Instutitionen för Ekonomi
Industriell Ekonomi FEC 635
Kandidatuppsats 10p
Våren 2003

Är ISO standarder något intressant för alla företag?

Författare: Anne Johansson
Ineska Silajdzic

Handledare: Hervé Corvellec
Leif Holmberg

Sammanfattning

Rubrik	Är ISO standarder något intressant för alla företag?
Typ	Kandidatuppsats i industriell ekonomi
Tidpunkt	Vårterminen 2003
Författare	Anne Johansson Ineska Silajdzic
Handledare	Leif Holmberg
Problem	Är ISO standarder något intressant för alla företag?
Syfte	Förklara vad ISO standarderna är, intresse, spridning och hur det prioriteras i företag. Förklara varför företag väljer att inte certifierar sig, utan använder sig av standardernas riktlinjer.
Avgränsningar	Det finns många standarder, men vi har valt att gå djupare in på ISO 9 000, ISO 14 000 och ISO 17 000. Vi vill se hur företag förhåller sig till certifieringarna mot de olika standarderna.
Metod	För att uppnå syftet med uppsatsen har vi utifrån både primär och sekundärdata, inhämtat material för att redogöra och beskriva varför företag använder sig av de tre standarderna. Genom en enkätundersökning med nyckelpersoner inom de fyra utvalda företagen har vi samlat in data för att kunna analysera.

Slutsats Arbetet har lett fram till att vi kan urskilja vissa samband.

- Företag väljer hellre att använda sig av standardernas riktlinjer istället för att certifiera sig.
- Externa och interna intressenter har inga höga krav på företaget när det gäller certifiering mot standarderna, i synnerhet ISO 14 000 och ISO 17 000.
- Företag väljer att göra egna informationssäkerhetssystem istället för att certifiera sig mot ISO 17 000.
- Företag väljer att avvakta med certifiering mot ISO 17 000, tills marknaden kräver det.

Nyckelord ISO 9 000, ISO 14 000, ISO 17 000.

Definitioner:

SS 62 77 99-2: Benämns för enkelhetens skull som ISO 17 000.

ISO 17 000: Ett ledningssystem, verktyg, för företaget eller organisationer att styra och kontrollera informationsflödet.

ISO 9 000: Ett ledningssystem för kvalitet som ska hjälpa företag att samordna tekniska, administrativ och mänskliga faktorer

ISO 14 000: Ett ledningssystem för miljö är ett verksamhetssystem för företag och organisationer som vill bedriva ett effektivt och strukturerat miljöarbete.

SIS: Swedish Standards Institute

SWEDAC: Styrelsen för ackreditering och teknisk kontroll

LIS: Projektgrupp på SIS.

SFK: SFK Certifiering AB är helägt av Svenska Förbundet för Kvalitet, som är ett ideellt förbund med ca 3000 medlemmar i Sverige. SFK Certifiering grundades 1992 och är ackrediterat av SWEDAC för att utföra systemcertifieringar.

Innehållsförteckning

1. INLEDNING

1.1 Bakgrund 1
1.2 Problemdiskussion 3
1.3 Problemformulering 4
1.4 Syfte 4
1.5 Avgränsningar 5
1.6 Målgrupp 5
1.7 Disposition-läsanvisningar 5

2. METOD

2.1 Val av ämne 6
2.2 Val av metod 6
2.3 Insamling av material 7
2.3.1 Insamling av sekundärdata 8
2.3.2 Insamling av primärdata 8
2.4 Bortfall 10
2.5 Intervjuaren 10
2.6 Respondenten 10
2.7 Källkritik 10

3. TEORI

3.1 Inledning 12
3.2 Certifiering 12
3.2.1 Regler vid certifiering 13
3.3 SIS 13
3.4 Ackreditering 13
3.5 ISO Standard 14
3.6 ISO 9000 15

3.7 ISO 14 000 16
3.8 Vad är informationssäkerhet 17
3.8.1 ISO 17 000 17
3.9 Fördelar med ISO certifiering 18
3.9.1 Fördelar med ISO 9 000 19
3.9.2 Fördelar med ISO 14 000 21
3.9.3 Fördelar med ISO 17 000 21
3.10 Nackdelar med ISO certifiering 21
3.11 Möjligheter med ISO certifiering 22

4. FALLSTUDIE 23

5. ANALYS

5.1 Analys av argumenten för användning av enbart riktlinjer eller en certifiering 30
5.2 Analys av informationshantering i företag 34

6. SLUTSATS 35

KÄLLFÖRTECKNING 37

BILAGOR

Bilaga 1 Enkät med kommentarer
Bilaga 2 ISO 9 000 delstandarder
Bilaga 3 ISO 14 000 delstandarder

1. Inledning

I detta kapitel behandlas uppsatsens bakgrund, problemdiskussion och problemformulering. Vidare behandlas syfte och avgränsning. Kapitlet avslutas med en disposition-läsanvisning.

1.1 Bakgrund

De senaste åren har det förts en diskussionen kring företags situation, som ofta handlat om vilken inverkan den ständiga förändringen i världen har.
Det gör att det föreligger en viss osäkerhet som driver företaget att ständigt ta åt sig av nytänkande. Det är naturligtvis positivt eftersom företag skapar nya möjligheter till ständiga förbättringar.
Standarder har existerat en längre tid och berör alla i företaget, både internt och externt.. Vissa äldre standarder används fortfarande medan andra har tagits bort eller utvecklats. Standarder ges ut av olika standardiserings Institutioner runt om i världen som samarbetar för samma mål.
ISO, International Organization for Standardization, är en världsomfattande sammanslutning av nationella standardiseringsorgan (ISO: s medlemmar) som ger ut standarder och dess riktlinjer.
(http://www.sis.se/DesktopDefault.aspx?tabId=21)
1977 publicerades första ISO 9000 serie och har sedan hållits uppdaterad och utvecklat nya delstandarder. De olika delstandarderna har utvecklats för att hjälpa företag av alla typer och storlekar. Standarder kan hjälpa företag att samordna faktorer för att ge förtroende hos kunder och marknaden.
Med åren har det blivit allt viktigare för olika slags företag att begränsa sin påverkan på miljö, därför publicerades man 1996, ISO 14000 serie. Delstandarder ska hjälpa företag att bättre organisera sitt miljöarbete. (Brunson, Nils & Jacobsson, Bengt, *Standardisering*, 1998)
Genom engagemang i det internationella standardiseringsarbetet kan enskilda företag påverka framtida regler och krav för sina produkter och tjänster. Samtidigt

får de tidigt information om vilka önskemål marknaden kan ha och vad myndigheterna kan komma att kräva. *(SIS broschyr)*
I media och i olika standard informationsblad framställs det att standarder är bland det bästa för företaget när det gäller styrning, kontroll och kundtillfredsställelse. I början av arbetet hade vi därför en tanke att undersöka varför företag använder sig av standarder. Efter en kort period visade sig att de företag som vi har valt att studera inte är certifierade mot någon standard, utan använder sig av dess riktlinjer.

Vi kontaktade i början 40 företag där det visade sig att endast 10 företag var villiga att ställa upp i vår undersökning. Anledning till det kan vara att företag inte vill avslöja att de inte är certifierade utan att de enbart använder sig av standardernas riktlinjer. Det kan bero att företag var rädda att vi gjorde en undersökning åt en organisation och därmed få de att framstå som en dålig organisation.
Av de 10 företag som ställde upp i vår undersökning valde vi ut fyra företag att analysera närmare. Urvalet vi gjorde baseras på hur fullständiga svar vi fick och graden av samarbetsvilja från företagen. I och med att inga av dessa fyra företag är certifierade mot de standarder som finns beskrivna i vår teori, var vi tvungna att omformulera vårt syfte. Vårt syfte nu är att undersöka om ISO är något för alla.

1.2 Problemdiskussion

Företag kan certifiera sig mot ett antal olika standarder i hopp om att öka sin stabilitet på marknaden. Vanligaste är att företag certifierar sig mot ISO 9 000 för att uppnå en god kvalitet på sina varor och tjänster. Sedan kan företag gå vidare och certifiera sig mot de övriga standarderna, vanligtvis ISO 14 000. På detta sätt integreras de flera standarder i företaget. Är detta nödvändigt? Måste företaget vara certifierade för att uppnå kvalitet och resurseffektivitet?

Om man väljer att implementerar standarder i företag kommer det vara bra, kommer alla att följa den och se till att den fungerar?

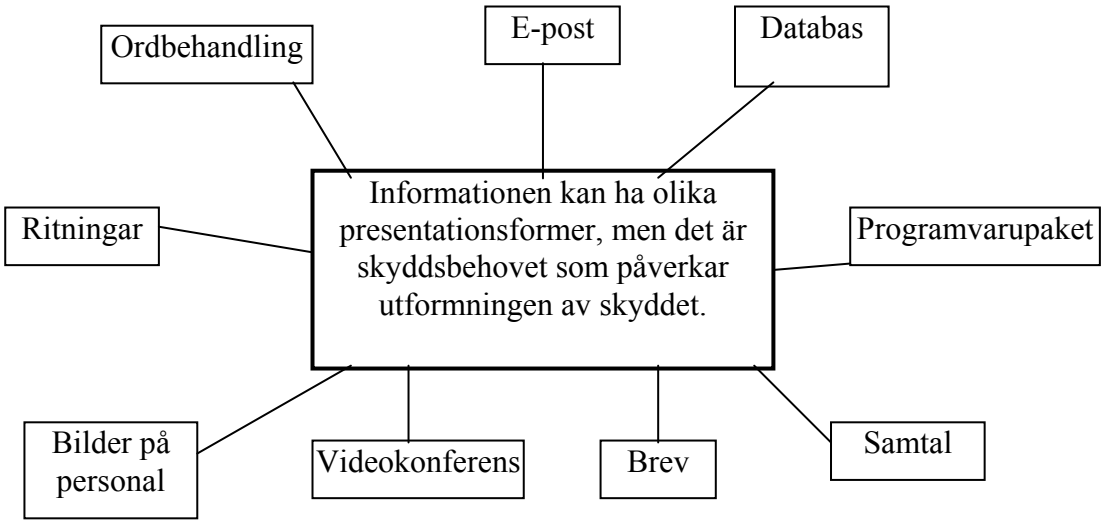
Vad är det som påverkar ett företag att inte certifierar sig? Kan det vara att man uppnå samma fördelar genom att använda sig av standardernas riktlinjer och undviker nackdelarna som en certifiering innebär?

