Södertörns Högskola
Institutionen för företagsekonomi och företagande
Företagsekonomi, Magisteruppsats 10 poäng
Vårterminen 2007
Handledare: Eron Oxing

Riskhanteringens utmaning

- En studie som identifierar svenska organisationers riskhantering avseende informationssäkerhet samt dess prioritering.

Författare:
Clara Siwertz & Amir Tehrani

Tack till

Vi vill börja med att tacka vår handledare Eron Oxing för den värdefulla handledningen under resans gång. Sedan vill vi även rikta ett stort tack till de organisationer och respondenter som tagit sin tid till att besvara våra frågor. Ett speciellt tack till Ulf Rönndahl på IF, Lars Rosenquist på Länsförsäkringar samt ”Rolf” och ”Ralf”, ni vet vilka ni är. Slutligen vill vi tacka alla opponenter som gett oss en upplyftande vägledning samt Stefan och Peiman för de oförglömliga luncherna.

Flemingsberg, 2007-05-30

_____ _____

Clara Siwertz Amir Tehrani

Abstract

Authors: Clara Siwertz & Amir Tehrani

Tutor: Eron Oxing

Title: The challenge of Risk Management – A study on Risk Management regarding information security in Swedish organizations and their priorities.

Background: Risk Management plays an important part of the enterprises strategic business activity. Efficient Risk Management will secure the businesses survival, assets and creates market advantages. The interest of information security has consequently gained in Swedish corporations. Corporations have realized the importance of the information which is stored in the IT systems. IT is the tool for businesses future progress and growth and therefore a source of risks. For managing these risks standards and frameworks are needed. *To what extent are information security standards and frameworks used in Swedish organizations? Are information security integrated with operational Risk Management?*

Purpose: The purpose of this study is to identify the Risk Management regarding information security in the studied organizations and to recognize the priority of information security.

Method: The main part of this study is based on case studies including four organizations, with the purpose to identify the Risk Management regarding information security in these organizations. The study is also added with a complementary survey carried out on Large Cap corporations on the Nordic exchange. The later survey will create a more general apprehension.

Conclusions: Findings shows that the Swedish organizations have realized the importance of standards and frameworks and the accompanying benefits. The main elements for using standards and frameworks are - better control, identification of business opportunities and gained security. The findings also suggested that the organizations should invest more resources in integrating information security with Risk Management and on the executive management involvement.

Keywords: Risk Management, Information Security, Operational risks, Standards, Frameworks & Regulations.

Sammandrag

Författare: Clara Siwertz & Amir Tehrani

Handledare: Eron Oxing

Titel: Riskhanteringens utmaning – En studie som identifierar svenska organisationers riskhantering avseende informationssäkerhet samt dess prioritering

Bakgrund: Riskhantering har idag blivit en viktig del av företagens strategiska verksamhet och ska hjälpa företaget att säkra dess överlevnad, tillgångar inklusive personal samt att maximera marknadsfördelar. Intresset för säkerhetsfrågor har därmed ökat i svenska företag och fler bolag har insett att informationen som finns lagrade i systemen är en av de största tillgångarna för verksamheten. Informationsteknologi (IT) är ett avgörande verktyg för verksamhetens framtida utveckling. IT kan därför ses som källan till verksamhetens risker. För att hantera dessa risker menar forskare att standarder och ramverk för informationssäkerhet är nödvändiga. I likhet med den finansiella redovisningens problem, där standarder behövs för ett harmoniserat finansiellt klimat, behövs även standarder och ramverk för hanteringen av information och IT. *I vilken utsträckning används ramverk och standarder för informationssäkerhet hos företag i Sverige? Integreras informationssäkerheten med operationell riskhantering i verksamheten?*

Syfte: Syftet är att identifiera de undersökta organisationernas riskhantering avseende informationssäkerhet samt hur den prioriteras i förhållande till organisationernas övriga riskhantering.

Metod: Den huvudsakliga delen av studien innefattar fallstudier av fyra organisationer med syftet att identifiera riskhanteringen avseende informationssäkerhet hos de olika företagen. Studien kompletterades med en enkätundersökning av Large-capbolagen på Stockholmsbörsen för att få en mer allmän uppfattning om problemområdet.

Slutsats: Svenska organisationer har insett vikten av standarder och ramverk samt vilka fördelar de kan ge. Bättre kontroll, möjlighet till att identifiera nya affärsmöjligheter och ökad säkerhet är faktorer som ligger till grund för användandet av ramverk och standarder. Svenska organisationer bör överlag satsa mer resurser på integrering av informationssäkerheten i den operationella riskhanteringen samt att involvera ledningen i arbetet för att uppnå en säkrare och effektivare informationshantering.

Nyckelord: Riskhantering, informationssäkerhet, operationella risker, standarder, ramverk, regelverk.

Innehåll

Figurer & Tabeller

1 Inledning

Under detta kapitel presenteras bakgrunden till studien och som leder läsaren fram till problemdiskussionen. Diskussionen ligger sedan till grund för studiens problemformulering och syfte. Kapitlet avslutas med en definitionslista samt uppsatsens disposition.

1.1 Problembakgrund

Vi lever idag i ett allt mer komplext samhälle där företag utsätts för snabba och oförutsedda förändringar. Enron och Worldcom är endast ett fåtal av de ekonomiska skandaler som uppmärksammats den senaste tiden där bristande redovisning, förskönande av bolagens resultat samt andra oegentligheter bidragit till minskat förtroende för företagsledningar (Luthy & Forcht 2006, ss.155, 157). I USA bidrog skandalerna till Sarbanes-Oxley Act (SOX) som bland annat reglerar företagets bolagsstyrning och kräver bättre kontroll av ledningen. Den svenska motsvarigheten är ”Svensk kod för bolagsstyrning”, men som till skillnad från SOX inte är ett regelverk. Bolag som är noterade på A-listan samt O-listan med ett marknadsvärde överstigande 3 miljarder omfattas av ”koden” men kan avvika från den om de motiverar för de avsteg som de gör (Svensk kod för bolagsstyrning, ss. 10). Koden har i likhet med SOX syftet att förbättra transparensen genom bättre styrning samt att öka förtroendet för företagsledningen.

I Sverige var det senast uppmärksammade fallet Skandia där ledningens bristande transparens bidrog till kursfall samt ett minskat förtroende för ledningen. Nya riktlinjer, regelverk samt standarder för hur bolagens ledning ska agera samt styra bolagen har efter dessa skandaler bidragit till att organisationers bild av riskhantering förändrats. Riskhantering har idag blivit en viktig del av företagens strategiska verksamhet och ska hjälpa företaget att säkra dess överlevnad, tillgångar inklusive personal samt att maximera marknadsfördelar (Kubitscheck 2000, ss. 38). I och med riskhanteringens utbredelse har även intresset för säkerhetsfrågor i svenska företag ökat drastiskt enligt den årliga undersökningen Global Information Security Survey som genomförs av Ernst & Young. (Computer Sweden, 2004) Fler och fler bolag har insett att informationen som finns lagrade i systemen är en av de största tillgångarna för verksamheten. Informationsteknologi

(IT) är därför ett avgörande verktyg för verksamhetens framtida utveckling. Akademiker och professorer argumenterar för IT som morgondagens konkurrensfördelar. (Barua, 1995, ss. 4)

IT ses idag som källan till verksamhetens risker (Berinato 2004). Han menar vidare att företagen är exponerade för risker när verksamheten står och faller med dess system och att ett dåligt ”IT-beslut” kan fallera ett helt företag. Makro-faktorer som exempelvis terrorism och naturkatastrofer har bidragit till att bolagen idag är mer uppmärksammade för risker än tidigare. I sin artikel om varför riskhantering är viktig tas även mikrofaktorer fram där virus och stöld av affärshemlig information bidragit till riskhanteringens framfart. För att hantera dessa risker menar forskare att standarder och ramverk för informationssäkerhet är nödvändiga. Det räcker ofta inte med enskilda tekniska säkerhetslösningar utan det behövs även olika administrativa rutiner. (Statskontoret, 1997, ss. 3). Ramverket COSO´s Enterprise Risk Management (ERM) ska hjälpa företagen med just de administrativa rutinerna. Ramverket ska bidra till att organisationen får en bättre riskbild som i sin tur ska leda till en effektivare riskhantering och verksamhetsstyrning (COSO, ss. v). Standarder som ISO 17799 och COBIT är andra verktyg som organisationer kan tillämpa för att säkerställa riskhanteringen med fokus på informationssäkerhet.

> *”Are you on board with enterprise Risk Management? You had better be. It's the future of how businesses will be run.”* (Berinato, 2004)

1.2 Problemdiskussion

Företagen kan bland annat inte längre få konkurrensfördelar endast genom den finansiella riskhanteringen. Det är främst genom modern operationell riskhantering som företagen kan säkra organisationen. I och med informationsteknologins framfart ökar även medvetenheten vad gäller IT-säkerhet. Det är inte längre bara frågan om teknik där IT-avdelningen har hand om säkerhetsfrågorna med tekniska lösningar utan dessa frågor måste mer eller mindre även flyttas upp till ledningsnivån. Det är de organisatoriska perspektiven som måste lyftas fram. Riksbankens säkerhetschef Jan-Olof Andersson menar trots att IT-frågorna blir allt viktigare sitter ofta inte den ansvarige på IT-avdelningen med i ledningsgruppen (Computer Sweden 2001).

Informationssäkerheten bör vara en integrerad del av företagens övriga riskhantering. Det finns idag heller inte en gemensam bas för informationssäkerheten. Standarder, ramverk och andra rekommendationer skulle kunna vara den gemensamma basen för företagen. Forskare menar också att det idag finns för få IT- och informationssäkerhetsstrategier på företagen. Detta kan ha sitt ursprung i att området ännu inte har forskats mycket kring. Det som dagligen går att utläsa i finansiella och tekniska tidskrifter är att säkerheten inte längre handlar om virus och trojaner, utan om lagar och regler. I likhet med den finansiella redovisningens problem, där standarder behövs för ett harmoniserat finansiellt klimat, behövs även standarder och ramverk för hanteringen av information och IT.

1.3 Problemformulering

- I vilken utsträckning används ramverk och standarder för informationssäkerhet hos organisationer i Sverige?
- Integreras informationssäkerheten med operationell riskhantering i verksamheten?

1.4 Syfte

Syftet är att identifiera de undersökta organisationernas riskhantering avseende informationssäkerhet samt hur den prioriteras i förhållande till organisationernas övriga riskhantering.

1.5 Definitioner

Basel II	Regelverk för finansiella institutioner. Huvudsyftet med Basel II är att åstadkomma en bättre genomlysning och hantering av risker i företagen, och därmed en ökad stabilitet i det finansiella systemet.
Benchmark	Utvärdering av sin verksamhet i förhållande till de som man uppfattar beter sig bäst inom en viss bransch.
Electronic Data Interchange	Ett standardiserat protokoll som innebär att olika organisationers affärssystem kan utbyta information per automatik utan mänsklig inblandning. Bygger på en teknik där filerna har standardiserad struktur och följer bland annat samma syntaktiska uppbyggnad
Electronic Funds Transfer at Point of Sale	Elektroniskt betalningssystem där betalkort används som betalning.
Informationssäkerhet	Förutom tekniska hjälpmedel för att säkerställa informationshanteringen så att obehöriga ej får tillträde, innebär informationssäkerhet administrativa och organisatoriska skyddsåtgärder, dessa åtgärder kan vara definiering av regler och policy för organisationen, behörighetskontroll, utbildning och analys.
Operationella risker	Kan definieras olika beroende på bransch. Den allmänna definitionen är; risken för förlust som har ursprung i inadekvata eller misslyckade processer, personer, system och externa händelser. Detta inkluderar legala risker.
Patchar	Ett uppdateringstillägg till en dataapplikation. Uppdateringen motverkar bland annat säkerhetshål, buggar och ibland endast ett uppdaterat grafiskts gränssnitt.
Risk	Sannolikheten för att något oönskat ska inträffa med positiv eller en negativ inverkan eller bådadera.
Riskhantering	En process som genomförs av en organisations styrelse, ledning och annan personal, och som genomförs i ett strategiskt sammanhang över hela företaget. Hanteringen är utformad för att identifiera potentiella händelser som kan påverka organisationen och hantera risker inom ramen för dess riskaptit samt ge rimlig försäkran om att organisationens mål uppnås.

Sarbanes-Oxley Act (SOX)	Regelverk för bolag som är noterade på den amerikanska börsen (NYSE & NASDAQ). Huvudsyftet är att återställa investerarnas och den aktieköpande allmänhetens förtroende för noterade bolag efter inträffade företagsskandaler. SOX fokuseras kring bolagens intern kontroll och förbättra rapporteringen av finansiell information.
Solvency II	Försäkringsbolagens motsvarighet till Basel II. Är en EU-initierad lag om soliditet för försäkringsbolag. Lagen har till syfte att öka kraven på riskhanteringsprocessen.
Svensk kod för bolagsstyrning	Innehåller en samling regler för bolagsstyrning i stora svenska företag. Koden infördes på Stockholmsbörsen under 2005 och gäller initialt börsnoterade bolag på A- och O-listorna som har ett marknadsvärde på över tre miljarder kronor. Den bygger vidare på den svenska aktiebolagslagen. ”Koden” har till syfte att förbättra bolagsstyrningen i svenska börsnoterade bolag. Koden kompletterar bl.a. aktiebolagslagen genom att ange en norm för vad som i allmänhet kan anses vara god bolagsstyrning.

1.6 Disposition

Kapitel	Titel	Innehåll
1	Inledning	*I detta kapitel presenteras bakgrunden till det valda problemet, dess frågeställning, samt vilket syfte studien har.*
2	Teori	*Detta kapitel behandlar de teorier och den tidigare forskningen som ligger till grund för forskningens teoretiska referensram.*
3	Metod	*Detta kapitel behandlar metoden och tillvägagångssättet för forskningen.*
4	Empiri	*Detta kapitel presenterar relevant bakgrundinformation som för läsaren underlättar förståelsen kring problemområdet samt resultatet från den genomförda undersökningen.*
5	Analys	*Detta kapitel syftar till att koppla empirin med den teoretiska referensramen för att skapa en grund för vidare slutsats och diskussion.*
6	Resultat	*I detta kapitel presenteras en kort sammanfattning av analysen och som sedan kopplas till uppsatsens syfte.*
7	Slutsats	*Detta kapitel presenterar de slutsatser som har dragits utifrån uppsatsens problemformulering.*
8	Diskussion	*Detta kapitel syftar till att ge läsaren vidare reflektioner över den genomförda studien. Detta görs i form av en forskningsanknytning. Därtill kommer en mer kritisk granskning av forskningens uppslag samt förslag på vidare forsknings kring ämnet.*

2 Teori

Under detta kapitel presenteras den tidigare forskningen kring Risk Management och Informationssäkerhet. Dessa forskningar kommer sedan att ligga till grund för uppsatsens teoretiska referensram som presenteras under kapitel 2.3.

2.1 Risk Management

2.1.1 Behovet av standarder och ramverk

Det var under 1950-talet som begreppet Risk Management första gången introducerades. Sedan dess har länder som England, Nya Zeeland och Australien skapat egna Risk Managementorgan. Simister påpekar att det fortfarande är oklart vad Risk Management innebär och att om man ber sex personer att definiera begreppet är chansen stor att du får sex olika svar. Risk Management eller riskhantering innebär enligt Simister att identifiera, planera och handla gentemot risker. Ett annat problem är att ordet risk uppfattas olika. För vissa kan begreppet innebära allt från eld till utrymningsplanering. Detta har varit orsaken till varför standarder för riskhantering har varit nödvändiga. Standarders främsta syfte är att just skapa en enhetlig bild över vad riskhantering och risk innebär. Även om standarden i sig inte kan identifiera risken presenterar den en strukturerad och systematisk metod för hur organisationen kan gå tillväga för att analysera riskerna och tillämpa samma metod och tillvägagångssätt konsekvent. Simister sammanfattar sin artikel med att påpeka bolagsstyrningens vikt. Han menar att om styrningen och riskhanteringen tas på allvar kan arbetet tillföra värde till företaget. Motsatsen är att onödiga resurser läggs på ett arbete som i slutändan endast leder till en ”certifiering” där arbetet likt en checklista kryssas av i slutet på året. Hur arbetet mottages och effektiviseras är beroende på revisorers och controllers attityd gentemot riskhanteringen. En standard skapar en bas för revisionen och där riskhanteringen får samma betydelse oavsett organisation och avdelning. (Simister, 2000, ss.9-10)

2.1.2 Riskhanteringens utmaning

Enligt Galloway och Funston finns det två drivande faktorer bakom risker i företag, att sänka riskhanteringskostnaderna exempelvis försäkringar samt att skapa marknadsfördelar för företaget.

Denna artikel har koncentrerats kring den sistnämnda faktorn. Marknadsvärdet är den kritiska punkten – det finns idag på marknaden så kallade ”high trust” företag som Galloway uttrycker det, det vill säga att ledningen har ett stort förtroende från marknaden, så mycket att marknaden i många fall har överseende för vissa misslyckanden. Om nu marknaden ser företaget som riskabelt, där bristande ledning och överraskningar leder till högre kapitalkostnad och lägre marknadsvärde minskar denna tolerans. Vidare måste företagsstrategier tillföra värde till företaget inom ett eller två år vilket annars leder till att ledningen får lämna företaget. Detta tankesätt bortser inte från långsiktlighet, utan betyder endast att disponeringen av strategier och att hantera riskerna gentemot strategierna är kritiska. Det bästa sättet att genomföra strategierna och få alla ombord är att identifiera företagets mest kritiska risker, adressera dem, få understöd samt att hantera dem effektivt. Vidare menar Galloway och Funston att risker kan uppstå var som helst i verksamheten, från IT-systemet till individuella personer. (Galloway & Funston 2000, ss.22)

Källan till riskhanteringslösningar har sitt ursprung i många olika verksamheter och branscher, bland annat i den kvalitativa internrevisionen och internkontrollen, den aktuariella branschen som försäkringsbolag och den kvantitativa branschen där finans- och kreditmarknaden återfinns. Varje enskild lösning har sitt eget riskhanteringsspråk. Alla dessa ”språk” måste översättas till ett gemensamt språk, det vill säga språket för värdeskapande. Värdebyggande företag använder riskhantering för att skapa värde. Dessa företag hanterar enkla processer effektivt, till låg risk och kostnad. Detta resulterar i att de kan ta högre risker och på så sätt skapa marknadsfördelar. (Galloway & Funston 2000, ss.22-23)

Ett sådant effektivt företag som Galloway & Funston beskriver som ”riskkapabla organisationer” har fyra karaktäristiker; Focused And Simply Transparent (FAST). Riskkapabla organisationer fokuserar (F) på de viktigaste och mest kritiska riskerna istället för alla risker som kan förekomma. And (A) reflekterar tre viktiga beståndsdelar; att hitta de nyckelområden som är mest kritiska inom varje avdelning, tillgodose företagets kompetens och integritet, slutligen att vara en elastisk organisation för att snabbt kunna återhämta sig efter ett misslyckande. Simple (S) återkopplar till att försöka genomföra strategin så enkelt som möjligt. Enkelhet är oftast svårare

att uppnå än komplexitet. Med detta menar man att enkelhet lättast kan uppnås genom att lokalt belysa på problemet. Transparent (T) uppnås genom att organisationen klargör riskhanteringen för varje medarbetare och på så sätt involverar alla. (Galloway & Funston 2000, ss.23)

Genom att följa 5 enkla steg kan organisationen använda ovanstående i praktiken. Steg 1 är Start; många organisationer börjar idag inte vid start utan i mitten. Vid start gäller det för ledningen att identifiera risk och risksystemet. Frågor som man kan ställa sig är vad detta kommer att tillföra organisationen? Kommer detta arbetet att sänka våra riskkostnader? Vilka är de kritiska framgångsfaktorer? Steg 2 är design, här gäller det att utveckla styrningen på företaget och hitta lämpliga strukturer och ansvariga för varje del inom organisationen. Det är under detta steg som eventuella ramverk och standarder, ansvariga personer och riskspråk utses. Steg 3: det är vid detta steg som uppskattning och identifiering av risker tar plats varefter man börjar tillämpa riskhanteringen. Vid steg 4 skapar organisationen så kallade ”Score cards”. Score cards summerar arbetet och ger en övergriplig bild på arbetet. Avslutningsvis, Steg 5, gäller det att följa upp och övervaka arbetet för att uppnå effektiv och värdeskapande riskhantering. (Galloway & Funston 2000, ss.24-25)

