Kompatibilitet mellan standarder inom samhällssäkerhet

– En studie av kompatibilitet mellan standarder framtagna av ISO/TC 223 – Societal Security och ISO/TC 262 – Risk Management

Tore Klarström

Division of Risk Management and Societal Safety
Lund University, Sweden

Avdelningen för Riskhantering och Samhällssäkerhet
Lunds tekniska högskola
Lunds universitet

Report 5462, Lund 2014

Kompatibilitet mellan standarder inom samhällssäkerhet

En studie av kompatibilitet mellan standarder framtagna av ISO/TC 223 – Societal Security och ISO/TC 262 – Risk Management

Tore Klarström

Lund 2014

Titel: Kompatibilitet mellan standarder inom samhällssäkerhet – En studie av kompatibilitet mellan standarder framtagna av ISO/TC 223 – Societal Security och ISO/TC 262 – Risk Management

Title: Compatibility between standards in societal security – A study of compatibility between standards developed by ISO/TC 223 – Societal Security and ISO/TC 262 – Risk Management

Author: Tore Klarström

Report: 5462
ISSN: 1402-3504
ISRN: LUTVDG/TVBB--5462--SE

Number of pages: 63
Illustrations: If not specified, by Tore Klarström

Keywords: Standardization, International Organization for Standardization, compatibility, societal security, risk management, business continuity management system, risk management framework

Sökord: Standardisering, International Organization for Standardization, kompatibilitet, samhällssäkerhet, riskhantering, ledningssystem för kontinuitetshantering, ramverk för riskhantering

Abstract: In this thesis, the compatibility between the standards developed in ISO/TC 223 – Societal Security and the standards developed in ISO/TC 262 – Risk Management, is examined. A joint qualitative method of analysis, consisting of document analysis and semi-structured interviews, is applied. With the help of an operational definition of compatibility, the study results in a coefficient of compatibility with the value 0.83, where 1 would be maximum compatibility. Some incompatibilities between standards are identified in the study, such as differing descriptions of the risk management process. Possible causes to the incompatibilities are identified, such as the fact that some standards are developed in accordance with Annex SL, while others are not. Some suggestions to handle these incompatibilities are derived, such as revising ISO 31000:2009 in accordance with Annex SL.

Riskhantering och samhällssäkerhet
Lunds tekniska högskola
Lunds universitet
Box 118
221 00 Lund

risk@risk.lth.se
http://www.risk.lth.se
Telefon: 046 - 222 73 60
Telefax: 046 - 222 46 12

Division of Risk Management and Societal Safety
Faculty of Engineering
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

risk@risk.lth.se
http://www.risk.lth.se
Telephone: +46 46 222 73 60
Fax: +46 46 222 46 12

Förord

I denna rapport avrapporteras det examensarbete som författaren har utfört under våren 2014 vid Avdelningen för Riskhantering och Samhällssäkerhet vid Lunds Tekniska Högskola. Examensarbetet består i en kompatibilitetsstudie av olika standarder på samhällssäkerhetsområdet och är en avslutande del i utbildningen som leder till en civilingenjörsexamen i riskhantering och en brandingenjörsexamen. Examensarbetet har utförts inom ramen för Program for Risk and Vulnerability Analysis Development (PRIVAD).

Examensarbetet hade inte varit genomförbart utan insatser av intervjurespondenter, hjälp från handledare och stöd från familj och vänner. Författaren vill därför rikta ett stort tack till:

Clas Herbring – Myndigheten för Samhällsskydd och Beredskap
Fredrik Pettersson – Actea Consulting AB
Hedvig Landahl – Linnéuniversitetet
Henrik Tehler – Lunds Tekniska Högskola
Omar Harrami – Myndigheten för Samhällsskydd och Beredskap
Peter Månsson – Lunds Tekniska Högskola
Stefan Tangen – Myndigheten för Samhällsskydd och Beredskap
Åsa Kyrk Gere – Myndigheten för Samhällsskydd och Beredskap.

För ypperlig handledning av examensarbetet förtjänar Peter Månsson ett särskilt stort tack.

Tore Klarström
Lund 2014

Sammanfattning

I ett samhälle där komplexitet och beroenden mellan olika samhällsviktiga funktioner ständigt ökar, samtidigt som dessa funktioner sköts av allt fler olika aktörer, växer behovet av att samhällssäkerhet och risker hanteras på ett likartat sätt i olika organisationer. Internationella standarder på samhällssäkerhetsområdet är ett försök att tillgodose detta växande behov. För att standarderna ska kunna bidra till att likrikta arbetet i olika organisationer och uppnå en samsyn på samhällssäkerhetsområdet, behöver dock dessa standarder vara kompatibla med varandra.

I denna studie undersöks kompatibiliteten mellan två viktiga familjer av standarder på området. Den ena familjen består av de standarder som har tagits fram av International Organization for Standardization (ISO), i kommittén ISO/TC 223 – Societal Security. Den andra familjen består av de standarder som har tagits fram av ISO i kommittén ISO/TC 262 – Risk Management.

Undersökningen utgår från följande frågeställningar:

- Hur kompatibla är de standarder som har tagits fram av ISO i kommittén ISO/TC 223 – Societal Security, med de standarder som har tagits fram av ISO i kommittén ISO/TC 262 – Risk Management?
- Vad är inte kompatibelt mellan dessa standarder?
- Vilka är orsakerna till att dessa standarder inte är helt kompatibla?
- Hur kan standarder på området samhällssäkerhet göras mer kompatibla?

För att besvara dessa frågeställningar appliceras en tudelad kvalitativ analysmetodik. Metoden består av dokumentanalys av standardtexterna och semi-strukturerade intervjuer med personer som antingen har varit med och utvecklat standarderna eller som har implementerat standarderna i organisationer. Med hjälp av en operationell definition av kompatibilitet resulterar studien i en kvantitativ kompatibilitetskoefficient som antar värden mellan 0 och 1. Koefficienten utgör ett mått på graden av kompatibilitet mellan standarderna. Den resulterande kompatibilitetskoefficienten mellan standarderna i studien är 0,83.

I analysen identifieras några inkompatibla inslag mellan standarderna, däribland beskrivningar av riskhanteringsprocessen, dess ingående delar och relationerna dem emellan samt beskrivningar av relationer mellan ledningssystem och processer. Möjliga orsaker till de inkompatibla inslagen identifieras. En av dessa orsaker är att standarderna i ISO/TC 223 utgår från mallen för ledningssystem i Annex SL, vilket inte är fallet med standarderna i ISO/TC 262. Några lösningar för att råda bot på de inkompatibla inslagen härleds, däribland att revidera ISO 31000:2009 utifrån Annex SL.

Summary

In a society where complexity and dependencies increases between different critical functions in infrastructure, while the different functions are run by an increasing number of different actors, there is a growing need to manage societal security and risks in a consistent manner across different organizations. International standards on societal security is an attempt to satisfy this emergent need. In order for the standards to harmonize work processes and perspectives on societal security in different organizations, the standards need to be compatible with each other.

In this thesis, the compatibility of two important families of standards on societal security is examined. One family consists of the standards developed by International Organization for Standardization (ISO) in the committee ISO/TC 223. The other family consists of the standards developed by ISO in the committee ISO/TC 262.

The study sets out from the following questions:

- How compatible are the standards developed by ISO in the committee ISO/TC 223 – Societal Security, with the standards developed by ISO in the committee ISO/TC 262 – Risk Management?
- What is not compatible between these standards?
- What are the causes to incompatibility between these standards?
- How can standards in societal security be made more compatible?

To answer these questions a two-fold qualitative method of analysis is applied. The method consists of document analysis of the texts in the standards and semi-structured interviews with individuals who have developed or implemented the standards. With the help of an operational definition of compatibility, the study results in a quantitative coefficient of compatibility with values between 0 and 1. The coefficient of compatibility constitutes a measure of the extent to which the studied standards are compatible. The resulting coefficient of compatibility between the standards in the study is 0.83.

Some incompatibilities are identified in the study, such as differing descriptions of the risk management process and the relationship between management systems and processes. Possible causes to the incompatibilities are identified. One of these causes is the fact that the standards in ISO/TC 223 are developed in accordance with a guide for management system standards, called Annex SL, while this is not the case for the standards in ISO/TC 262. Some suggestions to handle these incompatibilities are derived, such as revising ISO 31000:2009 in accordance with Annex SL.

Innehåll

1 Inledning

I denna rapport redovisas den kompatibilitetsstudie av tongivande standarder på samhällssäkerhetsområdet som författaren utför under våren 2014 vid Lunds Tekniska Högskola.

I detta kapitel beskrivs bakgrunden till studien, dess syfte, mål och frågeställningar, samt de avgränsningar som författaren har valt att göra.

1.1 Bakgrund

Standarder kan ses som generaliserade och formaliserade regler som beskriver och dokumenterar effektivitet och kontroll inom och mellan organisationer (Antonsen, Skarholt, & Ringstad, 2012). Standarder kan syfta till att förenkla och koordinera arbetsprocesser, att göra produkter och tjänster kompatibla med varandra eller att homogenisera information (Johansson & Nilsson, 2006; Chungoora et al., 2013). Utvecklingen av standarder startade under det tidiga 1900-talet då de första standardiseringsorganisationerna grundades (Johansson & Nilsson, 2006). Sedan dess har standardiserandet ständigt ökat, mycket till följd av globaliseringen och det växande handelsutbytet mellan länder och företag. Detta utbyte har nämligen ställt ökade krav på kompatibla produkter och homogeniserad information mellan organisationer (Johansson & Nilsson, 2006).

Under de senaste tio åren har det blivit allt vanligare med standardisering på samhällssäkerhetsområdet (Antonsen, Skarholt, & Ringstad, 2012). Då samhällsutvecklingen ständigt går mot fler och starkare beroenden mellan olika samhällsviktiga funktioner, samtidigt som fler av dessa funktioner sköts av olika aktörer, så uppstår ett allt större behov av att arbeta på ett likartat sätt i olika organisationer (Myndigheten för Samhällsskydd och Beredskap [MSB], 2012a; Lidberg, 2009). Internationella standarder inom samhällssäkerhet syftar bland annat till att uppnå en sådan likriktning (Lidberg, 2009). Under de senaste fem åren har International Organization of Standardization (ISO), bland annat bidragit med två viktiga ”familjer” av standarder inom samhällssäkerhet och riskhantering. Den ena familjen består av de standarder som har tagits fram i kommittén ISO/TC 262 – Risk Management och den andra familjen består av de standarder som tagits fram i kommittén ISO/TC 223 – Societal Security. De standarder som har utarbetats i kommittén ISO/TC 262 – Risk Management syftar bland annat till att harmonisera riskhanteringsprocesser i existerande och framtida standarder (ISO 31000:2009). De standarder som utarbetats i kommittén ISO/TC 223 – Societal Security syftar bland annat till att underlätta samverkan och informationsutbyte mellan olika aktörer före, under och efter en kris (Swedish Standards Institute [SIS], 2012).

Myndigheten för Samhällsskydd och Beredskap (MSB) hyser stora förhoppningar om att en gemensam grundsyn på samhällssäkerhet och fungerande samverkan mellan olika aktörer ska kunna uppnås genom standardisering på området (Myndigheten för Samhällsskydd och Beredskap [MSB], 2012b). Detta dels genom användande av själva standarderna men också genom de nätverk som skapas mellan olika aktörer i utvecklingen av standarderna (Lidberg, 2009). MSB är därför involverade i standardiseringsarbetet på såväl nationell som internationell nivå och sedan 2005 leder Sverige, genom Swedish Standards Institute (SIS) och MSB, den internationella kommittén ISO/TC 223 - Societal Security (Myndigheten för Samhällsskydd och Beredskap [MSB], 2010).

Det är viktigt att påpeka att standarder utgör frivilliga riktlinjer och således inte är tvingande (Skr. 2007/08:140). Standarder transformeras dock ofta till föreskrifter (Lidberg, 2009). Det är även viktigt att påpeka att de tekniska kommittéer som tar fram standarder är sammansatta av både offentliga och privata aktörer, där deltagare medfinansierar projekten (Myndigheten för Samhällsskydd och Beredskap [MSB], 2012c). Detta innebär att privata aktörer får direkt inflytande över standardernas utformning och kan få indirekt inflytande över lagstadgade regelverk.

Författaren anser att en grundförutsättning för att uppnå den samsyn som standarderna syftar till, är att standarderna är kompatibla med varandra, vilket också påpekas av Johansson och Nilsson (2006). Av denna anledning anser författaren att det finns en nytta med att undersöka kompatibiliteten mellan olika standarder som tagits fram inom området samhällssäkerhet.

1.2 Syfte och mål

Syftet med denna studie är att bidra till ökad kunskap om kompatibilitet mellan tongivande standarder på området samhällssäkerhet, samt att ge förslag till hur sådana standarder kan göras mer kompatibla. Kompatibilitet mellan standarder på området samhällssäkerhet är viktigt för att standarderna ska kunna bidra till en större samsyn mellan de olika aktörer som tillsammans upprätthåller en samlad krisberedskapsförmåga.

Målet med studien är att utvärdera kompatibiliteten mellan de standarder på området samhällssäkerhet, som har tagits fram av ISO i kommittéerna ISO/TC 262 och ISO/TC 223. Utvärderingen ska belysa eventuella inkompatibla inslag och deras orsaker samt tillhandahålla förslag på hur standarder inom samhällssäkerhetsområdet kan göras mer kompatibla.

1.2.1 Frågeställningar

De frågeställningar som studien söker besvara är:

- Hur kompatibla är de standarder som har tagits fram av ISO i kommittén ISO/TC 223 – Societal Security, med de standarder som har tagits fram av ISO i kommittén ISO/TC 262 – Risk Management?
- Vad är inte kompatibelt mellan dessa standarder?
- Vilka är orsakerna till att dessa standarder inte är helt kompatibla?
- Hur kan standarder på området samhällssäkerhet göras mer kompatibla?

1.3 Avgränsningar

Endast de standarder som har tagits fram av ISO i kommittéerna ISO/TC 262 och ISO/TC 223 kommer att studeras. Det finns en mängd andra standarder som också berör samhällssäkerhet i någon mån. Både standarder som har tagits fram av ISO, men också standarder som har tagits fram av andra organisationer. Eftersom MSB verkar inom ISO genom kommittén ISO/TC 223, samtidigt som myndighetens uttalade syfte att uppnå samsyn på samhällssäkerhetsområdet utgör en stor del av bakgrunden till studien, är det mest intressant att undersöka de standarder som har tagits fram av just ISO. De valda standarderna är även tänkta att utgöra ett slags huvudstandarder på området, varför det är centralt att studera just dessa.

De stora kontaktytorna mellan de standarder som har tagits fram i ISO/TC 262 och ISO/TC 223 finns i de standarder som berör ledningssystem för kontinuitetshantering och ramverk för riskhantering samt i de standarder som innehåller övergripande vokabulär och definitioner. Det är därför mest intressant att fokusera på dessa standarder i studien. De övriga standarderna som bland annat berör videoövervakningar, övningar och krishantering beaktas inte i jämförelsen. De standarder som undersöks i studien är således:

- ISO 22300:2012 - Societal Security – Terminology
- ISO 22301:2012 - Societal security – Business continuity management systems – Requirements
- ISO 22313:2012 - Societal security – Business continuity management systems – Guidance
- ISO_IEC 73:2009 Risk management - Vocabulary
- ISO 31000:2009 - Risk management – Principles and guidelines
- ISO_TR 31004:2013 - Risk Management - Guidance for the Implementation of ISO 31000.