Vilket behov svarar det till om företag väljer att använda sig av riktlinjerna istället för att certifierar sig? Certifierar sig företag bara för att framstå som en bra verksamhet i marknadens ögon? Om omvärlden tvingar fram en certifiering kan detta bli en nackdel för företaget?

Att säkerställa informationen i företaget har varit en svår uppgift. Målet är att hitta en jämvikt mellan kostnader och säkerheten för att få det bästa informationsskyddet till så låg kostnad som möjligt. (SIS handbok, *Ledningssystem för informationssäkerhet*, 2001)

I dagens läge är det i företags intresse att skydda sin information. Därför ökar intresset för standarden ISO 17 000 ledningssystem för informationssäkerhet. Anledningen till det är att få förtroende från intressenter att både företagets och kundernas information inte sprids till obehöriga. (SIG Security, *Riktlinjer för god informationssäkerhet*, 1997)

Information förekommer i många olika former. Den kan bland annat vara tryckt, skriven, elektroniskt lagrad, skickad via post, e-mail eller muntlig (se nedanstående figur nummer 1). Oavsett vilken form den har ska den alltid ha ett acceptabelt skydd.



Figur 1 (Källa: SIG Security, *Riktlinjer för god informationssäkerhet*, 1997, sid 21)

1.3 Problemformulering

Är ISO något intressant för alla företag?

1.4 Syfte

Syftet med uppsatsen är

- Se företagens intresse för ISO standarder
- Att förklara vad ISO standarder är och hur de är uppbyggda.
- Förklara varför företag väljer att inte certifierar sig, utan använder sig av standardernas riktlinjer.

1.5 Avgränsningar

Det finns många standarder, men vi har valt att gå djupare in på ISO 9 000, ISO 14 000 och ISO 17 000. Vi vill se om det är intressant för företag att använda sig av eller att certifierar sig mot ISO standarderna.

1.6 Målgrupp

Uppsatsen riktar sig i första hand till ekonomi och teknikstuderande på Högskolan Kristianstad. Samtidigt vänder vi oss till övriga intressenter och hoppas att de genom vårt arbete blir mer medvetna om standarderna.

1.7 Disposition-läsanvisningar

Kapitel 1: Här redovisar bakgrund, problemdiskussion samt problemformulering. Vidare behandlas syfte, avgränsningar och målgrupp.

Kapitel 2: Här redovisas val av ämnet och metoden. Vidare beskriver vi vårt tillvägagångssätt vid insamling av primärdata och sekundärdata. Kapitel avslutas med bortfall, intervjuaren och respondentens inverkan på arbetet samt källkritik.

Kapitel 3: Här beskriv de tre standarderna och institutioner som har inverkan på standarderna. Vi beskriver fördelar, nackdelar samt möjligheter med certifiering.

Kapitel 4: Här redovisas resultatet av vår fallstudie som gjort på fyra företag genom enkätundersökning.

Kapitel 5: Här analyserar vi insamlad primärdata och sekundärdata, i form av utförd fallstudie. Diskussionen förs om företags behov av certifieringar mot standarder.

Kapitel 6: Innehåller slutsats.

2. Metod

I detta kapitel diskuterar vi upplägget på vårt arbete. Vi beskriver den metoden vi valt att använda oss av och hur vi har gått tillväga till färdig uppsats. Vidare behandlar vi val av sekundär-primärdata samt tillvägagångssättet vid enkätundersökningen. Kapitlet avslutas med bortfall, intervjuaren, respondenten och källkritik av använt material.

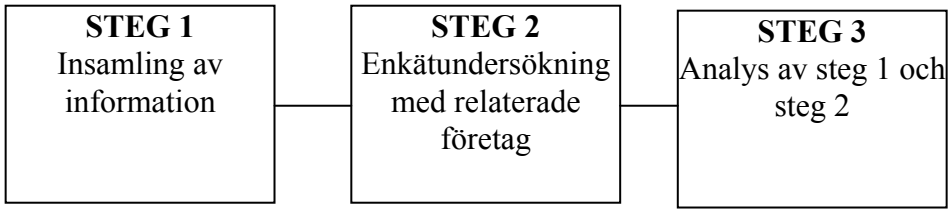
2.1 Val av ämne

Vårt intresse för ISO standarder väcktes när vi läste kursen kvalitetsteknik under vårterminen 2002. Kursen gav oss endast en ytlig förståelse av ISO standarder, men samtidigt fångade den vårt intresse.
Genom Framtidsdagen på Kristianstad Högskola fick vi kontakt med KPMG. På deras hemsida hittade vi ett intressant ämne som handlade om ISO 17 000 och dess inverkan på företaget. Vi valde att utveckla frågeställningen till att undersöka hur företag ställer sig till de olika standarderna. Vi koncentrerade oss på de tre största ISO standarderna: ISO 9 000, ISO 14 000 och ISO 17 000.
Av LIS, en projektgrupp hos SIS, fick vi en lista på företag som är i någon grad intresserade av ISO standarder.

2.2 Val av metod

Val av metod och angreppssätt sker utifrån att hitta en lösning till ett problem. Andra faktorer kan påverka valet av metod eller angreppssättet bland annat tid och ekonomi men även undersökarens kunskaper och värderingar.
Man kan välja att antingen göra en kvalitativ eller kvantitativ metod. Med kvalitativ metod skapar man en djupare förståelse av de problem man studerar. Om man använder sig av den kvantitativa metoden, samlar man mycket data om problemet, men går inte in på djupet. (Anderssen Ib *Den uppenbara verkligheten- Val av samhällsvetenskaplig metod, 1998*)
Vi kommer att använda oss av en kvalitativ undersökningsmetod som är en metod som går ofta mer på djupet än på bredden.

Anledning till val av kvalitativ datainsamlingsmetod är att vi inte tänker använda av oss siffror och beräkningar utan istället analysera utifrån talade och skrivna informationskällor.
Vår metod består av tre olika steg:



- Elektroniska källor
- Publicerade källor
- Opublicerade källor
- Tidskrifter

I steg 1 ska vi samla relevant teori om ISO 9 000, ISO 14 000 och ISO 17 000. Här kontaktar vi LIS för att få insikt i standarderna. Vidare kommer vi att använda oss av elektroniska, publicerade och opublicerad källor.
Steg 2 består av empirisk undersökning som vi ska genomföra. Undersökningen genomförs genom enkät med de utvalda företagen.
Steg 3, som är det sista steget i vår metod, ska innehålla en analys av steg 1 och steg 2 samt en slutsats där vi sammanställer vårt resultat.

2.3 Insamling av material

När vi började samla in material hade vi endast en vag uppfattning om vad de olika standarderna var och vad certifieringarna innebar.
Det finns två olika metoder att samla i data, primär och sekundärdata. De två metoderna ligger till grund för vårt arbete.

2.3.1 Insamling av sekundärdata

Sekundärdata kallas även andrahandsdata eftersom materialet redan finns. Den samlade vi in genom att ta kontakt med LIS. De har varit mycket samarbetsvilliga och hjälpsamma med att förse oss med material, bland annat broschyrer över de standarder vi använt oss av och de företag som är inblandade i projektet.
När vi sökte information som visade de negativa faktorer som standarder innebär, blev sökningen svårare än väntat. Fördelar med de olika standarderna var mycket lättare att finna än nackdelarna.
Högskolebibliotekets databaser har varit en källa för den litteratur och ett flertal av de artiklar som vi samlat in om det aktuella ämnet, ISO certifieringar.
De elektroniska källorna som till exempel Internet har varit till stor hjälp vid insamling av material.

2.3.2 Insamling av primärdata

Primärdata som är data som man själv samlar in genom att använda sig av flera olika datainsamlingsmetoder.
När man ska samla in datamaterialet kan man gå tillväga på olika sätt:

1. Intervjuer
   - besöksintervjuer
   - telefonintervjuer

2. Enkäter
   - postenkäter
   - gruppenkäter
   - besöksenkäter

Vilken metod man väljer påverkas av de yttre förutsättningarna som till exempel tid, plats, kostnad och antal undersökningsobjekt. Det som är gemensamt för alla insamlingsmetoderna är att frågeformuläret och intervjufrågorna måste vara väl

genomtänkta för att minska risken för missförstånd. (Anderssen Ib *Den uppenbara verkligheten- Val av samhällsvetenskaplig metod, 1998*)

Genom att skicka en förfrågan via e-mail till 40 olika företag om intresse att delta i enkäten, kunde vi utifrån intresset välja de företag vi ansåg var lämpligast. Det visade sig att endast 10 företag var intresserade att delta i vår undersökning. Anledningen till bortfallet kan vara att företag inte vill avslöja att de har valt att inte certifierar sig, utan använder sig av riktlinjer. En annan orsak kan vara att företag är rädda att vi utförde undersökningen för en organisation och därmed få dem att framstå som sämre än de som är certifierade.

Av de 10 företag som ställde upp i vår undersökning valde vi ut fyra företag att analysera närmare. Urvalet vi gjorde baseras på hur fullständiga svar vi fick och graden av samarbetsvilja från företagen.

Vi sammanställde en enkät som vi sedan skickade via e-mail tillsammans ett introduktionsbrev, till tre tjänsteföretag och ett byggföretag. Anledningen till valet var att se om det fanns någon skillnad eller likhet mellan de olika branscherna och om storlek var påverkande faktor.

Introduktionsbrevet hade som mål att ge respondenten en god bild av vad undersökningens syfte var. För att garantera att respondenten var så sanningsenlig som möjligt, garanterade vi anonymitet.

För att bevara en positiv relation med samarbetsvilliga företag, skickade vi ut tackbrev.