2.1.3 Operationella risker inom försäkringsbranschen

Definitionen av operationella risker varierar beroende på vilken bransch som får frågan. Ibland delas definitionerna in i olika grupper av operationella risker och i andra fall inkluderar det allt som inte är möjligt att klassas in under andra riskområden. I Basel, som är ett regelverk för riskhantering inom bankväsendet, definieras operationella risker enligt följande: (Manning & Gurney, 2005, ss. 294)

> ” *the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.*” (Manning & Gurney, 2005, ss. 294)

Mannings och Gurneys uppfattning är att operationella risker bör inkludera både direkta och indirekta förluster. Risker som därav bör räknas som operationella risker är internt/externt bedrägeri, arbetsmiljösäkerhet, klient-, produkt- samt affärstillämpningar, skador på fysiska tillgångar, affärsavbrott samt systemfel och utförande-, leverans samt processhantering. Operationella risker är svåra att mäta och det har därför varit svårt att rättfärdiga kostnader för

operationell riskhantering. En anledning är att det kan upplevas som svårt att urskilja operativa förluster från förluster relaterade till andra riskområden, därför bör gränsen för en operationell risk dras med hjälp av orsak och verkan. Om förlusten sker i det finansiella området men själva orsaken till förlusten är en felaktig process i affärssystemet är förlusten och risken därav operationell. Manning och Gurney utrycker det enligt följande: (2005, ss. 293-295)

> *"…even if you can´t measure it (at least accurately) you can se it; you know that it is there; and therefore it can be managed."* (Manning & Gurney, 2005, ss. 293-295)

Sett ur ett marknadsmässigt perspektiv rättfärdigas kostnaderna genom att operationella risker har inverkan på faktorer som marknadsvärde, intäkter och företagets rykte eftersom omvärldens uppfattning av företaget påverkas av hur väl de operationella riskerna hanteras. Framförallt i bank- och försäkringsvärlden är det nu en del i verksamheten att tilldela operationella risker egna resurser och uppmärksamhet. Regelverk som exempelvis SOX och Basel II har riktat särskild uppmärksamhet mot operationell riskhantering. (Manning & Gurney, 2005, ss. 295-296)

Åtgärder för operationella risker har sin grund i det tidigare nämnda begreppet orsak och verkan. Exempelvis kontroller som hindrar återupprepning, identifiering av nyckelindikatorer för särskilda risker och skapa förståelse för ursprungskällor och -kostnader till operationella risker. Operationella risker kan därför ses mer som riskhantering än som mätning av risker. (Manning & Gurney, 2005, ss. 296, 300)

2.1.4 Integrering av informationssäkerhet i riskhanteringen

Syftet med denna artikel är enligt författarna att utveckla ett ramverk för integrerad riskhantering för IT. Enligt andra studier består 1/3 av bolagens kostnader av IT-kostnader, vilket gör IT-riskhantering en av de viktigaste aspekterna för bolagens informationssystem. Målet med IT-riskhantering är att skydda IT-tillgångar, data, hårdvara, mjukvara, personal och fastigheter från externa och interna hot. (Bandyopadhyay, Mykytyn P., Mykytyn K. 1999, ss. 437)

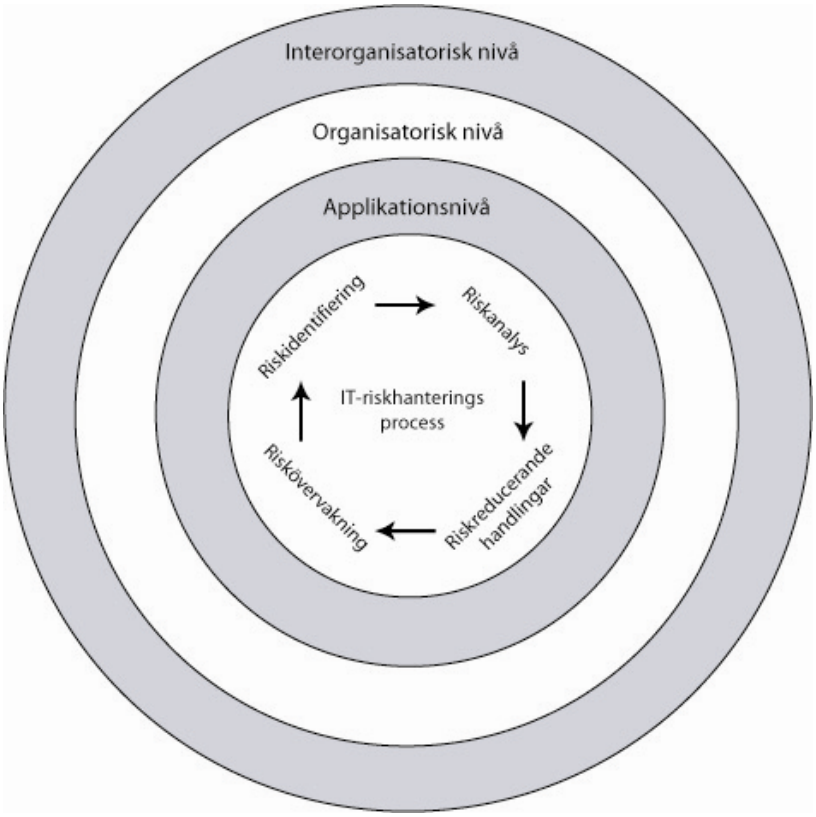
Bandyopadhyay et al. har identifierat fyra viktiga komponenter när det gäller den traditionella riskhanteringen; riskidentifiering, riskanalys, riskreducerande handlingar och riskövervakning.

Författarna menar att de ramverk som är tillgängliga inte är omfattande nog och att de olika komponenterna isoleras från varandra. På detta sätt kan ledningen inte förflytta sig mellan komponenterna och förstå dess inverkan på organisationen. Det ramverk som författarna vill lyfta fram bygger på samma komponenter, men där förflyttningen mellan komponenterna sker sekventiellt, där komponenterna kopplas till varandra och skapar ett effektivare riskhanteringssystem. (Bandyopadhyay, Mykytyn P., Mykytyn K. 1999, ss. 437)

Enligt föreslagen riskhantering sker riskidentifieringen på en applikationsnivå, organisatorisk nivå och en interorganisatorisk nivå. På applikationsnivån ska riskidentifieringen koncentreras kring tekniska risker och implementering av IT-applikationer. Dessa risker har sitt ursprung i naturkatastrofer, konkurrenshandlingar, hackers och virus. En aspekt på de tekniska riskerna som oftast glöms bort är de interna hoten som kommer ifrån berättigat och icke berättigat missbruk av IT-system. På den organisatoriska nivån ska fokus ligga på organisationens funktionella områden och informationsteknologins inverkan på dessa områden. Det gäller att få IT:n att gå ihop med organisationens övriga mål och att IT i detta läge ska fungera som ett verktyg för att uppnå dessa mål. Risker som organisationen kan utsättas för i detta fall är strategiska och hållbarhetsrisker vilket påverkar kontinuiteten. På den interorganisatoriska nivån ska fokus ligga på IT-risker som ligger utanför organisationen. Dessa risker uppstår ofta då IT-system är kopplade i ett nätverk mellan två eller flera organisationer. Interorganisatoriska system kan samtidigt som de ger oerhörda konkurrensfördelar, bidra till lika stora risker. De tre största riskerna är naturkatastrofer, intrång av hackers, svag och ineffektiv kontroll. (Bandyopadhyay, Mykytyn P., Mykytyn K. 1999, ss. 438-439)

Efter att ha identifierat riskerna ska dessa risker analyseras. Författarna menar att dagens ramverk inte involverar hela organisationen. Lösningen är att ha olika ansatser; kvantitativa, kvalitativa och/eller en kombinerad ansats. Genom exempelvis intervjuer, enkäter och scenarioövningar kan organisationen analysera riskerna, fastställa sannolikheter och deras påverkan. Det tredje steget i riskhanteringsprocessen är att hitta handlingar för att reducera riskerna. Det gäller att gräva djupare och hitta riskernas ursprung och sedan implementera metoder för att reducera dessa risker. Det mest fundamentala under detta steg är att inte endast titta på datasäkerhetsrisker, utan

även på de strategiska och legala riskerna. Detta är något som andra ramverk inte värdesätter i samma grad som med föreslaget ramverk. Det sista steget är att införa övervakande komponenter för att öka säkerheten i IT-miljön. En aktiv övervakning av riskerna garanterar effektiva motåtgärder. Riskövervakningen bidrar inte endast till mätning av prestationen, utan den bidrar även till revisionsverktyg och en bättre kontinuitet. (Bandyopadhyay, Mykytyn P., Mykytyn K. 1999, ss 440.



Figur 2.1: Ramverk för integrerad IT-riskhantering
Figuren visar de sekventiella stegen i riskhanteringsprocessen. Figuren är hämtad från artikelt; *”A framework for integrated Risk Management in informations security”* ss. 438 (egen översättning)

2.1.5 Lagar och regelverk

Ett antal lagar och regelverk påverkar idag organisationers informationshantering. SOX och Basel II är två exempel på detta. Sarbanes-Oxley Act 2002 (SOX) blev resultatet av de skandaler som florerade i USA för ett antal år sedan. Bristande intern kontroll var orsaken till att många aktieägare och andra investerare förlorade oerhörda summor på bolagens svagheter. Bolag som är noterade i USA ska från och med 2002 följa dessa regelverk för en bättre styrning och en ökad intern kontroll. SOX belyser inte informationshanteringen nämnvärt, förutom vissa sektioner i lagen där tillsättning av interna och externa IT-revisorer och designen för intern kontrollen till viss del benämns. SOX rekommenderar därför ramverket COSO – integrated framework som är fullt kompatibelt med just SOX för informationshanteringen. (Luthy & Forcht 2006, ss.155, 157)

Ett regelverk som har en större fokus på informationshantering är Basel II. Regelverket riktar sig främst till finansiella institutioner. Luthy & Forcht menar att Basel II är bättre lämpad för hanteringen av informationsteknologi. Basel utvecklades ursprungligen för beräkning av finansiella risker. I och med IT:s allt viktigare roll och komplexitet i organisationer utvecklades Basel II. Basel II specificerar ett mät- och rapportsystem som inkorporerar ett antal olika risker. Riskerna delas in i komponentrisker, kreditrisker, marknadsrisker och operationella risker. Det är under de operationella riskerna som informationshanteringen har sin plats. Basel II tar upp risker som IT-säkerhet, bedrägeri och systemfel. De operationella riskerna är en av Basel II viktigaste beståndsdelar då regelverket tillåter ledningen att utveckla egna modeller för hur riskerna kan mätas och kontrolleras. (Luthy & Forcht 2006, ss.158)

Som nämndes tidigare är SOX och Basel II inte fullt utvecklade regelverk för informationshanteringen. Därför finns ett antal ramverk som organisationer kan tillämpa för att säkra informationen och sina system. COSO är ett sådant ramverk där en större fokus ligger på riskhanteringen och den interna kontrollen. COSO sätter upp kriterier för kontrollsystem i organisationen, tar upp hur organisationen ska fördela arbetet mellan rollerna samt rekommenderar ett antal evalueringsverktyg för effektivisering av den interna kontrollen. Luthy och Forcht menar att även COSO är generell vad gäller IT. Controll And Audit for Information

and Related Technology (COBIT) ramverket har en mer detaljerad vägledning för IT och informationshanteringen. Luthy & Forcht menar vidare att mer fokus måste läggas på IT-relaterade risker i komplexa IT-system och därför är COBIT ett bra verktyg för detta. COBIT tar upp tre dimensioner; 1) IT-processer 2) IT-resurser 3) informationskriterier. IT-processer inkluderar de aktiviteter som organisationen genomför med hjälp av IT. IT-resurser kan vara människor, applikationer, teknologier och data. Informationskriterier inkluderar attributen integritet, effektivitet, tillgänglighet, reliabilitet och konfidentiellitet. Var och en av dessa dimensioner arbetar efter fyra domäner som är: 1) planering och organisering 2) implementering 3) underhåll 4) uppföljning. Varje domän har i sin tur en uppsättning av kontrollpunkter, 34 totalt. På detta sätt kan komplexa system brytas ned till minsta möjliga nivå för att sedan studeras och säkerställas. Slutsatsen av denna artikel är att lagar och regelverk inte belyser informationshanteringen nämnvärt. I och med informationsteknologins alltmer komplexa struktur måste ledningen hitta alternativa vägar för att säkra organisationen mot oegentligeter. Olika ramverk och standarder finns därför att tillgå för detta ändamål. Ett par av de mest utvecklade ramverken presenterades ovan. (Luthy & Forcht 2006, ss.161-165)

2.2 IT & Informationssäkerhet

2.2.1 En studie i informationssäkerhetshantering

I undersökningen som Mitchell et al. genomförde på 40 industriföretag 1998 i England hittade författarna att majoriteten av de undersökta företagen inte arbetade proaktivt med informationssäkerhet och att dessa inte var förberedda på oförutsedda händelser. Orsaken till detta var att de inte var medvetna om de hot som informationssystemen kunde utsättas för. Vidare kunde man konstatera att ledningen förlitade sig på IT-avdelningen och den tekniska organisationen. En annan orsak som kunde utläsas från resultatet var att företagen såg information som en immateriell tillgång och att det var svårt att värdera dessa tillgångar. Den viktigaste orsaken till varför företagen inte belyste informationssäkerhet som en viktig del i organisationen var för att de tidigare inte blivit utsatta för säkerhetshot och andra informationssäkerhetsproblem. Det som författarna såg som alarmerande var att endast två av de undersökta företagen hade ansvariga informationssäkerhetschefer som aktivt arbetade med informationssäkerhet. Vidare antog författarna att bristen på informationssäkerhet kunde bero på

att det ansågs som ett tekniskt problem. Säkerhetspolicys, utbildning av personal vad gäller säkerhet och kommunikation som oftast lyfts fram i ramverk och standarder var allt för utspritt i organisationerna och som betraktas som de mjukare värdena. Detta resulterade därför luckor i informationssäkerheten. (Mitchel, Marcella & Baxter 1999, ss. 213, 225-226)

2.2.2 Betydelsen av standarder

Det blir allt mer vanligt att företag och andra organisationer sammanlänkar sina IT-system med varandra via exempelvis Internet, EDI (Electronic Data Interchange) eller EFTPoS (Electronic Funds Transfer at Point of Sale). Kraven på informationssäkerhet blir därför allt större. Lika viktigt som det är för företagen att själva inneha ett säkert IT-system är det likväl betydelsefullt att de affärspartners vars IT-system de är sammankopplade med har en likvärdig säkerhetsnivå. En leverantör som inte har ett säkerhetsklassat IT-system kan därför gå miste om detaljister/kunder som kräver säkra elektroniska förbindelser med sina leverantörer, och därmed förlora viktiga inkomster. (von Solms, 1999, ss. 50)

Det är lättare att kontrollera den egna IT-säkerheten än vad det är att försäkra sig om hur affärspartners sköter sin IT-säkerhet. Regler och gemensamma föreskrifter är därför viktiga när organisationers IT-system interagerar med varandra. USA tog år 1983 fram standarden TCSEC för hur enskilda produkter till exempel separata datorprogram ska utvärderas ur säkerhetssynpunkt för att sedan kunna tilldelas ett certifikat. Motsvarande standard, ITSEC, togs fram år 1990 av europeiska kommissionen, men med skillnaden att den innefattar utvärdering för hela IT-system så väl som för enskilda produkter. För att en produkt eller ett IT-system ska få certifieras med TCSEC eller ITSEC utvärderas det genom att tre oberoende faktorer granskas: (von Solms, 1999, ss. 50-51)

1. Funktionalitet, det vill säga de säkerhetsegenskaper en produkt eller ett system innehar.
2. Försäkran av korrekthet, det vill säga noggrannheten i utvärderingen.
3. Försäkran av effektivitet, det vill säga tillämpas säkerhetsrutinerna på ett korrekt sätt.

TCSEC utvärderar alla tre faktorer tillsammans medan ITSEC utvärderar korrekthet och effektivitet separerat från funktionaliteten. Innan en utvärdering enligt ITSEC-standard påbörjas, analyserar organisationen som ber om utvärderingen, de hot det aktuella IT-systemet kan tänkas utsättas för samt identifierar de säkerhetsmekanismer som är tänkta att skydda IT-systemet från hoten. Utvärderingen sker sedan i tre steg där det första steget är en kontroll av att säkerhetsmekanismerna faktiskt finns i IT-systemet för att i ett andra steg besiktiga att de är korrekt installerade. Sista steget är till för att försäkra sig om att säkerhetsmekanismerna verkligen är lämpliga åtgärder för de identifierade hoten. (von Solms, 1999, ss. 51)

Enbart tekniska säkerhetsregleringar ger inte automatiskt en säker IT-miljö utan tekniken måste kompletteras med lämpliga operationella regleringar som instruerar användarna om hur IT-systemet och informationen ska hanteras. Enkelt förklarat kan det jämföras med ett hus som har installerats med den senaste larmtekniken. Huset har de bästa förutsättningarna för att ses som ett säkert hem, men om inte de boende aktiverar larmet samt låser dörrar och fönster är hemmet inte mer säkert än det var före installationen. TCSEC- och ITSEC-utvärderade produkter säkerställer alltså inte i sig själva informationssäkerheten i en verksamhet, men de är däremot bidragande faktorer. Tekniska säkerhetsåtgärder måste därför kompletteras med rätt sorts hantering av IT-systemet. För att affärspartners ska kunna försäkra sig om att respektive part har en korrekt hantering av information utöver eventuella certifierade IT-system är det viktigt att följa gemensamma standarder för detta. Exempel på en standard är den brittiska *Code of Practice for Information Security Management*, även kallad BS7799. Syftet med standarden är att ge företag en gemensam grund att bygga och implementera ett effektivt IT-säkerhetsarbete och skapa förtroende i företagens interna affärer mellan varandra. För att kunna införa en säker hantering av IT-systemet i en verksamhet krävs omfattande IT-säkerhetsplanering. ISO/IEC utvecklade år 1996 en standard för IT-säkerhetsplanering i form av en teknisk rapport kallad TR 13335/GMITS (*Guidelines for the Management of IT security*) som består av fem delar. De tre första delarna behandlar hur informationssäkerhet bör tillämpas i en organisation vilket kommer att beskrivas kortfattat nedan. (von Solms, 1999, ss. 52)

Del 1 av GMITS har målgruppen chefer med ansvar för generell säkerhetsplanering samt chefer med fokus på IT-säkerhet. Ledande befattningshavare ska sättas in i IT-säkerhetsfrågor och bli medvetna om vad som ingår i IT-säkerhet. Målet är att de ska kunna basera sina beslut, rörande IT-säkerhet, på kunskap. Del 2 beskriver IT-säkerhet avseende planering samt hantering och riktas mot chefer för implementering, testning, inköp eller drift av IT-system. Även chefer på avdelningar med betydande användning av IT-systemet berörs av del 2 i GMITS. Etablering av en omfattande IT-säkerhetsplan är nödvändig för ett effektivt säkerhetsarbete. Planen ska på ledningsnivå innehålla en företagspolicy avseende IT-säkerhet. Utöver policyns praktiska syften är den även ett medel för att visa ledningens engagemang i säkerhetsarbetet. Organisationen måste därefter välja strategi för riskanalys huruvida den ska fokusera på den övergripande praktiska nyttan eller gå ner på detaljnivå i varje IT-system. Oavsett vilken strategi som väljs ska förslag till rekommendationer, policy, och en plan ges för IT-säkerheten i verksamheten, detta för att göra en effektiv implementering av den valda strategin möjlig. När förslaget har blivit godkänt är det viktigt att förmedla en säkerhetsmedvetenhet och förståelse hos användarna vilket görs genom en medvetenhetsplan. Del 3 är till för att beskriva de olika tekniker som finns för att leda en detaljerad riskanalys. Målgruppen är därav de personer som är involverade i säkerhetsrelaterade aktiviteter eller riskmoment. Att på ett strukturerat vis införa informationssäkerhet med exempelvis GMITS är av stor vikt, men likväl bör en uppsättning av effektiva säkerhetskontroller identifieras, rekommenderas och implementeras. Den tidigare nämnda standarden BS7799 är ett exempel på en manual för att ta fram ett fundament för säkerhetskontroller. (von Solms, 1999, ss. 53-56)