Kompatibiliteten mellan standarderna kommer främst att undersökas genom jämförelse av olika perspektiv, definitioner och beskrivningar i själva standarderna. Olika tillämpningar av standarderna i specifika verksamheter undersöks inte. Detta då

författaren anser att kompatibilitet i implementering av standarder till stor del är en följd av kompatibilitet mellan standardtextera och att kompatibilitet på textnivå således är mer central och intressant att studera. Den operationella definition av kompatibilitet som används i studien inkorporerar ett antal men långt från alla aspekter av de standarder som undersöks. De ingående aspekterna utgör de relevanta kontaktytor som identifieras mellan standarderna.

2 Metod

Enligt Trost (2005) består studier generellt av de tre huvudstegen datainsamling, analys och tolkning. Trost påpekar även att vart och ett av dessa tre steg kan utföras kvalitativt eller kvantitativt. Även om studier kan vara helt kvalitativa eller helt kvantitativa är de flesta studier blandformer, där några delmoment utförs kvalitativt medan andra utförs kvantitativt. Vid val mellan kvalitativt och kvantitativt angreppssätt kan följande generella vägledning beaktas: ”Om frågeställningen gäller hur ofta, hur många eller hur vanligt så ska man göra en kvantitativ studie. Om frågeställningen däremot gäller att förstå eller att hitta mönster så skall man göra en kvalitativ studie” (Trost, 2005, s. 14). Utifrån denna vägledning och studiens frågeställningar anser författaren att det vore lämpligast att i huvudsak använda kvalitativa metoder.

Enligt Boolsen (2007) finns ingen ”riktig” kvalitativ metod, utan forskaren är alltid tvungen att värdera vilken metod som passar bäst och anpassa den till det material han har. I denna studie är innebörden av begreppet kompatibilitet helt avgörande för vilka metoder som är mest lämpliga. Kompatibilitet mellan standarder skulle kunna innebära en mängd olika saker. Till exempel skulle begreppet kunna innebära att standarder kan implementeras i en organisation sida vid sida, utan att de stör varandra och hamnar i konflikt med varandra. Det skulle också kunna innebära att standarderna i själva texten innehåller liknande eller likadana beskrivningar av de aktiviteter och processer som standarderna söker standardisera, det vill säga att de textmässiga beskrivningarna i standarddokumenten inte står i konflikt med varandra. Den första innebörden är viktigast sett ur ett samhällssäkerhetsperspektiv, då det är sådan kompatibilitet som organisationer faktiskt behöver handskas med i praktiken. Samtidigt kan sådan kompatibilitet vara en följd av den senare innebörden av begreppet. En harmonisk implementering av standarderna bör till stor del följa av och vara beroende av kompatibilitet mellan standarderna i själva texten. Kompatibilitet mellan standarder i implementering vore dessutom svårt att mäta, då det skulle kräva omfattande undersökningar av säkerhetsarbetet i ett antal organisationer som har implementerat standarderna. Av dessa anledningar anser författaren att det i denna studie vore lämpligast och nyttigast att undersöka kompatibilitet på textnivå i standarddokumenten.

En metod som lämpar sig särskilt väl för kvalitativa fallstudier av texter är dokumentanalys, även kallad innehållsanalys (Bowen, 2009). Bowen uppger flera fördelar med dokumentanalys jämfört med andra kvalitativa metoder:

- Då dokumentanalys kräver dataselektion istället för insamling av data är det en förhållandevis effektiv metod.
- Dokument är ofta lättillgängliga.
- Dokument påverkas inte av forskningsprocessen, vilket innebär att bias till följd av forskarens interaktion med objektet undviks.

Då de standarder som undersöks i studien finns nedtecknade i sin helhet i förhållandevis lättillgängliga dokument, anser författaren att dokumentanalys är en mycket lämplig metod. I jämförelse mellan texter utförs ofta dokumentanalyser med hjälp av kvantitativa inslag såsom räkning av ord och teman (Weber, 1990). För att fånga upp eventuella diskrepanser och inkompatibla inslag mellan standarder anser dock författaren att ett sådant tillvägagångssätt vore bristfälligt. En lika stor förekomst av specifika ord i olika standarder, torde inte vara en god indikator på kompatibilitet, främst då standarderna fokuserar på olika delar av en organisations säkerhetsarbete. Det torde vara lämpligare att applicera en kvalitativ analysmetodik för att identifiera mönster, koncept och perspektiv i texterna.

För att få resultat med hög validitet kan en triangulerad metod användas (Bekhet & Zauszniewski, 2012). Detta innebär att mer än en metod används i studien för att få flera uppsättningar med data vilka kan konfirmera eventuella fynd och validera resultat. Som komplement till dokumentanalyser utförs ofta intervjustudier (Bowen, 2009). Att använda en kombination av dessa två metoder är fördelaktigt då dokumentanalysen kan generera relevanta intervjufrågor, samtidigt som intervjuerna kan ge intressanta uppslag att fokusera på i dokumentanalysen. Det är också möjligt att använda ett homogeniserat kodningssystem mellan fynden i dokumentanalysen och svaren i intervjuerna (Bowen, 2009).

Intervjuer kategoriseras ofta i strukturerade, semistrukturerade och ostrukturerade former, ibland kallade strukturerade, guidade respektive informella former (Walliman, 2006; Vanderstoep & Johnston, 2008). I den strukturerade formen följer intervjun en förutbestämd utformning och ordning av frågor. Inga avsteg från den förutbestämda intervjuplanen görs, vilket innebär att intervjun i stor grad är oberoende av utföraren (Wellington & Szczerbinski, 2007). En fördel med denna intervjuform är att den genererar jämförbar data mellan respondenter som är förhållandevis lätt att analysera och generalisera. Den största nackdelen med strukturerade intervjuer är att ingen möjlighet ges att ställa spontana följdfrågor kring intressanta och oväntade svar (Vanderstoep & Johnston, 2008). I en ostrukturerad intervju används inte några förutbestämda frågor. Istället improviseras frågorna fram under intervjuns gång, samtidigt som samtalet tillåts flöda fritt i olika riktningar som anses vara intressanta (Walliman, 2006; Vanderstoep & Johnston, 2008). En stor fördel med ostrukturerade intervjuer är att intervjuaren kan följa upp på de intressanta spår som upptäcks under intervjuns gång. Den största nackdelen med ostrukturerade intervjuer är att de genererar data som både är svår att analysera och generalisera (Vanderstoep & Johnston, 2008). Semistrukturerade intervjuer kan ses som en kompromiss mellan strukturerade och ostrukturerade intervjuer (Wellington & Szczerbinski, 2007; Vanderstoep & Johnston, 2008). I den semistrukturerade formen utgår utföraren från någon slags intervjuguide men kan ändra, lägga till eller ta bort frågor under intervjuns gång (Walliman, 2006). Ofta tillåter en semistrukturerad form att forskaren kan dra nytta av de tidigare nämnda formernas fördelar och samtidigt undvika deras nackdelar. Beroende på frågornas karaktär kan data som är lätt att analysera erhållas, samtidigt som intervjuaren tillåts

ställa följdfrågor på intressanta svar (Vanderstoep & Johnston, 2008; Walliman, 2006; Kvale, 1997).

I denna studie anser författaren att en semi-strukturerad intervjumetodik är lämpligast, eftersom det är svårt att förutse vilka svar och fynd som är intressanta i förväg. Det är därför fördelaktigt om möjlighet ges till att följa upp på intressanta spår som dyker upp under intervjuns gång. Samtidigt anser författaren att det är fördelaktigt om svaren på de flesta frågorna kan jämföras mellan respondenter. Av denna anledning är en semistrukturerad form att föredra framför en helt ostrukturerad form. Med anledning av möjligheten att följa upp på de upptäckter som görs under intervjuns gång, anser författaren även att intervjuer av detta slag är lämpligare än andra tillgängliga metoder för att samla in den sökta informationen, exempelvis enkätundersökningar. Potentiella respondenter är individer som har varit med och utvecklat standarderna, eller som varit med och implementerat standarderna i olika verksamheter.

I kapitel 4 Metodutveckling utvecklas och anpassas de valda metoderna utifrån de frågeställningar och det material som ligger till grund för studien.

3 Teori

I detta kapitel behandlas det teoretiska ramverk kring begreppet kompatibilitet som nyttjas i studien.

3.1 Kompatibilitetsbegreppet

Kompatibilitet är ett begrepp som förekommer i flera olika vetenskapliga sammanhang, ofta med vitt skilda betydelser. Inom mekaniken är kompatibilitet en likformig deformation av olika kroppar i kontakt med varandra (Yavari, 2013). När det gäller elinstallationer används begreppet elektromagnetisk kompatibilitet, vilket betyder förmågan hos elektronisk utrustning att verka i den tänkta elektromagnetiska miljön utan att åsamka eller åsamkas oacceptabla elektromagnetiska störningar (ANSI C63.14-1992). Inom geokemi är kompatibilitet ett mått på hur lätt ett specifikt spårämne kan ersätta ett huvudgrundämne i ett mineral (Pearce, Hough, Cleverley & Timms, 2013). Kompatibilitet är alltså ett begrepp med många olika betydelser, även om det alltid handlar om någon slags samstämmighet, överensstämmelse eller lämplighet. I Svenska Akademiens ordlista förklaras begreppet kompatibel som ”möjlig att samordna med något” (SAOL, 2006, s. 453). Denna betydelse är kanske den som oftast åsyftas när begreppet kompatibilitet används i dagligt tal eller i vetenskapliga kontexter, där det ännu inte fått en vedertagen definition.

Mot bakgrund av studiens frågeställningar behöver kompatibiliteten mellan två familjer av standarder mätas på något sätt. I kapitel 2 Metod argumenterar författaren för att det är kompatibilitet mellan själva texterna som bör undersökas i studien. För att sådan kompatibilitet ska kunna undersökas och mätas behöver den tydligt definieras, likt hur kompatibiliteten definieras i de exempel som nämns i föregående stycke. Ett sätt att göra detta är med en så kallad operationell definition som beskrivs av Ennis (1964). Den operationalism som Ennis beskriver bygger på en förståelse av att forskarens resultat är helt beroende av de instrument och metoder som används för att nå resultaten. Detta är av särskild betydelse för storheter och begrepp som inte är möjliga att observera och mäta direkt. Innebörden av sådana begrepp blir oundvikligen starkt förknippad med de metoder som används för att mäta dem. Operationella definitioner är ett sätt att beakta och tydliggöra de metoder som används för att mäta begreppen (Ennis, 1964).

Jämför den fysikaliska storheten massa, som anger ett objekts materieinnehåll, med begreppet vikt, som är den skattning av objektets massa, som erhålls genom vägning med en våg. Oftast saknas metoder för att mäta massan hos ett objekt direkt. Istället används en våg för att mäta objektets tyngd, som är en storhet direkt proportionerlig mot objektets massa. Med kännedom om den lokala gravitationskonstanten kan sedan massan skattas utifrån tyngden, skattningen kallas för objektets vikt. Hur väl den vikt som skattats med vågen stämmer överens med objektets verkliga massa, beror helt av storleken på den lokala gravitationskonstanten. På månen får därför objektet en helt

annan vikt än på jorden trots att det fortfarande har samma massa. Detta gäller dock bara för fjädervågar. En balansvåg visar samma vikt oavsett storlek på den lokala gravitationskonstanten. En forskare som presenterar mätresultat av ett objekts vikt bör därför beskriva vilken av dessa två sätt att väga objektet som använts. Detta skulle han kunna åstadkomma genom att göra en operationell definition av vikten. En enkel sådan definition skulle kunna lyda: ”Vikt är den skattning av objektets massa som erhålls genom mätning med balansvåg”.

I denna studie låter sig det abstrakta begreppet kompatibilitet inte mätas direkt genom användning av linjaler och liknande. Likt exemplet i föregående stycke behövs därför någon eller några mer mätbara aspekter av standarderna, vilka kan ge indikationer om kompatibiliteten. Kompatibiliteten kan med hjälp av sådana aspekter definieras operationellt, vilket innebär att begreppet definieras utifrån de mätbara aspekterna och hur dessa mäts. Av praktiska skäl kan det vara lämpligt att gruppera aspekterna i ett antal huvudvariabler och undervariabler (Boolsen, 2007). Då erhålls ett kompatibilitetsbegrepp uppbyggt av ett antal huvudaspekter som i sin tur är uppbyggda av ett antal underaspekter. Med hjälp av de riktlinjer för operationella definitioner som Ennis (1964) lägger fram, kan kompatibilitet mellan standarder operationaliseras och definieras på följande sätt:

Om standarderna $X_1, X_2, \dots, X_p$ jämförs med standarderna $Y_1, Y_2, \dots, Y_q$ enligt författarens beskrivna metod; då är standarderna $X_1, X_2, \dots, X_p$ kompatibla med standarderna $Y_1, Y_2, \dots, Y_q$ till graden k, om och bara om, den sammanlagda viktade kompatibilitetskoefficienten $c = \sum \frac{e \cdot w}{n}$ är lika med k.

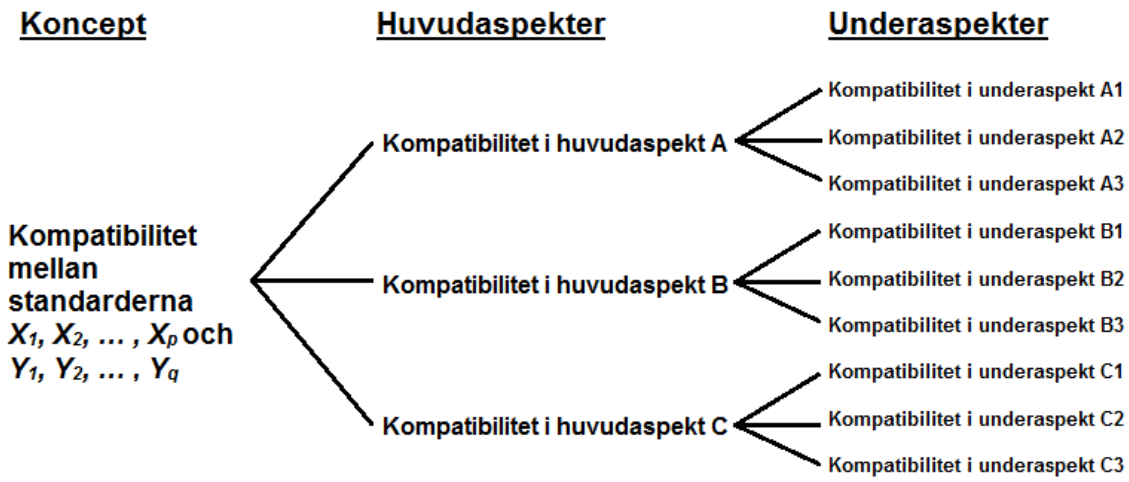
Här är c kompatibilitetskoefficienten för standarderna och e kompatibilitetskoefficienten för varje enskild huvudaspekt som ingår både i standarderna $X_1, X_2, \dots, X_p$och i standarderna $Y_1, Y_2, \dots, Y_q$. Variabeln w är vikten för varje enskild huvudaspekt relativt övriga huvudaspekter och n är antalet ingående huvudaspekter. Kompatibilitet mellan huvudaspekter kan i sin tur definieras på följande sätt:

Om huvudaspekt Z i standarderna $X_1, X_2, \dots, X_p$ jämförs med huvudaspekt Z i standarderna $Y_1, Y_2, \dots, Y_q$ enligt författarens beskrivna metod; då är huvudaspekt Z i standarderna $X_1, X_2, \dots, X_p$ kompatibel med huvudaspekt Z i standarderna $Y_1, Y_2, \dots, Y_q$ till graden i, om och bara om, den sammanlagda viktade kompatibilitetskoefficienten $e = \sum \frac{d \cdot v}{m}$ är lika med i.