Enkäten består av tre delar:

- Den första delen innehåller allmänna frågor om företag och den intervjuade.
- Den andra delen innehåller djupingående frågor som har som mål att ta reda på vilka orsaker som finns att inte certifierar sig mot standarderna och vilka konsekvenser blir om man väljer att avstå.
- Den tredje delen innehåller kompletterande frågor till företag där certifiering mot de tre ISO standarderna, inte är aktuellt. Orsaken till det är att få en djupare insikt i ämnet.

Enkäten, kommentarer och våra förväntningar på resultatet finns i bilaga 1.

2.4 Bortfall

Antalet svar på vår förfrågan blev inte som förväntat. Att det var så få som svarade kan bero på att företag är ovilliga att dela med sig av information angående styrning och säkerhet. Vissa intervjuade var inte ens villiga att förklara anledningarna att inte ställa upp på intervjun.
Av de 40 enkäter vi skickade ut, fick vi enbart 10 svar utav vilka vi använda oss av fyra. Anledningen till vårt beslut att använda oss av fyra är att de var fullständiga och gav mest information om det valda ämnet.
Vi fick inga bortfall på de kompletterande frågorna. En orsak till att de tio företagen svarade på de kompletterande frågorna kan vara de tackbrev som skickats ut till de intervjuade.

2.5 Intervjuaren

Intervjuaren spelar en viktig roll när det gäller insamling av svaren och påverkan på respondenten. Vi valde att använda oss av e-mail vid enkätundersökningen för att minska vår påverkan på svaren samtidigt som respondenten gavs god tid att besvara frågorna.

2.6 Respondenten

Respondenten kan avsiktligt eller oavsiktligt ge felaktig information och på så sätt ge ett missvisande resultat. Vi har förtydligat i vårt introduktionsbrev att respondenten ska undvika att svara på frågor där de har bristande kunskap.

2.7 Källkritik

När man kritiskt granskar källor kan data beskrivas utifrån begrepp som validitet, reliabilitet och relevans. Graden av validitet visar om den valda metoden verkligen mäter det den ska. Man kan inte med säkerhet säga att den insamlingsmetod vi använde oss av var den bästa. Reliabilitet bedömer om datan är korrekt och trovärdig (Lekvall P & Wahlbin C, *Information för*

marknadsföringsbeslut, 1993). Genom den valda undersökningsmetoden anser vi att reliabiliteten är hög. Respondenten fick frågor via e-mail samt större tidsram med mindre press vilket betyder att respondenten ger genomtänkta svar.

Informationen är relevant om den är användbar för alla. Vid utformandet av enkäten tog vi oss tid för att säkerhetsställa att frågorna vi ställde var relevanta enligt vårt syfte genom att se till att varje fråga som vi ställde hade ett syfte bakom sig. Under arbetets gång fick vi ändra inriktning på vårt syfte, vilket betydde att vi skickade ut kompletterade frågor till berörda företag. På detta sätt hoppas vi få relevant information.

3. Teori

I detta kapitel behandlas teorier om standarder ISO 9000, ISO 14 000 och ISO 17 000. Standarders fördelar, nackdelar och möjligheter.

3.1 Inledning

Standard är inget nytt påfund, utan har existerat inom det amerikanska försvaret sedan 1950-talet. Den har sedan spridit sig till flera olika områden och länder. Vissa äldre standarder används fortfarande medan andra har tagits bort eller utvecklats. (Brunsson, Nils & Jacobsson, Bengt, *Standardisering*, 1998).
Företag påverkas av det som händer i samhället. En standard kan sägas vara ett slags råd eller regel som om vad som är lämpligt, tillåtet i vissa situationer.
*”Standard: Ett dokument upprättat i samförstånd och fastställt av erkänt organ, som för allmän och upprepad användning ger regler, vägledningar eller egenskaper för aktiviteter eller deras resultat, i syfte att nå största möjliga reda i visst sammanhang. (*http://www.ltc.se/aktuella_projekt/infosak/certifiering.htm)
Företagsstandarder handlar ofta om hur företaget ska finna sina speciella uppgifter eller affärsidéer, hur de ska uppnå bättre intern styrning och kontroll samt hur de ska bli mer rationella.

3.2 Certifiering

Certifiering har förekommit långt innan ISO 9000 serien först publicerades. På 1970-talet utfärdade ASME (American Society for Mechanical Engineers) certifikat för sin standard för kvalitetssystem (Brunsson, Nils & Jacobsson, Bengt, *Standardisering*, 1998)
För att certifiera sig måste företaget uppnå vissa krav. De ska ha ett system som uppfyller kraven i den standarden som ska tillämpas. Vidare ska systemet vara väl beskrivet, underhållas löpande samt tillämpas i den vardagliga verksamheten.
(http://www.ltc.se/aktuella_projekt/infosak/certifiering.htt)
När företag beslutar att certifiera sig mot en standard tar det kontakt med SIS, för att få information om vilka krav som finns. Vidare kontaktas ackrediterat

certifieringsföretag till exempel SWEDAC för att se om det uppfyller de krav som finns för att uppnå en certifiering.

3.2.1 Regler vid certifiering

Med hjälp av existerande regler, införs en väl genomtänkt kvalitetspolicy som ska sätta upp både realistiska och mätbara mål för företag samt uppföljningen av dem. Detta kommer inte att fungera tillfredsställande om inte företagsledningen och anställda inom företaget är engagerade samt har samarbetsvilja i frågan. Det är i företagsledningens ansvar att förmedla informationen vidare i företaget så att alla känner engagemang, ansvar och delaktighet i kvalitetsarbetet.

3.3 SIS (Swedish Standards Institute)

SIS är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Tillsammans med CEN (European committee for standardization), har de tagit fram cirka 16 000 gällande standarder. Genom att delta i standardiseringsarbetet kan svenska företag och svenska myndigheter påverka detaljstandarderna inom sin marknad.
(http://www.sis.se/DesktopDefault.aspx?tabId=21)
SIS uppgift är också att utarbeta nationella standarder samt att verka för användning av och informera om betydelsen av standarder.
(http://www.sis.se/DesktopFront.aspx)

3.4 Ackreditering

I Sverige är SWEDAC, Styrelsen för ackreditering och teknisk kontroll, en central myndighet under Utrikesdepartementet med uppgifterna att verka som nationellt ackrediteringsorgan samt att ansvara för kontrollfrågor enligt lagen om teknisk kontroll. SWEDAC ger som myndighet råd och information samt ger ut föreskrifter inom sitt verksamhetsområde.
(http://www.swedac.se/sdd/System.nsf/(GUIview)/index.html, SIG Security, *Riktlinjer för god informationssäkerhet*, 1997)

3.5 ISO Standard

ISO, International Organization for Standardization, är en världsomfattande sammanslutning av nationella standardiseringsorgan (ISO: s medlemmar). Utarbetandet av internationella standarder görs normalt inom ISO: s tekniska kommittéer som bildades 1979. Internationella företag, statliga och icke statliga som har samarbetat med ISO deltar även i arbetet i framställning av standarder. De förslag till nya standarder som utarbetas av tekniska kommittéer måste godkännas av 75 % av ISO: s medlemmar. (http://www.iso.org/iso/)

3.6 ISO 9000

”ISO 9000 består av internationellt överkomna principer och krav för hur verksamheter skall skötas för att ge förtroende hos kunder och marknad. ” (http://www.sis.se/DesktopDefault.aspx?tabname=@iso9000&menuItemID=1580) Första ISO 9000 serien publicerades 1977 och har sedan dess uppdaterats och utvecklat nya delstandarder.

De olika delstandarderna utgör tillsammans olika moment i ett kvalitetssystem för produktionsprocess. I bilaga 2 finns en lista över ISO 9 000 delstandarder. (http://www.sis.se/DesktopDefault.aspx?tabname=@iso9000&menuItemID=121)

Standarden ska hjälpa företag att samordna tekniska, administrativa och mänskliga faktorer för att öka kundnyttan och tillfredsställa de krav och önskemål som finns. Samt uppmuntra företag till att analysera kundkraven, utveckla och styra de produktprocesser som är värdefulla för både kunden och dem själva.

Alla aktiviteter som sker i företaget ska bidra till ökad produktkvalitet både när det gäller varor och tjänster. För att kontrollera att systemet fungerar utförs först en interrevision, vidare anlitas ett ackrediterat certifieringsorgan som utför en externrevision.

I dag finns cirka en halv miljon företag världen över med utställda certifikat. Många fler arbetar just nu med införandet av kvalitetsledningssystem enligt ISO 9001.