Sammanfattningsvis är IT-systemets uppgift att utgöra en säker teknisk grund, men för att skapa en säker IT-miljö måste IT-systemet hanteras på ett säkert sätt samt ges ett certifikat för att uppvisa den faktiska säkerheten. Grundstenen för säkerhet är därför gemensamma standarder som TCSEC, ITSEC, GMITS och BS7799. (von Solms, 1999, ss. 57)

2.2.3 Informationssäkerhetskrav

Tyngdpunkten i säkerhetstänkande har flyttats från fysiska datortillgångar till informationstillgångar därav behövs ett annat angreppssätt för att säkra ett företags information. Elektronisk handel ställer högre krav på informationssäkerheten, men samtidigt handlar skyddet

av informationen i en organisation inte enbart om att säkerställa IT-säkerheten, vilket följande citat av Michael Wills, brittisk minister för departementet för småföretagande inom handel och industri, beskriver: (Gerber, von Solms, Overbeek, 2001, ss. 32)

> *"Information security is now generally recognized as having a critical part to play in ensuring that small to medium enterprises (SME´s) can take full advantage of electronic commerce. Quite clearly the information society of the future will just not work if the information we rely on - the lifeblood of a business – is not secured. Note that the word "IT (Information Technology) security" was not mentioned, since the issue is not just about protecting the technology, it is about protecting business or personal information wherever it resides"*. (Wills, 1999, ss.1)

Riskanalyser har länge använts för att identifiera och värdera tillgångar samt vilken sannolikhet och påverkan eventuella hot innehar. Därefter ges förslag på åtgärder för att minimera riskerna. Riskanalys är fortfarande ett bra sätt för att skydda fysiska tillgångar då det för dessa är lätt att mäta hot både kvalitativt och kvantitativt, men att skydda information fokuserar inte längre på infrastrukturen och därför krävs andra metoder. (Gerber, von Solms, Overbeek, 2001, ss. 33)

Informationssäkerhetens huvudmål är att skapa konfidentiellitet, integritet, tillgänglighet, ansvarsskyldighet och tillförlitlighet. För varje huvudmål är det viktigt att fastställa hur hög säkerhetsnivå som krävs. Uppsättningen av huvudmål med individuellt tilldelade säkerhetsnivåer utgör organisationens informationssäkerhetskrav. Säkerhetskraven i en organisation grundas på följande; uppskattade risker, lagliga krav samt de informationsprocesser som har utvecklat för att stödja verksamheten. I standarder avsedda för informationstillgångar, som GMITS (Guidelines for the Management of Information Technology Security) och BS7799 framhävs att identifieringen av en organisations säkerhetsbehov i form av säkerhetskrav har stor betydelse vid effektivt framtagande av lämpliga säkerhetsregleringar för organisationen. (Gerber, von Solms, Overbeek, 2001, ss. 32-33)

Gerber et al. (2001) beskriver en formaliserad metod som de kallar för ”Security Requirements Exercise”, målet med metoden är att fastställa en organisations informationssäkerhetskrav i syfte att identifiera de informationssäkerhetsregleringar som bäst möter organisationens behov. Metoden går ut på att utefter organisationens behov placera in de tidigare nämnda huvudmålen konfidentiellitet, integritet, tillgänglighet, ansvarsskyldighet och tillförlitlighet i följande nivåer av säkerhet låg, mellan eller hög. När varje huvudmål har blivit tilldelat en säkerhetsnivå har ett informationssäkerhetskrav skapats. (Gerber, von Solms, Overbeek, 2001, ss. 33) Efter att säkerhetskraven har fastställts är det möjligt att välja ut de regleringar och åtgärder som lever upp till den säkerhetsnivå som framgår av organisationens säkerhetskrav. Lämpligt är att använda regleringar och åtgärder från de olika standarder som finns för informationssäkerhet exempelvis BS 7799 och GMITS. (Gerber, von Solms, Overbeek, 2001, ss. 36)

2.2.4 Teori om informationssäkerhetshantering

Hong et al. har i sin artikel från 2003 lyft fram bristen av ett teoretiskt ramverk gällande informationssäkerhetsmanagement. Denna artikel har till syfte att integrera säkerhetspolicyteori, riskhanteringsteori, kontroll- och revisionsteori och kontingensteori till en gemensam teori författarna kallar för ”integrated system theory of information security management” (IST). Denna teori är enligt författarna en bra grund för att skapa bättre förståelse för informationssäkerhet och dess implementering. Hong et al. definierar informationssäkerhet som tillämpning av teknik samt företagsledande handlingar på informationsresurser, för att säkerställa organisatoriska informationstillgångar samt privat data. Enligt ISO 17799 är informationssäkerhetshantering: (Hong et al. 2003, ss. 244)

- Etablering av informationssäkerhetspolicy
- Organisation och ansvarsförbindelse för informationssäkerhet
- Säkerhetshantering och utbildning
- Systemsäkerhetshantering
- Nätverkssäkerhetshantering
- Systemutveckling
- Säkerhetshantering av informationstillgångar
- Fysisk och miljösäkerhetshantering
- Företagsplanering och ledning

Säkerhetspolicyteori

Enligt Hong et al. finns det idag ingen konsistent policyteori, utan det finns vedertagna modeller för hur säkerhetspolicys ska utformas. Målet med upprättandet av säkerhetspolicy är att ställa upp krav för säkerheten, forma samförstånd i organisationen samt att följa dessa krav för bättre säkerhet. (Hong et al. 2003, ss.244)

Riskhanteringsteori

Riskhanteringsteorin föreslår att organisationen genom riskanalyser och evaluering identifierar och hanterar hot och sårbarhetsaspekter inom informationssäkerhet. Evalueringen kan sedan användas för att skapa informationssäkerhetskrav samt kontroll av risker. Målet är att få informationssäkerhetsrisker under en acceptabel nivå. Hong et al. refererar till Wright 1999 som menar att riskhantering delvis är en process för att etablera samt underhålla informationssäkerheten i en organisation. (Hong et al. 2003, ss.244)

Kontroll- och revisionsteori

Kontroll och revisionsteorin föreslår att organisationen upprättar informationssäkerhetskontrollsystem för att genom revisionsmetoder kontrollera säkerheten. Enligt Hong et al. menar många forskare att informationssäkerhetshantering är en del av ett kontrollsystem. Ett kontrollsystem kan upprättas om organisationen följer exempelvis ISO 17799 och/eller ramverket COBIT. (Hong et al. 2003, ss.244-245)

Management systemteori

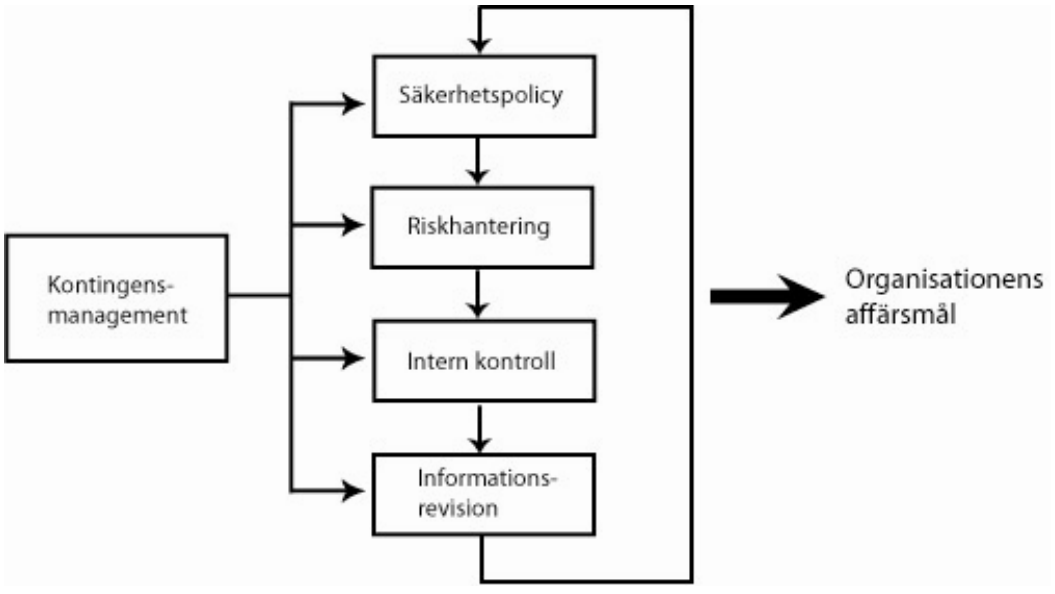
Management systemteorin förslår att organisationen upprättar ett så kallat dokumenterat informationssäkerhetsmanagementsystem (ISMS) för att kontrollera och skydda information. ISMS kan uppnås genom sex steg: (Hong et al. 2003, ss.245)

1. upprätta säkerhetspolicy
2. definiera målet med ISMS
3. åta sig riskhantering
4. hantera risker
5. välja kontrollpunkter
6. tillämpa en standard

Kontingensteori

Enligt kontingensteorin ska organisationen arbeta för att förutse, detektera och agera gentemot hot och sårbarheter som kan påverka organisationen från insidan och utsidan. Kontingensteorin har till syfte att skapa strategier för säkerhetspolicyn, riskhantering, kontroll och revision samt management system. För att möta företagsvärldens ständigt föränderliga natur, menar Hong att risk managers oftast blandar dessa teorier för att skapa en informationssäkerhetshantering. Enligt kontingenssynsättet gäller det att anpassa varje variabel till situationen, dvs. att tillämpa de teorier som bäst passar för stunden. (Hong et al. 2003, ss.245)

Då dessa teorier skiljer sig åt vad gäller tillämpningen på informationssäkerhet, gäller det enligt Hong et al. att anpassa arbetssättet efter situationen för att skapa en effektiv informationssäkerhetshantering och som ska leda till organisationens affärsmål. Detta kan genomföras då organisationer har kontingensteorin som grundstomme i informationssäkerhetsarbetet. De flesta av ovanstående teorier är så kallade ”top-down”-teorier, det vill säga att varje steg i teorin ska tillämpas uppifrån och ned, medan IST har till syfte att vara mer iterativ. (Hong et al. 2003, ss.246)



Figur 2.2: Integrerad systemteori
Bilden visar en illustration på Hongs teori om informationssäkerhetshantering. Bilden är hämtad ur artikeln ”An integrated system theory of information security management, ss.247 (egen översättning)

2.2.5 IT-styrning

Misslyckade IT-projekt, missade deadlines, övertrasserade budgetar och dåliga avkastningar på dessa projekt är ett fåtal av de faktorer som är bakgrunden till dålig IT-styrning menar Robinson. Målet med IT-styrning är att skapa en kontrollmiljö för effektiv och säker användning av informationsteknologi. Kontrollmiljön skapas utifrån attityder, attribut, medvetenhet och handling från ledningens sida. Robinson klargör att bolagsstyrning och IT-styrning är en integrerad del av organisationens riskhantering. Ett IT-styrningsramverk, som COBIT bör inte vara isolerad vare sig från bolagsstyrningen eller från riskhanteringsramverket. IT-styrning möjliggör för organisationen att uppnå tre vitala mål: (Robinson 2005, ss.45-46)

1. Uppfyllelse av regelverk, exempelvis SOX och Basel II.
2. Operationellt övertag genom att skapa IT-projekt som tillför organisationen värde. Robinson refererar till en studie som genomfördes av Peter Weill och Jeanne W. Ross där 250 internationella företag studerades utifrån deras IT-styrning. Studien visade att IT-styrning är i särklass den viktigaste faktorn huruvida IT tillförde värde till organisationen. Vidare fastställde de att organisationer som hade följt specifika strategier och styrning över genomsnittet, hade 20 % högre profit än de organisationer som följde samma strategier med dålig styrning.
3. Optimering av riskhanteringen. I ett allt mer konkurrensutsatt företagsklimat med komplexa IT-system behöver företag idag utveckla sin riskhantering med fokus på operationella risker. Ett IT-styrningsprogram definierar därför IT-strukturen och mäter detta där sedan övervakande ramverk behövs för att effektivt identifiera och hantera riskerna som uppstår.

De ramverk och standarder som Robinson anser som mest effektiva och utbredda är: **COBIT** (Control Objectives for Information and related Technology) är en öppen IT-styrningsstandard för kontroll över informationsteknologin. Standarden är fri från mjukvara och hårdvara. **ITIL** (Information Technology Infrastructure Library) definierar IT-kvalitet som nivån mellan IT-tjänster och organisationens IT-behov. COBIT definierar för vad som ska göras medan ITIL bistår med praktiska steg för hur det ska göras. **ISO 17799** The Code of Practice for Information Security Management är en uppsättning vedertagna riktlinjer och kontrollpunkter för

informationssäkerhet. Kontrollpunkterna kan antingen baseras på regelmässiga krav som lagar eller ”best practise” för implementering av informationssäkerhet. (Robinson 2005, ss.48)

Slutsatsen av denna artikel är att när styrningen är effektiv blir IT en värdefull tillgång som är oskiljbar från verksamheten och inte en kostnad. För att IT-styrningen ska bli effektiv ska organisationen anamma ett ramverk eller en standard för ändamålet. Detta för att skapa konsekventa regler och kontroller samt att uppmuntra individer och grupper till att ta mer ansvar. (Robinson 2005, ss.45)

2.3 Teoretisk referensram

I teorikapitlet presenterades den forskning kring Risk Management och informationssäkerhet som legat till grund för uppsatsens teoretiska referensram. Risk Management har på senare år fått allt mer uppmärksamhet i företagsvärlden och inte minst inom informationssäkerhet. Riskhanteringens syfte är enligt Galloway och Funston (2000) att skapa marknadsfördelar, dvs att den ”riskkapabla” organisationen arbetar på ett sådant sätt att mervärde adderas till organisationen. Enligt Simister (2000) gäller det att skapa en enhetlig bild över vad riskhanering innebär och på ett metodiskt och systematiskt sätt genomgå riskhanteringen och därför behövs standarder som exempelvis ISO och ITIL. Informationssäkerhet är dels grundat på hur informationen hanteras i informationssystem, men framförallt av hur människor hanterar informationen vilket ger en klar koppling till organisationens operationella risker. Försäkringsbranschen har på senare år gått i bräschen för hur de operationella riskerna kan hanteras och därtill informationssäkerheten. Mannings och Gurney (2005) menar att definitionen av operationella risker är viktigt och att informationssäkerheten indirekt ska hanteras inom den operationella riskhanteringen. Enligt Bandyopadhyay et al. (1999) ska riskhanteringen ske på flera nivåer i organisationen och där informationssäkerheten spelar in i alla nivåer. Riskhanteringen ska ske enligt den traditionella processen, men en mer sekventiell process som många av dagens ramverk för riskhantering saknar. Bandyopadhyay et al. påpekar vikten av involvering samt kopplingen mellan riskhanteringens olika komponenter.

Något som påverkar riskhanteringen och informationssäkerheten och dess hantering i organisationer är de lagar och regelverk som måste följas (Luthy & Forcht, 2006). Finansiella institutioner måste följa Basel II, medan försäkringsbolag ska tillämpa regelverket Solvency II. Bolag som är noterade i USA ska från och med år 2002 följa Sarbanes-Oxley Act (SOX) för en bättre styrning och en ökad intern kontroll. Dessa regelverk har olika synsätt på riskhanteringen och informationssäkerheten. Medan Basel II har en större fokus på IT lämnar SOX en större lucka vad gäller IT och rekommenderar därför ramverk som är mer lämpade för ändamålet. De ramverk som rekommenderas är bland annat COSO ERM och COBIT.

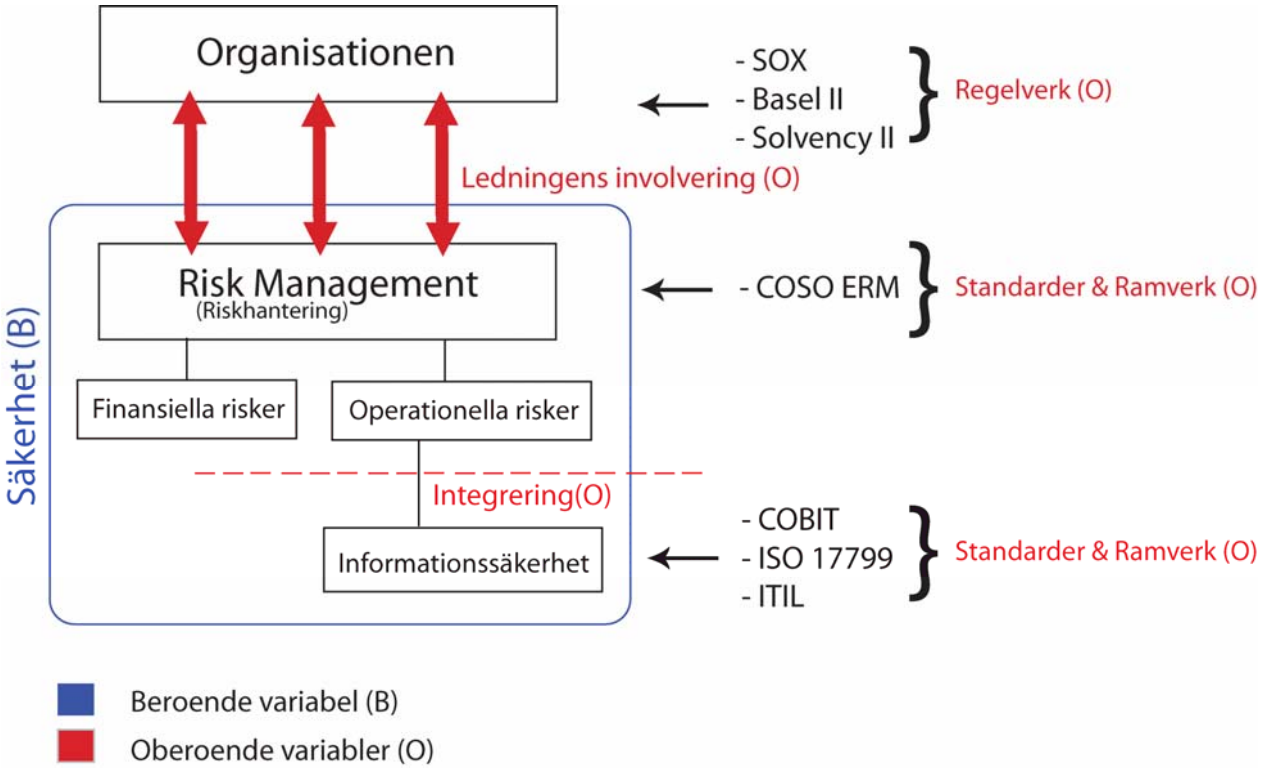
Enligt tidigare forskning (Mitchel et al. 1999) förlitar sig organisationen i alltför stor grad på IT-avdelningen och den tekniska organisationen. Ledningen har för lite kontroll över informationsteknologin. Enligt samma undersökning ansåg ledningen att IT endast var ett tekniskt problem och därav försumningen av informationssäkerheten. Varför är det då viktigt att följa standarder vad gäller informationssäkerhet? Enligt von Solms (1999) är det bland annat för att affärspartners ska kunna försäkra sig om att respektive part har en korrekt hantering av information. Syftet med en standard blir därför att skapa en gemensam grund och implementera ett effektivt IT-säkerhetsarbete och på så sätt skapa ett förtroende företag emellan och mellan kunder och företag. Informationssäkerhetens huvudmål är att skapa konfidentiellitet, integritet, tillgänglighet, ansvarsskyldighet och tillförlitlighet. Enligt Gerber och Manings (2001) kan dessa mål uppnås med just standarder. I teorikapitlet har även en alternativ teori behandlats, den integrerade systemteorin. Hong et al. (2003) menar att det idag finns en brist på teoretiskt ramverk gällande informationssäkerhet och att en blandning av relevanta teorier skulle skapa en effektivare hantering av informationssäkerhet.