Här är e kompatibilitetskoefficienten för huvudaspekten och d kompatibilitetskoefficienten för varje enskild underaspekt som ingår i huvudaspekten. Variabeln v är vikten för varje enskild underaspekt relativt övriga underaspekter och m är antalet ingående underaspekter. Kompatibilitet mellan underaspekter kan i sin tur definieras på följande sätt:

Om underaspekt Z i standarderna $X_1, X_2, \dots, X_p$ jämförs med underaspekt Z i standarderna $Y_1, Y_2, \dots, Y_q$ enligt författarens beskrivna metod; då är underaspekt Z i standarderna $X_1, X_2, \dots, X_p$ kompatibel med underaspekt Z i standarderna $Y_1, Y_2, \dots, Y_q$ till graden j, om och bara om, kompatibilitetskoefficienten d för underaspekten är lika med j. Om någon diskrepans finns i underaspekten är kompatibilitetskoefficienten $d = 0$. Om inga diskrepanser finns i underaspekten är kompatibilitetskoefficienten $d = 1$.

De operationella definitionerna ovan innebär att fundamentet i kompatibilitetsundersökningen, utgörs av bedömningar av kompatibilitet i underaspekter. Bedömningarna resulterar i att underaspekternas kompatibilitetskoefficienter $d_1, d_2, \dots, d_m$ sätts till 0 eller 1, beroende på om diskrepanser finns eller ej. Med hjälp av underaspekternas relativa vikter $v_1, v_2, \dots, v_m$ vägs underaspekternas kompatibilitetskoefficienter $d_1, d_2, \dots, d_m$ ihop i huvudaspekternas kompatibilitetskoefficienter $e_1, e_2, \dots, e_n$. Med hjälp av huvudaspekternas relativa vikter $w_1, w_2, \dots, w_n$ vägs i sin tur huvudaspekternas kompatibilitetskoefficienter $e_1, e_2, \dots, e_n$ ihop till den mellan standarderna övergripande kompatibilitetskoefficienten c. Kompatibilitet mellan standarder är enligt definitionerna alltså en sammanvägning av kompatibilitet i samtliga ingående underaspekter. På detta sätt kan kompatibiliteten mellan standarder kvantifieras. För att de operationella definitionerna ska vara användbara behöver dock de ingående aspekterna identifieras samtidigt som aspekternas relativa vikter v och w behöver bestämmas. I de operationella definitionerna kan $X_1, X_2, \dots, X_p$ och $Y_1, Y_2, \dots, Y_q$ exempelvis utgöras av enskilda standarder eller familjer av standarder. Kompatibilitetsbegreppet i studien åskådliggörs i figur 3.1.



Figur 3.1 Skisserad uppbyggnad av kompatibilitetsbegreppet i studien.

4 Utveckling av metod

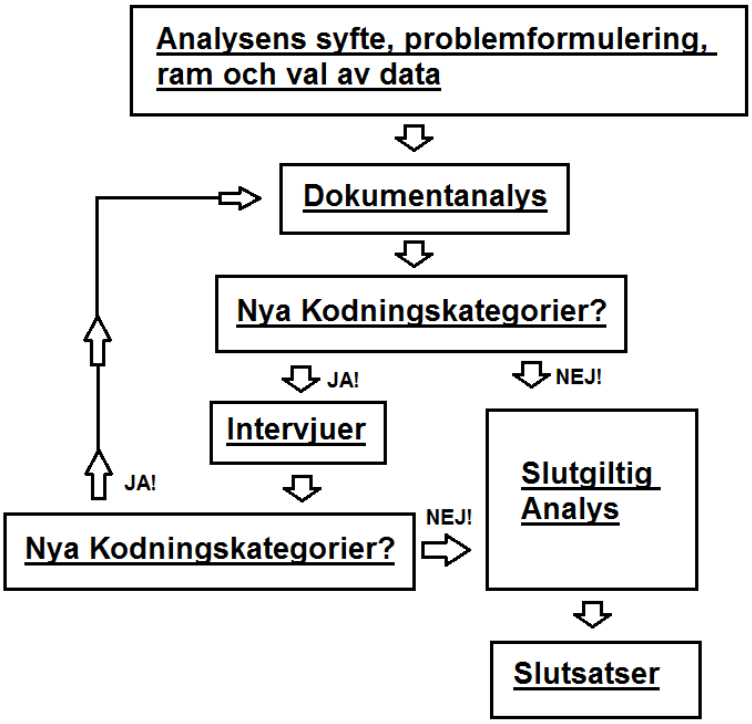
Mot bakgrund av resonemangen i kapitel 2 Metod, avser författaren att applicera en tudelad kvalitativ analysmetodik bestående av dokumentanalys och semi-strukturerade intervjuer. Som tidigare nämnts finns det ingen fastlagd ”riktig” kvalitativ metod, utan metoden måste alltid anpassas inom de ramar och till det material som föreligger (Boolsen, 2007). Samtidigt kritiseras ofta kvalitativa analyser för brist på transparens, vilket innebär att det är otydligt hur undersökningen gått till och vilka val forskaren har gjort (Boolsen, 2007). Av denna anledning är det viktigt att tydligt dokumentera vilka val som görs under hela forskningsprocessen och tydligt beskriva den för situationen anpassade metoden. Som tidigare nämnts består studier generellt av de tre delstegen datainsamling, analys och tolkning (Trost, 2005). I den metod som utvecklas i detta kapitel och som appliceras i studien, utförs datainsamlingen och analysen kvalitativt medan tolkningen både har kvantitativa och kvalitativa inslag.

4.1 Identifiering av aspekter och kodning

Genom innehållsanalys kan slutsatser dras om ett budskaps sändare och mottagare eller budskapet självt (Weber, 1990). I olika dokument kan det finnas mängder av aspekter som kan användas för sådana slutsatser, allt från färgval i illustrationer och val av typsnitt till uttryckta perspektiv och tankegångar (Boolsen, 2007). Detta gäller även för standarderna i denna studie. Kompatibilitet mellan standarder ska i denna studie, som tidigare nämnts, innebära samstämmighet och avsaknad av konflikter mellan textmässiga beskrivningar i olika standarder. Mot bakgrund av detta vore det därför mest relevant att undersöka de aspekter som har med sådana beskrivningar att göra.

En mycket central del i kvalitativa analyser är kodning av material i olika kategorier (Weber, 1990; Kvale, 1997; Boolsen, 2007). I kodningen fattas de, för senare analysmöjligheter, avgörande besluten som rör data. Kategoriseringen kan antingen göras induktivt eller deduktivt (Boolsen, 2007). I en deduktiv analys är kategorierna som ska undersökas bestämda på förhand, medan i en induktiv analys bestäms kategorierna kontinuerligt utifrån undersökningsmaterialet. I denna studie vore det praktiskt om kodningskategorierna i analysen är identiska med underaspekterna i kompatibilitetsbegreppet. Detta då en sådan överensstämmelse begränsar analysen av varje enskild underaspekt till innehållet i en kategori. Identifieringen av kodningskategorier blir därför således helt identisk med identifieringen av underaspekter i kompatibilitetsbegreppet. Författaren anser att det vore svårt att identifiera och fånga upp alla relevanta aspekter innan studien påbörjas. Nya aspekter kommer oundvikligen dyka upp under studiens gång, varför det vore fördelaktigt att tillämpa en induktiv analysmetod. Detta kan dock bli problematiskt då det kan leda till flera omkodningar av redan kodat material allt eftersom nya kategorier läggs till. Det vore därför praktiskt eller rentav nödvändigt att tillämpa något slags ramverk för hur

nya kategorier ska identifieras och inkorporeras under studiens gång. För att i dokumentanalysen kunna dra nytta av de aspekter som identifieras i intervjuerna, och vice versa, ser författaren fördelar med att applicera en iterativ kodningsprocess. I ett första steg bestäms syfte, problemformulering och ram för analysen. Härefter arbetas kodningskategorierna fram efter upprepade genomläsningar av dokumenten. Med dessa kategorier som underlag utförs intervjuerna. Sedan revideras kodningskategorierna utifrån eventuella nya aspekter som identifieras i intervjumaterialet. Om nya kategorier tillkommit studeras dokumenten på nytt med den nya uppsättningen av kategorier i åtanke. Om detta ger upphov till ytterligare kategorier studeras intervjumaterialet på nytt med utgångspunkt från den nya uppsättningen av kategorier. Denna process itereras tills dess att inga nya aspekter identifieras i genomläsningarna, varefter dokumenten analyseras utifrån den slutgiltiga uppsättningen av kategorier. Den iterativa processen för identifiering av kategorier åskådliggörs i figur 4.1.



Figur 4.1 Illustration av arbetsgången i studien.

Då studien avser att jämföra större perspektiv och mönster mellan standarder, är det viktigt att påpeka att kodningskategorierna bör återspegla dessa större strukturer och inte gå in på en allt för detaljerad nivå. I litteraturen beskrivs ofta en mer detaljerad kodningsprocess i smalare kategorier (Kvale, 1997; Boolsen, 2007). För den kvalitativa analys som appliceras i denna studie anser författaren dock att det är mer lämpligt med bredare kategorier på en högre strukturell nivå.

4.2 Jämförande analys av standarder

Med den slutgiltiga uppsättningen av kodningskategorier ska datamaterialet analyseras. Detta innebär att materialet bryts ner i textstycken som sorteras in under de olika kodningskategorierna. När standarderna $X_1, X_2, \dots, X_p$ jämförs med standarderna $Y_1, Y_2, \dots, Y_q$ jämförs sedan de textstycken som tillhör standarderna $X_1, X_2, \dots, X_p$ med de textstycken som tillhör standarderna $Y_1, Y_2, \dots, Y_q$ i varje enskild kategori med varandra. Kompatibilitetskoefficienten d för varje kategori som undersöks ges sedan värdet 0 eller 1, beroende på om diskrepanser återfinns i kategorin eller ej.

Vid jämförelser av detta slag förekommer troligtvis några av de identifierade aspekterna enbart i standarderna $X_1, X_2, \dots, X_p$ eller enbart i standarderna $Y_1, Y_2, \dots, Y_q$. Detta eftersom uppsättningen av kodningskategorier innehåller samtliga aspekter som identifieras i samtliga standarder. De kategorier som inte förekommer både i standarderna $X_1, X_2, \dots, X_p$ och i standarderna $Y_1, Y_2, \dots, Y_q$ utesluts i sådana fall helt från jämförelsen.

Vid jämförelser av aspekter i standarderna är gränsen mellan vad som utgör en diskrepans och inte mycket avgörande. Textmässigt olika beskrivningar i olika standarder är att vänta. Om andemeningen bakom beskrivningarna är densamma borde dock inte en olikartad frasering betraktas som en diskrepans. Samtidigt kan en beskrivning vara mer uttömmande och inkorporera mer information om fler företeelser än en annan beskrivning. En sådan skillnad bör enligt författaren heller inte betraktas som en diskrepans. Endast direkt motstridiga påståenden bör enligt författaren betraktas som diskrepanser. När det gäller definitioner av begrepp finns det dock fog för en striktare bedömning. Detta eftersom ett homogent språkbruk är en viktig del i den samsyn som standarderna syftar till att uppnå.

Ett begrepp som ofta förekommer i ISO 31000:2009 och i ISO_TR 31004:2013 är *risk management framework*. Samtidigt används inte alls begreppet *risk management system* i dessa standarder. Studeras ramverket för riskhantering närmare, inses att ramverket i princip ser ut precis som ett ledningssystem. I flera fall används också begreppet ramverk i stort sett synonymt med begreppet ledningssystem vilket illustreras med följande citat: ”[I]f a formal management system does not exist, a risk management framework can serve this purpose” (ISO_TR 31004:2013, s. 11). ”Wherever possible, other components of the risk management framework should be embedded into components of existing management systems” (ISO_TR 31004:2013, s. 11). ”These individual management systems should form an integrated management system, […] where an organization has individual management systems to manage particular risks, the risk management framework should extend to, and incorporate, those systems” (ISO_TR 31004:2013, s. 35). Vid jämförelsen av de två standardfamiljerna betraktas därför oftast dessa två begrepp som helt synonyma. Utan detta grepp vore det överhuvudtaget svårt att jämföra standarderna, då standarderna skulle ha mycket få kontaktytor om de två begreppen betraktades som vitt skilda fenomen. Samtidigt

vidhålls medvetenhet om att den egentliga skillnaden mellan begreppen i vissa fall har en signifikant betydelse.

En annan viktig skillnad mellan ISO 31000:2009 och ISO 22301:2012 är att den senare är certifierbar. Detta innebär att ISO 31000:2009 ger rekommendationer medan ISO 22301:2012 ställer krav som organisationer kan certifieras mot. Denna skillnad yttrar sig i att ISO 31000:2009 ger utförligare beskrivningar av *hur* aktiviteter kan utföras medan ISO 22301:2012 mest beskriver *vad* som ska utföras och ställer krav på det mest centrala. Författaren anser att denna fundamentala skillnad ur ett analysperspektiv främst innebär en skillnad i detaljnivå mellan textmässiga beskrivningar och att den inte ger upphov till sådana diskrepanser som beskrivs i tidigare stycken. I analysen bedöms därför ISO 22301:2012 enligt samma metod och enligt samma kriterier som övriga standarder.

4.3 Sammanvägning av aspekter

Av de aspekter som identifieras i standarderna är troligtvis några viktigare än andra för kompatibilitet mellan standarder. Sådana skillnader bör på något sätt tas i beaktning när kompatibilitetskoefficienter för underaspekter vägs samman i kompatibilitetskoefficienter för huvudaspekter, och när kompatibilitetskoefficienter för huvudaspekter vägs samman i kompatibilitetskoefficienter mellan standarder. Detta kan åstadkommas genom att låta respondenterna i intervjuerna gradera de enskilda aspekternas vikt för kompatibiliteten på en kvotskala mellan noll och fem. Utifrån respondenternas graderingar kan varje huvudaspekt och underaspekt tilldelas en vikt u_h respektive u_u som är lika med medelvärdet av respondenternas enskilda graderingar. Utifrån dessa absoluta vikter kan de relativa vikterna v och w, som används vid sammanvägningarna, bestämmas som:

$$v = \frac{u_u}{\bar{u}_u} = \frac{u_u \cdot m}{\sum u_u} \quad (1)$$

$$w = \frac{u_h}{\bar{u}_h} = \frac{u_h \cdot n}{\sum u_h} \quad (2)$$

där m är antalet underaspekter och n är antalet huvudaspekter. I dessa ekvationer normeras de relativa vikterna så att kompatibilitetskoefficienterna efter sammanvägning uttrycks i ett mätetal mellan 0 och 1, där ett högre värde innebär större kompatibilitet.