3.7 ISO 14 000

Ett ledningssystem för miljö är ett verksamhetssystem för företag och organisationer som vill bedriva ett effektivt och strukturerat miljöarbete. Ledningssystemet utgör ett frivilligt verktyg som ska underlätta arbetet, och standarderna ger en arbetsmodell för ständiga förbättringar.
*(*www.sis.se/DesktopDefault.aspx?tabname=@iso14000&menuItemID=5845*)*

Första ISO 14000 serien publicerades 1996 och har sedan dess uppdaterats med nya delstandarder.
De olika delstandarderna utgör tillsammans olika moment i ett miljösystem för produktionsprocess. I bilaga 3 finns en lista över delstandarder i 14 000 serien.
Det har blivit allt viktigare för olika slags företag att begränsa deras påverkan på den yttre miljön. De ska kunna visa upp ett bra resultat i enlighet med deras miljöpolicy och miljömål. (EN ISO 14 000: 1996)
”Standarderna för miljöledning ger anvisningar om hur ditt företag organiserar, följer upp, utvärderar och redovisar miljöarbetet. Andra teman som behandlas i standarderna är hur man tar hänsyn till miljöaspekter i produktutvecklingen, hur man beskriver produkters miljöegenskaper samt en gemensam terminologi för området.”
*(*www.sis.se/DesktopDefault.aspx?tabname=@iso14000&menuItemID=5845*)*

3.8 Vad är informationssäkerhet?

Informationssäkerheten har tre egenskaper: sekretess, riktighet och tillgänglighet.
Sekretess: Den ska säkerställa att det endast är behöriga som har tillgång till informationen i företaget (SIS handbok, *Handbok i informationssäkerhetsarbetet*, 2002).
Behov att skydda information och program från obehöriga finns hos såväl myndigheter som företag. Det finns lagar som de måste följa till exempel skydd av personuppgifter. Vidare kan det var frivilligt hur mycket av informationen företaget väljer att skydda, beroende på krav som ställs av interna och externa intressenter.
Dåligt skydd av information och program kan medföra att:

- Personers enskilda integritet skadas
- Företagshemligheter sprids till obehöriga
- Någon obehörig kan avsiktligt eller oavsiktligt förstöra företagets data eller program
- Obehöriga kan tjäna pengar genom otillåten användning av systemet

(Statskontoret, *Handbok i IT-säkerhet* del 2, 1998)

3.8.1 ISO 17 000

”Informationssäkerhetens syfte är att skydda informationen mot en mängd olika hot för att säkerställa verksamhetens kontinuitet, minska skador på verksamheten och maximera avkastning på investerat kapital samt affärsmöjligheter.” (ISO/IEC17799: 2000 sid 7)

ISO 17 000 är ett ledningssystem, verktyg, för företaget eller organisationer att styra och kontrollera informationsflöde. Införandet av ett informationssäkerhetssystem spänner över ett helt företag och innebär även en förändring av nuvarande arbetssätt.
Standarden ger verksamheten ett handfast och praktiskt stöd att införa riktlinjer, rutiner för att hantera informationssäkerhetsfrågor på ett affärsmässigt sätt. Alltså ska den vara uppbyggd på ett sätt så att alla inblandade ska ha förståelse, kunskap och vilja att uppnå målet.
(SIS handbok, *Ledningssystem för informationssäkerhet*, 2001)

Målet med standarden är att öka medvetandet om behovet av informationssäkerhet ur ett affärs- och verksamhetsperspektiv. (http://www.iso.org/iso/)

3.9 Fördelar med ISO certifiering

Anledningen till certifiering, i de flesta fall, är krav från kunder men det finns också andra skäl. Det kan bland annat vara ett internt behov att förbättra ordning och reda samt att konkurrenterna har certifierat sig.
Nedan följer de fyra vanligaste anledningar till certifikation:

1. Krav från kunder

Företaget ska se till kundernas bästa det vill säga att kunden är nöjd med den levererade kvaliteten på varor och tjänster. Genom att certifiera sig får de en chans att visa att de aktivt arbetar med kvalitet och miljö samt att samtliga medarbetare är involverade i arbetet.
(http://www.smelink.se/startadriva/miljokval/kvalitet/kstandard/iso9000/iso9000.htm)

2. Effektivare verksamhet

En motivation för att certifiera sig är att företaget insett sina brister i rutiner och processer samt önskar att förbättra dessa. Alla i företaget ska vara delaktiga och ha tillgång till den nödvändiga informationen för att delta i utvecklingen. Om man lyckas med detta kan det innebära att styrningen bedrivs på ett bättre och mer resurssnålt sätt. Om företaget går bra kan detta leda till att de anställda känner sig tryggare som i sin tur leder till ökad trivsel.
(http://www.smelink.se/startadriva/miljokval/kvalitet/kstandard/iso9000/iso9000.htm)

3. Marknadsföringsfördelar

Genom att ha en väldokumenterad och effektiv kvalitetsstyrning får företag vissa fördelar i jämförelse med sina konkurrenter. Ur marknadsföringssynpunkt kan företaget vinna på att certifiera sig. Vidare kan det var viktigt för vissa intressenter att handla med det certifierade företaget.

(http://www.smelink.se/startadriva/miljokval/kvalitet/kstandard/iso9000/iso9000.htm)

4. Minimering av bristkostnader

Genom att införa ISO certifieringar kan företag minska kostnader kopplade till kvalitet och miljö som till exempel omarbetningar och reklamationer.
(http://www.smelink.se/startadriva/miljokval/kvalitet/kstandard/iso9000/iso9000.htm)

Genom att arbeta mot certifiering kan man få följande fördelar:

- Företag lär sig att göra rätt från början, det vill säga görs mindre antal kostsamma misstag. Även om det kan vara dyrt att införa ISO standarder så kan det leda till vinst på längre sikt.
- Man kan få ett effektivare flöde i företaget som kan leda till att det bland annat blir lättare att leverera i tid.
- Kvaliteten kan förbättras på både produkter och tjänster.
- Certifiering kan ge företag en konkurrensfördel.

(home.swipnet.se/KSSolutions/Verksamhet1-02.htm)

3.9.1 Fördelar med ISO 9 000

Ledningssystemet för kvalitet kan ge grunden för ständig förbättring för att öka tillfredsställelsen hos kunder och andra intressenter.
Fasta rutiner dokumenteras och ska finnas tillgängliga i företagets kvalitetshandbok.
Det finns åtta principer som fungerar som stöttepelare i ISO 9000 serien och som motiverar företag att certifiera sig:

Princip 1: Kundfokusering

Företaget måste inrikta sig på att få en nöjd kund och skapa mervärde. Det finns tre huvudsakliga fördelar med att överträffa kundernas förväntningar: ökad vinst, marknadsandelar och en ökad kundlojalitet.

Princip 2: Ledarskap

En god ledare ska se till att företagets syfte, inriktning och interna mål överensstämmer. Det uppnås genom att bland annat skapa engagemang hos personalen. Aktiviteter utvärderas och möjligheter ges för förbättringar.

Princip 3: Medarbetarnas engagemang

Företagens främsta tillgång är dess anställda och med deras engagemang kan man lättare uppnå sina mål. Anställda ska känna ansvar och aktivt delta i förbättringar.

Princip 4: Processangreppssätt

Om man kopplar samman resurser och aktiviteter kan man lättare uppnå effektivt resursutnyttjande, sänkta kostnader och jämnare resultat.

Princip 5: Systemangreppssätt för ledningen

Att man har givna mål och förståelse kan leda till att företaget blir effektivare och mer värdefull. Detta kan leda till ökat förtroende från intressenter.

Princip 6: Ständig förbättring

Företag är i behov av ständig förbättring för att inte förlora kunder och marknadsandelar samt ökad motståndskraft från konkurrenterna.

Princip 7: Faktabaserade beslut

För att kunna fatta effektiva och välgrundade beslut måste man ha tillgång till exakt och pålitlig information.

Princip 8: Ömsesidigt fördelaktiga relationer till leverantörer

Genom god relation med leverantörer kan företag bli mer flexibel och mindre känslig för förändringar.

(http://www.sis.se/DesktopDefault.aspx?tabname=@iso9000&menuItemID=5870
)

3.9.2 Fördelar med ISO 14 000

Alla företag, organisationer och myndigheter som vill ge ett miljömedvetet intryck kan dra nytta av de olika standarderna i ISO 14000-serien. De kan med hjälp av miljöledningssystem bättre organisera sitt miljöarbete. Standarderna kan vara ett mått för utomstående att bedöma hur väl fungerande miljöarbete ett företag har.

3.9.3 Fördelar med ISO 17 000

I dagens läge väljer vissa företag att certifiera sig mot ISO 17 000 ledningssystem för informationssäkerhet för att få förtroende från intressenter att både företagets och kundernas information inte sprids.

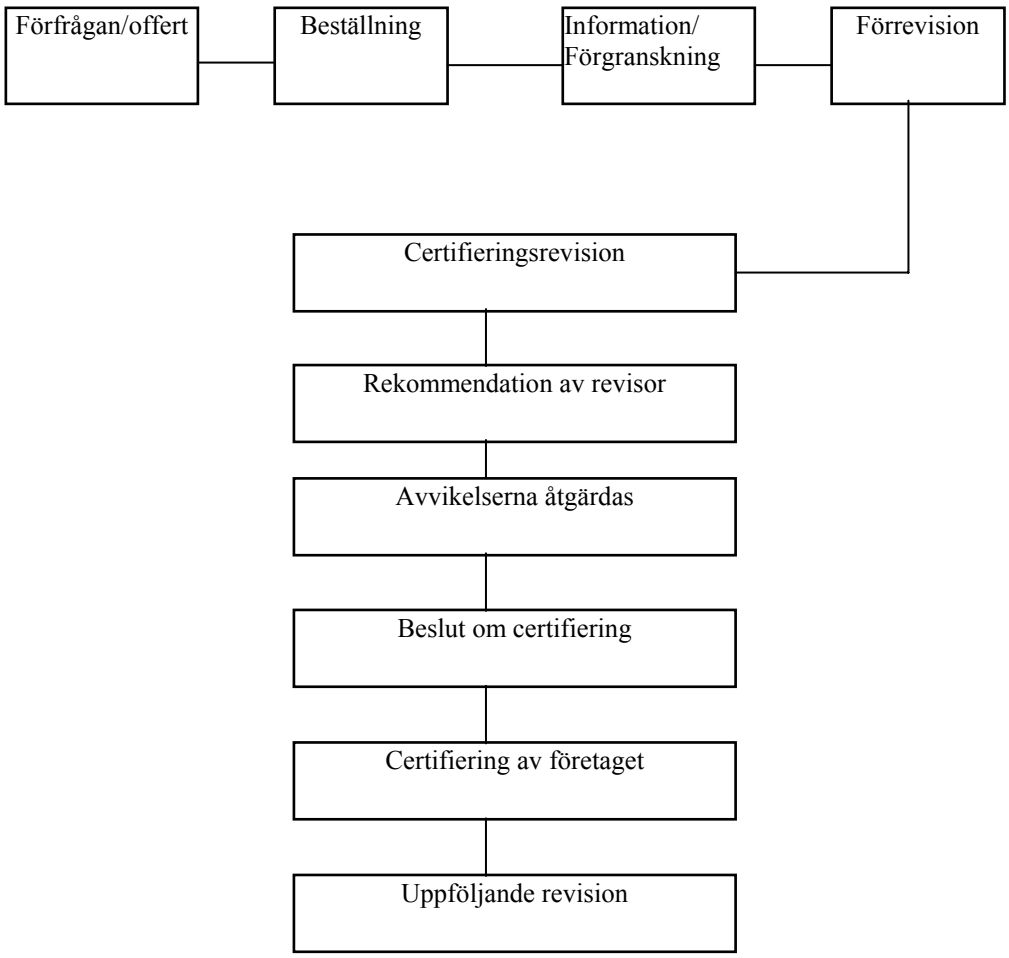
3.10 Nackdelar med ISO certifiering

När ett företag ska ta beslutet att certifiera sig måste den ta i beräkning, de risker och fallgropar som en certifiering kan innebära. Man kan få intrycket av att det enbart finns fördelar med certifiering mot olika standarder men så är inte fallet. Nedan följer några risker och fallgropar med certifiering:

- Risk att dokumentation av arbetsprocesser får stort egenvärde och blir ett mål i sig.
- Risk att dokumentation och utarbetande av procedurer tar för mycket tid och uppmärksamhet från annat viktigt arbete.
- Risk att medarbetarna inte känner sig delaktiga i systemet.
- Systemet garanterar inte ambitionsnivån i företaget.
- Risk för mycket rutinstyrning och regler som hindrar personalens utveckling.