Riskhantering och informationssäkerhet ska leda till en högre säkerhet för organisationen. Säkerhet betraktas därför som den beroende variabeln i denna undersökning. De oberoende variablerna som i sin tur påverkar säkerheten är:

- Standarder
- Ramverk

- Regelverk
- Integrering
- Ledningens involvering

Följande figur är framtagen i syfte att ge förståelse kring hur informationssäkerhet, riskhantering och olika standarder förhåller sig till organisationen samt presentera den beroende variabeln som påverkas av de oberoende variablerna. De oväntade och ej önskvärda incidenter som en organisation utsätts för är risker, riskhantering är därmed de metoder och strategier organisationen tillämpar för att handskas och förebygga dessa risker. Indelningen av risker sker vanligast i de två grupperna finansiella och operationella risker, i den senare kan IT och informationssäkerhet antingen vara en integrerad del i samtliga operationella riskundergrupper eller stå som en fristående egen grupp. De tidigare nämnda standarderna har olika perspektiv och används på olika nivåer i organisationens riskhantering.



Figur 2.3: Uppsatsens teoretiska modell.
Bilden visar uppsatsens teoretiska modell och är egenutvecklad

3 Metod

Under detta kapitel presenteras metoden samt uppsatsens angreppssätt, datainsamlingsmetod, urval, bortfall samt uppsatsens validitet och reliabilitet.

3.1 Angreppssätt

Den huvudsakliga delen av studien innefattar fallstudier av fyra organisationer med syftet att identifiera riskhanteringen avseende informationssäkerhet hos de olika företagen. Intervjuer genomfördes med nyckelpersoner på företagen för att ge en djupare inblick i hur riskhantering sker och hur stor roll informationssäkerheten har i hanteringen. Studien kompletterades med en enkätundersökning för att få en mer allmän uppfattning om problemområdet. Standardiserade enkäter skickades ut till Large-caplistade bolag på stockholmsbörsen för att ge en helhet över hur informationssäkerheten hanteras i dessa bolag. Undersökt data jämfördes sedan med tidigare utförda studier som har hittats i publicerade vetenskapliga artiklar, vilket ligger till grund för uppsatsens slutsatser.

3.2 Datainsamlingsmetod

Datainsamlingsmetoder delas vanligtvis in i två olika grupper, kvalitativ och kvantitativ. Det finns inte alltid en klar linje mellan de två tillvägagångssätten utan ofta använder sig samhällsforskare inslag från båda metoderna. Kriterier och förutsättningar för hur data samlas in liknar varandra i så väl kvalitativ och kvantitativ forskning, det som skiljer är hur data behandlas samt analyseras efter insamlandet. (Denscombe, 2000, ss. 203)

3.2.1 Kvalitativ

Kvalitativ forskning fokuserar på att undersöka ett fenomens karaktärsdrag och egenskaper (Widerberg, 2002, ss. 15-17). I en kvalitativ ansats omvandlas ord, bilder och intryck till data genom en forskares tolkningsprocess, det vill säga existensen av data skapas först när information analyseras (Denscombe, 2000, ss. 244). Metoder vid kvalitativ insamling är exempelvis en djupanalys av intervjuer, texter, bilder eller observationer. Intervjun är den metod som lämpar sig bäst när syftet är att belysa människors förståelse för ett fenomen. (Widerberg, 2002, ss. 15-17) Då syftet med denna uppsats är att identifiera svenska organisationers riskhantering avseende

informationssäkerhet krävs det mer djupgående intervjuer inom området. Därav består den kvalitativa delen i uppsatsen av intervjuer med personer kunniga om verksamhetens riskhantering beträffande informationssäkerhet. Intervjuerna inför uppsatsen var av semistrukturerad natur det vill säga frågor skapades innan samt under intervjuns gång. Frågebatteriet skickades ut i förväg till informanterna för att de skulle ha möjlighet till nödvändig förberedelse och chansen att ge en korrekt bild av organisationens riskhantering. Frågorna ställdes i en flexibel ordningsföljd samtidigt som informanten gavs möjlighet att tala fritt om ämnet vilket är det som utmärker en semistrukturerad intervju (Denscombe, 2000, ss. 135). Informanterna fick efter genomförd intervju godkänna de svar som finns publicerad i uppsatsen.

3.2.2 Kvantitativ

Data vid kvantitativ forskning ska vara mätbara och kunna rangordnas (Andersen, 1990, ss. 70). Statistiska metoder används vid analys och för detta krävs numerisk data vilket skapar kvantifierbara enheter (Denscombe, 2000, ss. 204). De kvantifierbara enheterna i uppsatsen består av de Large-caplistade bolagen på stockholmsbörsen till vilka det skickades ut ett enkätformulär för att finna svar på vilket förhållningssätt de har till riskhantering förenat med informationssäkerhet. Enkätundersökningen är menad att komplettera den kvalitativa studien för att på så sätt stärka uppsatsens validitet samt att få en mer allmän uppfattning om riskhantering med fokus på informationssäkerhet inom svenska organisationer.

3.2.3 Skriftliga källor

De huvudsakliga skriftliga källorna är vetenskapliga artiklar som återfinns på databaserna Emerald och JStore. Sökord som används är; Information Security, Risk Management, Information Technology, IT, Standards, ISO 17799, COSO, CoBIT, SOX, Riskhantering, Ramverk, Operationella risker. Till viss del används även kurslitteratur, främst för att ge grunden till uppsatsens vetenskapliga forskningsmetodik.

3.3 Urval

I urvalsprocessen är en central del val av vilken forskningspopulation som är väsentlig för studiens syfte, det vill säga den grupp människor eller objekt som utgör studiens kärna. När forskningspopulationen är vald är det vanligt att olika urvalstekniker används för att göra

ytterligare selekteringar då det vanligtvis är allt för omfattande att studera en hel population eller grupp av objekt. (J.M. Ruane, 2006, ss.129) Vid kvantitativa undersökningar är det viktigt med ett representativt urval för att möjliggöra generaliseringar. *Sannolikhetsurval* är det vanligaste sättet att få fram en representativ grupp ur en hel population och ska helst ske ur en slumpmässig urvalsprocess för att undvika personliga böjelser och skevheter. Vid sannolikhetsurval utgår forskaren från en urvalsram bestående av samtliga element inom en population där kriterier för att tillhöra den totala populationen har definierats. (J.M. Ruane, 2006, ss.135-138)

Vid kvalitativ forskning är det vanligt att använda ett *icke-sannolikhetsurval*, en teknik som används då det inte går att skapa en urvalsram (Denscombe, 2000, ss. 35). Ett exempel är bekvämlighets- eller tillfällighetsurval som bygger på att forskaren använder sig av de personer eller objekt som för tillfället finns tillhands. Nackdelen är att representativiteten försvagas eftersom de personer eller objekt som inte finns nära till hands, men som annars skulle vara intressanta för studien hamnar utanför studiens resultat. (Denscombe, 2000, ss. 142) En motivering till att använda sig av teknik som inte ger en representativ grupp av populationen är att kvalitativ forskning i första hand är en upptäcktsprocess och inte har som syfte att pröva hypoteser (Denscombe, 2000, ss. 35).

3.3.1 Fallstudieföretag

Det första kriteriet vid urvalet av fallstudieföretag är att organisationen har riskhantering som en del i verksamheten. Tillfällighetsfaktorer som spelar in i urvalet är lokaliseringen av företagen och villigheten att svara på frågor rörande riskhantering. Det vill säga den avdelning som sköter riskhanteringen ska vara belägen i Stockholm, detta för att göra personliga möten möjliga vid intervjutillfällena, samt att företagens policy tillåter denna typ av frågor. I första hand vänder sig fallstudien till organisationer i försäkringsbranschen i den mån de är villiga att ställa upp. Försäkringsbolag är intressanta i studien för att de själva säljer produkter baserade på sin kunskap i riskanalys, det är därför intressant hur de hanterar sina egna risker i organisationen och hur de prioriterar informationssäkerheten i sin riskhantering. Efter kontakt med de största försäkringsbolagen i stockholmsområdet avtalades tid för intervju med IF och Länsförsäkringar.

I komplement till de två förstnämnda organisationerna är det även intressant för rapporten att studera organisationer utan koppling till försäkringsbranschen för att se om resultatet skiljer sig från de andra organisationerna. Efter slumpmässigt uppringda organisationer av stora och Large-caplistade bolag på stockholmsbörsen avtalades även intervjutid med ett anrikt svensk industriföretag där organisationens policy kräver företagsnamnet hålls konfidentiellt. En e-postintervju genomfördes med en IT-säkerhetschef inom den statliga sektorn. Sektor och informant hålls anonymt på grund av sekretess.

3.3.2 Enkätföretag

Vid den kvantitativa undersökningen består urvalet av Large-caplistade bolag på stockholmsbörsen (se bilaga 2 – Undersökta Large-capbolag). Valet av börsnoterade bolag gjordes på grund av att dessa organisationer sannolikt har de ekonomiska resurserna för riskhantering. E-postadresser att skicka enkäten till söktes på respektive organisations webbplats. De organisationer som har valt att inte publicera e-postadresser på Internet kontaktades via telefon och en förfrågan om lämplig e-postadress gjordes.

3.4 Bortfall

Vid enkätundersökningen förväntades en stor del bortfall då besvarandet antas ses som låg prioritet hos de undersökta organisationerna. Insatta åtgärder för att öka svarsfrekvensen är först och främst genom ett lågt antal frågor som inte bör anses tidskrävande av respondenterna samt genom utskickande av påminnelser via e-post. Enkäten är skriven i Adobe Designer för att på så sätt skapa ett enkelt formulär med digitala kryssrutor. Programmet gör det även möjligt att placera in en sänd-knapp med e-postfunktion direkt i enkäten. Pdf-filformatet som skapas i Adobe Designer kan läsas i Acrobat Reader vilket är ett vanligt förekommande program hos datoranvändare och är även gratis att ladda ner från Internet, men till de respondenter som trots detta meddelade att de inte kunde öppna den bifogade filen skickades enkäten i en word-fil. Kompatibilitet mellan den bifogade filen och respondentens mjukvara är viktig del för att minska bortfallet.

3.5 Validitet och reliabilitet

Validitet och reliabilitet är beroende av varandra, men det ena ger inte nödvändigtvis det andra. Validitet (överensstämmelse) är beroende av att data har hög reliabilitet (pålitlighet), men ifall fel data mäts kan själva mätningen fortfarande vara pålitlig och ändå inte stämma överens med det undersökta fenomenet. (Patel et al. , 2003, ss. 98-99)

3.5.1 Validitet

Validitet innebär hur väl framforskad data stämmer överens med verkligheten samt huruvida det är de rätta indikatorerna som mäts. Vid valet av forskningsenheter är det därför viktigt att dessa på ett tydligt sätt baseras på studiens syfte. Andra sätt att säkerställa validiteten i en studie är exempelvis att undersöka alternativa förklaringar, låta informanterna ta del av resultatet samt kontrollera hur pass väl slutsatser överensstämmer med redan existerande kunskaper. (Denscombe, 2000, ss. 251 & 283) En studie har hög validitet när hela det fenomen som avsetts mätas mäts och inga andra mätningsvariabler läggs till (Andersen, 1990, ss. 92). Frågor i så väl enkät som intervjubatteri är grundade på tidigare vetenskaplig forskning inom riskhantering och informationssäkerhet för att bidra till en högre validitet. De kvalitativa intervjuerna har spelats in digitalt via en MP3-spelare och därefter har konversationen skrivits ner ordagrant för att ge den kortare sammanställningen en bättre överensstämmelse med verkligheten. Sammanställningen av intervjuerna är genomlästa samt godkända av respondenterna.

3.5.2 Reliabilitet

Reliabilitet kallas även för tillförlitlighet och innebär att de mätningar som har genomförts ska ge samma resultat om mätningen upprepas vid annat tillfälle eller av en annan forskare (Andersen, 1990, ss. 92). Variationer ska endast bero på förändringar av mätningsobjektet och inte orsakas av mätmetod eller mätinstrument (Denscombe, 2000, ss. 282).

Beträffande den kvalitativa delen av studien kan reliabiliteten antas som hög i den meningen att intervjuerna med största sannolikhet kommer ge samma svar även vid senare tillfälle förutsatt att företagen har bibehållna processer och samma respondenter intervjuas. Sett ur ett större perspektiv kan reliabiliteten ses som låg då de undersökta organisationerna inte kan ses som

representativ för hela populationen inom samma bransch och storlek, vilket till stor del beror på studiens bekvämlighetsurval. En lägre reliabilitet kan förknippas med den kvantitativa undersökningen då bortfallet påverkar resultatets utfall. Det inkomna svaren har var för sig en hög reliabilitet, men det totala resultatet kommer att se annorlunda ut vid senare mätningar om bortfallet antingen blir mindre eller större.

4 Empiri

Nedan presenteras relevant bakgrundinformation som för läsaren underlättar förståelsen kring problemområdet. Kapitlet inleds med en sammanfattande text om standarder och ramverk för att sedan avslutas med de genomförda intervjuerna samt enkätundersökningen.

4.1 Standard

Enligt ISO (International Organization for Standardization) ska ISO-standarder specificera krav för service, processer, material, system och för en god likriktad utvärdering, analys samt ledningens och organisationens handling. ISO-systemet är ett globalt nätverk som skapar internationella standarder som behövs i affärslivet, myndigheter och andra organ. De internationella standarderna får sin input från den nationella nivån för att sedan skapa ett system som kan implementeras världen över. ISO 17799 etablerar riktlinjer, principer för initiering, implementering, underhåll och förbättring av informationssäkerhetshantering i en organisation. (ISO, a) Följande huvudsakliga områden belyses i ISO 17799 (ISO, b):

- Etablering av informationssäkerhetspolicy
- Organisation och ansvarsförbindelse för informationssäkerhet
- Säkerhetshantering och utbildning
- Systemsäkerhetshantering
- Nätverkssäkerhetshantering
- Systemutveckling
- Säkerhetshantering av informationstillgångar
- Fysisk och miljösäkerhetshantering
- Företagsplanering och ledning

ITIL (IT Infrastrukture Library) däremot är ingen standard utan en vedertagen metod för att tillämpa IT service management. ITIL är en samling ”best practice” tillämpningar från den privata och offentliga sektorn. ITIL består av en samling böcker som ska vägleda organisationer mot en bättre, effektivare och mer kvalitativ IT-hantering. (ITIL)

4.2 Ramverk

Ramverk är en grundstruktur eller en grundstomme. Ramverk består oftast av ”best practice”-tillämpningar som organisationer kan följa för att skapa en strukturerad arbetsmiljö. COSO ERM och COBIT är två exempel på vedertagna ramverk som tillämpas världen över. COSO ERM som “Committee of Sponsoring Organizations of the Treadway Commission” ger ut är ett ramverk för riskhantering. Genom att implementera ramverket kan organisationer skapa en mer enhetlig riskhantering. COBIT däremot är ett ramverk speciellt inriktat på informationsteknologi och informationssäkerhet. Ramverket hjälper organisationen med hanteringen av IT och dess risker samt erbjuder en strukturerad vägledning.

4.2.1 COSO ERM

Riskhantering innebär enligt ERM (COSO, b, ss.5):

- koppla samman riskaptit och strategi
- fatta bättre beslut om riskåtgärder
- minska risken för överraskningar och förluster i verksamheten
- identifiera och hantera risker som är sammansatta och som skär rakt igenom hela företaget
- ta tillvara gynnsamma möjligheter
- Förbättra kapitalanvändningen

> *” Enterprise Risk Management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”* (COSO, a, ss.2)

4.2.2 COBIT

Andra institutioner som rekommenderar normer för informationssäkerhet är ”The IT Governance Institute” som genom sitt ramverk eller IT-styrningsstandard COBIT menar att standarder ska implementeras om bolaget vill uppnå en hög intern kontroll vad gäller informationsteknologi.

Ramverket COBIT ska bidra till att (COBIT, ss.6):

- IT har rätt placering i organisationen
- IT möjliggör maximering av vinsten
- IT-resurser används ansvarsfullt
- IT-risker hanteras på ett lämpligt sätt

De områden som ramverket koncentreras kring är:

- IT-strategier
- Mervärde för organisationen
- Resurshantering
- Riskhantering
- Prestationsmätning

4.3 Intervjuer

I detta avsnitt presenteras de svar som erhölls genom de djupgående intervjuerna med valda personer inom respektive organisation. Svaren som erhållits delas således in efter varje respondent och presenteras avskilt från varandra. Då syftet inte är att jämföra företag emellan, blir denna uppdelning mer överskådlig.

Intervju 1: ”Rolf”, Group IT Manager, Företaget X (Industri). Stockholm, 2007-04-04

Intervju 2: Ulf Rönndahl, General Risk Manager, IF. Stockholm, 2007-04-12

Intervju 3: Lars Rosenquist, Informationssäkerhetschef, Länsförsäkringar. Stockholm, 2007-05-02

E-postintervju 4: ”Ralf”, IT-säkerhetschef, (Myndighet). Stockholm, 2007-04-23

4.3.1 Företaget X

Finns det någon riskhanteringsavdelning?

Rolf menar att det finns två perspektiv att se det hela ur, huvudkontorsperspektivet och divisionsperspektivet. Ur huvudkontorsperspektivet finns det i dagsläget två delar som arbetar med riskhantering. En Internal control-avdelning som arbetar med riskhantering ur finansiellt perspektiv och sedan Rolf som arbetar med viss riskhantering ur ett IT-säkerhetsperspektiv. Rolf påpekar att det självklart finns andra avdelningar som exempelvis arbetar med personalfrågor och globala katastrofer. Det finns inte något informationsriskhanteringsperspektiv och heller ingen utpekad avdelning för detta.

Var i organisationen sker den huvudsakliga riskhanteringen (fokus på operationella risker)?

Rolf menar att det även finns en riskhantering ur divisionsperspektivet. Det finns utsedda personer som är ansvariga för att titta på de operationella riskerna ur ett finansiellt perspektiv och IT-säkerhetsriskerna. Rolf påpekade att riskhanteringen är något som ständigt hålls under utveckling och att det inte kan bli 100-procentigt färdigt. Han menade att om 10 år kanske vi kan titta tillbaka på år 2007 och se hur okoordinerade arbetet skedde.

Följer ni något regelverk gällande styrning? (SOX, Basel II)

Företaget X har tidigare varit noterade på den amerikanska börsen och har varit tvungna att tillämpa SOX. Rolf berättade om den nya lagen i USA som medför att utländska företag lättare ska få avregsitrera sig i USA. Tidigare har det inneburit att eftersom företaget har varit registrerade på amerikanska börsen har de ändå haft så pass mycket amerikanska aktieägare att de varit tvungna att uppfylla SECs[1] lagar inklusive SOX-lagstiftningen. Det nya lagförslaget som har gått igenom och som ska fattas i senaten i juni, kommer att innebära att företaget inte kommer att behöva uppfylla SOX-lagstiftningen. Kontentan av den aspekten av lagändringen är att man inte tittar på antalet aktieägare längre utan man tittar på var omsätts aktien och 99,99 procent av omsättningen sker i Stockholm och det är nästan ingen omsättning i USA. Därför kan företaget avregistrera sig och behöver inte längre uppfylla lagstiftningen.

[1] http://www.sox-online.com/sec.html, 2007-04-05, 13:04

Kommer ni att fortsätta använda SOX?