Av ekvationerna ovan och de operationella definitionerna i avsnitt 3.1 Kompatibilitetsbegreppet, följer att:

$$e = \sum \frac{d \cdot v}{m} = \sum (d \cdot \frac{u_u}{\sum u_u}) \quad (3)$$

$$c = \sum \frac{e \cdot w}{n} = \sum (e \cdot \frac{u_h}{\sum u_h}) \quad (4)$$

där c är kompatibilitetskoefficienten mellan standarderna, e är kompatibilitetskoefficienterna för huvudaspekterna och d är kompatibilitetskoefficienterna för underaspekterna. Dessa två ekvationer är av praktisk nytta vid sammanvägning av aspekter. Detta då de möjliggör beräkningar av kompatibilitetskoefficienterna e och c, direkt utifrån värden på d, u_h och u_u, utan att vikterna v och w först behöver beräknas.

4.4 Intervjuunderlag och utförande

Utifrån studiens frågeställningar och de aspekter som identifieras vid den första genomläsningen av standarddokumenten tas ett underlag för intervjuerna fram, se bilaga A. Intervjuerna syftar främst till att finna orsaker och lösningar till inkompatibla inslag samt till att bidra med ett underlag för sammanvägning av aspekter. Intervjuguiden utformas med dessa grundsyften i åtanke. I beaktning tas den vägledning för hur guider till kvalitativa intervjuer kan utformas som Trost (2005) presenterar. Bland annat bör en intervjuguide enligt Trost snarare innehålla för litet än för mycket och inte vara allt för detaljerad.

Intervjuerna i studien utförs som tidigare nämnts i en semistrukturerad form. I praktiken innebär detta att intervjuerna utgår från en checklista med frågor, samtidigt som frågornas ordning improviseras fram. Den del av intervjuerna som berör gradering av aspekternas vikt utförs i en nästan helt strukturerad form. Följdfrågor på intressanta spår som dyker upp under intervjuns gång kan förekomma, samtidigt som respondenten tillåts utveckla sina svar och avvika från aktuella frågor.

Trost (2005) ger även råd kring sådant som berör själva utförandet av intervjuerna, såsom användande av bandspelare, klädsel, konfidentiellitet, plats för intervjun etcetera. Dessa råd tas i beaktning då intervjuerna utförs. Intervjumaterialet behandlas konfidentiellt. Inspelningsutrustning används istället för anteckningar med papper och penna. Då respondenterna återfinns på flera olika orter med stora avstånd utförs några intervjuer via telefon.

4.5 Val av datakällor

Då de standarder som undersöks finns nedtecknade i sin helhet i olika dokument utgör dessa dokument de huvudsakliga datakällorna. Det finns troligtvis flera andra dokument som också innehåller relevant information om standarderna, exempelvis mötesprotokoll, affärsplaner etcetera. Sådana datakällor undersöks dock inte i studien då författaren anser att det är mest centralt att undersöka själva standarddokumenten. De dokument som undersöks i studien utgörs därför av:

- ISO 22300:2012 - Societal Security – Terminology
- ISO 22301:2012 - Societal security – Business continuity management systems – Requirements

- ISO 22313:2012 - Societal security – Business continuity management systems – Guidance
- ISO_IEC 73:2009 Risk management - Vocabulary
- ISO 31000:2009 - Risk management – Principles and guidelines
- ISO_TR 31004:2013 - Risk Management - Guidance for the Implementation of ISO 31000.

Urvalet av respondenter i intervjustudien är målinriktat, vilket innebär att personer som är relevanta för frågeställningarna identifieras och intervjuas (Bryman, 2012). Författaren anser att personer som har varit med och utvecklat standarderna eller som har varit med och implementerat standarderna i organisationer är mest relevanta. För att finna sådana respondenter appliceras en så kallad ”snowball”-sampling. Detta innebär att en individ med de sökta egenskaperna identifieras och kontaktas, varefter denna individs sociala nätverk används för att finna fler individer med de sökta egenskaperna (Sadler, Lee, Lim & Fullerton, 2010). I denna studie kontaktas i ett första skede personer som har deltagit i de kommittéer som har utvecklat standarderna. Dessa personer kan sedan förmedla kontakter till andra personer som har varit med i kommittéerna eller som har implementerat standarderna i olika organisationer. De respondenter som deltar i intervjustudien är:

- Clas Herbring, MSB
- Fredrik Pettersson, Actea Consulting AB
- Omar Harrami, MSB
- Stefan Tangen, MSB.

Samtliga respondenter har varit involverade i kommittén ISO/TC 223 – Societal Security. Stefan Tangen har dessutom varit involverad i kommittén ISO/TC 262 – Risk Management. Fredrik Pettersson har arbetat med att implementera standarderna i olika organisationer.

5 Resultat och analys

I detta kapitel presenteras resultaten av intervjuerna och dokumentanalysen. Studien följer den arbetsgång och utgår från den ram som beskrivs i kapitel 4 Utveckling av metod. I studien jämförs de tre förstnämnda med de tre sistnämnda av de standarder som listas i avsnitt 4.5 Val av datakällor.

5.1 Iterativ framtagning av kodningsprinciper

Kodningskategorierna bestäms enligt kapitel 4 Utveckling av metod, i en iterativ process där nya kategorier identifieras i dokumenten och intervjumaterialet kontinuerligt.

5.1.1 Inledande genomläsning av dokumenten

I den inledande genomläsningen av dokumenten identifieras ett flertal aspekter som kan vara relevanta för syftet och frågeställningarna. Av dessa identifieras tre övergripande huvudaspekter:

- A: Definitioner av begrepp
- B: Beskrivningar av ramverk och ledningssystem
- C: Beskrivningar av processer för riskhantering och kontinuitetshantering.

Ett antal underkategorier till dessa huvudaspekter identifieras också:

- A0: Definition av audit/risk management audit
- A1: Definition av business continuity
- A2: Definition av business continuity management
- A3: Definition av business continuity management system
- A4: Definition av business impact analysis
- A5: Definition av consequence
- A6: Definition av control
- A7: Definition av effectiveness
- A8: Definition av event
- A9: Definition av interested party och stakeholder
- A10: Definition av management system
- A11: Definition av monitoring
- A12: Definition av objective
- A13: Definition av probability
- A14: Definition av residual risk
- A15: Definition av risk
- A16: Definition av risk analysis

- A17: Definition av risk assessment
- A18: Definition av risk evaluation
- A19: Definition av risk management
- A20: Definition av risk management framework
- A21: Definition av risk management process
- A22: Definition av risk owner
- A23: Definition av risk treatment, control och mitigation
- A24: Definition av societal security
- A25: Definition av vulnerability
- B1: Beskrivning av relation mellan ledningssystem och processer
- B2: Beskrivning av hur extern kontext bör etableras
- B3: Beskrivning av hur policy bör upprättas
- B4: Beskrivning av relation mellan olika delar i ett ledningssystem
- B5: Beskrivning av planering av processer
- B6: Beskrivning av implementering av processer
- B7: Beskrivning av övervakning och granskning
- B8: Beskrivning av kontinuerliga förbättringar
- B9: Beskrivning av hur intressenter bör tas i beaktning
- B10: Beskrivning av ledningens roll, ansvar och engagemang
- B11: Beskrivning av hur ledningssystem bör implementeras i organisationen
- B12: Beskrivning av ledningssystemens inbördes relation
- C1: Beskrivning av relation mellan riskhanteringsprocessens delsteg
- C2: Beskrivning av kommunikationsaktiviteter
- C3: Beskrivning av dokumentationsaktiviteter
- C4: Beskrivning av business impact analysis
- C5: Beskrivning av risk assessment
- C6: Beskrivning av risk analysis
- C7: Beskrivning av risk evaluation
- C8: Beskrivning av risk treatment
- C9: Beskrivning av business continuity strategy
- C10: Beskrivning av business continuity procedures.

5.1.2 Inledande genomgång av intervjumaterialet

I genomgången av intervjumaterialet identifieras ett antal nya aspekter:

- A26: Definition av policy/risk management policy
- A27: Definition av resilience
- A28: Definition av hazard
- A29: Definition av risk source
- A30: Definition av risk appetite
- B13: Beskrivning av relation mellan policy, mål och planer.

Dessa aspekter sorteras in under de redan identifierade huvudaspekterna.

5.1.3 Fördjupad genomläsning av dokumenten

Under den sista fördjupade genomläsningen av dokumenten innan kodningen identifieras en ny aspekt:

- C11: Beskrivning av riskidentifiering.

Denna aspekt sorteras in under huvudkategori C: Beskrivningar av processer för riskhantering och kontinuitetshantering.

5.1.4 Slutgiltig uppsättning av kodningskategorier

Under den slutgiltiga kodningen av materialet stryks ett antal kategorier som endast återfinns i en av de två standardfamiljerna. Under kodningen slås även en del närbesläktade kategorier ihop. Den slutgiltiga uppsättningen av kodningskategorier för jämförelsen består därefter av dessa underaspekter:

- A1: Definition av audit och risk management audit
- A2: Definition av consequence
- A3: Definition av event
- A4: Definition av hazard
- A5: Definition av interested party och stakeholder
- A6: Definition av monitoring
- A7: Definition av policy och risk management policy
- A8: Definition av probability
- A9: Definition av residual risk
- A10: Definition av resilience
- A11: Definition av risk
- A12: Definition av risk appetite
- A13: Definition av risk assessment
- A14: Definition av risk management
- A15: Definition av risk owner
- A16: Definition av risk source
- A17: Definition av risk treatment, control och mitigation
- A18: Definition av vulnerability
- B1: Beskrivning av relation mellan ledningssystem och processer
- B2: Beskrivning av hur extern kontext bör etableras
- B3: Beskrivning av hur policy bör upprättas
- B4: Beskrivning av ingående delar i ett ledningssystem och relationerna dem emellan
- B5: Beskrivning av planering av processer
- B6: Beskrivning av implementering av processer

- B7: Beskrivning av övervakning och granskning
- B8: Beskrivning av kontinuerliga förbättringar
- B9: Beskrivning av ledningens roll, ansvar och engagemang
- B10: Beskrivning av hur ett ledningssystem bör implementeras i organisationen och integreras med andra ledningssystem
- C1: Beskrivning av riskhanteringsprocessens delar och relationen dem emellan
- C2: Beskrivning av kommunikationsaktiviteter
- C3: Beskrivning av dokumentationsaktiviteter
- C4: Beskrivning av riskbedömning
- C5: Beskrivning av riskanalys
- C6: Beskrivning av riskvärdering
- C7: Beskrivning av riskbehandling
- C8: Beskrivning av riskidentifiering.

5.2 Sammanvägningsprincip

Utifrån de graderingar av aspekternas vikt för kompatibilitet som erhålls i intervjumaterialet bestäms de absoluta och relativa vikterna för de ingående aspekterna i kompatibilitetsbegreppet, se tabell 5.1 och tabell 5.2. De relativa vikterna bestäms med hjälp av ekvation (1) och ekvation (2) i avsnitt 4.3 Sammanvägning av aspekter.

Tabell 5.1 Huvudaspekternas vikter i kompatibilitetsbegreppet.

Huvudaspekt	u_h	w	$\frac{u_h}{\sum u_h}$
A: Definitioner av begrepp	4,11	1,06	0,352
B: Beskrivningar av ramverk och ledningssystem	3,22	0,829	0,276
C: Beskrivningar av processer för riskhantering och kontinuitetshantering	4,33	1,11	0,371

Tabell 5.2 Underaspekternas vikter i kompatibilitetsbegreppet.

Underaspekt	u_u	v	$\frac{u_u}{\sum u_u}$
A1: Definition av audit och risk management audit	2,00	0,671	0,0373
A2: Definition av consequence	3,00	1,01	0,0559
A3: Definition av event	3,67	1,23	0,0683
A4: Definition av hazard	3,00	1,01	0,0559
A5: Definition av interested party och stakeholder	3,67	1,23	0,0683
A6: Definition av monitoring	2,00	0,671	0,0373
A7: Definition av policy och risk management policy	3,67	1,23	0,0683
A8: Definition av probability	3,00	1,01	0,0559
A9: Definition av residual risk	2,00	0,671	0,0373
A10: Definition av resilience	2,44	0,820	0,0455
A11: Definition av risk	4,33	1,45	0,0807
A12: Definition av risk appetite	2,00	0,671	0,0373
A13: Definition av risk assessment	3,56	1,19	0,0662
A14: Definition av risk management	3,78	1,27	0,0704
A15: Definition av risk owner	3,00	1,01	0,0559
A16: Definition av risk source	3,00	1,01	0,0559
A17: Definition av risk treatment och mitigation	3,00	1,01	0,0559
A18: Definition av vulnerability	2,57	0,862	0,0479
B1: Beskrivning av relation mellan led.sys. och processer	3,29	0,868	0,0868
B2: Beskrivning av hur extern kontext bör etableras	3,33	0,881	0,0881
B3: Beskrivning av hur policy bör upprättas	5,00	1,32	0,132
B4: Beskrivning av delar i led.sys. och relation dem emellan	3,43	0,906	0,0906
B5: Beskrivning av planering av processer	4,00	1,06	0,106
B6: Beskrivning av implementering av processer	3,00	0,793	0,0793
B7: Beskrivning av övervakning och granskning	3,57	0,944	0,0944
B8: Beskrivning av kontinuerliga förbättringar	3,33	0,881	0,0881
B9: Beskrivning av ledningens roll, ansvar och engagemang	5,00	1,32	0,132
B10: Beskrivning av hur ledningssystem implementeras.	3,89	1,03	0,103
C1: Beskrivning av riskh.proc., dess delar och relationer.	3,43	0,996	0,124
C2: Beskrivning av kommunikationsaktiviteter	3,11	0,904	0,113
C3: Beskrivning av dokumentationsaktiviteter	3,57	1,04	0,130
C4: Beskrivning av riskbedömning	3,67	1,07	0,133
C5: Beskrivning av riskanalys	3,33	0,968	0,121
C6: Beskrivning av riskvärdering	3,43	0,996	0,124
C7: Beskrivning av riskbehandling	3,00	0,871	0,109
C8: Beskrivning av riskidentifiering	4,00	1,16	0,145

5.3 Jämförande analys av aspekter

I jämförelsen mellan de två standardfamiljerna undersöks och jämförs varje kategori var för sig. För varje enskild kategori ges kompatibilitetskoefficienten d värdet 0 eller 1 beroende på om kategorin bedöms vara kompatibel eller inte, utgående från eventuella diskrepanser mellan de textstycken som kodas till kategorin från de olika standardfamiljerna. En detaljerad beskrivning av hur texten i varje enskild kategori analyseras och jämförs vore alldeles för uttömmande. Av denna anledning presenteras analysen av ett urval kategorier som författaren anser vara särskilt intressanta. För övriga kategorier presenteras endast resultatet. I urvalet som presenteras ingår bland annat samtliga kategorier som bedöms vara inkompatibla. I tabell 5.3 redovisas analysens resulterande kompatibilitetskoefficienter för samtliga underaspekter. Analysen av de enskilda aspekterna presenteras i de närmast följande avsnitten.

Tabell 5.3 Resultat av den jämförande analysen.