(home.swipnet.se/KSSolutions/Verksamhet1-02.htm)

Nedan följer en figur som visar det krångliga arbetet med certifieringsprocessen.



Figur 2 (Källa:http://www.sfkcertifiering.se/cert.html)

3.11 Möjligheter med ISO certifiering

Även om företaget har infört ISO certifiering behöver det inte betyda att den ska sluta att söka möjligheter till förbättringar. Vi använder oss av uttrycket ”Den som slutar att vara bättre slutar snart att vara bra”.

Några möjligheter som finns är bland annat:

- Uppnår status gentemot intressenterna
- Att förbättra kommunikationen både internt och externt
- Tillgodose de krav som ställs av marknaden

(home.swipnet.se/KSSolutions/Verksamhet1-02.htm)

4. Fallstudie

I detta kapitel redovisas resultat av vår undersökning om företags och organisationers attityder till ISO standarder, samt intresse för informationssäkerheten. Vi sammanställer ett flertal frågor under samma rubrik och därefter redovisar vi om vad samtliga företag anser.
Anledningen till att företag är anonyma är att informationen ska inte komma i orätta händer, samt ge utrymme för våra tolkningar.

1. Kort beskrivning av de företag som medverkade i vår fallstudie

Serviceföretag 1
Är ett stort företag med 26 200 anställda och har en årsomsättning på 60,7 miljarder.
De finns i Sverige, Danmark, Norge, Finland och Baltikum.

Konsultföretag 1
Är ett medelstort företag med ett 80-tal anställda och har en årsomsättning på 70 Mkr. kr. Deras ekonomiska tillväxt ligger för tillfället runt noll.
De har kontor i Bålsta, Linköping och Uppsala, men verkar rikstäckande.
Deras affärsidé är att leverera kvalificerade IT-tjänster och produkter inom området tekniska system.

Konsultföretag 2
Är ett stort företag med 1723 anställda i Sverige och 110 000 anställda internationellt. Deras omsättning är på 2 Miljarder kr per räkenskapsår i Sverige. Årliga ekonomiska tillväxten varierar per affärsområde, ca 9 % i genomsnitt.
Konsultföretag 2 finns från norr till söder i Sverige samtidigt som den är en världsomfattande organisation.

Byggföretag 1

Är ett företag som har mål att utveckla, bygga och underhålla den fysiska miljön för att bo, resa och arbeta. Det grundades 1887 har idag ca. 75 000 anställda i koncernen och ca. 16 000 i Sverige. Deras omsättning ligger på ca 146 miljarder kr i koncernen och ca. 28 miljarder kr i Sverige. Tillväxten beror på marknadens geografiska område och varierar från –8 % -+5 %.

De har sin verksamhet i många länder runt om i världen till exempel: Storbritannien, Danmark, Ryssland, Brasilien och Moçambique.

2. Är eller har företagen varit certifierade mot någon ISO standard?

Serviceföretag 1

De har tidigare varit certifierade mot ISO 9001. För tillfället är företaget inte certifierade mot någon standard men använder sig ändå av de olika standardriktlinjer som finns.

Konsultföretag 1

Företaget är inte själva certifierade mot några standarder. Det har tidigare använts sig av ISO 9000. Vidare har konsultföretag 1 erfarenheter av Common Criteria (ISO 15 408) som de anser också är ett utmärkt verktyg för att säkerställa assuransnivån rörande olika produkter.

Konsultföretag 2

Tidigare var ett kontor certifierat enligt ISO 9000. Idag är företaget inte certifierade mot några standarder.

Byggföretag 1

Samtliga företag i koncernen är certifierade mot ISO 14 001, vilket de anser ligger "rätt" i deras bransch. Standarder ISO 9 000 och ISO 17 000 prioriteras inte i deras företag.

3. Motivation till certifiering

Serviceföretag 1

Numera är företaget inte längre certifierat mot ISO 9 000.

En av orsakerna till certifieringen var att många företag i samma bransch valde att certifiera sig och då följde med strömmen. Efter en tid upplevde de inte fördelarna som förväntats. Istället visade sig att det var för mycket arbete runt om kring och inte så stort vinst annat än internt.

Idag finns det ett intresse i företaget för ISO 17 000. Serviceföretag 1 arbetar i enlighet riktlinjerna för standarden, men har för tillfället inga planer på att certifiera sig. Det på grund av att de anser att troligtvis inte finns några direkta vinster med införandet. Däremot kan företaget uppnå interna vinster genom att använda sig av standardens riktlinjer.

Företaget har nyligen genomfört en sammanslagning med ett liknande företag. Det medför att frågor runt certifieringen mot ISO 17 000 inte är aktuella just nu. Om några år kommer troligtvis beslutet om certifiering kunna tas.

Inställningen till certifieringen av ISO 17 000 har troligtvis inte påverkats av vad andra företag inom liknande branscher har fattat för beslut.

Förhoppningarna är att en eventuell certifikation mot standarden, i framtiden ska leda till alla medverkande i företaget talar samma språk och har ett gemensamt riktmärke.

Konsultföretag 1

Företaget anser att ISO 9 000 är ett utmärkt verktyg för att skapa god ordning och ökad kvalitet, men väljer istället att ha ett eget system för styrandet av företaget. Detta på grund av för mycket arbetet, kostnader och byråkrati.

I dagens läge med låg konjunktur är det inte aktuellt med certifieringen mot nya ISO standarder. En annan anledning är att det inte finns tillräckligt med ekonomisk värde, då den kräver en del medel. Om företaget ska certifiera sig mot standarden måste investeringen på något sätt betalas tillbaka. Den möjligheten ser de inte idag, men det innebär inte att de inte arbetar med frågor rörande standarden.

Deras beslut påverkades till en viss del av vad andra inom liknande bransch har ställts sig till frågan. Hade branschen värdesatt certifieringen mot till exempel ISO 17 000 vid upphandling hade det varit ett tungt beslut, men sådana krav från deras intressenter har ännu inte dykt upp.
Med hjälp av de olika standardriktlinjer som konsultföretag 1 har använt sig av, har det bidragit till att skapa ordning och reda, samt kunskap och förståelse för egna behov och krav.
Förhoppningar angående ISO 17 000 standarden är att den ska bli accepterad i svenska näringsliv och svenskt offentlig verksamhet. Samtidigt att samtliga företag använder sig av standarden som en förutsättning för att kunna göra affärer, utbyta information med mera.
Hittills har användningen av standardens ISO 17 000 riktlinjer bidragit till större kontaktnät och har varit en dörröppnare. På längre sikt hoppas de att den ska bidra till ökade intäkter.

Konsultföretag 2
Tidigare har företaget varit certifierat mot ISO 9 000, men beslöt sig att inte gå vidare. Anledningen till det är att de anser att en certifiering innebär för mycket arbete och inga stora konkurrensfördelar. Företaget använder sig idag av standardens riktlinjer, men det har inte bidragit till mycket fördelar. Kundkretsen och marknadsandelar har blivit nästan detsamma.

Byggföretag 1
Företaget anser att deras behov är uppfyllda och har inga framtida planer på flera certifieringar. Det finns en möjlighet att beslutet kommer att omprövas om en eller flera kunder kräver en certifiering.

4. Hur organiseras företagen utan att vara certifierade mot någon av ISO standarder?

Serviceföretag 1
Trots att företaget inte är certifierat mot någon av ISO standarder, hindrar det inte de att utnyttja de fördelar som finns i användandet av standarders riktlinjer.

Konsultföretag 1

Företaget har varit tidigare certifierat mot ISO 9 000, men idag väljer de att använda sig av de riktlinjer som de olika standarderna har, för att tillfredsställa sina interna och externa intressenter.

Konsultföretag 2

Den har egna utformade program och riktlinjer som är anpassade till företaget vilka ger mycket mer kontroll.

Byggföretag 1

Idag är det inte aktuellt för företaget att certifiera sig mot några andra standarder till exempel ISO 9 000 och ISO 17 000, men de arbetar ändå utifrån standardernas riktlinjer.

5. Hur sprids informationen om de olika ISO standarderna i företaget?

Serviceföretag 1

Spridning av information angående olika riktlinjer sker genom Intranäten och föredrag. För att försäkra sig om att alla inblandade följer de rutiner och regler som finns, har företaget uppföljningar av säkerhetspersonal.

Konsultföretag 1

Spridning av kunskap om standarderna och dess riktlinjer sker genom orienteringar, utbildningar med mera. Standarders riktlinjer ska ”paketeras” för respektive behov och krav. Idag finns det inget egenvärde att göra en företagsförändring med standarder som anledning.

Konsultföretag 2

För att sprida information och kunskap använder sig konsultföretag 2 medvetet av program, tips, anvisningar samt webbsidor.

