svårigheter som uppkommer på grund av lagen men som inte går att mäta i pengar (Tacket, Wolf & Claypool, 2006). Överbelastningen av information märker inte ABB:s respondenter av då implementeringen av den nya versionen av GRC är betydligt snabbare och mer effektiv än den tidigare samt att ABB använder sig av det strategiska datacenter som ABB har i Tyskland för att använda sig av den serverbas som finns där nere. Detta för att klara av den ökade mängden informationsflöden, så som alla konflikter som visas på när det kommer till roller och transaktioner.

Att välja att inte efterleva SOX medför också väldigt höga kostnader, då ett syfte med lagen är att avskräcka med monetära konsekvenser för att inte efterleva lagen, och risk för långa fängelsestraff. (Prentice, 2007).

Att ställa detta mot att implementera GRC som också medför höga kostnader, men dessa kostnader är en så kallad icke återvinningsbar kostnad som gäller själva investeringen, men kommer i det långa loppet innebära att kostnaden för revisionen kommer att bli dyrare för ABB än vad den var innan var tvungna att efterleva SOX. Då i och med SOX så ökar ansvaret på revisorerna och de måste kontrollera systemen för intern kontroll (Tacket, Wolf & Claypool ,2006).

Konsultarvodena däremot kommer inte att fortsätta att öka i kostnad så länge det inte kommer till eventuella problem med GRC som kräver framtida extern experthjälp.

I och med införandet av SOX menar McCauley Parles, O'Sullivan & Shannon (2007) att en majoritet av företagen upplever att deras interna kontroll har tydligt stärkts. Detta påvisar även uppsatsens respondenter som menar på att ABB:s interna kontroller aldrig har varit starkare än vad de har varit i dag i och med implementeringen av SOX samt GRC. Detta ser ut att vara en genomgående trend som även Prentice (2007) styrker när han påvisar att sedan införandet av SOX har inga större redovisningsskandaler inträffat i USA och antalet stämningsansökningar för bedräge-

rier har även minskar. Precht (2005) kan även påvisa att införandet av SOX har gett en tydligare fördelning av roller och ansvar, ställa detta mot ABB finns det inget som kan påvisa att detta har skett i och med implementeringen.

ABB har även innan av implementeringen drivit sin verksamhet i en SAP-miljö. ECC6 systemet från SAP bygger på ett antal roller, vilket används även inom GRC-applikationen. Rolluppdelningen inom ABB var redan omfattande sedan tidigare. Precht (2005) menar också att i och med rolluppdelningen kan detta kan bidra till en lugnare arbetsmiljö och även ge trygghet till de anställda i ett företag. Då uppsatsens respondenter inte varit anställda på ABB innan SAP-miljön utvecklades går det inte att ställa i relation till hur det var tidigare, men respondenterna påvisar att kontrollerna känns säkrare samtidigt som arbetsuppgifterna har skiftat. Eftersom kontrollerna numera är automatiserade så är det inte längre samma press på att hela tiden ligga steget före med de interna kontrollerna, och därför har arbetstempot blivit lite lugnare.

6 Slutsats

I detta kapitel presenteras de slutsatser som har genererats i analysen.

- Hur sker implementeringen av SAP GRC v.10 inom ABB Ltd?

Implementeringen kan delas upp i tre delmoment, det är den ekonomiska planeringen, den praktiska planeringen och det praktiska utförandet. Trots att ABB tidigare har använt sig av en äldre GRC applikation, saknades det internkompetens för att genomföra en så infattande implementeringsprocess som att implementera GRC faktiskt är. ABB valde istället att ta in en extern tredjepart i form av det finska konsultbolaget GRC Nordic.

I samarbete med GRC Nordic utförde ABB implementeringsarbetet enligt en nio faser lång process. Dessa nio faser skulle lika väl kunna appliceras på vilket annat företag som helst. Dock är det som sker under de olika faserna är helt unik för ABB Ltd, och när implementeringen sker i de andra länderna, kommer arbetet fortsätta enligt detta faser. Innehållet i faserna anpassas dock efter riskerna som just finns för ABB i Storbritannien, Finland, Norge och Sverige. Samma sak är gällande när det kommer till lagar och verksamhetsmålen som finns på de olika nationella nivåerna.

Implementeringen sker i varje land inom regionen med en månads mellanrum, detta innebär att varje land bara har haft en månad på sig att få saker och ting på plats. Detta har vidare betytt att det har varit svårigheter i regionens andra länder. I Storbritannien har dock tidsplanen följts till punkt och prickar trots svårigheter med implementeringen.

- Varför väljer ABB Ltd att implementera SAP GRC v.10?