Underaspekt	Kompatibilitets-koefficient *d*
A1: Definition av audit/risk management audit	1
A2: Definition av consequence	1
A3: Definition av event	0
A4: Definition av hazard	1
A5: Definition av interested party och stakeholder	0
A6: Definition av monitoring	1
A7: Definition av policy/risk management policy	1
A8: Definition av probability	1
A9: Definition av residual risk	1
A10: Definition av resilience	1
A11: Definition av risk	1
A12: Definition av risk appetite	1
A13: Definition av risk assessment	1
A14: Definition av risk management	1
A15: Definition av risk owner	1
A16: Definition av risk source	1
A17: Definition av risk treatment och mitigation	1
A18: Definition av vulnerability	1
B1: Beskrivning av relation mellan ledn.system och processer	0
B2: Beskrivning av hur extern kontext bör etableras	1
B3: Beskrivning av hur policy bör upprättas	1
B4: Beskrivning av delar i ett led.sys. och relation dem emellan	1
B5: Beskrivning av planering av processer	1
B6: Beskrivning av implementering av processer	1
B7: Beskrivning av övervakning och granskning	1
B8: Beskrivning av kontinuerliga förbättringar	1
B9: Beskrivning av ledningens roll, ansvar och engagemang	1
B10: Beskrivning av hur led.sys. implementeras och integreras.	1
C1: Beskrivning av riskh.proc., dess delar och relationer.	0
C2: Beskrivning av kommunikationsaktiviteter	1
C3: Beskrivning av dokumentationsaktiviteter	1
C4: Beskrivning av riskbedömning	0
C5: Beskrivning av riskanalys	1
C6: Beskrivning av riskvärdering	1
C7: Beskrivning av riskbehandling	1
C8: Beskrivning av riskidentifiering	1

5.3.1 Definitioner av audit och risk management audit

I ISO_IEC 73:2009 definieras begreppet *risk management audit* som:

> *[S]ystematic, independent and documented process for obtaining evidence and evaluating it objectively in order to determine the extent to which the risk management framework (2.1.1), or any selected part of it, is adequate and effective.* (s. 12)

I ISO 22301:2012 definieras begreppet audit som:

> *[S]ystematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.* (s. 2)

Skillnaden mellan dessa definitioner är att den förstnämnda relaterar specifikt till ramverket för riskhantering. Samtidigt ska den objektiva utvärderingen i den sistnämnda definitionen göras för att avgöra till vilken grad *audit criteria* uppnås. I den förstnämnda definitionen ska den istället avgöra till vilken grad ramverket är adekvat och effektivt. Här kan det tyckas föreligga en diskrepans. Vid en närmare undersökning om vad som menas med *audit criteria* inses dock att begreppet kan omfatta effektivitet av de planer, policys och procedurer som utgör ett ledningssystem eller ramverk. Uttrycket: ”the extent to which audit criteria are fulfilled” utgör alltså en generell form av det mer specifika uttrycket: ”the extent to which the risk management framework (2.1.1), or any selected part of it, is adequate and effective“. Då begreppet *risk management audit* relaterar specifikt till riskhantering är en definition som också relaterar specifikt till riskhantering att vänta, varför författaren anser att det inte föreligger någon diskrepans i definitionerna. Kategorin bedöms därför vara kompatibel.

5.3.2 Definitioner av event och incident

Definitionen av begreppet *event* är precis likadan i både ISO 22300:2012 och i ISO_IEC 73:2009. Definitionen lyder:

> *Occurrence or change of a particular set of circumstances. NOTE 1 An event can be one or more occurrences, and can have several causes. NOTE 2 An event can consist of something not happening. NOTE 3 An event can sometimes be referred to as an “incident” or “accident”. NOTE 4 An event without consequences (3.6.1.3) can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.* (ISO_IEC 73:2009, s. 6)

I ISO 22300:2012 ges även en definition av begreppet *incident* som lyder: ”Situation that might be, or could lead to, a disruption, loss, emergency or crisis” (s. 3).

Enligt NOTE 3 i definitionen av *event* kan begreppet *incident* användas istället för *event.* Även om grunddefinitionerna av *incident* och *event* är olika anser författaren att de inte är motstridiga. Däremot finns det en diskrepans mellan definitionen av *incident* och beskrivningen av *incident* under NOTE 4 i definitionen av *event*. Beskrivningen av *incident* under NOTE4: ”An event without consequences” stämmer uppenbarligen inte

överens med definitionen av *incident* i ISO 22300:2012. Författaren anser att denna diskrepans är tillräcklig för att kategorin ska bedömas som inkompatibel.

5.3.3 Definitioner av stakeholder och interested party

I ISO_IEC 73:2009 definieras begreppet *stakeholder* som: "[P]erson or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity" (s. 3).

I ISO 22301:2012 ges precis samma definition både av begreppet *stakeholder* och av begreppet *interested party*. I ISO 22300:2012 ges dock en avvikande definition av *stakeholder* som lyder: "[P]erson or group of people that holds a view that can affect the *organization* (2.2.9)" (s. 1).

Då den förstnämnda definitionen både inkorporerar de som kan påverka beslut och de som kan påverkas av beslut, medan den sistnämnda definitionen endast beaktar de som kan påverka, anser författaren att det föreligger en diskrepans definitionerna emellan. Av denna anledning bedöms kategorin vara inkompatibel.

5.3.4 Definitioner av risk

I samtliga standarder där begreppet *risk* definieras lyder definitionen: "Risk - effect of uncertainty on objectives" (ISO_IEC 73:2009, s. 1).

Till definitionerna ges även fem identiska noter som förklarar vad effekter och mål kan vara och att risk ofta karaktäriseras och uttrycks i kombinationer av sannolikheter och konsekvenser. I ISO 22301:2012 ges ytterligare en not som lyder:

> *NOTE 6 In the context of business continuity management system standards, business continuity objectives are set by the organization, consistent with the business continuity policy, to achieve specific results. When applying the term risk and components of risk management, this should be related to the objectives of the organization that include, but are not limited to the business continuity objectives as specified in 6.2.* (s. 8)

Då den tillagda noten inte beskriver en annan innebörd av begreppet utan ger exempel på tillämpning av det, anser författaren att noten inte innebär någon diskrepans mellan definitionerna. Kategorin bedöms därför vara kompatibel.

5.3.5 Definitioner av risk treatment och mitigation

I ISO_IEC 73:2009 definieras begreppet *risk treatment* som:

> *[R]isk treatment [-] process to modify risk (1.1)*
> *NOTE 1 Risk treatment can involve:*
> *— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;*
> *— taking or increasing risk in order to pursue an opportunity;*
> *— removing the risk source (3.5.1.2);*

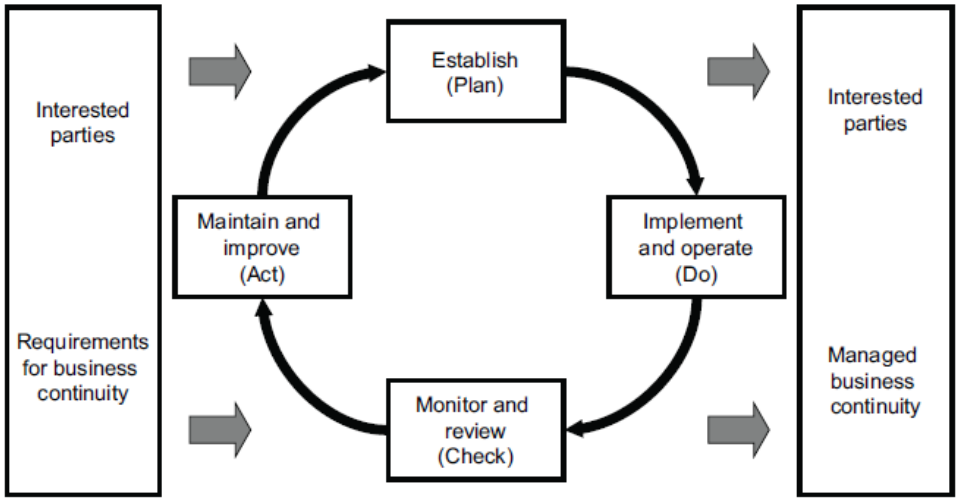
> *— changing the likelihood (3.6.1.1);*
> *— changing the consequences (3.6.1.3);*
> *— sharing the risk with another party or parties [including contracts and risk financing (3.8.1.4)]; and*
> *— retaining the risk by informed decision.*
> *NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".*
> *NOTE 3 Risk treatment can create new risks or modify existing risks.* (SS. 9-10)

I ISO 22300:2012 definieras begreppet *mitigation* som: "[M]easures taken to prevent, limit and reduce impact of the negative *consequences* (2.1.9) of incidents, emergencies and disasters" (s. 3).

Enligt NOTE 2 I den första definitionen kan begreppet *risk mitigation* användas för *risk treatment* som hanterar negativa konsekvenser. Även om definitionen av *risk treatment* ger en mer detaljerad beskrivning av de aktiviteter som kan vidtas än vad definitionen av *mitigation* ger, anser författaren att de är överensstämmande och att det inte föreligger någon diskrepans dem emellan. Kategorin bedöms därför vara kompatibel.

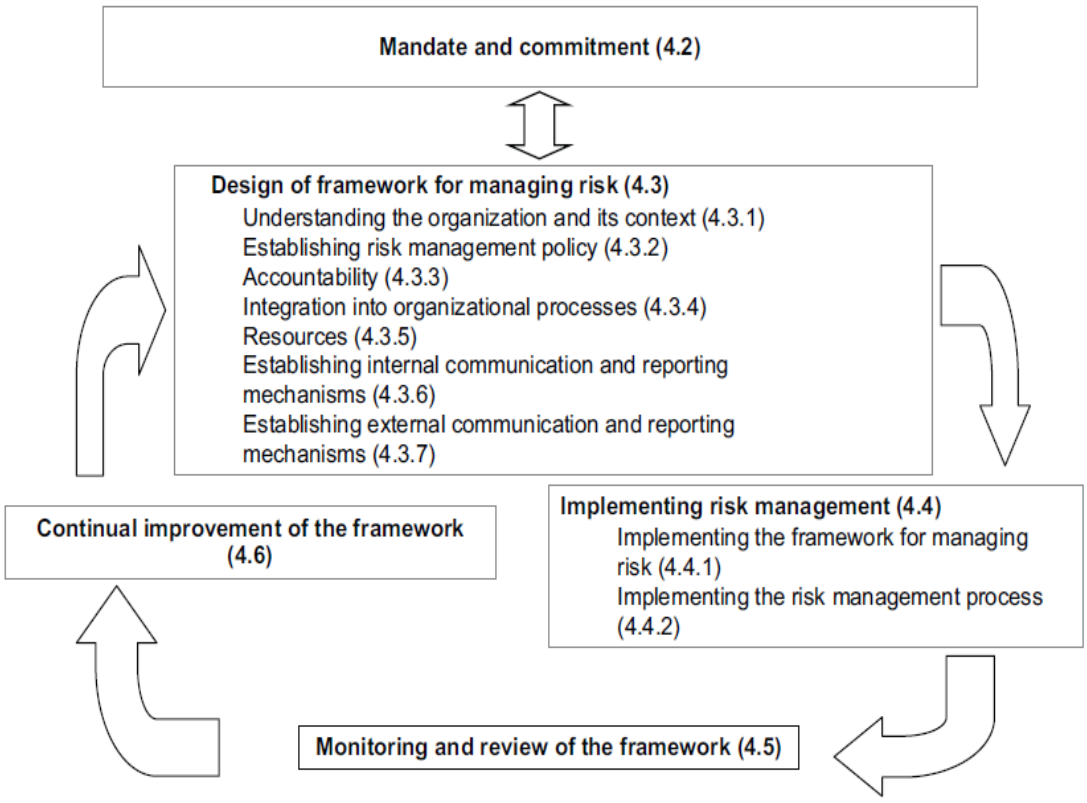
5.3.6 Relation mellan ledningssystem och processer

I båda standardfamiljerna beskrivs riskhanteringsprocesser och kontinuitetshanteringsprocesser som ingående komponenter i ledningssystemet eller ramverket och inte tvärtom. I båda standardfamiljerna utgör den så kallade PDCA-cykeln ett viktigt fundament i de ledningssystem och ramverk som beskrivs, även om namnet PDCA-cykeln inte används i ISO 31000:2009. I båda fallen beskrivs hur processerna utförs i enlighet med PDCA-cykeln se figur 5.1 och figur 5.2. I ISO 31000:2009 betraktas i många sammanhang riskhanteringsprocessen som en helt självständig del av ramverket för riskhantering. Till exempel ges den en helt egen apparat av planering, implementering, övervakning och granskning. Detta kan skönjas i figur 5.2 där implementering av ramverket och implementering av riskhanteringsprocessen skiljs åt. I ISO 22301:2012 betraktas riskhanteringsprocessen och processer för kontinuitetshantering långt mycket mer som en integrerad del av ledningssystemet. I övervakningsavsnittet listas till exempel komponenter som bör utvärderas från riskhanteringsprocessen tillsammans med komponenter från övriga ledningssystemet. En särskild övervaknings- och granskningsapparat för riskhanteringsprocessen skiljs inte ut så som den görs i ISO 31000:2009. Författaren anser att denna skillnad har så pass stor inverkan på många av de beskrivna aktiviteterna i standarderna, att den bör betraktas som en diskrepans. Kategorin bedöms därför som inkompatibel.



Plan (Establish)	Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

Figur 5.1 PDCA-cykeln applicerad på ledningssystem för kontinuitetshantering (ISO 22301:2012, s. vi).



Figur 5.2 Schematisk illustration av PDCA-cykeln applicerad på ramverket för riskhantering (ISO 31000:2009, s.9).

5.3.7 Hur extern kontext etableras

I båda standardfamiljerna ges utförliga beskrivningar av hur organisationens externa kontext bör kartläggas och tas i beaktning. I båda fallen ges nästan identiska beskrivningar av vilka externa faktorer som bör tas i beaktning, däribland: ”[…] the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment” (ISO 31000:2009, s. 10). I båda fallen ges även mer specifika beskrivningar av hur den externa kontexten ska tas i beaktning när mål, policy och riskkriterium bestäms. I ISO 31000:2009 beskrivs hur en extern kontext ska etableras för ramverket men också hur en mer detaljerad kontext ska etableras för själva riskhanteringsprocessen. Ett exempel på den mer detaljerade etableringen av kontexten är att externa intressenters mål och värderingar tas i beaktning vid bestämmande av riskkriterium. I den andra familjen av standarder återfinns inte detta perspektiv, även om upprättande av kontext nämns som ett steg i riskbedömningen. Det är svårt att avgöra om åtskillnaden mellan kontext för ramverket och kontext för riskhanteringsprocessen som återfinns i den ena familjen av standarder bör betraktas som en diskrepans från hur kontexten beskrivs i den andra familjen av standarder. Då det i ISO 22313:2012 tydligt framgår att externa intressenters värderingar och perspektiv ska tas i beaktning vid utformning av hela ledningssystemet inklusive riskbedömningen, anser författaren att skillnaden kan betraktas som en skillnad i detaljnivå beskrivningarna emellan. Kategorin bedöms därför vara kompatibel.

5.3.8 Övervakning och granskning

Båda standardfamiljerna innehåller mycket omfattande beskrivningar av hur övervakning och granskning bör utföras. Det allra mesta är samstämmigt mellan standarderna och handlar bland annat om att undersöka hur väl policy och planer implementeras och efterföljs, hur den externa kontexten förändras, hur lämpliga policys, planer, mål, riskkriterium etcetera är med hänsyn till nya externa och interna faktorer, hur effektivt ledningssystemet är och hur effektiva olika riskbehandlingsåtgärder är.