Då företaget X har lagt ned stora investeringar för att tillämpa SOX, kommer man att behålla de kontroller som adderar värde till företaget och göra sig av med dem som inte gör det. Detta är en diskussion som förs med företagets revisorer huruvida de krav som tidigare har ställt genom SOX kan tas bort eller inte.

Hur involverad är ledningen i riskhanteringen?

Företagets CEO, (Chief Executive Officer) är inte direkt involverad i riskhanteringen. Den person som är djupt involverad är företagets CFO (Chef Financial Officer). Tittar man sedan på riskhanteringen ur ett IT-perspektiv är det inte någon annan än IT-chefen som är involverad i det. Detta arbete är delegerat till honom och sedan är det Rolf som sköter det praktiska.

Hur ser riskindelningen ut?

Riskerna delas efter finansiella, operationella risker samt IT-säkerhetsrisker.

Vad ska riskhanteringen leda fram till (kostnadsbesparingar, nöjda aktieägare etc.)?

Företaget ska se till att de känner till riskerna och att de bygger upp en intern kontrollmiljö som gör att de varken har för höga eller låga interna kontrollkrav. Det ska leda dels till optimerade interna processer men också till att inte blir för nedtyngda av kontrollarbetet. Det är naturligtvis ur ett kostnadsperspektiv och effektivitetsperspektiv och så vidare.

Hur ser prioriteringen ut, baserad på indelningen?

Det är en svår fråga att uttala sig om menar Rolf. Naturligtvis kan man ändå säga att de finansiella har en högre prioritering, det får man kanske erkänna men IT-säkerhetsriskhanteringen har ju ändå en väldigt hög prioritering. Rolf tror ändå inte att någon speciell person skulle säga att de prioriterar den finansiella riskhanteringen högre. Man prioriterar båda två högt. Huvudkontoret ansvarar för finansiella och IT-säkerhetsrisker, men de operationella riskerna sköts helt och hållet på divisionsnivå och det är då upp till divisionen hur det prioriteras/hanteras.

Hur stor fokus ligger på informationssäkerheten?

Rolf menar att fokusen är större när det gäller de finansiella riskerna och hanteringen. Detta tror han beror på de oerhörd stora summorna som hanteras dagligen i verksamheten. Han menar att de summor som kan riskeras på den finansiella sidan är mycket större än de summor som kan

förloras genom IT-säkerhetsrisker. Ändå menar Rolf att om han var CEO eller CFO skulle fokuseringen fördelas jämt över verksamhetens olika risker. Rolf berättade vidare att bara för att man arbetar med informationssäkerhetsriskhantering är inte det viktigaste. Att inte kunna ta fram rätt produkter, att inte kunna leverera rätt produkter eller att leverera fel produkter, det är viktiga aspekter menade han. Han menar att arvet måste förvaltas och att inte endast använda teoretiska ramverk som bara slukar resurser, utan att se till att det hanteras pragmatiskt och att det verkligen levererar värde

Är informationssäkerhet en integrerad del av den traditionella riskhanteringen?

Informationssäkerheten är helt fristående från den traditionella riskhanteringen. Däremot har SOX-arbetet gjort att de varit tvungna att integrera mycket av den finansiella riskhanteringen med informationsriskhanteringen. Detta ansåg Rolf som nyttigt, men att det varit ett svårt arbete och att det inte på något sätt är enkelt att få saker och ting att fungera tillsammans.

Ser du informationssäkerheten som en del av de operationella riskerna?

Rolf menar att det är ett komplext förhållande. Rolf menar att när han säger informationsriskhanteringen menar han IT-säkerhetshanteringen. Det ligger naturligtvis en del av informationsriskhantering inom IT-säkerhet. Sedan ligger en del informationsriskhantering inom den finansiella riskhanteringen och det finns ett överlappande område kring generell informationssäkerhetshantering som inte hanteras 100 procent enhetligt och professionellt kanske. Rolf anser att IT-säkerheten hanteras rimligt proffsigt och den del av informationssäkerheten som ligger inom IT-säkerheten och den finansiella rapporteringen hanteras proffsigt. Sedan ansåg Rolf att det finns mycket mer inom informationssäkerhet som ingen har riktigt fokus på idag.

Följer ni något speciellt ramverk eller standard (COSO, COBIT, ISO 17799)?

Företaget X har varit influerade av alla de ovanstående ramverken och standarderna när de implementerat de i deras interna ramverk Det är däremot inte någon speciell standard som har tillämpats fullt ut. COSO och COBIT har varit de mer övertagande då SOX rekommenderar dessa.

Varför just denna standard eller varför ingen alls (egenutvecklad)?

Detta för att de olika standarderna och ramverken har olika fokus på saker och ting. Det har inte varit möjligt att tillämpa de fullt ut då de inte har passat verksamheten menar Rolf. Företaget X har gjort en mix av dem, med att det ändå varit ISO och COBIT som de rigoröst implementerat. Andra standarder, som ITIL har också använts, men som företaget endast varit influerade utav. Ramverken COSO och COBIT används också delvis på grund av att de ställs som krav i SOX.

Har IT-avdelningen hand om den i så fall?

ISO hanteras på Rolfs avdelning och där Rolf är ansvarig ur ett IT-säkerhetspolicyperspektiv. COSO och COBIT kommer från CFO-perspektivet, dvs ledningsgruppen.

Sitter IT-chefen med i ledningsgruppen?

Den högste IT-ansvarig (IT-chefen) sitter i ledningsgruppen och även i koncernledningsgruppen

Vilka risker kan företagets system vara utsatt för?

Det finns ju tusentals risker som yttre, inre risker, mänskliga faktorn och interna manipulatörer, externa manipulatörer. COBIT en bra vägledning över hur man bör tänka på de organisatoriska perspektiven

Är organisationens IT-system sammankopplat med ett utomstående system? Om ja, vilka krav ställer ni på det systemet?

Företagets system är sammankopplat med andra system externt. SOX-arbetet har medfört att företaget X har upptäckt problem som tidigare inte varit möjliga att upptäcka. COBIT har enligt Rolf varit till bra hjälp vid informationshanteringen. De samarbetspartners som har sina system sammankopplade med företagets X:s system måste tillämpa samma kontroller för att säkerställa kraven enligt SOX. Vidare har de system som varit kopplade till den finansiella rapporteringen varit tvungna att upprätta ett SAS70-avtal. Detta dokument ska beskriva hur samarbetspartnern har implementerat sin interna kontrollmiljö. Tidigare har SOX krävt detta avtal, men då företaget inte längre behöver följa SOX har de lättat på den regeln och kräver endast att samarbetspartnern genomför en riskanalys och dokumenterar detta för att säkerställa kontrollmiljön.

Vad är nackdelarna med att inte använda sig av standarder och ramverk?

Rolf menar att man får det svårare att argumentera internt och externt för omfattning av kontroller om man ej baserat det på vedertagna standarder. Nackdelen med att inte ha en strukturerad riskhantering är att det då inte går att kontrollera samtliga risker och hur de hanterats för samtliga orter, system och dylikt.

4.3.2 IF

Finns det någon riskhanteringsavdelning?

IF har en övergripande riskhanteringsavdelning med en General Risk Manager under honom finns underavdelningar med ansvariga Risk Managers enligt följande:

- Risk Manager – Scandinavia Security and Personal safety
- Risk Manager – Finland
- Risk Manager – Norge Security and Personal Safety
- Risk Manager – Internal Affairs and Ethical standards
- Risk Manager – IT Security and Information Security
- Risk Manager – Operational Risks and Analysis
- Risk Manager – Operational Risks and ORA-process samt Risk Manager – Information Security Risk specialist

Var i organisationen sker den huvudsakliga riskhanteringen (fokus på operationella risker)?

De tre sistnämnda Risk Managers arbetar med risker ur ett omvärldsanalysperspektiv det vill säga de arbetar med omvärldsbevakning och identifierar risker utanför organisationen. En utav dessa är specialiserad på att identifiera IT-risker och arbetar bland annat med kritisk infrastruktur. Linjeorganisationerna på IF hanterar sina egna risker och Rönndahl menar att det optimala för företag är att ha en riskkultur där det är linjens ansvar att sköta processer och hantera risker. Den centrala riskhanteringsavdelningen bör istället mer fungera som en stödfunktion i linjens riskarbete.

Följer ni något regelverk gällande styrning? (SOX, Basel II)

Försäkringsbolag omfattas av Solvency II och Svensk kod för bolagsstyrning. IF följer även instruktioner från finansinspektionen FFS 2005:19. De höga kraven på försäkringsbolagen och banker medför att dessa organisationer ligger i framkant gällande informationssäkerhet.

Hur involverad är ledningen i riskhanteringen?

En Risk Management-plan läggs fram varje år som både ledningen och styrelsen är involverade i. Rapportering sker kvartalsvis till VD.

Hur ser riskindelningen ut?

På IF delas risker in i finansiella och operationella risker med tillhörande undergrupper. Rönndahl berättar om en studie utförd av Fortune 1000 år 2001 visar att av de 100 bolag som sjönk med minst 25 % värde på sitt aktievärde hänvisade 35 % till operationella risker medan endast 6 % av nedgångarna berodde på finansiella risker. Operationella risker har alltså en stor påverkan på ett företags värde, men det är ganska nytt att man har börjat utpeka detta enligt Rönndahl. I en stor organisation finns det risk för att en operationell risk hamnar mellan två stolar där den ena individen/avdelningen tror att risken hanteras av en annan individ/avdelning som i sin tur har samma uppfattning fastän omvänt. Därför anser Rönndahl att det är viktigt med tydliga definitioner på operationella risker och att följande definition i Basel II är lämplig; *en operationell risk är en risk som skapar förluster från ineffektiva interna processer, människor, vitala tekniska system eller externa händelser*.

Vad ska riskhanteringen leda fram till (kostnadsbesparingar, nöjda aktieägare etc.)?

Riskhanteringen ska tillföra mervärden och hjälpa linjen att hitta nya affärsmöjligheter. Mervärden innefattar exempelvis att stärka varumärket genom att göra företaget stabilt och säkert. Kostnadseffektivitet är ett annat perspektiv där en riskhanteringsåtgärd som kostar 500 000 kr sparar åtskilliga miljoner åt företaget om den har som syfte att undanröja en risk som skulle kosta 20 miljoner om den förverkligades.

Hur ser prioriteringen ut, baserad på indelningen?

Det som är mest prioriterat är det som har högst negativ påverkan på verksamheten. Rönndahl menar att de mjuka värdena är viktiga att komma ihåg då de operationella riskerna kan orsaka

stora nedgångar i verksamheten, ett driftuppehåll i verksamheten på grund av exempelvis ett systemhaveri kan leda till förlorandet av flertalet kunder.

Enligt IFs årsbokslut, tar verksamheten in runt 38 miljarder i premieintäkter och betalar ut ungefär 32 miljarder i skadeersättning med driftkostnader adderade blir det ca 3 miljarder till, det innebär att 38 miljarder ska in på 220 arbetsdagar och 35 miljarder ska ut på 220 dagar. Rönndahl ställer upp frågeställningen om verksamheten ska ha in 100 miljoner varje dag, vad händer då om IT-systemen inte fungerar?

Hur stor fokus ligger på informationssäkerheten?

IF lägger stor fokus på informationssäkerheten då hela verksamheten bygger på att deras IT-system är tillgängligt för kunderna. Det är av denna anledning som IF utöver en IT-säkerhetschef även har en person som arbetar heltid med att identifiera IT-risker på så sätt får IT-avdelningen en kontinuerlig uppföljning av existerande risker i verksamhet och omgivning. Det finns exempelvis krav på hur de ska gå till när en individ pluggar i sladdar, hänger upp sladdar och städar i ett serverrum. Ytterligare säkerhetsåtgärder kan vara förbud på att uppdatera programvaror mitt under en kampanj. Verksamheten är koncentrerad kring fyra olika orter vilket gör att ett avbrott i infrastrukturen, IT, telefoni och eltillförseln är extra känsligt. Ett längre avbrott i IT-systemet graderas till en inverkningsgrad på 9 av 9 möjliga och skulle innebära näst intill en katastrof.

Är informationssäkerhet en integrerad del av den traditionella riskhanteringen?

Informationssäkerheten är väl integrerad i verksamheten. Rapportering av IT-risker sker på samma vis som för rapportering av skadefrekvenser.

Ser du informationssäkerheten som en del av de operationella riskerna?

IT-säkerhetsrisker och informationssäkerhetsrisker ligger som en egen riskgrupp under huvudgruppen operationella risker.

Följer ni något speciellt ramverk eller standard (COSO, COBIT, ISO 17799)?

Rönndahl berättar att IF följer i princip alla ramverken och är också standardiserade på IT-sidan, men den standard som huvudsakligen används och efterföljs är ISO 17799.

Har IT-avdelningen hand om den i så fall?

IT-avdelningen ansvarar för standarden.

Sitter IT-chefen med i ledningsgruppen?

CIO, Chief Information Officer sitter i ledningen

Vilka risker kan företagets system vara utsatt för?

IT-systemet kan utsättas för både interna och externa angrepp och det kan vara allt ifrån terrordåd till att en bakfull grävmaskinist gräver av en elkabel av misstag, men det viktiga är inte orsaken utan vilka åtgärder som ska sättas in när det blir strömlöst. Operationella risker är de största farorna där 9/11 var väckarklockan. Numera finns det inget amerikanskt försäkringsbolag som beviljar avbrottsförsäkringar till bolag som inte har välgjorda kontinuitetsplaner för att upprätthålla verksamheten eller som saknar en krisorganisation.

Hur säkerställer ni att dessa risker förebyggs?

IF arbetar mycket med kontinuitetsplanering och krishantering. Business Impact Analysis är ett arbetssätt som används inom organisationen med utgångspunkten; vilka kritiska affärsprocesser finns i verksamheten och vilka aktiviteter ligger till grund för de här kritiska processerna och vad är det för olika resurser som behövs sättas in för riskhanteringen. I praktiken innebär detta att identifiera vad incidenterna har för påverkan på verksamheten för att sedan lista de mest kritiska processerna. Alternativa lösningar och planer arbetas fram för att säkra processerna var på en organisation skapas som ska arbeta med de alternativa lösningarna. Slutligen körs övningar i organisationen för att se om planen fungerar. Målet med IFs arbetssätt är att skapa en riskkultur där det blir naturligt för individer och avdelningar att rapportera in incidenter för att organisationen på så sätt kan agera med aktiv riskhantering.

Är organisationens IT-system sammankopplat med ett utomstående system? Om ja, vilka krav ställer ni på det systemet?

IF ansvarar för uppdatering av patchar men själva driften ligger hos TietoEnator och de är därför i allra högsta grad inblandade i processen. Andra system som är länkade till IF är bland annat banksystem som hanterar in- och utbetalningar. IFs krav på deras samarbetspartners är att de ska följa avtalade internationella standarder. IF är även tydliga med att de inte accepterar så kallade

down-time, det vill säga att systemen ligger nere mer än en viss avtalad maxtid. TietoEnator har även kravet på sig att de ska vara med på övningar och vid scenarioplanering.

Vad är nackdelarna med att inte använda sig av standarder och ramverk?

Det är svårt att bedöma kvaliteten i utfört arbete och det tar bort möjligheten att benchmarka med andra organisationer för att bli bättre inom det specifika området. Företaget utsätts för stora ekonomiska risker genom att det inte finns en god kontroll på riskerna i verksamheten. I fler fall äventyras hela bolagets existens genom avsaknad av en god riskkontroll. Organisationen går miste om möjligheten att identifiera nya affärsmöjligheter. En konkurrent som är bättre inom området kommer att vinna fler upphandlingar då kunderna/köparna börjat se dessa frågor som oerhört viktiga frågor vid upphandlingar.

4.3.3 Länsförsäkringar

Finns det någon riskhanteringsavdelning?

Det finns ingen avdelning som har hand om specifika IT-risker. Den riskhanteringsavdelning som finns har hand om finansiell riskhantering. IT-risker ses inte som en del av operationella riskerna. Alla länsbolag har fristående avdelningar. Länsförsäkringar har 24 olika länsbolag som ägs av 3,2 miljoner ägare. Under dessa länsbolag finns sedan LFAB som i sin tur består av 5 divisioner. Divisionerna är Bank, Sale, Liv, AGRIA och ITC.

Var i organisationen sker den huvudsakliga riskhanteringen (fokus på operationella risker)?

Då länsförsäkringar inte har en specifik avdelning sker IT-riskhanteringen och informationssäkerheten hos CIO. Arbetet innebär policy, regler etc. Utförandet sker däremot hos ITC, Länsförsäkringars IT-organisation.

Följer ni något regelverkgällande styrning? (SOX, Basel II)

Länsförsäkringar följer Basel II, Svensk lag, Solvency.

Hur involverad är ledningen i riskhanteringen?

Ledningen visar inte det intresse som de borde visa menar Rosenquist och säger vidare att organisationens affärsbeslut går före. Det finns en viss okunnighet hos ledningen gällande

informationssäkerhet. Nackdelen med ett icke IT-bolag är att här förväntas det mestadels att det ska fungera.

Hur ser riskindelningen ut?

Indelningen är finansiella, operationella och sedan informationssäkerhet.

Vad ska riskhanteringen leda fram till (kostnadsbesparingar, nöjda aktieägare etc.)?

Då Länsförsäkringar, främst banken handskas med pengar, gäller det att ha ett säkert system för inte riskera kundernas information och pengar.

Hur ser prioriteringen ut, baserad på indelningen?

De finansiella riskerna prioriteras högre än informationssäkerheten, men Rosenquist menar att riskområdena sällan ställs mot varandra. Då Länsförsäkringar inte jobbar efter den traditionella riskhanteringen där IT ingår i operationella risker är det enligt Rosenquist svårt att sätta en siffra på hur högt det prioriteras.

Hur stor fokus ligger på informationssäkerheten?

Lars menar att det är för liten fokus på informationssäkerhet. Det är en större fokus kring informationssäkerhet i bankverksamheten vilket främst beror på de attacker som Nordea har blivit utsatt för och därför har Länsförsäkringar också varit tvungna att se över saken.

Är informationssäkerhet en integrerad del av den traditionella riskhanteringen?

Nej, den är fristående och inte tillräckligt integrerad.

Följer ni något speciellt ramverk eller standard (COSO, COBIT, ISO 17799)?

COBIT används av organisationens revisorer. ISO 17799 har använts tidigare men nu planeras en övergång till den nyare ISO 270001. ITIL används för drift och produktion.

Varför just denna standard?

Rosenquist anser att användandet av dessa standarder faller sig naturligt då dessa standarder belyser olika delar av IT-säkerheten och är allmänt kända i andra organisationer.

Har IT-avdelningen hand om den i så fall?

ISO-standarderna handskas av Rosenquist själv medan COBIT handskas av revisorerna.

Sitter IT-chefen med i ledningsgruppen?

Rosenquists chef (CIO) sitter i ledningsgruppen och är den som Rosenquist rapporterar till.

Vilka risker kan företagets system vara utsatt för?

Det är svårt att räkna upp de risker som organisationen kan vara utsatta för, självklart finns det alltid onda människor som vill stjäla kundernas pengar. Länsförsäkringar har tidigare inte blivit utsatta för IT-hot, detta tror Rosenquist beror främst på att de som bank är relativt små och att hackers oftast inte är svenskar och därför inte vet att Länsförsäkringar är en bank. De interna riskerna anser Rosenquist är större än de externa eftersom det rent generellt på ett modernt företag är omöjligt att hacka sig in utifrån utan hjälp inifrån.

Hur säkerställer ni att dessa risker förebyggs och med säkerhetsarbetet?

Det sker genom kontinuerliga kontroller, både tekniska och administrativa. Det finns inget som heter 100-procentig säkerhet menar Rosenquist, men de gör så mycket som möjligt för att anpassa säkerheten för organisationen. Bland annat anlitas externa företag för att leta svagheter i systemen och länsförsäkringars medarbetare tillfrågas i undersökningar om deras kännedom om regler.

Är organisationens IT-system sammankopplat med ett utomstående system? Om ja, vilka krav ställer ni på det systemet?