Huvudanledningen till varför ABB väljer att implementera GRC är att de på grund av att de saluförs på den amerikanska börsen, detta innebär att enligt amerikansk lag är de skyldiga att efterleva lagen SOX. SOX syfte är att höja de interna kontrollerna och förbättra bolagsstyrningen i amerikanska bolag för att reducera bedrägerier och bokföringsbrott.

Varför ABB Ltd väljer att implementera v.10 istället för att bibehålla den tidigare v.5.2 som de har tidigare nyttjat i Storbritannien är för att ABB i denna process har valt att implementera GRC i hela regionen, för att detta ska gå så smidigt som möjligt, samt förena så mycket nytta och effektivitet som möjligt. I det interna förarbetet vägde projektledningen för implementeringen de olika versionerna mot varandra, slutsatsen av denna vägning var att den senaste versionen skulle vara

den version som ansågs mest passande för hela regionen. Man valde då att implementera GRC applikationen i varje land i regionen med en månads mellanrum.

- Hur skulle ABB Ltd kunna nyttja GRC på ett djupare plan?

Denna delfråga har inte författarna av uppsatsen kunnat besvara på vetenskapliga grunder, utan väljer istället att ta upp den frågan i diskussionen istället. För att beskriva de förbättringsåtgärder författarna ser utifrån att ha genomfört denna fallstudie.

7 Diskussion

I det avslutande kapitlet presenteras författarnas egna tankar och reflektioner kring ämnet som har kommit upp under arbetet med uppsatsen. Avslutningsvis ges förslag för framtida forskning inom ämnet.

När vi startade med att skriva denna uppsats, visste vi väldigt lite om det vi gav oss in på. Dock efter att ha utfört hela arbetet så har vi införskaffat oss så pass mycket kunskap av vi anser oss kunna uttala oss om vår syn på GRC.

En av de största brister vi har stött på under arbetets gång är det faktum att en definition av GRC som sådant inte existerar. Det var inte bara i litteratur och artiklar detta blev ett problem, vid samtal med våra respondenter insåg vi hur oerhört mycket uppfattningen kunde ske mellan olika individer på samma företag. Även konsultbolagen och revisionsbolagen kände att detta var en brist, då det var svårt att veta hur de skulle marknadsföra en produkt som är så pass individ att den ser olika ut för mer eller mindre varje företag. Efter att ha ställt frågan till respondenterna av denna uppsats, om hur de själva skulle vilja definiera GRC. Har vi valt att definiera GRC som sådant: GRC är ett automatiserat och standardiserat verktyg som ska eliminera och förebygga risker som står i vägen för företaget att nå sin strategi. Vi är av den meningen att detta är den rakaste definitionen av förklarandeform till vad GRC verkligen är.

Vi har även sett att det finns en otydlighet om drivkraften hos GRC hos våra olika respondenter. Enligt användarna av GRC så är den huvudsakliga drivkraften bakom GRC just att efterleva SOX, medans hos konsulter och revisorer tycker de dock sett från ett mer skandinaviskt perspektiv att den huvudsakliga drivkraften bakom GRC är de interna kontrollernas påverkan på kostnaden för revision. Enligt vår åsikt så är båda synsätten korrekta, det är bara att de grundas i olika miljöer och förhållanden. Användarna av GRC som vi har talat med lever i en kontrollmiljö där SOX måste efterlevas, medan de konsulter och revisorer vi har talat med i stället lever i den kontrollmiljön där SOX inte har någon laga kraft. Därav är det de interna kontrollerna som blir viktiga och inte SOX ifrån det skandinaviska synsättet. Vi är av den meningen att hade vi talat med konsulter och revisorer från USA, hade deras svar antagligen varit identiskt med det som respondenterna från ABB har givit oss.

Vidare under vårt arbete och i och med samtal med ABB, så har vi sett ett par saker som vi tror skulle kunna göras bättre för att ytterligare få större användning av GRC-verktyget. Som vi ser och har förstått det, så visar GRC-verktyget på tusentals konflikter mellan olika roller och transaktioner vid varje kvartal när *outputs* tas ut för att gås igenom. Dessa konflikter är redan bedömda att vara av olika risk/prioritering i systemet. Vilket vi tycker är bra samt att det ska vara så, men

det vi ser är också att det inte finns skillnad på *viewing* och *editing*. Detta innebär i praktiken att en som jobbar på lagret och har i sin roll möjlighet att kolla på fakturor för att se vad en kund har beställt. Trots att denna lageranställda inte har möjlighet att ändra något i fakturan *editing-rights* utan bara möjlighet att läsa innehållet i den *viewing-rights* så ser GRC-verktyget detta som en risk. Detta är vid en närmare koll vid varje kvartal väldigt lätt att inse att detta inte de facto är en risk för företaget, så det som sådant är inget problem. Det som dock blir problematiskt i våra ögon är att detta är bara ett exempel av flera, så utav tusenstals konflikter är väldig många egentligen inte konflikter. Detta riskerar att bli farligt, då de faktiska konflikterna och riskerna kan riskera att falla emellan dessa triviala risker och missas av företaget.