Vilka delar av ledningssystemen och processerna som bör övervakas, granskas och utvärderas är till största delen samstämmigt mellan standardfamiljerna även om vissa komponenter nämns i några av standarderna men inte i andra. Sådana skillnader anser författaren dock inte utgöra diskrepanser med hänvisning till avsnitt 4.2 Jämförande analys av standarder. När det gäller övervakning och granskning av ledningssystemets prestanda ska enligt ISO 31000:2009 detta göras gentemot så kallade *performance indicators*. I ISO 22301:2012 används istället begreppet *performance metrics*. Även om språkbruket skiljer sig åt handlar det egentligen om samma saker, nämligen mätbara parametrar som indikerar på prestanda.

En påtaglig skillnad är att ISO 31000:2009 i vanlig ordning skiljer ut riskhanteringsprocessen från resten av ramverket. Detta innebär att övervakning och granskning av riskhanteringsprocessen beskrivs i egna avsnitt. Likt resonemanget kring den externa kontexten anser författaren även i detta fall att det främst rör sig om en

skillnad i detaljnivå. De flesta komponenterna i riskhanteringsprocessen som enligt 31000:2009 bör granskas och övervakas återfinns dessutom i ISO 22301:2012, om än inte i ett eget avsnitt. Av dessa anledningar bedöms kategorin vara kompatibel.

5.3.9 Ledningens roll, ansvar och engagemang

Vad gäller ledningens roll och engagemang betonar båda familjerna av standarder att ett starkt engagemang hos ledningen är avgörande för att ledningssystemet ska lyckas. Många aktiviteter som ledningen bör utföra beskrivs i båda standardfamiljerna. Några exempel är att upprätta och kommunicera policys, se till att mål och policys för kontinuitetshantering och riskhantering stämmer överens med organisationens övergripande mål och policys, tillhandahålla tillräckliga resurser för riskhantering och kontinuitetshantering, se till att övervakning och granskning utförs och att fördela ansvar och roller i organisationen. I båda fallen förespråkas även att en enskild person i ledningen ges det övergripande ansvaret för ledningssystemet.

I ISO 31000:2009 nämns några ytterligare aktiviteter som inte nämns i den andra familjen av standarder, bland annat att ledningen bör säkerställa att organisationens kultur och policy är i linje och att ledningen ska bestämma så kallade *risk management performance indicators*. I ISO 22301:2012 nämns också några aktiviteter som inte nämns i ISO 31000:2009 eller i ISO_TR 31004:2013, bland annat att ledningen bör förespråka effektiv kontinuitetshantering och kontinuerliga förbättringar. Författaren anser inte att dessa skillnader utgör diskrepanser enligt avsnitt 4.2 Jämförande analys av standarder, varför kategorin bedöms vara kompatibel.

5.3.10 Implementering och integrering av ledningssystem

Både ISO 31000:2009, ISO_TR 31004:2013 och ISO 22301:2012 gör gällande att de ledningssystem eller ramverk som standarderna beskriver syftar till att integreras i organisationens övergripande ledningssystem. Detta illustreras med följande citat:

> *[B]usiness continuity management system[,] BCMS[, -] part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.* (ISO 22301:2012, s. 2)

> *[T]he framework for managing risk should be realized by integrating its components into the organization's overall system of management and decision making, irrespective of whether the system is formal or informal.* (ISO_TR 31004:2013, s. 2)

I ISO 31000:2009 och ISO_TR 31004:2013 ges en del råd kring hur ramverket kan implementeras och integreras rent praktiskt. Följande citat ger exempel på detta:

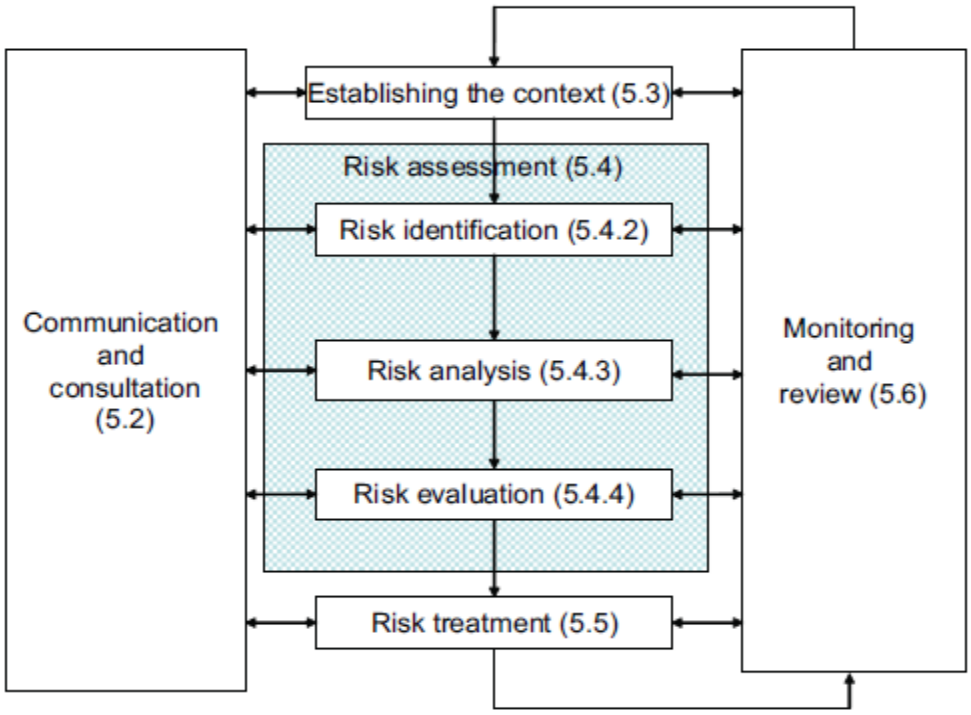
> *Typically, the implementation process includes the following:*
> *a) acquiring mandate and commitment, if required;*
> *b) a gap analysis;*
> *c) tailoring and scale based on organizational needs, culture and creating and protecting value;*
> *d) evaluating risks associated with transition;*

> *e) developing a business plan:*
> *— setting objectives, priorities and metrics;*
> *— establishing the business case, including alignment with organizational objectives;*
> *— determining scope, accountabilities, timeframe and resources;*
> *f) identifying the context of implementation, including communication with stakeholders.* (ISO_TR 31004:2013, s. 3)

I de andra standarderna ges egentligen inga praktiska råd av det här slaget. En likartad beskrivning av vilka faktorer som bör tas i beaktning när ett ledningssystem eller ramverk implementeras, ges dock i båda standardfamiljerna. Att ISO 31000:2009 och ISO_TR 31004:2013 ger mer praktiska råd kring implementeringen anser författaren inte utgöra någon diskrepans, varför kategorin bedöms vara kompatibel.

5.3.11 Riskhanteringsprocessens delsteg

I ISO 31000:2009 ges mycket utförliga beskrivningar av riskhanteringsprocessens ingående delar och relationerna dem emellan, vilka illustreras i figur 5.3.



Figur 5.3 Riskhanteringsprocessen (ISO 31000:2009, s.14).

I ISO 22301:2012 och i ISO 22313:2012 används inte begreppet *risk management process* på ett enda ställe. Det ges däremot två korta beskrivningar av de liknande begreppen *process for business impact analysis and risk assessment* samt *risk assessment process*. I dessa beskrivningar nämns följande ingående aktiviteter: ”establish context”, ”identify risks”, ”systematically analyse risk”, ”evaluate”, ”Identify treatments” och ”communicate risks”. Vid jämförelse av dessa aktiviteter med de ingående delarna i den riskhanteringsprocess som beskrivs i ISO 31000:2009, inses att de överensstämmer någorlunda väl. Dock saknas övervakning och granskning helt som

ett ingående moment i beskrivningarna av *risk assessment process*. Dessutom berör beskrivningarna endast identifiering av riskbehandlingsåtgärder, inte val och implementering av åtgärder, vilket ingår i det riskbehandlingssteg som beskrivs i ISO 31000:2009. I ISO 22301:2012 finns beskrivningar av riskbehandling, övervakning och granskning i andra avsnitt. Aktiviteterna tar dock samma plats i det flödesschema som visas i figur 5.3. Alla dessa omständigheter gör att det är svårt att avgöra kompatibiliteten i kategorin. Först och främst rör sig beskrivningarna om olika begrepp, varför det vore något strängt att avkräva samstämmiga beskrivningar av ingående komponenter. Samtidigt finns de delar som ingår i riskhanteringsprocessen i ISO 31000:2009, beskrivna i 22301:2012, även om de inte är sammanförda under ett och samma begrepp. Författaren anser dock att processen i sin helhet är så pass central i båda standarderna att den bör benämnas och struktureras på samma sätt, för att beskrivningarna av den ska vara kompatibla. Av denna anledning bedöms kategorin vara inkompatibel.

5.3.12 Riskbedömning

I figur 5.3 illustreras vilka delmoment som enligt ISO 31000:2009 ingår i riskbedömningen. Av figuren framgår att riskbehandling inte är en del av riskbedömning, utan en del av den övergripande riskhanteringsprocessen. I ISO 22301:2012 ges som tidigare nämnts en beskrivning av riskbedömning som även inkluderar identifiering av riskbehandlingsåtgärder. I ISO 31000:2009 ingår detta i begreppet riskbehandling och ligger således utanför riskbedömningen. I övrigt innehåller beskrivningen av riskbedömning i ISO 22301:2012 de tre delmomenten som inkluderas i riskbedömning enligt figur 5.3. Att ISO 22301:2012 inkorporerar delar av riskbehandling i riskbedömningen anser författaren dock vara en tillräckligt stor diskrepans för att kategorin ska bedömas som inkompatibel. Det bör dock påpekas att definitionen av *risk assessment* i ISO 22300:2012 endast innehåller de tre delmomenten i figur 5.3.

5.3.13 Riskidentifiering, riskanalys och riskvärdering

Riskbedömningens tre delsteg riskidentifiering, riskanalys och riskvärdering, beskrivs väldigt utförligt i ISO 31000:2009 och ISO_TR 31004:2013. Bland annat förekommer dessa tre beskrivningar:

> *Risk identification [-] The organization should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences.* (ISO 31000:2009, s. 17)

> *Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur.* (ISO 31000:2009, s. 18)

> *Risk evaluation [-] The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment […].* (ISO 31000:2009, s. 18)

I ISO 22313:2012 ges bland annat dessa två kortare beskrivningar:

> *[A] structured process for analysing risk in terms of consequences and likelihood […] This structured process attempts to answer some fundamental questions:*
> *a) What may happen and why (risk identification)?*
> *b) What might be the consequences?*
> *c) What is the likelihood of them happening? and*
> *d) Is there anything that might mitigate the consequences.* (s. 20)

> *[E]valuation of risks: Evaluate which disruption related risks require treatment.* (s. 20)

Beskrivningarna i ISO 22313:2012 är långt ifrån lika uttömmande som beskrivningarna i ISO 31000:2009, där varje enskilt steg tillägnats ett eget avsnitt. Vid jämförelse av beskrivningarna kan dock en god överensstämmelse skönjas samtidigt som författaren inte finner några diskrepanser. De tre kategorierna bedöms därför vara kompatibla.

5.3.14 Övriga kategorier

I de kategorier som inte behandlas i de föregående avsnitten har författaren inte kunnat finna några diskrepanser och samtliga av dessa kategorier bedöms vara kompatibla.

5.4 Resulterande kompatibilitetskoefficient

Med hjälp av resultaten i tabell 5.3, variablernas vikter i tabell 5.2 samt ekvation (3) i avsnitt 4.3 Sammanvägning av aspekter, bestäms kompatibilitetskoefficienterna e_A, e_B och e_C för huvudaspekt A: Definitioner av begrepp, B: Beskrivningar av ramverk och ledningssystem och C: Beskrivningar av processer för riskhantering och kontinuitetshantering till 0,86, 0,91 respektive 0,74. Utifrån dessa värden och huvudaspekternas vikter i tabell 5.1, samt ekvation (4) i avsnitt 4.3 Sammanvägning av aspekter, bestäms den övergripande kompatibilitetskoefficienten c mellan de två standardfamiljerna till 0,83.

5.5 Orsaker till inkompatibla inslag

I intervjuerna pekar flera respondenter på att den viktigaste orsaken till eventuella inkompatibla inslag standarderna emellan torde vara ISO:s grundstruktur. ISO är en mycket decentraliserad organisation, där de individuella kommittéerna har stor makt när de utformar standarderna genom sina egna politiska förhandlingsprocesser. I dessa förhandlingsprocesser deltar individer, med olika bakgrund, intressen, perspektiv och ibland, enligt en respondent, även helt egna agendor. Följden av detta blir att förhandlingar i olika kommittéer kring en och samma aspekt, kan få helt olika utfall, beroende av vilka som deltagit i de olika förhandlingsprocesserna. En respondent beskriver till och med incidenter där kommittén försökt göra en standard kompatibel med någon annan standard, men där det uppstått politiska förhandlingar kring vad som egentligen ska anses vara kompatibelt och inte. En respondent påpekar att detta

grundproblem har blivit väldigt tydligt när det gäller just olika standarder som rör ledningssystem. Antalet certifierbara ledningssystemstandarder har enligt respondenten fullständigt exploderat på senare år och omfattar idag ett 20-tal olika standarder, jämfört med ett fåtal på nittiotalet. Att homogenisera förhandlingsprocesserna mellan två kommittéer kan enligt respondenten vara nog så svårt för att inte tala om ett 20-tal olika kommittéer. Ett annat problem är att kommittéerna tar fram standarder vid olika tidpunkter, vilket ytterligare försvårar försök att homogenisera utformningen.

ISO har enligt två respondenter nyligen tillsatt en arbetsgrupp vid namnet joint technical group, i vilken en av respondenterna även har deltagit. Denna arbetsgrupp har tagit fram en standardiserad mall, som fastlägger ett ramverk för hur ledningssystemstandarder ska utformas. Mallen går under namnet Annex SL. I mallen är hela strukturen och kapitelindelningen för ett ledningssystem fastlagd medan de individuella kommittéerna ges möjlighet att plocka in sina olika kärnområden på avsedda platser i den redan fastlagda strukturen. På flera ställen i mallen återges hela textstycken som ska finnas med i samtliga ledningssystemstandarder, i textstyckena ges de individuella kommittéerna möjligheten att stoppa in lite egna ord i avsedda luckor. Dessutom standardiserar Annex SL en mängd definitioner och begrepp som ska användas i ledningssystemstandarderna.

Enligt en respondent uppstod det flera politiska strider mellan olika kommittéer om vilken roll riskhantering skulle ha i Annex SL och vilka perspektiv på riskhantering som skulle inkorporeras i mallen. Kommittén ISO/TC 262 insisterade, enligt respondenten, på att riskhanteringsdelarna i Annex SL skulle utföras helt i enlighet med ISO 31000:2009, vilket flera andra kommittéer motsatte sig. Enligt respondenten blev resultatet av striderna att riskhantering inkorporerades i Annex SL, men att den samtidigt kom att skilja sig från ISO 31000:2009 på flera sätt. Bland annat fick begreppet risk en annan definition i Annex SL som lyder: ”[R]isk [-] effect of uncertainty” (International Organization for Standardization [ISO], 2012, s. 144). Från och med nu ska enligt respondenten alla nya ledningssystemstandarder utformas enligt Annex SL, samtidigt som flera existerande standarder ska revideras enligt Annex SL. Respondenten påpekar att ISO 22301:2012 är den första publicerade standarden som följer mallen i Annex SL. Detta innebär att inkompatibla inslag mellan Annex SL och ISO 31000:2009 har kunnat fortplantas in i ISO 22301:2012. Enligt respondenten beslöt dock kommittén ISO/TC 223 att göra ett avsteg från mallen när det gäller definitionen av risk, som istället definierades på samma sätt som i ISO 31000:2009.