Länsförsäkringar samarbetar med externa partners. De har en rutin för hur systemen ska sammankopplas. Partnerna måste följa länsförsäkringens regler om systemen ska kunna kopplas ihop. De externa partnerna behöver inte följa specifika standarder, detta menar Rosenquist är för att de inte kan ställa sådana krav på exempelvis en bilverkstad.

Vad är nackdelarna med att inte använda sig av standarder och ramverk?

Risken är att verksamheten missar viktiga säkerhetsaspekter och att säkerhetsarbetet på så sätt inte blir lika heltäckande som det blir vid användandet av ISO 17799 eller 27001.

4.3.4 Myndighet

Finns det någon riskhanteringsavdelning?

Det finns ingen organisatorisk del som har som enskild uppgift att enbart hantera risker dock har en funktion som hanterar detta växt fram. Inom organisationen finns det en funktion för att integrera verksamhetskrav i IT-system. Denna ska väga samman olika krav och klara ut vilken nytta organisationen kommer att få av ett nytt IT-system eller IT-lösning. Denna funktion samverkar tätt med informationssäkerhetsfunktionen. Säkerhetsfunktionen har sällan sådan verksamhetskunskap att man kan bedöma vilka konsekvenser ett beslut kan ge på verksamheten. Därför vägs alltid viktigare informationssäkerhetsfrågor samman med verksamhetsnyttan.

Var i organisationen sker den huvudsakliga riskhanteringen (fokus på operationella risker)?

Riskhanteringsbeslut bereds alltid på handläggarnivå och föredras alltid för den högsta chefen för verksamheten. I föredragningen ingår normalt de som har tagit fram beslut och en föredragande.

Följer ni något regelverk gällande styrning? (SOX, Basel II)

Organisationen följer ett egenutvecklat regelverk samt svensk lag.

Hur involverad är ledningen i riskhanteringen?

Variationen är stor när det gäller ledningens involvering. Inom det ordinarie verksamhetsområdet är riskhantering väldigt vanligt men kopplat till informationssäkerhet är det inte lika vanligt. Oftast är inte ledningen inblandad i beredningsarbetet, men dock inför beslut.

Hur ser riskindelningen ut?

Ekonomiska, verksamhetsmässiga samt säkerhetsmässiga konsekvenser är de vanligast förekommande riskindelningarna.

Vad ska riskhanteringen leda fram till (kostnadsbesparingar, nöjda aktieägare etc.)?

Riskhanteringen ska leda fram till väl avvägda säkerhetsbeslut. Ralf tror att detta i förlängningen kommer att leda till dels kostnadsbesparingar samt en högre produktionstakt i verksamheten.

Hur ser prioriteringen ut, baserad på indelningen?

Verksamhetsmässiga vinster/effekter är absolut högst prioriterat, särskilt då det ofta finns operativa krav som kan gå före både ekonomi och rena säkerhetsåtgärder. När en säkerhetsåtgärd vidtas syftar den till att exempelvis hindra informationsförlust vilket i sin tur skulle påverka produktionstakt och trovärdighet. Om säkerhetsåtgärden är allt för komplicerad och dyr kan det få effekten att produktionstakten och trovärdigheten får en större törn än vid en mindre incident. Det är en mycket svår avvägning som ledningsgruppen måste vara involverad i.

Hur ser företaget säkerhetsorganisation ut?

Inom organisationen finns en säkerhetschef, IT-säkerhetschef och ett antal handläggare som arbetar med säkerhet på heltid. Säkerhetschef och IT-säkerhetschef är direkt underställda chefen för organisationen.

Hur stor fokus ligger på informationssäkerheten?

En mycket stor fokus vilar på informationssäkerheten, det är en naturlig del för samtliga medarbetare i det dagliga arbetet. En stor del av organisationens trovärdighet handlar om att kunna hantera information på ett trovärdigt sätt. De uppgifter som hanteras måste vara riktiga.

Är informationssäkerhet en integrerad del av den traditionella riskhanteringen? (Var placeras informationssäkerheten i riskhanteringen)

Helt klart, det som inte fungerar lika bra är att göra professionella ekonomiska avvägningar i riskhanteringen.

Följer ni något speciellt ramverk eller standard (COSO, COBIT, ISO 17799)?

ISO 17799 och till viss del egenutvecklade regelverk följs.

Varför just denna standard eller varför ingen alls?

Det är en inom myndigheten överenskommen standard och där organisationen ska följa ISO 17799. Det finns till viss del egna regelverk som reglerar det som inte tas upp i ISO 17799. I många fall är säkerhetskraven hårdare än det som anges i standarden.

Har IT-avdelningen hand om den i så fall?

I dagsläget är det IT-säkerhetschefen som ansvarar för att kontrollera och följa upp att ISO 17799 följs. Genomförandet ska dock göras av IT-avdelningen. Detta fungerar inte bra idag, det är svårt att motivera användandet av ISO 17799 för tekniker och utvecklare. Informationssäkerhetschefen tror att det kan bero på att de tycker att byråkratin standarden medför saktar ner utvecklingsprocessen.

Sitter IT-chefen med i ledningsgruppen?

Nej, tyvärr medger Ralf. Organisationen är väldigt hierarkisk och vissa viktiga funktioner är inte representerade i ledningsgruppen som IT-chef, säkerhetschef samt ekonomichef. Resurshållare för dessa funktioner är normalt representerade i ledningsgruppen men kan sällan ta ställning i sakfrågor.

Vilka risker kan företagets system vara utsatt för?

Intrångsförsök, manipulation av data, stöld av information, informationsförlust (genom brand, strömavbrott med mera), sabotage, brist på nyckelpersoner m.m. listan kan göras lång.

Hur säkerställer ni att dessa risker förebyggs och med säkerhetsarbetet?

Inom organisationen finns en fastställd metod med ett antal olika beslutpunkter för att hantera utveckling, innan ett system driftsätts eller avvecklas fattas ett säkerhetsbeslut där underlagets omfattning baseras på hur känslig information systemet ska hantera. I underlaget kan kodgranskning, dokumentationsgranskning med mera ingå.

Är organisationens IT-system sammankopplat med ett utomstående system? Om ja, vilka krav ställer ni på det systemet?

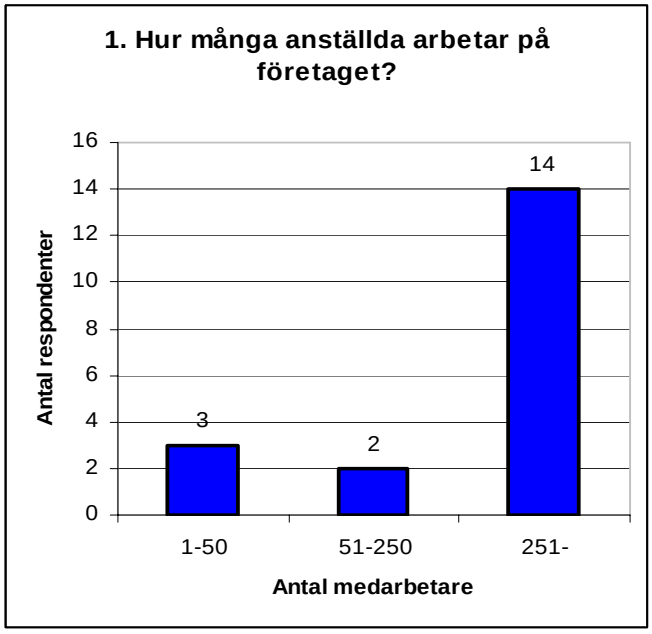
Systemen är inte kopplade mot utomstående system.

Vad är nackdelarna med att inte använda sig av standarder och ramverk?

Inom organisationen är en av de största prioriteringarna att vara interoperabel med andra länder och organisationer. Använder man vedertagna internationella standarder är det mycket lättare att samarbeta internationellt. En vedertagen standard ger ju också ett ramverk som är testat och utvärderat av många, en kvalitetsstämpel på verksamheten. Nackdelarna blir alltså det motsatta att inte kunna samverka på ett enkelt sätt med andra länder, där varje regelverk måste matchas för att se att man har motsvarande krav.

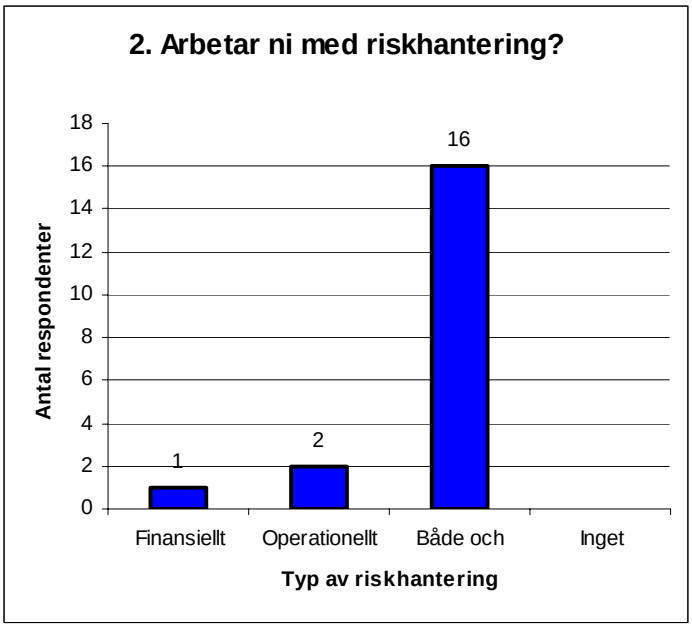
4.4 Enkätundersökning

I detta avsnitt presenteras det kvantitativa data som erhållits genom enkätundersökningen vilken utfördes på svenska Large-caplistade bolagen på Stockholmsbörsen (se bilaga 2 - Undersökta Large-capbolag) De bolag som inkluderades i undersökningen var endast de som hade huvudkontor i Sverige. 19 av de 70 noterade bolagen valde att deltaga i undersökningen, varav fyra bolag ej hade huvudkontor i Sverige och som exkluderades. Detta ger en svarsfrekvens på 27 %. Totalt svarade 26 bolag, därav sex bolag som avstod från undersökningen.



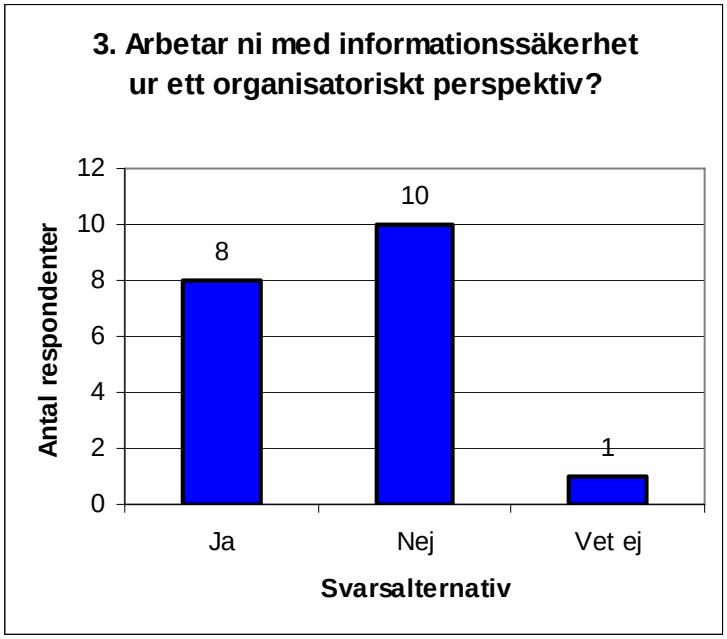
Figur 4.1: Antal anställda på enkätbolagen

14 av de 19 svarande bolagen hade mer än 251 anställda. Dessa 14 bolag anses som stora organisationer och som anses ha resurser för riskhantering. Denna fråga ställdes för att få en övergripande bild på hur stora dessa bolag egentligen var och har ingen direkt koppling till uppsatsens problemformulering.



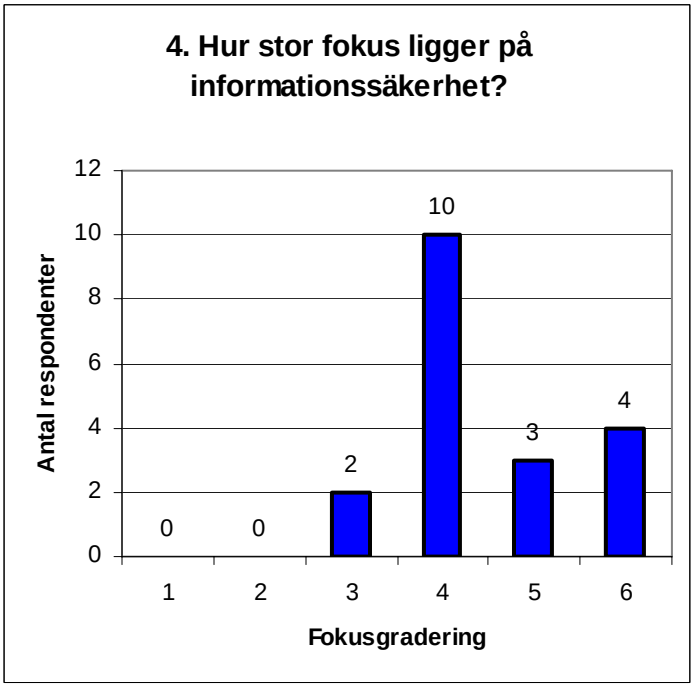
Figur 4.2: Hur många bolag arbetar med riskhantering

På frågan om bolagen arbetade med riskhantering svarade 16 bolag att de arbetade med både finansiell och operationell riskhantering. Två bolag arbetade endast med operationell medan ett bolag endast med finansiell riskhantering.



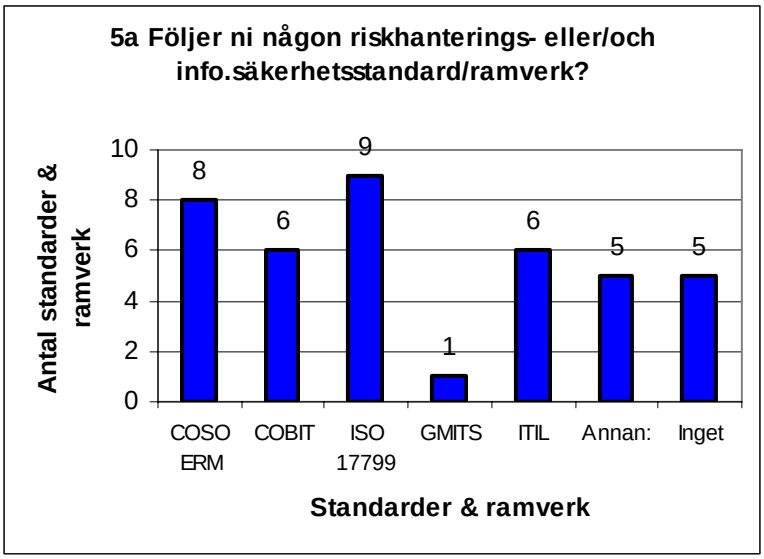
Figur 4.3: Informationssäkerhet, inte enbart ur ett tekniskt perspektiv

På frågan om bolagen arbetade med informationssäkerhet ur ett organisatoriskt perspektiv (se figur 4.3) svarade tio bolag ”nej”, medan åtta bolag arbetade med informationssäkerhet ur ett organisatoriskt perspektiv och inte enbart tekniskt. En utav respondenterna visste inte hur bolaget arbetade. Av svaren tolkat kan det konstateras att de åtta bolag som svarade ”ja” på denna fråga befinner sig inom de 16 bolag som svarade att de arbetade med både finansiell och operationella riskhantering på föregående fråga.



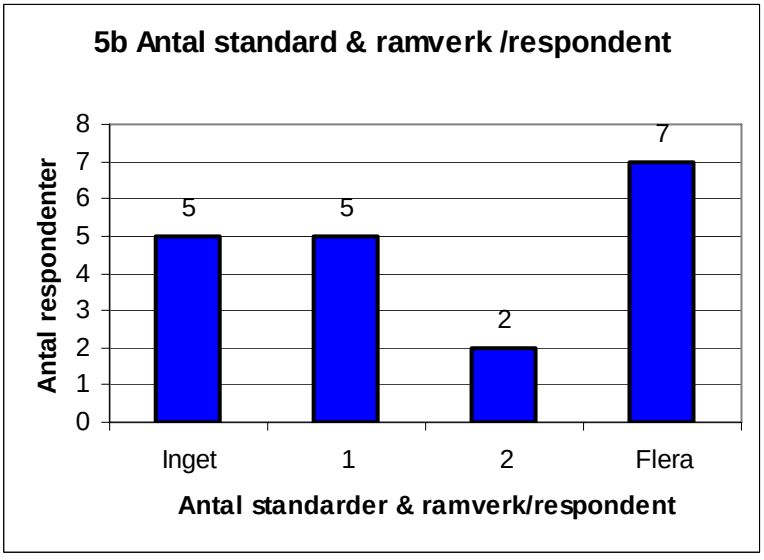
Figur 4.4: Fokusering på informationssäkerhet

Av figuren intill kan det utläsas att 12 bolag hade en medelmåttig fokusering (fokusgradering, 3-4) på informationssäkerhet. Endast tre bolag ansåg sig ha en hög fokus på informationssäkerhet, medan fyra bolag hade en mycket hög fokus på informationssäkerhet.



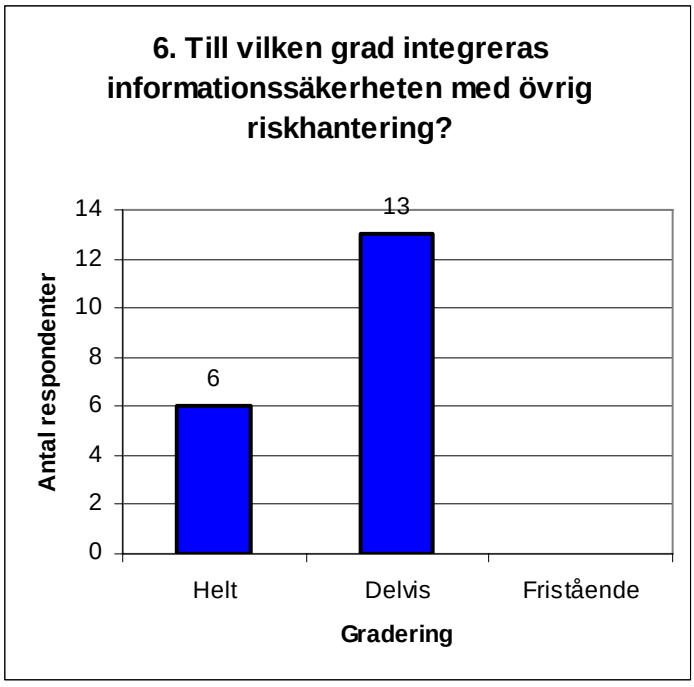
Figur 4.5: De ramverk & standarder som följs

På frågan om bolagen följde någon riskhanterings- eller/och informationssäkerhetsstandard/ ramverk var svaren jämt fördelade över de olika svarsalternativen. ISO 17799 var den mest använda standarden hos bolagen. Totalt var det nio bolag som använde ISO-standarden. Notera att denna fråga hade flera svarsalternativ och att bolagen kunde välja flera standarder. Fem av respondenterna använde inte någon standard eller ramverk. Andra ramverk och standarder som respondenterna angav under svarsalternativet ”Annan” var: egenutvecklad, ISF (Information Security Forum) - Standard of Good Practice for Information Security, SOX och FIRM.