Att ändra detta skulle vara ett väldigt omfattande jobb, och ett jobb som berör systemet och inte ABB. Det vi från ett tredjeperspektiv dock ser som en möjlighet att minimera dessa triviala risker är dock att gå från det rollsystem ABB Ltd idag använder sig av. Det så kallade *role-based* där transaktionerna är förutbestämda utifrån en roll. Istället för att använda sig av detta skulle det vara får rekommendation att gå till ett *user-based* rollsystem i stället, där man utgår ifrån individen och vilka transaktioner denne individ behöver kunna göra. Det går att argumentera huruvida systemet då skulle bli mer godtyckligt och inte lika stabilt då samma roll kan bestå av olika transaktioner beroende på individ. Enligt vår åsikt skulle detta dock kunna hjälpa till att eliminera triviala konflikter avsevärt. Då de transaktioner som de olika rollerna besitter är faktiskt de som används och blir mer aktuella att kontrollera, än som det är idag. Då många transaktioner kopplade till en roll inte används, de finns där bara för att så som rollen har blivit förutbestämd så finns de transaktionerna med. Detta leder till mer arbete, mer triviala konflikter och även i vår åsikt ett stelare system.

7.1 Förslag till framtida forskning

Det finns nästintill ingen forskning på området GRC, så vårt förslag till framtida forskning utöver detta arbete skulle vara att fastställa en vetenskaplig definition av termen. Vi föreslår dessutom vidare forskning inom området på hur GRC ytterligare skulle kunna täcka den lagstiftning som stipuleras inom SOX.

Litteraturförteckning

ABB. (2010, 15 januari). *Handel med ABB-aktien och tickersymboler*. Hämtad 2012-03-14, från http://www.abb.se/cawp/abbzh259/db55cbd966a7d380c1256ce200344097.aspx

ABB. (2011a, 10 mars). *Från Asea till ABB*. Hämtad 2012-03-12, från http://www.abb.se/cawp/seabb361/dd5ce102d6e2635ac1256b880042aee5.aspx

ABB. (2011b, 4 januari). *120 års tekniskt ledarskap*. Hämtad 2012-03-14, från http://www.abb.se/cawp/seabb361/405b0f36a9fe8d95c1256dc2002d5016.aspx

ABB. (2012a). *Överföring av likström långa sträckor*. Hämtad 2012-03-12, från http://www.abb.se/cawp/db0003db002698/4a887b82483de2c0c125733a00348d9c.aspx

ABB. (2012b, 15 februari). *Vår verksamhet*. Hämtad 2012-03-14, från http://www.abb.se/cawp/seabb361/9d604138cc8089b2c12571990031abeb.aspx

ABB. (2012c, 16 februari). *Vår strategi*. Hämtad 2012-03-14, från http://www.abb.se/cawp/seabb361/c10d8838bed4b721c125719900326297.aspx

Arwinge, O. (2010). Internal Control – A study of the Concept and Themes of Internal Control. Linköping: LiU-Tryck.

Bjorlin, C. (2011, 23 mars). *SAP GRC 10 Release Includes Embedded BI, Move from Java to ABAP*. Hämtad 2012-03-15, från http://www.asugnews.com/2011/03/23/sap-grc-10-release-includes-embedded-bi-move-from-java-to-abap/

Bradford, M., & Brazel, J. (2007). Flirting with SOX 404. *Strategic Finance, Vol. 89, Issue 3*, 48-53

COSO. (1992). *Internal Control – Integrated Framework*. New York: AICPA.

COSO. (2012). *About Us*. Hämtad 2012-04-23, från http://www.coso.org/aboutus.htm

Dagens Industri. (2012). *Svenska aktier I NY*. Hämtad 2012-05-07, från www.di.se - Börslistor – Svenska aktier I NY.

Dawson, C. W. (2000). The essence of computing projects: a student's guide. Harlow: Pearson Education.

Freeman, J. (2009, 15 december). *The Supreme Case Against Sarbanes-Oxley*. Hämtad 2012-04-02, från http://online.wsj.com/article/SB10001424052748704431804574539921864252380.html

Haglund, A., Sturesson, J., & Svensson, R. (2005). *Intern kontroll – En del av verksamhets- och ekonomistyrningen*. (2:a utökade uppl.). Stockholm: Komrev.

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

Hayes, R., Dassen, R., Schilder, A., & Wallage, P. (2005). *Principles of auditing – An introduction to international standards on auditing*. (2:a uppl.). Harlow: Pearson Education.

Jacobsen, D. I. (2002). Vad, hur och varför? – om metodval i företagsekonomi och samhällsvetenskapliga ämnen. Lund: Studentlitteratur.