Byggföretag 1

För att kunna informera samtliga behöriga om standardens riktlinjer, har de ett koncernövergripande intranät samt att varje bolag har sitt specifika intranät. Dessutom har de sen en tid tillbaka en "Code of Conduct" som omfattar alla anställda.

6. Säkerhetsmedvetande i företagen

Serviceföretag 1

Företaget anser sig vara säkerhetsmedvetet med skydd för nästan allt som kan inträffa. Alla de anställda och underleverantörer/konsulter skriver på samma sekretessförbindelse för att de ska kunna känna sig trygga med att deras information inte ska spridas till obehöriga. Företaget vill att kunderna ska känna sig trygga med att använda sig av dem.

Konsultföretag 1

Skyddet mot obehöriga är mycket omfattande. På grund av sekretess skäl kan inte företaget kommentera utförligt frågan, då de har ett så kallat SUA- klassat företag. Vidare har de sekretessavtal med alla anställda och andra intressenter.

Konsultföretag 2

I offertsammanhang efterfrågas ibland hur företaget hanterar säkerhetsfrågor.
Styrningen i företaget har blivit effektivare genom användning av både deras egna utvecklade säkerhetsprogram och standardens riktlinjer. Istället för att certifiera sig mot ISO 17 000, har företaget utvecklats ett internationellt uppföljningsprogram med säkerhetskontroller, åtgärdsprogram och självdeklarationer.

Byggföretag 1

Företaget har sekretessavtal med anställda och leverantörer, men övrig information om hur de skyddar sin information kan inte delges till utomstående.

7. Förhoppningar angående ISO 17 000

Serviceföretag 1

Förhoppningar med införandet av standarden är att alla företag talar samma språk och har ett gemensamt riktmärke.

Konsultföretag 1

Intresse för ISO 17 000 väcktes upp under 1990-talet i samband med arbete rörande olika informationssystem. De såg stora möjligheter i standarden, genom att på bredd kunna ena företaget runt en gemensam ”best practice”. Det innebär totalt sett stora förändringar av säkerheten med en mängd positiva bieffekter.

Konsultföretag 2

Intresse för informationssäkerhet väcktes upp på sena 1980-talet. Anledningen till det var hotbilden samt att säkerhetsaspekter har börjat dominera.

Förhoppningarna angående standarden ISO 17 000 är att få systematik i säkerhetsarbete som är mer generell och internationell lättare att få accepterad.

Byggföretag 1

Byggföretag 1 började intressera sig för informationssäkerhet för ca 5 år sedan och har hoppningar att en certifiering mot standarden ISO 17 000 ska skapa en gemensam ram för säkerheten inom företaget. Det kan i sin tur leda till konkurrensfördelar. För närvarande finns det inga planer på en certifiering mot ISO 17 000, eftersom de anser att det för närvarande inte gagnar företaget.

Konsultföretag 2

Beslutet om certifieringen mot standarden ISO 17 000 fattades internationellt och på hög ledningsnivå. En omfattande internationell kommission ledde utredningsarbetet och lämnade rekommendation till ledningen.

Vidare påverkades inte beslutet av vad andra liknande företag och organisationer i samma bransch beslutade i frågan.

Även om företaget beslutade att inte certifiera sig idag, betyder det inte att de tänker sluta med sitt engagemang i frågan om certifieringen mot standarden ISO 17 000.

5. Analys

I detta kapitel har vi för avsikt att behandla och föra en diskussion kring det material som samlats in.. Kapitel ligger till grund för de slutsatser som presenteras i kapitel 6.

5.1.Analys av argumenten för användning av enbart riktlinjer eller en certifiering.

Diskussion kan föras om företagens ja eller nej till standarder. Vad blir konsekvenserna, samt kan man säga både ja och nej? Vad vinner företagen samt vad förlorar det?

Företag som väljer att säga ja kan få flexibilitet i företaget, skapa kontroll samt behålla den. En certifiering kan innebära en förbättrad image, arbetssätt, legitimitet, trovärdighet. Genom att visa att man uppfyller de krav på kvalitet på sina produkter som standarden kräver, kan man i sin tur få mer förtroende från sina kunder.

Om företagen väljer att säga nej kan orsaken vara att undvika kostnader och arbetet som krävs för att upprätthålla certifiering. Det kan även vara krångligt och stelt att certifiera sig, där företagen upplever att de förlorar kontrollen.

För företagen som sägen nej är det inte värt mödan och pengarna att använda sig av olika standarder. De upplever att de inte har behov av standarderna.

Huvudmotiven för att införa standarden ISO 9000:

- Samordna tekniska, mänskliga och administrativa faktorer
- Ständigt utvecklas och förbättras för att vara värdefulla för både de externa och interna intressenterna.
- Utveckla aktiviteterna för att få ökad produktkvalitet på sina varor och tjänster

Alla dessa motiv har som mål att på olika vis skapa konkurrensfördelar

Huvudmotiv för att införa ISO 14 000:

- Fungera som bedömningskriterier för externa intressenter och förbättra företagets image.
- Minska risken för olyckor och miljöskador

- Minska kostnaderna för utsläpp och miljöfarligt avfall

Företag ska med hjälp av standarden organisera sitt miljöarbete på bäst möjliga vis för att få konkurrensfördelar och vinna marknadsandelar.

Huvudmotiv för att införa ISO 17 000

- Ge fast och praktiskt stöd av informationshanteringen
- Skydda personernas integritet och företagshemligheter
- Rätt information ska finnas tillgänglig vid beslutstagande

Runt om i världen finns det ett stort behov av att skydda företagsinformationen från obehörigas tillträde. Samtidigt ska företaget skydda sig mot interna skador såsom sabotage och slarv.

De fyra argumenten för att använda sig av standarder, som vi beskriver i teorin, använder sig företag av idag. Fördelarna så som effektiv informationsstyrning, bra samordning, förenkling för företaget vid problemlösning, består även om man väljer att inte certifiera sig.

Vid certifiering tillkommer även ett antal nackdelar som företag måste ta med i beräkningen. Genom att enbart använda sig av de riktlinjer som standarden förespråkar kan man minska kostnader för uppdatering och underhåll av certifieringen.

Det finns många steg som företag kan använda sig av vid införande av de olika standarderna. Exempelvis uppställning av bra policy, medarbetarnas engagemang, bra ledarskap, organisatorisk säkerhet, styrning av kommunikation och drift, bra relationer med kunder och leverantörer med mera. Många företag väljer att använda sig av de här stegen, men undviker att certifiera sig. På detta sätt kan de få det bästa av standarderna, det vill säga ett fungerande företag med nöjda externa och interna intressenter.

Det finns även möjligheter med certifiering mot ISO standarder som företag kan gå miste om, när de enbart följer de riktlinjer som finns tillgängliga. Därför är det bra att företag tar i beräkning de krav och önskemål som finns på marknaden.

I teorin om ISO 9 000 står det att fördelarna med certifieringen är till exempel god ordning och ökad kvalitet på varor och tjänster. Det behåller företaget genom att följa de riktlinjer och råd som standarden föreskriver.
Nackdelar kan vara av flera olika slag så som tidskrävande dokumentation, risk för låg ambitionsnivå, dåligt engagemang samt för mycket rutinstyrning.
I fallstudien fann vi att tre av fyra företag varit certifierade mot ISO 9 000. Orsaken till att företagen inte är certifierade längre beror på för mycket arbete, stor kostnad samt inte den markanta ökningen av konkurrensfördelar som de hoppats på. Det visade sig att de nackdelar som nämnts i teorin stämmer i verkligheten.

Vi tog med ISO 14 000 i vår teori och vår enkät eftersom vi trodde att standarden hade en inverkan på företag och deras beslut. Det visade sig att endast ett av de fyra företagen som är med i vår undersökning använder sig av standarden. Orsaken till det kan vara att tre av företagen finns inom servicebranschen och ett i byggbranschen. Därmed kan vi inte dra för stora slutsatser utan ytterligare undersökningar. Även om standarden förespråkar att både tjänst och produkttillverkande företag ska kunna använda sig av den, är det inte många som gör det. En av anledningarna till det kan vara att det inte finns samma krav från interna och externa intressenter att driva ett bra miljöarbete inom tjänstebranschen. Vidare kan det vara för tidskrävande, mycket arbete med dålig lönsamhet som resulterar i att certifieringen inte prioriteras.

Organisationer och företag har många svåra beslut att ta när det gäller hur mycket eller lite skydd som är acceptabelt.
I vårt teoriavsnitt tog vi med beskrivning av ISO standarden 17 000 samt vilka fördelar och nackdelar den har för företag.
Standarden innehåller två delar varav del 1 är riktlinjer och del 2 innehåller specifikationer för certifieringen. De företag vi undersökt har valt att använda sig av del 1 och slipper då arbetet med att uppfylla de krav som ställs, men vinner de fördelarna som finns.
Våra undersökningar visar att flertalet organisationer väljer att inte certifiera sig, för närvarande, mot standarden ISO 17 000. Anledningen till beslutet kan vara det

ekonomiska tillståndet, få konkurrenter som är certifierade samt få eller inga krav från interna och externa intressenter.

Vi anser att större företag har mindre behov av certifieringen mot de olika standarderna. Anledningen till det är att de är redan väl etablerade på marknaden och inte lika påverkbara vid förändringarna. Att enbart följa de riktlinjer standarderna föreskriver kan vara tillräckligt för dem. Olika intressenter kan möjligen skapa påtryckningar och kräva att de olika standarderna införs i företag. Det kan innebära problem för företaget att certifiera sig enbart på grund av krav utifrån. Det kan möjligen skapa svårigheter eftersom standarden är inte direkt anpassad för just deras verksamhet. Störningar kan uppstå i företags olika processer när certifieringens nya regler och rutiner införs.

Företag av alla storlekar kan ha fördelar med certifieringen mot de olika standarderna om man på någon sätt har problem med styrningen, kvaliteten och säkerheten.

Mindre företag kan däremot ha flera fördelar med certifieringen på grund av att de på något sätt måste utmärka sig för att vinna konkurrensfördelar gentemot de större företagen.