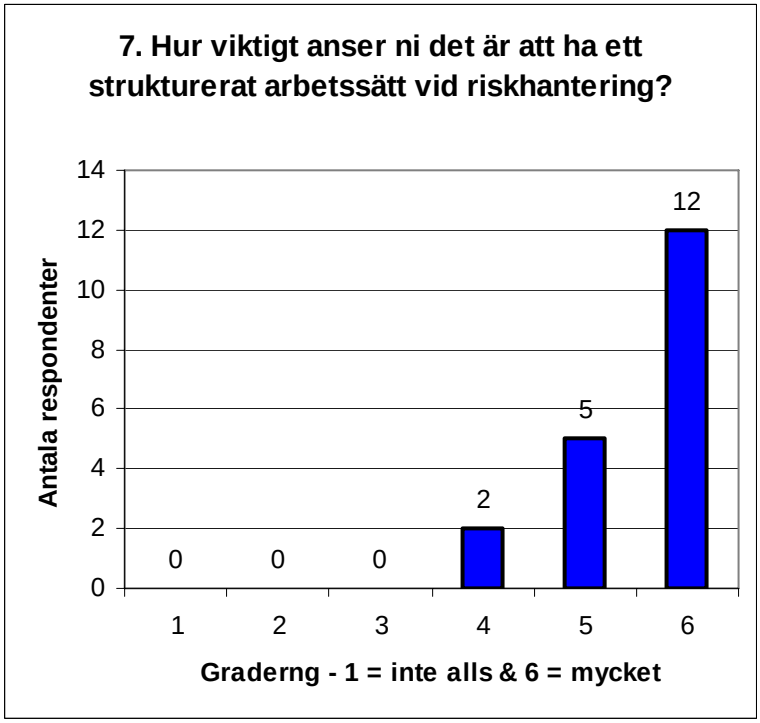
Figur 4.6: Antal standarder & ramverk per bolag

Ovan är en fördelning över antal standarder per bolag. Denna fördelning skapades utifrån de svar som erhölls från frågan ovan. Fem bolag använde inte någon standard eller ramverk. Fem av respondenterna använde endast en standard eller ramverk. Två bolag tillämpade två ramverk medan hela sju bolag använde tre eller flera standarder och ramverk.



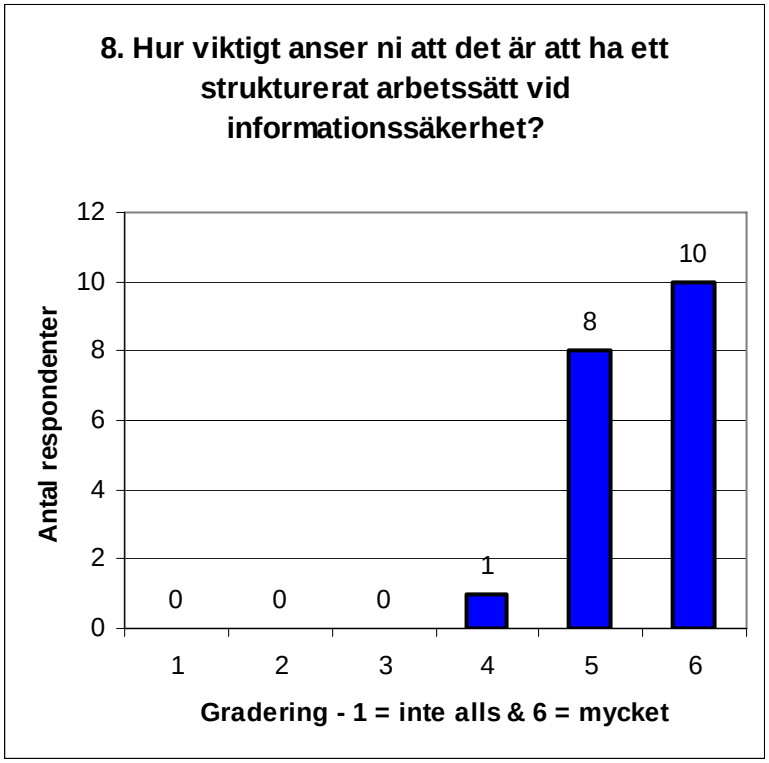
Figur 4.7: Integrering av informationssäkerheten i riskhanteringen

På frågan om till vilken grad informationssäkerheten integrerades med övrig riskhantering svarade 80 %, det vill säga 13 av respondenterna att de delvis integrerade informationssäkerheten. Endast sex bolag integrerade informationssäkerheten helt i den övriga riskhanteringen.



Figur 4.8: Strukturerad riskhantering

Nästa fråga vars svar redovisas i figur 4.8 intill ställdes frågan om hur viktigt bolagen ansåg det är att ha ett strukturerat arbetssätt vid riskhantering. 12 bolag ansåg att det var ytterst viktigt att ha ett strukturerat arbetssätt. Fem bolag ansåg att det var relativt viktigt medan endast två bolag hade svarat strax över medel.



Figur 4.9: Strukturerad informationssäkerhet

Nästa fråga som ställdes hade samma karaktär som föregående fråga, men där fokuseringen låg kring informationssäkerhet. Frågan som redovisas i figur 4.9 redogör för hur viktigt bolagen anser att det är att ha ett strukturerat arbetssätt vid informationssäkerhet. Av svaren tolkat är det nu två mindre bolag än förra frågan, dvs tio som ansåg strukturerat arbetssätt vid informationssäkerhet som mycket viktigt. Åtta bolag ansåg att det var relativt viktigt, medan endast ett bolag såg det som strax över medel.

Figur 4.10: Ledningens involvering

Den sista frågan var om den ansvariga för informationssäkerheten fanns representerad i ledningsgruppen för bolaget. Dessa svar jämt fördelade mellan svarsalternativen ”Ja” och ”Nej”. Tio bolag hade den ansvariga för informationssäkerheten med i ledningsgruppen, medan nio av bolagen inte hade det.

5 Analys

Detta kapitel syftar till att belysa empirin i relation till valda teorier. Kapitlet inleds med analys av de genomförda intervjuerna och avslutas med analys av enkätundersökningen på Large-caplistade bolag på Stockholmsbörsen.

5.1 Intervjuer

Det kan konstateras att samtliga fallstudieorganisationer utom en har en uttalad riskhanteringsprocess av operationell karaktär med fokus på informationssäkerhet. Strategier för informations- och IT-säkerhetsrisker samt arbetssätt skiljer sig dock mellan de olika organisationerna. Enligt Galloway & Funston, 2000, använder värdebyggande företag riskhantering för att skapa värde vilket syftar till att skapa marknadsfördelar samt att hantera enkla processer effektivt, till låg risk och kostnad. Tre av de intervjuade parterna nämner kostnadseffektivitet som syfte för riskhanteringen. IF har även som mål att genom riskhantering tillföra mervärden och hitta nya affärsmöjligheter medan Länsförsäkringar lyfte fram säkerheten som riskhanteringen viktigaste syfte.

Arbetssättet kring riskhantering skiljer sig åt mellan de intervjuade bolagen. Bandyyopadhyay har i sin studie belyst att riskhantering ska vara en sekventiell process för att ledningen lättare ska förstå hur det påverkar organisationen. Identifiering, analys, reducerande handlingar och uppföljning, med fokus på operationella risker, ska ske på flera olika nivåer var på den ökade integreringen ger en optimerad riskhantering. De intervjuade organisationerna har olika synsätt och arbetssätt. På företag X finns det två perspektiv dels huvudkontorsperspektivet som är uppdelat mellan finans- och IT-risker samt divisionsperspektivet där riskhanteringen är delegerad till ansvariga personer. Försäkringsbolaget IF har även de en uppdelning mellan finans och operation, men är mer detaljerad där det finns ett knappt tiotal riskmanagers i den operationella delen med egna ansvarsområden. Riskhantering sker även lokalt på varje avdelning, i linjen samt genom en övergripande omvärldsbevakning. Rönndahl på IF menar att försäkringsbolag ligger i framkant med riskhantering jämfört med andra branscher, vilket överensstämmer med tidigare forskning där riskhanteringslösningar sägs ha sitt ursprung i bland annat den aktuariella

branschen. Informationssäkerheten ses som en fristående del hos Länsförsäkringar och där IT-risker hanteras hos organisationens alla olika länsbolag samt divisioner individuellt. Myndigheten hanterar risker på handläggarnivå utan en särskild avdelning och där ledning är involverad vid beslut. En funktion finns som har till uppgift att integrera verksamhetskrav med IT-satsningar.

5.1.1 Standarder & Ramverk

Varför ska organisationer använda standarder och ramverk för riskhantering och informationssäkerhet? Standarder och ramverk identifierar inte själva risken, men som Simister (2000) beskriver det bidrar de till en enhetlig bild, metodiskt samt systematisk arbete, konsekvent tillvägagångssätt och korrekt hantering av information mellan partners och andra organisationer. von Solms (1999) menar att i och med utbredningen av sammanlänkade IT-system skapar standarder och ramverk ett förtroende företagen emellan. Företag X anser att standarder är viktiga för kontrollen av korrekt informationshantering dels för att det skapar väl underbyggda argument för varför kontroller ska utföras. Likaså anser Rönndahl på IF att standarder är viktiga för kontrollen, men vederbörande ser även fördelar i större möjligheter till kvalitetsbedömning, benchmarking och identifiering av nya affärsmöjligheter. Rosenquist på Länsförsäkringar menar att standarder är bra då de kan anpassas efter organisationen, att det som är relevant tas med och resten kan bortses ifrån. Trots att myndigheten i studien inte är sammanlänkade med andra system ses standarder som en underlättning vid samarbete med andra organisationer och speciellt vid internationella samarbeten.

De standarder som nämns i tidigare forskning är bland annat COSO, COBIT, ISO 17799 och ITIL. Enligt von Solms (1999) är standarder till för att skapa en säker IT-miljö av säkra IT-system genom en korrekt informationshantering. ISO är den mest använda av fallstudieorganisationerna, medan majoriteten hade fått influenser från de andra standarderna. Företag X är SOX-compliant och använder av den anledningen COSO och COBIT. Myndigheten har i en del fall högre säkerhetskrav än vad som innefattas av ISO 17799, standarden har därför kompletterats baserat på det egna regelverket. ISO 17799 handskas av IT-avdelningen i samtliga organisationer i studien där ansvaret för att kontrollera och följa upp ligger hos antingen IT-säkerhetschef eller informationssäkerhetschef. Intervjupersonen på myndigheten nämner att det är svårt att få tekniker och utvecklare motiverade att använda sig av standarden på grund av den

byråkrati det medför. Standarder ger en gemensam säkerhetsgrund för organisationer vid sammankoppling av IT-system menar von Solms (1999). Detta tankesätt går även hand i hand med Galloway & Funstons artikel (2000) om att företag med god riskhantering skapar marknadsfördelar samt marknadsvärde genom att vara en riskkapabel organisation och på så sätt får marknadens förtroende. Företagen i studien är samtliga sammankopplade med utomstående IT-system medan myndigheten inte är det. Företag X ställer i huvudsak samma krav på sina samarbetspartners som SOX-lagstiftningen ställer på dom, men beroende på graden av samarbete och säkerhetsrisk lättas kraven i vissa samarbeten. IF har som krav att deras samarbetspartners ska följa avtalade internationella standarder samt att de även har krav på max tillåtet driftavbrott där samarbetet avser affärskritiska processer. Länsförsäkringar har rutiner för hur systemen ska sammankopplas, vilka kräver att de externa parterna måste följa specifika regler för att en sammankoppling ska vara möjlig.

Enligt Hong et al. (2003) finns det idag brist på teoretiska ramverk gällande informationshantering. Författaren menar att en blandning av vedertagna teorier, som kontingensteorin och riskhanteringsteorier är den bästa utgångspunkten för en effektiv informationssäkerhetshantering. IF har ett sådant tänk som kännetecknas av ett strategiskt arbete och där organisationen försöker att skapa en riskkultur genom att involvera sina medarbetare i linjen. Företaget X har inte lika uttalad riskhantering och där divisionerna ha en större kontroll över hanteringen. Informationssäkerhetshanteringen sker ur två perspektiv. Huvudkontoret har hand om det övergripande medan divisionerna får sköta det som direkt påverkar dem. SOX har tidigare påverkat mycket av arbetet och därför befinner sig företaget i en förändringsfas. Länsförsäkringar har en mer koncentration kring finansiella risker och inte samma riskkultur som IF har. Detta beror på att informationssäkerheten inte integreras i den övriga riskhanteringen. Myndigheten har ingen organisatoriskt del som sköter riskhanteringen. Riskhanteringen ses mer som en funktion än en avdelning, men som fortfarande är integrerad i den operationella hanteringen.

5.1.2 Regelverk

Riskhantering och informationssäkerhet inom organisationer påverkas av de regelverk som bolagen måste följa. Vissa regelverk riktar sig till särskilda branscher eller riskområden medan andra är mer generella. (Luthy & Forcht 2006) Ett av fallstudieföretagen är SOX-compliant på grund av amerikansk lagstiftning. En kommande lagändring gör att företaget inte längre är skyldiga att följa SOX, men företaget har ändå valt att fortsätta följa SOX i de avseenden det tillför värde i organisationen. IF följer Solvency II, Svensk kod för bolagsstyrning och instruktioner från Finansinspektionen. Länsförsäkringar måste följa regelverken Solvency II, svensk lag, Finansinspektionens instruktioner i likhet med IF, men även Basel II då de har en bankverksamhet. Den svenska myndigheten använder sig av egenutvecklat regelverk och svensk lag.

5.1.3 Integrering

Ett utav de problem som denna uppsats är ämnad att undersöka är huruvida informationssäkerheten integreras med övrig operationell riskhantering i verksamheten. Enligt Bandyyopadhyay ska organisationer försöka att integrera IT:n med riskhanteringen och den operationella hanteringen. Detta ska ske på olika nivåer i organisationen, interorganisatoriskt nivå, organisatoriskt nivå och applikationsnivå. Mannings & Gurney (2005) menar att definitionen på operationella risker kan skilja sig mellan olika branscher, men att informationssäkerheten som inkluderar exempelvis bedrägerier, arbetsmiljösäkerhet, klient-, produkt- samt affärstillämpningar ska vara en del av de operationella riskerna. Företaget X har en fristående informationshantering men har integrerat den finansiella riskhanteringen med informationssäkerheten. Företaget X anser själva att förhållandet kan te sig en aning komplext då informationssäkerheten återfinns i båda grupperna av risker. IF däremot har en tydlig uppdelning mellan IT-riskerna och en väl integrerad informationssäkerhet, medan Länsförsäkringar inte ser informationssäkerheten och IT:n som en del i den operationella riskhanteringen. Myndighet däremot ser informationssäkerhet som en del av de operationella riskerna.

5.1.4 Ledningens involvering

Ledningen har för lite kontroll över informationssäkerheten eftersom de enligt Mitchel et al. (1999) endast ser det som en teknisk fråga. Istället bör en optimal riskhantering styras av en ledning som har möjligheten att basera sina beslut rörande IT-säkerhet på kunskap enligt von Solms synsätt. IT-säkerhet har tidigare fokuserat på den fysiska säkerheten, själva IT-systemet, nu är det större krav på den operationella hanteringen av information menar Gerber et al. (2001) vilket kräver ett nytt förhållningssätt. Företaget X och IF har en ledning som är involverad i riskhanteringen, medan ledningen för myndigheten endast är involverad vid beslutfattande. Hos Länsförsäkringar visar ledningen inte något större intresse för informationssäkerheten och det råder viss okunnighet kring ämnet. Prioriteringen är olika, men operationella risker är enligt IF de största riskerna och de risker som har störst negativ inverkan. Företag X och Länsförsäkringar däremot fokuserar mer på de finansiella riskerna. Inom myndigheten prioriteras verksamhetsmässiga risker högre om de medför negativa effekter. Samtliga organisationer i studien har stor fokus på informationssäkerheten där Företag X har en IT-chef i ledningen, IF och Länsförsäkringar har CIO sittandes i ledningen, men myndigheten saknar en IT-chef i ledningen på grund av en starkt hierarkisk organisation.

5.2 Enkätundersökning

84 % av enkätbolagen svarade att de arbetade med riskhantering ur både ett finansiellt och operationellt perspektiv medan endast 11 % arbetade enbart med operationell riskhantering. 42 % svarade att de inte enbart arbetade med informationssäkerhet ur ett tekniskt perspektiv, utan även ur ett organisatoriskt. Mitchel et al. (1999) menar att ledningen oftast förlitar sig på IT-avdelningen och bortser från de organisatoriska riskerna informationssäkerheten kan medföra. Informationssäkerheten återfinns oftast i de operationella riskerna. Hela 63 % av respondenterna svarade att deras bolag hade en medelmåttig fokusering på informationssäkerhet. Endast 21 % bolagen ansåg sig ha en hög fokus på informationssäkerhet. Gerber et al. (2001) menar att tyngdpunkten i säkerhetstänkandet har flyttats från fysiska datortillgångar till informationstillgångar och därav behöver företag säkra informationen genom nya angreppssätt och ställa högre krav på informationssäkerheten.

De standarder och ramverk som enkätbolagen använder sig utav är de som har belysts under teorikapitlet 2.1 & 2.2. Dessa standarder har varit COSO, COBIT, ISO 17799 och ITIL. Mer än 37 % av de undersökta bolagen tillämpade tre eller flera standarder, medan fem bolag inte använde någon standard eller ramverk alls. von Solms (1999) menar att det blir allt vanligare att företag och andra organisationer sammanlänkar sina IT-system med varandra vilket ökar kraven på informationssäkerhet. Han menar vidare att, likaväl som företaget själva måste inneha ett säkert system är det lika viktigt att de sammankopplade systemen har en likvärdig säkerhetsnivå och därav betydelsen av standarder.

Bandyyopadhyay et al. (1999) menar att det är viktigt att organisationer ser informationssäkerheten som en del i den övriga riskhanteringen. 68 % av de undersökta bolagen har delvis integrerat informationssäkerheten i den övriga riskhanteringen, medan resten helt integrerat informationssäkerheten. Enligt enkäten var det viktigare att ha ett strukturerat arbetssätt vid riskhanteringen än vid informationssäkerheten. Närmare 63 % av bolagen ansåg att det var mycket viktigt att ha ett strukturerat riskhantering, medan 26 % ansåg det som relativt viktigt. 53 % av bolagen ansåg däremot att det var mycket viktigt att ha strukturerad informationssäkerhetshantering, medan 42 % bolag såg det som relativt viktigt. De förstnämnda 53 procenten var de bolag som använde två eller flera standarder för riskhanteringen och informationssäkerheten. Robinson (2005) menar att effektiv IT-styrning är handling från ledningens sida och att IT-styrningen ska vara en del av organisationens riskhantering. von Solms (1999) menar vidare att ledande befattningshavare ska sättas sig in i informationssäkerhetsfrågor och bli medvetna om vad som ingår i IT-säkerhet. Målet med detta är att befattningshavarna ska kunna basera sina beslut på kunskap. Enkäten visade att mer än 53 % av bolagen hade ansvarig person för informationssäkerheten med i ledningen.

6 Resultat

Nedan presenteras först resultatet av den kvalitativa undersökningen påföljd av den kvantitativa enkätundersökningen. Det viktigaste ur analysen sammanfattas nedan för att sedan sättas i relation till uppsatsens syfte samt referensram.

Syftet med denna uppsats är att identifiera de undersökta organisationernas riskhantering avseende informationssäkerhet samt hur den prioriteras i förhållande till organisationernas övriga riskhantering. Tabellen nedan visar identifieringen som genomförts på organisationernas riskhantering avseende informationssäkerhet. Fokuseringen i tabellen grundas på den teoretiska referensramens oberoende variabler.

Tabell 6.1: Sammanställt resultat, kvalitativ studie
Tabellen visar de undersökta organisationernas koppling till den teoretiska referensramens oberoende variabler.

	Företaget X	IF	Länsförsäkringar	Myndighet
Standard & Ramverk	COSO, COBIT, ISO 17799. Viktiga för kontrollen.	Influerade av alla standarder och ramverk. Tillämpar ISO 17799 huvudsakligen. Kontroll och nya affärsmöjligheter	ISO 17799/27001, COBIT och ITIL. Bra då de kan anpassas efter organisationen.	ISO 17799. Underlättning vid samarbete.
Regelverk	SOX-compliant.	Solvency, ”Koden” och Finansinspektionen.	Solvency, Basel II och Finansinspektionen.	Egenutvecklat och svensk lag.
Integrering	Delvis fristående informationssäkerhet.	Integrerad informationssäkerhet i riskhanteringen samt de operationella riskerna.	Fristående informationssäkerhet.	Informationssäkerheten som en del av de operationella riskerna.
Ledningens involvering	Involverad.	Involverad i allra högsta grad.	Ej involverad.	Endast vid beslut.