En fundamental skillnad mellan ISO 31000:2009 och ISO 22301:2012 är som tidigare nämnts att ISO 31000:2009 beskriver ett ramverk för riskhantering istället för ett ledningssystem för riskhantering. Enligt en intervjurespondent beror denna skillnad på en rädsla för att en certifierbar ledningssystemstandard för riskhantering, skulle starta en certifieringsvåg av organisationers riskhantering. Att istället göra en icke certifierbar standard med ett ramverk för riskhantering var ett strategiskt beslut för att undvika en sådan certifieringsvåg. Enligt respondenten är dock ramverket för riskhantering i princip identiskt med ett ledningssystem och att det i praktiken egentligen bara rör sig om ett

annat ordval. Detta styrker valet att i studien betrakta begreppen som synonyma. Att ISO 31000:2009 principiellt inte utgör en ledningssystemstandard har dock den praktiska implikationen att standarden vid revidering inte behöver följa Annex SL, som ju bara berör ledningssystemstandarder. Detta innebär en möjlighet för inkompatibla inslag att överleva eventuella revideringsprocesser. Samtidigt kan det leda till att ISO 31000:2009 utvecklas i en annan riktning än ISO 22301:2012 och andra standarder som följer Annex SL, vilket i sin tur skulle kunna innebära att nya inkompatibla inslag uppstår.

5.6 Hur kompatibilitet kan faciliteras

Respondenterna i intervjuerna lyfter fram två mekanismer som används inom ISO för att likrikta arbetet i olika kommittéer och möjliggöra för mer kompatibla standarder. Den ena är användandet av så kallade liaisons. Liaisons mellan kommittéer innebär att kommittéerna får ta del av varandras dokument och att de officiellt utser personer som deltar på varandras möten. Tanken med detta är att möjliggöra för kommittéerna att få inblick i hur andra kommittéer hanterar vissa frågor. De utsända personerna ska kunna informera den gästade kommittén om hur den egna kommittén arbetar, och samtidigt informera den egna kommittén om hur den gästade kommittén arbetar. Flera av respondenterna påpekar dock att denna mekanism ofta fungerar dåligt i praktiken: ”Vi skickar dokumenten till varandra, men det är oftast ingen som läser dem, vi har ju så mycket annat att göra.”

En annan viktig mekanism som syftar till att likrikta arbetet i olika kommittéer är de standarder och andra styrdokument som tas fram helt i syfte att standardisera utformningen av olika standarder. Ett exempel är ISO_IEC 73:2009 Risk management – Vocabulary som syftar till att standardisera terminologin i standarder som relaterar till riskhantering. Ett annat exempel är den mall för ledningssystemstandarder, Annex SL, som diskuteras i föregående avsnitt. Enligt flera respondenter får sådana dokument oftast ett stort genomslag inom ISO och har stor praktisk nytta. Till exempel har enligt respondenterna både ISO 9001:2008 som standardiserar kvalitetsledningssystem och ISO/IEC 27001:2013 som standardiserar ledningssystem för informationssäkerhet redan reviderats utifrån Annex SL.

Mot bakgrund av fynden i intervjuerna anser författaren att standardiserande styrdokument såsom Annex SL är rätt väg att gå för att facilitera kompatibilitet mellan standarder som tas fram i olika kommittéer. När det gäller ledningssystemstandarder får den närmaste tiden utvisa hur lyckat försöket med Annex SL blir. För att göra standarderna i kommittén ISO/TC 262 mer kompatibla med standarderna i kommittén ISO/TC 223 anser författaren att de bör revideras utifrån Annex SL. När det gäller andra standarder på området samhällssäkerhet och riskhantering, skulle en arbetsgrupp inom ISO kunna tillsättas för att ta fram tydliga riktlinjer för hur sådana standarder ska utformas.

Ett annat verktyg för att facilitera kompatibilitet mellan standarder skulle kunna vara att i utvecklingsprocessen applicera en liknande metod som används i denna studie. ISO skulle till exempel kunna utveckla en förenklad, generaliserad och standardiserad sådan metod, som kan appliceras på en standard under utveckling eller en standard under revidering. Författaren har dock för lite kännedom om hur utvecklingsprocessen av standarder inom ISO ser ut, för att kunna avgöra om implementering av ett sådant verktyg vore genomförbart.

6 Diskussion

I detta kapitel diskuteras studiens metodval, den applicerade metodens reliabilitet och validitet samt förslag till vidare forskning.

6.1 Val av metod

En stor svårighet i denna studie har varit att avgöra vad som egentligen ska undersökas. Eftersom kompatibilitet mellan standarder kan ha många olika innebörder, måste det preciseras exakt vilken kompatibilitet som ska undersökas och varför. Detta blir helt avgörande för vilka metoder som är lämpligast för att undersöka kompatibiliteten. Det kompatibilitetsbegrepp som författaren preciserade och definierade gjorde valet av kvalitativ dokumentanalys som huvudsaklig metod naturligt. Detta då texten i standarddokumenten utgör den primära datan som författaren anser vara mest värdefull.

Valet av semi-strukturerade intervjuer som en komplementerande metod var inte lika självklart. Det fanns initialt förhoppningar om att intervjuerna skulle kunna validera eventuella fynd av inkompatibla inslag från dokumentanalysen. Detta visade sig dock vara svårt, då kännedom om sådana inslag hos respondenterna nästan kräver att de själva har utfört eller tagit del av utförliga undersökningar av kompatibiliteten. Intervjuerna var ändå nyttiga på flera vis. Framför allt för att finna orsaker till att standarder inte alltid blir helt kompatibla, samt för att finna idéer om hur sådana problem kan avhjälpas. Dessutom bidrog intervjuerna med ett nyttigt underlag för sammanvägning av aspekter. Det är dock möjligt att enkätundersökningar hade varit en mer lämplig och effektiv metod för att samla in data till detta underlag. Att den semi-strukturerade intervjuformen valdes framför en strukturerad eller ostrukturerad form anser författaren ha varit sunt, då formen möjliggjorde för insamling av strukturerad data som grund för sammanvägningen av aspekter. Formen tillät samtidigt respondenterna att ge de öppna och utförliga svar som var värdefulla för att identifiera orsaker till och lösningar på inkompatibla inslag. En strukturerad intervjuform hade troligtvis också kunnat ge ett nyttigt underlag för sammanvägningen, men sannolikt också minskat möjligheten att erhålla lika värdefulla svar om orsaker och lösningar. En ostrukturerad form hade tvärtom inte kunnat bidra med ett lika nyttigt underlag för sammanvägningen, men gett nyttiga svar om orsaker och lösningar.

6.2 Reliabilitet och validitet

Reliabilitet innebär tillförlitlighet hos en mätning och validitet innebär i vilken utsträckning mätningen mäter det som den avser att mäta (Akram, Ireland, Postlethwaite, Sandy & Jerreat, 2013). Tillförlitlighet hos en mätning kan bland annat innebära att mätningen producerar samma resultat oavsett utförare eller oavsett tidpunkt, så kallad ”test-omtest” reliabilitet. Undersökningen i denna studie består av en

mängd delmoment vars reliabilitet och validitet bör diskuteras. I följande avsnitt diskuteras reliabiliteten och validiteten i dessa delmoment var för sig.

6.2.1 Den operationella definitionen av kompatibilitet

Vid mätningar med hjälp av operationaliseringar är validitet ett uttryck för hur väl de operationella definitionerna stämmer överens med de fenomen som studeras (Scarneci, 2012). I denna studie finns alltså en övergripande validitetsaspekt i hur väl den operationella definitionen av kompatibilitet stämmer överens med den mellan standarderna inneboende egenskapen kompatibilitet. Den inneboende kompatibiliteten som studien avser att mäta är samstämmighet och avsaknad av konflikter mellan texter. Den operationella definitionen är ett försök att operationalisera denna egenskap i en mängd olika aspekter. Validitetsproblemet består alltså i huruvida den inneboende egenskapen mäts när den operationellt definierade kompatibiliteten mäts. Det är främst två delar av den operationella definitionen som avgör validiteten, vilka ingående aspekter som väljs och hur de väljs, samt vilka principer som används när aspekterna vägs samman och hur dessa principer bestäms.

Valet av ingående aspekter i den operationella definitionen av kompatibilitet är det enskilt viktigaste momentet i studien sett ur ett validitetsperspektiv. Valet av ingående aspekter är nämligen helt avgörande för resultatet av mätningarna. Författaren har inte funnit någon behjälplig litteratur som skulle möjliggöra en evidensbaserad bestämning av ingående aspekter. Detta var inte heller att vänta då kompatibilitet mellan standarder är en ganska specifik kontext. Lösningen på validitetsproblemet har istället varit att låta de ingående aspekterna växa fram i en induktiv kontinuerlig process genom hela studien. Genom denna process har författaren försökt vidhålla ett objektivt förhållningssätt gentemot olika aspekter. Författaren anser att detta resulterat i en uppsättning aspekter som väl återspeglar innehållet i texterna och kontaktytorna mellan standarderna.

Hur kompatibilitet i olika underaspekter vägs in i det övergripande kompatibilitetsbegreppet är också viktigt sett ur ett validitetsperspektiv. Kompatibilitet och inkompatibilitet i underaspekter skulle kunna vägas in i den övergripande kompatibiliteten på en mängd olika sätt. Även i detta fall har författaren inte funnit någon litteratur som skulle kunna möjliggöra en evidensbaserad sammanvägningsprincip. Det går att argumentera för en mängd olika tillvägagångssätt i sammanvägningen. Till exempel att ett enda inkompatibelt inslag i en underaspekt per automatik innebär att standarderna som helhet är helt inkompatibla. Det skulle också gå att argumentera för att endast kompatibiliteten i de absolut viktigaste aspekterna bör beaktas i sammanvägningen. I denna studie har aspekterna delats in i ett antal huvudaspekter och underaspekter medan samtliga aspekter har tilldelats en vikt för sammanvägning. Vikterna har bestämts utifrån respondenternas graderingar av hur viktiga aspekterna är för kompatibilitet mellan standarder. Även här hade det gått att argumentera för en annan bestämning av vikterna utifrån graderingarna. Till exempel hade alla aspekter som graderats under en viss nivå kunnat tilldelas vikten 0, medan

aspekter som graderats över nivån tilldelats den vikt de graderats till. Det finns egentligen inga argument för att den väg som valts i studien är mer riktig än någon annan väg. Författaren anser dock att den sammanvägningsprincip som valts är den mest riktiga i brist på argument för andra sammanvägningsprinciper.

Validiteten i metoden för hur graderingar av aspekterna samlas in är en annan viktig aspekt. Det går att ställa sig frågan om huruvida respondenterna i intervjuerna besitter tillräckliga och lämpliga kunskaper för att kunna gradera aspekterna på ett riktigt sätt. Författaren anser dock att personer som har varit med och utvecklat standarderna eller som har implementerat standarderna i organisationer, bör vara de som i störst grad besitter den sökta kunskapen.

6.2.2 Kodningsprocessen

Bortsett från validitetsaspekterna i bestämningen av kodningskategorier som diskuteras i föregående avsnitt, finns en viktig reliabilitetsaspekt i själva kodningsprocessen. I dokumentanalyser bör egentligen kodernas reliabilitet testas mellan olika utförare (Boolsen, 2007). Detta innebär att forskaren undersöker huruvida olika utförare kodar samma material på samma sätt. Dessutom bör forskaren undersöka om samma utförare kodar materialet på samma sätt vid olika tillfällen. Då denna studie har utförts av författaren allena har det förstnämnda reliabilitetstestet inte kunnat genomföras. Test-omtest reliabiliteten har å andra sidan, på sätt och vis, åstadkommits genom den iterativa bestämningen av kodningskategorier. Då författaren kontinuerligt reviderat kodningskategorierna efter materialet, anser författaren att den slutgiltiga uppsättningen av kategorier har hyfsat hög reliabilitet ur detta avseende. Då kodningskategorierna är ganska breda och omfattande är det svårt att i olika kodningar koda materialet till olika kategorier.

Det är troligt att andra utförare skulle landa i andra uppsättningar av kategorier, där till exempel några av författarens kategorier kan ha delats upp i mindre kategorier. Detta är en mycket viktig reliabilitetsaspekt. Låt säga att det till en viss huvudaspekt finns tio olika underkategorier och att de samtliga fått vikten $u_u = 4$. Detta innebär att $\frac{u_u}{\sum u_u} = \frac{4}{40} = 0{,}10$ för samtliga underkategorier. Om en av dessa kategorier istället hade brutits ned i tre mindre delar som var och en fått vikten $u_u = 2$ skulle dessa tre kategorier tillsammans ge ett större bidrag i sammanvägningen än vad den ursprungliga kategorin skulle ge, $\frac{2}{42} + \frac{2}{42} + \frac{2}{42} = 0{,}14$. Detta vore inte ett problem om respondenterna i sina graderingar av vikterna väger in kategoriernas bredder, så att smalare kategorier får mindre vikt än bredare kategorier. Författaren anser dock att det är mycket troligt att respondenter övervärderar smala kategorier och undervärderar breda kategorier. Exemplet ovan visar att om en kategori med vikten $u_u = 4$ delas i tre mindre delar, så behöver minst två av delarna graderas till 1 eller mindre om det sammanlagda bidraget från kategorierna inte ska överstiga bidraget från den ursprungliga kategorin. I studien har samtidigt inga aspekter graderats lägre än 2 oavsett bredd.

Kodningskategoriernas bredd har även stor inverkan på kompatibilitetsbedömningarna av enskilda kategorier. Låt säga att det finns en diskrepans i den ursprungliga kategorin i exemplet ovan. Diskrepansen innebär att kategorin som helhet betraktas som inkompatibel. Om kategorin istället hade bestått i tre mindre kategorier, så hade endast en av dessa kategorier bedömts som inkompatibel. Detta då diskrepansen endast kan förekomma i en av de tre kategorierna. Om antalet kategorier går mot oändligheten går kompatibilitetskoefficienten mellan standarderna mot 1. Om antalet kategorier går mot 1 går kompatibilitetskoefficienten mot 0. Förutsatt att antalet diskrepanser är större än 0 men mindre än oändligheten. Detta innebär alltså att smalare kategorier generellt ger högre kompatibilitetsvärden enligt den beskrivna metoden.

För att beakta dessa reliabilitetsproblem har författaren försökt hålla en konsekvent bredd på kodningskategorierna. Standarddokumentens indelningar i kapitel och avsnitt har utgjort nyttiga vägledningar för kodningskategoriernas bredd. Underkategorier i studien sammanfaller oftast med tydligt avgränsade avsnitt i standarddokumenten. Vad gäller definitionskategorier så avgränsas dessa mycket tydligt i form av de faktiska definitionerna i standarddokumenten.

6.2.3 Undersökning av kompatibilitet i enskilda aspekter

En viktig validitetsaspekt finns i bedömningen av huruvida underaspekter är kompatibla eller inte. Validiteten här består i huruvida de kriterier som används vid bedömningarna mäter den kompatibilitet som eftersöks. I denna studie har det viktigaste kriteriet, för att en aspekt ska bedömas som inkompatibel, varit förekomst av diskrepanser som består i direkt motstridiga uppgifter. Författaren anser att validiteten i detta grundkriterium är god, då det mäter samstämmighet och avsaknad av konflikter mellan texter relativt väl.