Lander, G. P. (2004). *What is Sarbanes-Oxley?*. New York: McGraw Hill.

Langlet, P., & Wärneryd, B. (1980) *Att* fråga. Stockholm: Liber förlag.

McCauley Parles, L., O'Sullivan, S. A., & Shannon, J. H. (2007). Sarbanes-Oxley: An Overview of Current Issues and Concerns. *Review of Business, Vol. 27, Issue 3,* 38-46

Merriam, S. (1994). *Fallstudien som forskningsmetod*. Lund: Studentlitteratur.

Moeller, R. R. (2004). *Sarbanes-Oxley and the New Internal Auditing Rules*. New Jersey: John Wiley & Sons.

Palley, T. I. (2007, 7 februari). *In Defense Of Sarbox*. Hämtad 2012-04-02, från http://www.thomaspalley.com/?p=67#more-67

PCAOB. (2012). *About the PCAOB*. Hämtad 2012-04-04, från http://pcaobus.org/About/Pages/default.aspx

Precht, E. (2005). Ändrade arbetssätt med Sarbanes-Oxley Act. *Balans, nr. 5*. Hämtad från FAR Komplett.

Prentice, R. A. (2007) Sarbanes-Oxley: The Evidence Regarding the Impact of Section 404, *Cardozo Law Review, Vol. 29, Issue 2,* 703-764

PwC. (2011). *White Paper – Governance, Risk Management and Compliance: Sustainability and Integration supported by Technology*. [Broschyr]. (Tillgänglig via PricewaterhouseCoopers i Sverige AB).

Ramos, M. (2004). *How to comply with Sarbanes-Oxley Section 404: Assessing the Effectiveness of Internal Control*. New Jersey: John Wiley & Sons.

Sarbanes-Oxley Act of 2002. (2002). Hämtad från http://www.sec.gov/about/laws.shtml

SAP. (2011). *Overview – About our company*. Hämtad 2012-03-01, från http://www.sap.com/corporate-en/our-company/index.epx

SAP. (2012) *SAP Businessobjects Governance, Risk and Compliance Solutions*. Hämtad 2012-03-06, från http://www.sap.com/solutions/sapbusinessobjects/large/governance-risk-compliance/index.epx

Sennholz, H. F. (1988). The Great Depression. *Freeman, 38(3),* 90-96

SIS (Swedish Standards Institute). (2012). *Effektiv företagsstyrning med ledningssystem – Verktyg för att uppfylla kraven från SOX och andra nya regelverk*. Hämtad 2012-04-04, från http://www.sis.se/pdf/sox.pdf

Svernlöv, C., & Blomberg, E. B. (2003). Sarbanes-Oxley – största värdepapperslagstiftningen på 70 år. *Ny Juridik, (1:03)*, 7-18.

Tacket, J. A., Wolf, F., & Claypool, G. A. (2006) Internal control under Sarbanes-Oxley: a critical examination. *Managerial Auditing Journal, Vol. 21, No. 3*, 317-323

Tarantino, A (2008) *Governance, Risk, and Compliance Handbook, New Jersey* John Wiley & Sons.

Trots, J. 2005. *Kvalitativa Intervjuer*. Lund, Studentlitteratur.

Yin, R. K. (2007). *Fallstudier: design och genomförande*. (B. Nilsson, övers.). Malmö: Liber. (Originalarbetet publicerat 1984)

Bilagor

Interview Questions

Of personal matter:

What is your position/title?

What are you main work tasks?

How do you work with or how does your work get affected by GRC?

Do you feel that GRC is used enough, or do you see possibilities for expanding the use of GRC? What possibilities in that case?

Your personal definition of GRC?

Have you been involved in the process of implementing GRC v10 or the older version?

Questions concerning the implementation process (if you have not been involved, ignore these questions)

What role have you had in the implementation of GRC?

Can you describe the different phases of the implementation process?

What goals were set for the project?

How did the project team look like?

On what criteria was the team put together?

How will the start of operations look like? (go live)

The main argument for switching from V5.2 to V10?

Have changes in the project plan occurred over time, or has the implementation followed the original time frame?

In what way has the organization been prepared for starting up/ switching to GRC version 10?

Which parts of GRC are you implementing? (AC PC RM?)

General problems encountered concerning the implementation process?

Specific problems encountered concerning the system (software)?

What type of problems?

How and when did these problems occur?

Were any unforeseen?

Are you satisfied with the implementation process and latest version of the software?

Would you do it in any other way if you could do it all over?

Do you think GRC are used in the best way for ABB or do you think there are areas of improvements, maximizing the use of GRC? What kind of improvements in that case?

When do you consider the project finished?

Life expectancy of GRC version 10?

The cost picture of GRC?