Beträffande prioriteringen av informationssäkerhet skiljer den sig åt i de undersökta organisationerna. Två av organisationerna har operationell riskhantering och informationssäkerhet som hög prioritet, medan de två övriga har en högre prioritet på den finansiella riskhanteringen. Riskhanteringen skiljer sig åt mellan de intervjuade organisationerna. Hur arbetet utförs varierar beroende på organisationsstruktur och kärnverksamhet. De två försäkringsbolagen har samma kärnverksamhet, men organisationsstrukturen skiljer sig åt vilket påverkar tillvägagångssättet vid riskhantering och informationssäkerhet.

Majoriteten av enkätbolagen använder standarder och ramverk och där samtliga bolag har en helt eller delvis integrerad informationssäkerhet i riskhanteringen. COSO ERM och ISO 17799 är de mesta använda ramverk/standard hos de undersökta organisationerna. Vidare sitter den ansvariga för informationssäkerheten med i ledningen i mer än hälften av organisationerna, vilket visar ledningens involvering. Av de bolag som ingår i enkätundersökningen svarade mer än hälften av dem att fokuseringen eller prioriteringen var medelmåttig gällande informationssäkerhet. Endast en femtedel av bolagen har en hög fokusering på informationssäkerhet. Majoriteten av bolagen anser att det samtidigt är mycket viktigt att ha strukturerat arbetssätt vid riskhanteringen samt informationssäkerheten vilket visar på standardernas och ramverkens betydelse. Mindre än hälften av enkätbolagen arbetar med informationssäkerhet ur ett organisatoriskt perspektiv, medan resten endast arbetar ur ett tekniskt perspektiv.

Identifiering samt prioritering av riskhanteringen med fokus på informationssäkerhet har urskiljts hos de undersökta organisationerna. Av de sammanlagda svaren ur uppsatsens kvalitativa samt kvantitativa metod kan det konstateras att det råder en jämn fördelning mellan organisationerna i vilken ordning finansiella respektive operationella risker prioriteras. Informationssäkerheten är en del av de operationella riskerna och har därmed en högre prioritet i de organisationer där de operationella riskerna sätts framför de finansiella.

7 Slutsats

Slutsatserna i följande avsnitt avser den totala studien vilket inkluderar både den kvalitativa och den kvantitativa undersökningen.

Uppsatsens problemformulering lyder enligt nedan:

- **I vilken utsträckning används ramverk och standarder för informationssäkerhet hos företag i Sverige?**
- **Integreras informationssäkerheten med operationell riskhantering i verksamheten?**

Svenska organisationer har insett vikten av standarder och ramverk samt vilka fördelar de kan ge. Bättre kontroll, möjlighet till att identifiera nya affärsmöjligheter och ökad säkerhet är faktorer som ligger till grund för användandet av ramverk och standarder. Ramverk och standarder används i stor utsträckning av svenska organisationer. ISO 17799 är den mest frekvent använda standarden. COSO ERM är det mest använda ramverket för riskhantering och COBIT används näst intill lika frekvent. Andra ramverk och regelverk som till viss del används av organisationerna är ISF, SOX och FIRM. Användandet av standarder och ramverk visar på en hög fokusering på informationssäkerhet.

Vad gäller integreringen visar resultatet att organisationerna till viss del integrerat informationssäkerheten i riskhanteringen medan endast åtta organisationer anser sig ha integrerat informationssäkerheten helt och hållet. Tidigare studier visar att informationssäkerheten bör integreras helt i riskhanteringen, detta i relation till undersökningen visar att svenska organisationer är på god väg, men har fortfarande inte nått till full integrering. Ledningens involvering och kunskap leder till en bättre riskhantering enligt tidigare forskning. Organisationer verkar idag ha en önskan samt insett betydelsen av att involvera ledningen i informationsriskhanteringen, men alla har ännu inte tillämpat det i praktiken. Det kan slutligen konstateras att svenska organisationer i överlag bör satsa mer resurser på integrering av informationssäkerheten i den operationella riskhanteringen samt att involvera ledningen i arbetet för att uppnå en säkrare och effektivare informationshantering.

8 Diskussion

I följande avsnitt reflekteras och diskuteras uppsatsens forskningsanknytning samt den kritiska granskningen av uppsatsens validitet och reliabilitet. Slutligen presenteras förslag till vidare forskning kring ämnet.

8.1 Forskningsanknytning

Riskhantering och informationssäkerhet är ämnen som ständigt är under utveckling. Organisationer verkar idag vara mer fokuserade på informationssäkerhet än vad tidigare forskning har visat. Den tidigare forskningen uttrycker behovet av att informationssäkerheten bör gå från en teknisk fokusering till en mer organisatorisk inställning för att skapa en säkrare miljö. De organisationer som integrerat informationssäkerheten i sin riskhantering har visat, att hur informationen hanteras av individer är minst lika viktigt som det tekniska perspektivet.

I tidigare studier, som ligger till grund för uppsatsen, uttrycker forskare ett behov av större engagemang för informationssäkerhet från ledningen, delvis för att de ska kunna basera beslut kring informationssäkerhet på kunskap men även för en bättre inblick i säkerhetsarbetet. Resultatet visade att den tidigare forskningen inte helt och hållet är legitim, då studien visar att drygt hälften av organisationerna har en involverad ledning. Organisationerna verkar ha insett vikten av ledningens involvering och därav resultatet. Detta kan författarna endast anta då studien inte har en hög generaliseringsnivå.

Utbudet av standarder och ramverk antas ha ökat i antal och blivit bättre under det senaste decenniet. Detta antagande baseras delvis på de teorier som anser att dåvarande ramverk varit bristande och inte omfattande nog, men även på de organisationer som medverkade i studien. Organisationerna visade på en väl utvecklad informationssäkerhetsriskhantering med en bra kombination av flera ramverk och standarder som de anpassar till sina säkerhetskrav.

8.2 Kritisk granskning

Resultatet påverkas av respondenternas olika kunskapsområden, bakgrund samt befattningar både vad gäller den kvalitativa och den kvantitativa undersökningen. Exempelvis besitter en risk manager stor kunskap inom den övergripande riskhanteringen inom organisationen, men är kanske inte lika insatt inom informationssäkerhet som en informationssäkerhetschef. Respondentens befattning kan ha bidragit till att svaren på frågorna inom respondentens huvudområde är mer omfattande. För att förebygga fenomenet har följdfrågor ställts vid kortfattade svar, däremot har detta inte varit möjlig vid enkätundersökningen. Hur pass utbredd riskhanteringen är i en organisation är bland annat beroende på vilken kärnverksamhet som bedrivs. Försäkringsbolag har exempelvis på grund av att de hanterar kunders pengar, större krav på sig från regelverk och tillsynsmyndigheter än en producerande organisation. Även organisationsstrukturen påverkar riskhanteringen då en allt för komplex struktur försvårar den. Författarna anser slutligen att organisationer med god riskhantering är mer benägna att svara på enkäten än organisationer med bristfällig riskhantering.

8.2.1 Validitet

Validiteten anser författarna som relativt hög då väl insatta personer har intervjuats på de undersökta organisationerna. För en högre validitet hade nyckelpersoner på fler avdelningar kunnat intervjuas inom samtliga organisationer. Lämpliga avdelningar skulle kunna vara ledningen, IT-avdelningen samt riskhanteringsavdelningen. Uppsatsens slutsatser skulle på så sätt få en högre giltighet. Validiteten gällande enkäten kan inte garanteras då författarna inte kunnat kontrollera om respondenterna tolkat frågorna korrekt.

8.2.2 Reliabilitet

Reliabiliteten antas som låg då författarna inte kan garantera att samma resultat erhålls vid senare tillfälle. Reliabiliteten gällande enkätundersökningen kan inte antas som hög då en efterkontroll, av att personer med rätt befattning har svarat på enkäten, inte kunnat genomföras. Svarsfrekvensen hade kunnat bli högre om påminnelser för enkätundersökningen hade skett via telefon istället för e-post, vilket hade lett till en högre tillförlitlighet och en högre generaliseringsnivå.

8.3 Förslag till vidare forskning

- Vilka faktorer ligger till grund vid val av standarder och ramverk för informationssäkerhet och används dessa standarder och ramverk fullt ut?
- En studie på organisationer som måste tillämpa regelverk, i syfte att kartlägga regelverkens inverkan på informationssäkerhet.
- En jämförande studie mellan ledningens uppfattning av sin involvering i informationssäkerheten och IT-avdelningens uppfattning.
- Djupare och mer omfattande enkätundersökning på samtliga börsbolag för möjlighet till generalisering.
- En fallstudie i hur operationell riskhantering sker i praktiken genom hela organisationen.

Referenser

Andersen, H. (1990) Vetenskapsteori och metodlära, ss. 70, 92, Studentlitteratur Lund.

Bandyopadhyay K., Mykytun P.P & Mykytyn K. (1999). *A framework for integrated risk management in information technology.* Management Decision, 37/5 1999, ss.437-444.

Barua, A., Kriebel C.H. & Mukhopadhyay T. (1995), *Information Technologies and Business Value: An Analytic and Empirical Investigation.* Institute for Operation Research and the Management Sciences.

Berinato, Nov. 1, 2004 Issue of CIO Magazine. (Elektronisk) Tillgänglig: <http://www.cio.com/archive/110104/risk.html> (2007-03-21.13:12).

Computer Sweden (2004). *”Säkerheten har flytta upp på ledningsnivå”* 04-09-10 (Elektronisk) Tillgänglig: <http://computersweden.idg.se/2.2683/1.24896>, (2007-03-20. 14:08).

Computer Sweden (2001). *”Varning för teknikfokusering”* 01-04-06 (Elektronisk), Källa: Affärsdata, Tillgänglig: <http://www.ad.se.till.biblextern.sh.se/> Sökord: ”Informationssäkerhet” (2007-03-21.14:38).

COBIT, *”Cobit 4.0, Control objectives, management guidelines, maturity models”*. (Elektronisk) Tillgänglig:<http://www.isaca.org/Template.cfm?Section=Downloads7&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=63&ContentID=13742> (2007-04-17. 15:29).

COSO, (2004 a), *Enterprise Risk Management – Integrated Framework, Executive Summary*. (Elektronisk) Tillgänglig som .pdf: <http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf > (2007-03-21.13:09).

COSO, (2004 b), *Enterprise Risk Management – Integrated Framework, Executive Summary*. (Elektronisk) Tillgänglig som .pdf: <http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary_Swedish.pdf > (2007-04-19. 11:36).

Denscombe, M. (2000). *Forskningshandboken*, ss. 203, 244, 204, 251&283, 282, Studentlitteratur, Lund.

Galloway D. & Funston R. (2000). *The challenge of enterprise Risk Management.* Balance Sheet, vol. 8, no. 6, 2000, ss. 22-25.

Gerber M., von Solms R., Overbeek P. (2001). *Formalizing information security requirements*. Information Management & Computer Security, 9/1 2001, ss. 32-37.

Hong K-S, Chi Y-P, Chao R. L. & Tang J-S. (2003). *An integrated system theory of information security management.* Information Management & Computer Security, 11/5 2003, ss. 243-248.

Illing, M. & Paulin, G. (2005) *Basel II and the cyclicality of bank capital, Canadian Public Policy / Analyse de Politiques*, Vol. 31, No. 2. (Jun., 2005), ss. 161-180.

ISO, a. *“ISO in brief”*. (Elektronisk) Tillgänglig som .pdf: <http://www.iso.org/iso/en/prods-services/otherpubs/pdf/isoinbrief_2006-en.pdf > (2007-04-17. 13:23).

ISO, b. *"Information technology -- Security techniques -- Code of practice for information security management"*. (Elektronisk) Tillgänglig: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3= (2007-04-18. 19:48).

ITIL, *"About itil"*. (Elektronisk) Tillgänglig: < http://www.itil.co.uk/about.htm> (2007-04-18. 14:34).

Kubitscheck, V. (2000). *Risk Management: finding the value within.* Balance sheet, vol 8, no 5 ss. 38-41.

Luthy D. & Forcht K. (2006). *Laws and regulations affecting information management and framework assessing compliance.* Information Management & Computer Security, vol. 14, no. 2, 2006, ss. 155-166.

Manning S., Gurney A. (2005). *Operational risk within an insurance market*. Journal of Financial Regulation and Compliance, Vol. 13 No. 4 2005, ss. 293-300.

Mitchel R. G., Marcella R. & Baxter G. (1999). *Corporate information security management; refereed article.* New Library World, vol. 100, no. 1150 1999, ss.213-227.

Patel, R. & Davidsson, B. (2003). *Forskningsmetodikens grunder*. ss. 98-99, Studenlitteratur Lund.

Robinson N. (2005). *IT excellence starts with governance.* Journal of investment compliance, vol. 6, no. 3 2005, ss. 45-49.

von Solms, R. (1999). *Information security management: Why standards are important.* Information Management & Computer Security, 7/1 1999, ss. 50-57.

Ruane, J. M., (2005). *A och O i samhällsvetenskaplig forskning*, Studentlitteratur Lund.

Simister T. (2000). *Risk Management: the need to set standards.* Balance Sheet, vol. 8, no. 4, 2000, ss. 9-10.

Statskontoret 1997:29a. *Handbok I IT-säkerhet.*

Svensk kod för bolagsstyrning (2004). (Elektronisk) Tillgänglig som .pdf: <http://www.bolagsstyrning.se/files/docs/Svensk_kod_f%F6r_bolagsstyrning.pdf > (2007-03-21: 14:14).

Widerberg, K. (2002). *Kvalitativ forskning i praktiken.* ss. 15-17, Studentlitteratur Lund.

Wills, M. (1999). *Personal communication, in URN 99/699 (New), Protecting Business Information – Overview*. Department of Trade and Industry, London.

Bilagor

Bilaga 1 - Intervjufrågor

1. Hur många anställda har företaget?
2. Finns det någon riskhanteringsavdelning?
3. Var i organisationen sker den huvudsakliga riskhanteringen (fokus på operativa risker)?
4. Följer ni något regelverk gällande styrning? (SOX, Basel II)
5. Hur involverad är ledningen i riskhanteringen?
6. Hur mycket av riskhanteringsarbetet redovisas i årsredovisningen?
7. Hur ser riskindelningen ut?
8. Vad ska riskhanteringen leda fram till (kostnadsbesparningar, nöjda aktieägare etc)
9. Hur ser prioriteringen ut, baserad på indelningen?
10. Hur ser företaget säkerhetsorganisation ut?

11. Hur stor fokus ligger på informationssäkerheten?
12. Är informationssäkerhet en integrerad del av den traditionella riskhanteringen?
13. Var placerar ni informationssäkerheten i riskhanteringen?

14. Följer ni något speciellt ramverk eller standard (COSO, COBIT, ISO 17799)? Vilken i så fall?
15. Varför just denna standard eller varför ingen alls (egenutvecklad)?
16. Har IT-avdelningen hand om den i så fall?
17. Sitter IT-chefen med i ledningsgruppen?

18. Vilka risker kan företagets system vara utsatt för?
19. Hur säkerställer ni att dessa risker förebyggs och med säkerhetsarbetet?
20. Är organisationens IT-system sammankopplat med ett utomstående system? Om ja, vilka krav ställer ni på det systemet?
21. Vad är nackdelarna med att inte använda sig av standarder och ramverk?

Bilaga 2 – Undersökta Large-capbolag

Bolag	Hemsida	Huvudkontor
Lundin Petroleum	www.lundin-petroleum.com/sve/	
Vostok Nafta SDB	www.vostoknafta.com	Ej HQ i Sverige
Boliden	www.boliden.com	
Holmen	www.holmen.com	
SCA	www.sca.com	
SSAB	www.ssab.se	
Alfa Laval	www.alfalaval.se	
Assa Abloy	www.assaabloy.com	
Atlas Copco	www.atlascopco.com	
Hexagon	www.hexagon.se	
NCC	www.ncc.info	
PEAB	www.peab.se	
SAAB	www.saab.se	
Sandvik	www.sandvik.com	
Scania	www.scania.com	
Securitas	www.securitas.com	
Skanska	www.skanska.com	
SKF	www.skf.com	
Autoliv	www.autoliv.com	
Eniro	www.eniro.com	
Nobia	www.nobia.se	
Axfood	www.axfood.se	
Hakon Invest	www.hakoninvest.se	
Elekta	www.elekta.com	
Getinge	www.getinge.com	
Meda	www.meda.se	
Nobel Biocare	www.nobelbiocare.com	
Q-med	www.q-med.com	
Castellum	www.castellum.se	
Carnegie	www.carnegie.se	
Fabege	www.fabege.se	
Hufvudstaden	www.hufvudstaden.se	
Industrivärden	www.industrivarden.se	
Investor	www.investorab.com	
JM	www.jm.se	
Kaupting Bank	www.kaupthing.net	
Kinnevik	www.kinnevik.se	
Kungsleden	www.kungsleden.se	
Latour	www.latour.se	
Lundbergföretagen	www.lundbergs.se	
Melker Schörling	www.melkerschorlingab.se	
OMX	www.omx.se	
Ratos	www.ratos.se	
Handelsbanken	www.handelsbanken.com	
Öresund	www.oresund.se	
Lundin mining	www.lundinmining.com	

Stora Enso	www.storaenso.com	
ABB	www.abb.com	
SAS	http://www.sasgroup.net	
Seco Tools	www.secotools.com	
Trelleborg	www.trelleborg.com	
Volvo	www.volvo.com/group/sweden/sv-se	
electrolux	www.electrolux.com	
HM	www.hm.com	
Husqvarna	www.husqvarna.com	
MTG	www.mtg.se	
Oriflame	www.oriflame.com	
Swedish match	www.swedishmatch.com	
Astra Zeneka	www.astrazeneca.com	
Nordea	www.nordea.com	
Old mutual	www.oldmutual.com	Ej HQ i Sverige
SEB	www.sebgroup.com	
Swedbank	www.swedbank.se	
Ericsson	www.ericsson.com	
Lawson software	www.lawson.com	
Nokia	www.nokia.com	Ej HQ i Sverige
Tieto enator	www.tietoenator.com	
Millicom	www.millicom.com	Ej HQ i Sverige
Tele2	www.tele2.com	
TeliaSonera	www.teliasonera.se	

Bilaga 3 – Enkätfrågor

1. Hur många anställda arbetar på företaget?

○ 1-50 ○ 51-250 ○ 251-

2. Arbetar ni med riskhantering?

○ Finansiellt ○ Operationellt ○ Både och ○ Inget

3. Arbetar ni med informationssäkerhet ur ett organisatoriskt perspektiv (inte enbart ur ett tekniskt perspektiv)?

○ Ja ○ Nej ○ Vet ej

4. Hur stor fokus ligger på informationssäkerhet? (1=låg fokus & 6=hög fokus)

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

5. Följer ni någon riskhanterings- eller/och informationssäkerhetsstandard/ramverk?
(Kryssa för flera alternativ om ni följer flera metoder enligt nedan)

☐ COSO ERM ☐ COBIT ☐ ISO 17799 ☐ GMITS ☐ ITIL

Annan ☐ Inget

6. Till vilken grad integreras informationssäkerheten med övrig riskhantering i verksamheten?

○ Helt ○ Delvis ○ Fristående

7. Hur viktigt anser ni att det är att ha ett strukturerat arbetssätt vid riskhantering? (1=inte alls & 6=mycket viktigt)

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

8. Hur viktigt anser ni att det är att ha ett strukturerat arbetssätt vid informationssäkerhet?(1=inte alls & 6=mycket viktigt)

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6

9. Sitter den ansvariga för informationssäkerheten med i ledningsgruppen?

○ Ja ○ Nej

Tack för din tid!

Sänd

Tryck på knappen ovan för att sända enkäten!

Siwertz & Tehrani 2007