I vår undersökning har det visat sig att ett företag inte behöver vara certifierat för att uppnå den kvalitet och resurseffektivitet som krävs på marknaden. Det baserar vi på att de företag som medverkat i vår undersökning är bland de största inom sin bransch.

Om företag beslutar sig att införa en ISO standard är det nödvändigt att alla i företaget följer dess rutiner och regler, samt se till att den fungerar. Det kan vara svårt att motivera personalen om certifieringen är påtvingad och anses inte nödvändig från ledningens sida. Om omvärlden tvingar fram en certifiering kan detta bli en nackdel för företaget.

Företaget kanske bara certifierar sig för att framstå som en bra verksamhet i marknadens ögon. Marknaden ska inte vara den avgörande faktorn vid en certifiering utan ska baseras på ett internt behov. När företag enbart använder sig av standardernas riktlinjer är det för deras egen skull, bland annat kvalitet och säkerhetskrav. Det ska vara bra internt för att kunna verka bra externt.

5.2 Analys av informationshantering i företag.

Teorier om styrning av information i företaget säger att den interna informationen inte har samma begränsning som den externa. Det är av stor betydelse att företag får den informationen som krävs för att uppnå en god styrning. Vi anser att begränsningar i den externa informationen hindrar företag från att lära sig av andras framgångar och misslyckande. Å andra sidan är företag tvungna att behålla företagshemligheter, så som framgångsfaktorer, för att kunna överleva på marknaden.

Om information skulle spridas till obehöriga skulle det kunna få oerhörda konsekvenser. Det beror självklart på vilket företag det skedde i och hur allvarligt angreppet var. Om ett läkemedelsföretag utsätts för en informationsstöld innan patent tagits, kan det betyda att företaget går miste om miljardbelopp. Medan mindre angrepp kan vara knappt märkbara. Med det menas inte att certifiering är den enda lösningen mot angrepp, eftersom ett företag kan uppnå en bra säkerhetsnivå utan införande av standarden ISO 17 000.

Ett av företagen som ingår i vår undersökningsstudie har valt att själv konstruera ett system för informationssäkerhet som är därmed skräddarsytt för deras verksamhet. En certifiering är inte aktuell så länge deras egna system fungerar.

Genom att följa de riktlinjer som ges kan man få ett gott resultat. En risk är att man blir för fokuserad på yttre angrepp och har en begränsad säkerhetsnivå inom företaget. Personal som antingen avsiktligt eller oavsiktligt sprider informationen till obehöriga kan skada organisationer betydligt mer än yttre hot.

Information, utbildning och kontroll är väsentligt om man ska kunna nå företagets mål och vision. Information och utbildning grundar sig på att man med hjälp av kunskap minskar risken för slarv. Genom kontroll ska man kunna finna källan för spridningen av information för att snabbt kunna åtgärda detta.

Det är fullt möjligt att styra ett företag utan att certifiera sig, men det kan tillföra andra fördelar såsom säkerhetskänsla för interna och externa intressenter. Nackdelen är att det kan vara en falsk säkerhetskänsla.

6. Slutsats

I detta kapitel redovisas de slutsats som kan dras av uppsatsen.

Slutsats som drar här baseras på de fyra företag som ingår i vår undersökning. Vi kan inte dra att för stora och betydande slutsatser av detta på grund av brist på certifierade företag i undersökningen.

Arbetet har lett fram till att vi kan urskilja vissa samband.

- Företag väljer hellre att använda sig av standardernas riktlinjer istället för att certifiera sig.
- Motiv till att inte certifiera sig är krånglighet, kostnad, mycket arbete samt rädsla för att förlora kontrollen över sitt företag.
- Externa och interna intressenter har inga höga krav på företaget när det gäller certifiering mot standarderna, i synnerhet ISO 14 000 och ISO 17 000.
- Företag väljer att göra egna informationssäkerhetssystem istället för att certifiera sig mot ISO 17 000.
- Företag väljer att avvakta med certifiering mot ISO 17 000, tills marknaden kräver det.
- Omvärldens krav på användning av standarder borde vara större. Genom att företag bara använder sig av riktlinjer och inte är certifierade, finns det mindre kontroll av hur företaget väljer att använda sig av sina resurser.

Standarden förespråkar riktlinjer för agerande vid olika händelser. Om alla företag ska göra lika hur finns det då utrymme för innovation och kreation? Om man implementerar standarden i företaget kommer det vara bra, kommer alla att följa den och se till att den fungerar? Det kan vara kostsamt för företag att införa ett nytt system, men det kan bli ännu mer kostsamt om man inför en standard som inte följs av anställda och ledning i företaget. Därför måste man skapa engagemang hos personal och ledning samt klargöra syftet med införandet.
Det kan vara svårt att motivera personalen om certifieringen är påtvingad och anses inte nödvändig från ledningens sida.

Omvärlden tvång på en certifiering kan bli en nackdel för företaget, eftersom det enbart vill framstå som en bra verksamhet i marknadens ögon. Marknaden ska inte vara den avgörande faktorn vid en certifiering utan ska baseras på ett internt behov.

Det finns en risk att företag enbart följer de riktlinjerna som ges, utan att anpassa och utveckla dessa för den egna verksamheten. Då förlorar man poängen med att certifiera sig mot en standard. Det är lätt att stirra sig blind på fördelarna. Vi drar slutsatsen att trycket från omvärlden är överskattat. Vår fallstudie som omfattade fyra företag av olika storlekar visade att man kan vara konkurrenskraftig på marknaden även om man väljer bort certifieringen.

I många företag saknas det riktlinjer för hur man ska anskaffa ny utrustning för informationsbehandling. Om det inte finns en dokumentation vilken utrustning företaget ska använda är det stort risk för missbruk av informationen. Det äventyrar i sin tur företagets affärsverksamhet.

Vidare kräver det att alla i företaget medverkar. Vi använder oss här av det berömda talesätten: Ingen kedja är starkare än dess svagaste länk. Inget system är heller säkrare än de som använder och sköter om det.

Källförteckning

Publicerade källor

Litteratur

- SIS handbok (2002). *Handbok i informationssäkerhetsarbetet*. Stockholm ISSN 0347-2019; 360

- SIS handbok (2001). *Ledningssystem för informationssäkerhet*. Stockholm ISSN 99-0275107-5

- SIG Security (1997). *Riktlinjer för god informationssäkerhet.* Stockholm ISBN 91-630-6220-8

- Brunsson, Nils & Jacobsson, Bengt (1998). Standardisering. Stockholm ISBN 91-648-0157-8

- Statskontoret (1998). Handbok i IT-säkerhet del 2. Stockholm ISBN 91-7220-298-X

- Anderssen Ib (1998). *Den* uppenbara verkligheten- Val av samhällsvetenskaplig metod. Lund

Opublicerade källor

Samtal

- Bengt Rydstedt, projektledare, SIS, 2003-04-08

- Anna-Karin Jansson, projektassistent, SIS, 2003-04-15

- Daniel Gräntz, informationsansvarig, KPMG, 2003-04-02

- Magnus Josefsson, IT-ansvarig, KPMG, 2003-05-13

Enkät

- Säkerhetschef, Serviceföretag 1, 2003-05-07, 2003-05-17

- Konsult, Konsultföretag 1, 2003-05-09, 2003-05-12

- IT-säkerhetschef, Konsultföretag 2, 2003-05-14

- IT-säkerhetschef, Byggföretag 1, 2003-04-29, 2003-05-16

Elektroniska källor

- Ifacts 2002, ISO/IEC 17799 ledningssystem för informationssäkerhet. Tillgängligt från URL: http://www.ifacts.se/Culdesac7799.pdf Accesdatum: 2003-04-02

- ltc, Att arbeta för certifiering. Tillgänglig från URL: http://www.ltc.se/aktuella_projekt/infosak/certifiering.htm Accesdatum: 2003-04-02

- ltc, Ledningssystem. Tillgänglig från URL: http://www.ltc.se/aktuella_projekt/infosak/ledningssystem.htm Accesdatum: 2003-04-02

- International Organization for Standardization. Tillgänglig från URL: http://www.iso.org/iso/ Accesdatum: 2003-04-02

- SIS, Swedish Standards Institute Tillgänglig från URL: http://www.sis.se/DesktopDefault.aspx?tabname=@iso9000 Accesdatum: 2003-04-03

- SIS, Swedish Standards Institute Tillgänglig från URL: http://www.sis.se/DesktopDefault.aspx?tabname=@iso14000 Accesdatum: 2003-04-03

- SIS, Swedish Standards Institute Tillgänglig från URL: http://www.sis.se/DesktopDefault.aspx?tabName=%40projekt&PROJID=1191&menu

  Accesdatum: 2003-04-03

- SFK Certifiering AB. Tillgänglig från Url: http://www.sfkcertifiering.se/cert.html

  Accesdatum:2003-04-13

- SWEDAC. Tillgänglig från URL:

  http://www.swedac.se/sdd/System.nsf/(GUIview)/index.html

  Acessdatum: 2003-04-13

- SIS, Swedish Standards Institute

  Tillgänglig:

  http://www.sis.se/DesktopDefault.aspx?tabname=@iso9000&menuItemID=121

  Acessdatum: 2003-04-03

- Tillgänglig från URL:

  http://www.smelink.se/startadriva/miljokval/kvalitet/kvarfor/kvarfor.htm

  Acessdatum 2003-04-03

- Tillgänglig från URL:

  home.swipnet.se/KSSolutions/Verksamhet1-02.htm

  Acessdatum: 2003-04-03

Bilaga 1.

Intervjufrågor

Allmänna frågor

1. Vad har Ni för funktion i verksamheten?

2. Hur stor är Er årsomsättning?

3. Hur många anställda har Ni?

4. Hur stor tillväxt har Er verksamhet?

Kommentar till frågorna 1-4:
De här frågorna ställdes för att få en god uppfattning av företaget och den intervjuade. Syftet med frågorna var att undersöka om företagets storlek inverkade på beslut vid certifiering.

Djupingående frågor

1. När började Ni intressera Er för informationssäkerheten?

2. Vilken motivation till införandet? Var det hotbilden, säkerheten eller konkurrenskraft?

3. Vad var visionen och förhoppningarna med införandet av standarden?

Kommentar till frågorna 1-3:
Syftet med frågorna var att se de motiven som företag har för en eventuell certifiering mot ISO 17 000. Vi förväntade att de undersökta företagen under lång tid varit engagerade i informationssäkerhetsfrågor.

4. Vad har Ni tidigare för erfarenheter av certifieringar?

5. Är Ni certifierade för andra standarder? Om ja, vilka, varför och vad har det fått för konsekvenser i personaltillfredsställelse?

6. Om Ni är eller har varit certifierade mot andra standarder (vilka i så fall), vilka har nackdelarna eller svårigheterna varit?

7. Vad har standarden fått för effekt på Er verksamhet? Har den bidragit till större marknadsandelar/ ökad kundkrets?

8. Har Ni prioriterat de olika standarderna olika? I så fall hur?

Kommentar till frågorna 4-8:

Tidigare erfarenheter kan ha spelat en stor roll när beslut om certifiering mot ISO 17 799 skulle tas. Vilka standarder företagen använder sig av och varför. Vi trodde att fler företag skulle vara certifierade mot ISO 9 000 och ISO 14 000 eftersom de är relativt välkända och har funnits under flera år.

9. Hur ska Ni gå tillväga för att certifiera Er mot standarden ISO 17 000?

10. Vad tror Ni att det kommer att få för konsekvenser om Ni väljer att inte certifiera Er mot standarden ISO 17 000?

Kommentar till frågorna 9-10:

Här ville vi få svar på hur företaget gör för att certifiera sig och vad konsekvenserna blir om man väljer att avstå. Vi förväntade att flertalet företag var villiga att certifiera sig mot standarden ISO 17 000. Resultatet blev förvånande när det visade sig att inga av de undersökta företagen är villiga att certifiera sig mot standarden idag.

11. Hur avser Ni att löpande följa upp kostnaderna för den dagliga hanteringen av standarden och hur kommer förväntade vinster att redovisas (både ekonomiska och sociala) ?

12. Vilka riktlinjer ska Ni följa? Exempelvis lagar, rekommendationer och så vidare.

13. Hur har Ni gått till väga för att sprida kunskap om standarderna och dess riktlinjer i verksamheten?

14. Hur ska Ni ändra Er organisation för att anpassa den till certifieringen?

15. Hur kontrollerar Ni att standarder följs i verksamheten?

16. Blir styrningen effektivare med hjälp av införandet av olika certifieringar? På vilket sätt märks det?

Kommentarer till frågorna 11-16:

Frågorna strukturerades upp för att vara avslutande och ge information om hur man väljer att informera, anpassa och kontrollera företaget. Förväntningar var att många företag aktivt deltog i certifieringsprocessen, men i och med att en certifiering inte är aktuell blev svaren mindre utförliga.

Kompletterande frågor (De är utformade till de företag där certifiering mot de tre ISO standaderna, inte är aktuellt)

1. Vad är anledningarna till att Ni inte är certifierade mot ISO 9 000?

2. Vad är anledningen till att Ni inte är certifierade mot ISO 14 000?

Kommentar till komoletterade frågorna 1-2:

I den första enkäten fick vi svar att tre av de fyra företagen har varit certiferade mot ISO 9 000, men numera använder sig endast av standardes riktlinjer. Vi ville veta orsaken till beslutet.

Det visade sig även att endast ett av företagen är certifierade mot 14 000. Vi ville få svar på varför de resterande företagen väljer att inte certifiera sig mot

standarden. Förväntningarna var att det ekonomiska tillståndet på marknaden påverkar företagets beslut att skjuta certifieringen på framtiden.

3. Varför är det inte aktuellt med certifiering mot standarden ISO 17 000?

4. Hur gick Ni tillväga för att ta beslutet?

5. Påverkades Ert beslut av vad andra organisationer, inom liknade branscher, tagit för beslut?

6. Har tidigare erfarenheter av certifieringar påverkar Er i beslutet?

7. Vilka var de pådrivande parterna för certifiering och vika var emot? (Ej namn, enbart vilken post som personen har i företaget)

Kommentar till de kompletterande frågorna 3-7:

Den första enkäten som skickades ut, levde inte upp till våra förväntningar. Vi trodde att flertalet företag var påväg att cetifiera sig mot ISO 17 000, men så var inte fallet. För att ta reda på orsaken till detta valde vi att skicka ut ytterligare en enkät med kompletterande frågor. Här ville vi ta reda på anledningen till att en certifiering mot ISO 17 000 inte är aktuell och vilka faktorer som var med och påverkade beslutet.

Bilaga 2.

The ISO 9000 family

The standards, guidelines and technical reports which make up the ISO 9000 family and which are listed below are available separately, or as collections. The ISO 9000 Compendium presents the ISO 9000 family in hard copy form.

Standards and guidelines	Purpose
ISO 9000:2000, *Quality management systems - Fundamentals and vocabulary*	Establishes a starting point for understanding the standards and defines the fundamental terms and definitions used in the ISO 9000 family which you need to avoid misunderstandings in their use.
ISO 9001:2000, *Quality management systems - Requirements*	This is the requirement standard you use to assess your ability to meet customer and applicable regulatory requirements and thereby address customer satisfaction. It is now the only standard in the ISO 9000 family against which third-party certification can be carried.
ISO 9004:2000, *Quality management systems - Guidelines for performance improvements*	This guideline standard provides guidance for continual improvement of your quality management system to benefit all parties through sustained customer satisfaction.
ISO 19011, *Guidelines on Quality and/or Environmental Management Systems Auditing* (currently under development)	Provides you with guidelines for verifying the system's ability to achieve defined quality objectives. You can use this standard internally or for auditing your suppliers.
ISO 10005:1995, *Quality management - Guidelines for quality plans*	Provides guidelines to assist in the preparation, review, acceptance and revision of quality plans.
ISO 10006:1997, *Quality management - Guidelines to quality in project management*	Guidelines to help you ensure the quality of both the project processes and the project products.
ISO 10007:1995, *Quality management - Guidelines for configuration management*	Gives you guidelines to ensure that a complex product continues to function when components are changed individually.

ISO/DIS 10012, *Quality assurance requirements for measuring equipment* - Part 1: *Metrological confirmation system for measuring equipment*	Give you guidelines on the main features of a calibration system to ensure that measurements are made with the intended accuracy.
ISO 10012-2:1997, *Quality assurance for measuring equipment* - Part 2: *Guidelines for control of measurement of processes*	Provides supplementary guidance on the application of statistical process control when this is appropriate for achieving the objectives of Part 1.
ISO 10013:1995, *Guidelines for developing quality manuals*	Provides guidelines for the development, and maintenance of quality manuals, tailored to your specific needs.
ISO/TR 10014:1998, *Guidelines for managing the economics of quality*	Provides guidance on how to achieve economic benefits from the application of quality management.
ISO 10015:1999, *Quality management - Guidelines for training*	Provides guidance on the development, implementation, maintenance and improvement of strategies and systems for training that affects the quality of products.
ISO/TS 16949:1999, *Quality systems - Automotive suppliers - Particular requirements for the application of ISO 9001:1994*	Sector specific guidance to the application of ISO 9001 in the automotive industry.

Bilaga 3.

The ISO 14000 family of standards, guides and technical reports – including drafts

T h e I S O 1 4 0 0 0 f a m i l y o f s t a n d a r d s

ISO 14001:1996 1996 Environmental management systems – Specification with
guidance for use

ISO 14004:1996 1996 Environmental management systems – General guidelines
on principles, systems and supporting techniques

ISO 14010:1996 1996 Guidelines for environmental auditing – General principles

ISO 14011:1996 1996 Guidelines for environmental auditing - Audit procedures
– Auditing of environmental management systems
–
ISO 14012:1996 1996 Guidelines for environmental auditing – Qualification criteria for environmental auditors

ISO 14015:2001 2001 Environmental management – Environmental assessment
of sites and organizations (EASO)

ISO 14020:2000 2000 Environmental labels and declarations – General principles

ISO 14021:1999 1999 Environmental labels and declarations – Self-declared environmental claims (Type II environmental labeling)

ISO 14024:1999 1999 Environmental labels and declarations – Type I

environmental labelling - Principles and procedures

ISO/TR 14025:2000 2000 Environmental labels and declarations – Type III environmental declarations

ISO 14031:1999 1999 Environmental management – Environmental performance evaluation – Guidelines
8 Environmental Management – 2002

ISO/TR 14032:1999 1999 Environmental management – Examples of environmental
performance evaluation (EPE)

ISO 14040:1997 1997 Environmental management – Life cycle assessment – Principles and framework

ISO 14041:1998 1998 Environmental management – Life cycle assessment – Goal and scope definition and inventory analysis

ISO 14042:2000 2000 Environmental management – Life cycle assessment – Life cycle impact assessment

ISO 14043:2000 2000 Environmental management – Life cycle assessment – Life cycle interpretation

ISO/TR 14047 Environmental management – Life cycle assessment – Examples of application of ISO 14042

ISO/TS 14048:2002 2002 Environmental management – Life cycle assessment –
Data documentation format

ISO/TR 14049:2000 2000 Environmental management – Life cycle assessment –
Examples of application of ISO 14041 to goal and scope
definition and inventory analysis

ISO 14050:2002 2002 Environmental management – Vocabulary

ISO/TR 14061:1998 1998 Information to assist forestry organizations in the use of
the Environmental Management System standards ISO
14001 and ISO 14004

ISO/TR 14062:2002 2002 Environmental management – Integrating environmental
aspects into product design and development

ISO/WD 14063 To be Environmental management – Environmental determined communications – Guidelines and examples

ISO/AWI 14064 Guidelines for measuring, reporting and verifying entity and project-level greenhouse gas emissions

ISO 19011:2002 2002 Guidelines for quality and/or environmental management
systems auditing (This standard replaces ISO 14010,
14011 and 14012)

ISO Guide 64:1997 1997 Guide for the inclusion of environmental aspects in product standards