I bedömningarna av kompatibilitet i enskilda aspekter finns även en reliabilitetsaspekt. Reliabiliteten i bedömningarna består i huruvida samma resultat erhålls vid olika tidpunkter och utförare av bedömningarna. Utförarreliabiliteten har inte kunnat testas då författaren varit den enda utföraren av bedömningarna. Test-omtest reliabiliteten har dock undersökts i viss mån, då författaren gjort upprepade bedömningar av samtliga underaspekter. Även om resultaten inte har varit helt konsistenta så har de inte varierat avsevärt mycket. Det rör sig om någon enstaka aspekt som bedömts annorlunda vid olika tillfällen. Skälet till detta har mest varit en skillnad i analysens djup vid olika tillfällen. De senare bedömningarna har varit mer djupgående och har då kunnat identifiera diskrepanser som en mer ytlig bedömning har kunnat förbise.

En annan viktig reliabilitetsaspekt i bedömningarna är de värden som kompatibilitetskoefficienterna kan anta. I studien kan kompatibilitetskoefficienterna endast anta värdena 0 och 1. Om koefficienterna utifrån bedömningarna istället hade fått anta värden på en kontinuerlig skala mellan 0 och 1, så hade troligtvis en större precision i mätningarna åstadkommits. Exempelvis hade tveksamma kategorier då kunnat ges värdet 0,5 vilket torde ligga närmare den sanna kompatibiliteten än värdena 0 = fullständigt inkompatibel eller 1 = fullständigt kompatibel. Att tillåta fler möjliga

värden på kompatibilitetskoefficienterna kan dock innebära att den individuella bedömaren får större inverkan på resultatet. Med endast två möjliga värden är det troligare att olika bedömare ger samma värde, än om det skulle finnas tio möjliga värden. För att i största mån undvika subjektivitet har författaren i denna studie valt så få möjliga utfall av bedömningarna som möjligt, det vill säga två stycken, inkompatibel eller kompatibel. I en studie där utförarreliabiliteten hade kunnat observeras och kontrolleras anser författaren dock att fler möjliga värden, med tydliga bedömningskriterier för varje värde, vore att föredra.

6.2.4 Intervjuer

Vad gäller intervjuerna är det främst graderingen av aspekternas vikt som haft stor inverkan på resultatet. Validiteten i metoden för hur graderingarna samlats in diskuteras i avsnitt 6.2.1 Den operationella definitionen av kompatibilitet. I metoden finns även några intressanta reliabilitetsaspekter som bör diskuteras. En aspekt som är intressant ur reliabilitetssynpunkt är urvalet av respondenter. Vilka respondenter som väljs och ges möjlighet att gradera aspekterna har stor inverkan på resultatet. Detta kan skönjas i att intervjustudiens respondenter gett mycket varierande graderingar av vissa aspekter. Ett större urval av respondenter hade minskat enskilda graderingars inverkan och hade således kunnat bidra till en högre reliabilitet hos resultatet. Reliabiliteten i resultatet av dessa mätningar beror också på hur intervjuerna utförs. Exempelvis kan respondenterna ges möjlighet att gå tillbaks och ändra tidigare graderingar, vilket torde ge högre reliabilitet. Vilka ämnen som har behandlats och vad som har sagts tidigare i intervjun är andra faktorer som också kan påverka respondentens graderingar. En enkätundersökning med ett större urval av respondenter hade troligtvis kunnat råda bot på flera av dessa faktorer. En sådan metod hade därför troligtvis varit mer lämplig sett ur ett reliabilitetsperspektiv.

6.2.5 Resultat

Alla faktorer som diskuteras i de föregående avsnitten bidrar till reliabiliteten och validiteten i det slutgiltiga resultatet. Mot bakgrund av de föregående avsnitten anser författaren att reliabiliteten i resultatet är någorlunda god. Det som främst drar ner den övergripande reliabiliteten är den låga reliabiliteten i graderingarna av aspekternas vikter. Validiteten av resultatet innebär till vilken grad den resulterande kompatibilitetskoefficienten utgör ett riktigt mått på den inneboende kompatibiliteten mellan standarderna. Denna validitet är svår att avgöra vilket ofta är fallet med operationella definitioner i kvalitativa studier (Scarneci, 2012). Det är främst validiteten i sammanvägningsprincipen och valet av ingående aspekter som är svår att avgöra.

På grund av att reliabiliteten inte är jättehög och att validiteten inte är helt känd, bör det resulterande kompatibilitetsmåttet tas med en viss nypa salt. Måttet bör främst ses som en indikation på kompatibilitet mellan standarderna. Värdet på kompatibilitetskoefficienten 0,83 vittnar om att standarderna till stor del är kompatibla, men att det finns väsentliga inkompatibla inslag. Den utförliga analysen av de

inkompatibla inslagen i underaspekterna kan ge större insikt om hur kompatibla standarderna egentligen är.

6.3 Förslag till vidare forskning

Under arbetets gång identifierades ett antal områden som vore intressanta att studera, men som inte rymdes inom ramen för detta arbete. Dessa områden lämnas som förslag till framtida forskning.

6.3.1 Fördjupad kompatibilitetsstudie

I denna studie studerades relativt breda aspekter av de ingående standarderna. För att nå en mer valid och reliabel utvärdering av kompatibiliteten skulle en mer fördjupad studie kunna utföras. I en sådan studie skulle exempelvis underaspekterna i denna studie kunna brytas ner i aspekter på en större detaljnivå. Dessutom skulle sammanvägningsprincipen av aspekter kunna utvecklas. Intresset och den praktiska nyttan av en sådan studie är dock oklar. Det är möjligt att utvärderingen, som denna studie utgör, är tillräckligt god för att kunna vägleda i beslut om eventuella åtgärder såsom revideringar.

6.3.2 Utveckling av verktyg för undersökning av kompatibilitet i utvecklingsprocessen av standarder

För att facilitera kompatibilitet mellan standarder skulle ett verktyg kunna tas fram för att undersöka kompatibiliteten mellan standarder redan i utvecklingsprocessen av nya standarder, eller i revideringsprocessen av existerande standarder. Verktyget skulle kunna likna den metod som används i denna studie, men skulle troligtvis behöva förenklas och generaliseras.

6.3.3 Studier av kompatibilitet mellan andra ledningssystemstandarder och samhällssäkerhetsstandarder

Liknande kompatibilitetsstudier som denna skulle kunna utföras på andra standarder inom samhällssäkerhet och riskhantering. För att uppnå den samsyn som flera av dessa standarder eftersträvar kan det vara nödvändigt att harmonisera standarderna med varandra. Ett viktigt första steg i sådana processer torde vara att undersöka och säkerställa kompatibiliteten mellan samtliga standarder på området.

6.3.4 Studier av utvecklingsprocessen av standarder

Kompatibilitet mellan standarder beror till stor del på de generella utvecklingsprocesserna av standarder. Framförallt verkar de politiska förhandlingar, som utgör en betydande del av dessa processer, ofta vara problematiska. Hur dessa förhandlingar och processer fungerar och hur de skulle kunna förbättras vore ett intressant ämne att studera mer ingående.

7 Slutsatser

I detta kapitel redovisas slutsatserna av den genomförda studien. Slutsatserna relateras till frågeställningarna i avsnitt 1.2.1 Frågeställningar. Frågeställningarna som ligger till grund för studien är:

1. Hur kompatibla är de standarder som har tagits fram av ISO i kommittén ISO/TC 223 – Societal Security, med de standarder som har tagits fram av ISO i kommittén ISO/TC 262 – Risk Management?
2. Vad är inte kompatibelt mellan dessa standarder?
3. Vilka är orsakerna till att dessa standarder inte är helt kompatibla?
4. Hur kan standarder på området samhällssäkerhet göras mer kompatibla?

Den första frågeställningen (1) besvaras med följande slutsats:

Standarderna ISO 22300:2012, ISO 22301:2012 och ISO 22313:2012 är kompatibla med standarderna ISO_IEC 73:2009, ISO 31000:2009 och ISO_TR 31004:2013 till graden 0,83, enligt den operationella definition av kompatibilitet mellan standarder som författaren härleder. Det är svårt att avgöra hur god denna skattning av kompatibiliteten mellan standarderna är, då det är svårt att avgöra validiteten i de operationella definitionerna.

Den andra frågeställningen (2) besvaras med följande slutsats:

Mellan standarderna ISO 22300:2012, ISO 22301:2012 samt ISO 22313:2012 och standarderna ISO_IEC 73:2009, ISO 31000:2009 samt ISO_TR 31004:2013 är följande inslag inte kompatibla:

- Definition av begreppet *event.*
- Definition av begreppen *interested party* och *stakeholder* .
- Beskrivning av relation mellan ledningssystem och processer.
- Beskrivning av riskhanteringsprocessen, dess delar och relationerna dem emellan.
- Beskrivning av riskbedömning.

Den tredje frågeställningen (3) besvaras med följande slutsats:

De två främsta orsakerna till inkompatibla inslag som identifieras är att standarderna inom ISO utvecklas genom förhandlingsprocesser i helt åtskilda kommittéer och att standarderna i kommittén ISO/TC 223 har utvecklats i enlighet med Annex SL, medan standarderna i ISO/TC 262 inte har utvecklats i enlighet med Annex SL.

Den fjärde frågeställningen (4) besvaras med följande slutsats:

Utvecklingen av standarder på området samhällssäkerhet skulle kunna homogeniseras ytterligare med hjälp av övergripande styrdokument som standardiserar utformningen av standarder. För att göra standarderna i kommittén ISO/TC 262 mer kompatibla med standarderna i kommittén ISO/TC 223 och andra ledningssystemstandarder, bör de revideras utifrån Annex SL. Möjligen skulle också en apparat för att undersöka kompatibilitet mellan standarder, liknande den som används i studien, kunna implementeras i utvecklingsprocessen av nya standarder eller i revideringsprocessen av existerande standarder.

8 Referenser

Akram, A. J., Ireland, A. J., Postlethwaite, K. C., Sandy, J. R., & Jerreat, A. S. (2013). Assessment of a condition-specific quality-of-life measure for patients with developmentally absent teeth: validity and reliability testing. *Othodontics & Craniofacial Research, 16*(4), 193-201.

ANSI C63.14-1992. *American National Standard Dictionary for Technologies of electromagnetic Compatibility (EMC), Electromagnetic Pulse (EMP), and Electrostatic Discharge (ESD).* New York: Institute of Electrical and Electronics Engineers.

Antonsen, S., Skarholt, K., & Ringstad, A. J. (2012). The role of standardization in safety management - A case study of major of a major oil & gas company. *Safety Science, 50*(10), 2001-2009.

Bekhet, A., & Zauszniewski, J. (2012). Methodological triangulation: an approach to understanding data. *Nurse Researcher, 20*(2), 40-43.

Boolsen, M. W. (2007). *Kvalitativa analyser.* (B. Kärnekull, Övers.). Malmö: Gleerups.

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal, 9*(2), 27-40.

Bryman, A. (2012). *Samhällsvetenskapliga metoder*. (B. Nilsson, Övers.). Malmö: Liber.

Chungoora, N., Cutting-Decelle, A.-F., Young, R., Gunendran, G., Usman, Z., Harding, J., & Case, K. (2013). Towards the ontology-based consolidation of production-centric standards. *International Journal of Production Research, 51*(2), 327-345.

Ennis, R. H. (1964). Operational Definitions. *American Educational Research Journal, 1*(3), 183-201.

International Organization for Standardization [ISO]. (2012). *Annex SL*. Hämtad 2014-04-26, från http://www.kvaliteta.net/files/AnnexSL.pdf

ISO 22300:2012. *Societal Security – Terminology.* Geneve: International Organization for Standardization.

ISO 22301:2012. *Societal security – Business continuity management systems – Requirements.* Geneve: International Organization for Standardization.

ISO 22313:2012. *Societal security – Business continuity management systems – Guidance.* Geneve: International Organization for Standardization.

ISO 31000:2009. *Risk management - Principles and guidelines.* Geneve: International Organization for Standardization.

ISO_IEC 73:2009. *Risk management – Vocabulary.* Geneve: International Organization for Standardization.

ISO_TR 31004:2013. *Risk Management - Guidance for the Implementation of ISO 31000*. Geneve: International Organization for Standardization.

Johansson, M., & Nilsson, P. (2006). *Towards International Emergency Standards.* Lund: Lunds Universitet.

Kvale, S. (1997). *Den kvalitativa forskningsintervjun.* (S.-E. Torhell, Övers.). Lund: Studentlitteratur.

Lidberg, L.(2009). Standarders betydelse ökar. *Standard Magazine, 4*, 6-9.

Myndigheten för Samhällsskydd och Beredskap [MSB]. (2010). *Sverige leder standardiseringsarbete för samhällssäkerhet*. Hämtad 2014-01-21, från https://www.msb.se/sv/Om-MSB/Internationellt-arbete/ISO/Sverige-leder standardiseringsarbete-for-samhallssakerhet/

Myndigheten för Samhällsskydd och Beredskap [MSB]. (2012a). *Studie om standarisering inom samhällssäkerhet.* Hämtad 2014-01-21, från https://www.msb.se/Upload/Utbildning_och_ovning/Konferenser_seminarier/Dokumentation/Workshop%20standarder/4.%20Studie%20stand%20samh%C3%A4llss%C3%A4kerhet.pdf

Myndigheten för Samhällsskydd och Beredskap [MSB]. (2012b). *Film om MSB:s standardiseringsarbete.* [videofil] Hämtad 2014-01-21, från http://streamio.com/api/v1/videos/50cf4f4c11581e1bcc00a806/public_show?player_id=4c9b6854b35ea807b5000001&width=560&height=420

Myndigheten för Samhällsskydd och Beredskap [MSB]. (2012c). *Standarder möjligheter och effekter.* Hämtad 2014-02-21, från https://www.msb.se/Upload/Utbildning_och_ovning/Konferenser_seminarier/Dokumentation/Workshop%20standarder/2.%20Standarders%20m%C3%B6jligheter%20och%20effekter.pdf

Pearce, M.A., Hough, R.M., Cleverley, J.S., & Timms, N.E. (2013). Reaction mechanism for the replacement of calcite by dolomite and siderite: Implications for geochemistry, microstructure and porosity evolution during hydrothermal mineralization. *Contributions to Mineralogy and Petrology, 166*(4), 995-1009.

Sadler, G. R., Lee, H.-C., Lim, R. S.-H., & Fullerton, J. (2010). Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy. *Nursing and Health Sciences, 12*(3), 369-374.

Scarneci, F. (2012). How I became a qualitative researcher?. *Sociologija: Mintis ir veiksmas,1*(30), 258-275.

Skr. 2007/08:140. *Standardiseringens betydelse i en globaliserad värld.* Hämtad 2014-01-21, från http://www.regeringen.se/sb/d/10266/a/1036450

Svenska Akademiens Ordlista [SAOL]. (2006). *Kompatibel.* Stockholm: Norstedts akademiska förlag

Swedish Standards Institute [SIS]. (2012). *Standardisering SIS/TK 494 - Samhällssäkerhet*. Hämtad 2014-01-14, från http://www.sis.se/ledningssystem/samh%C3%A4llss%C3%A4kerhet/sis-tk-494

Trost, J. (2005). *Kvalitativa intervjuer.* Lund: Studentlitteratur.

Vanderstoep, S. W., & Johnston, D. D. (2008). *Research Methods for Everyday Life.* New York: Jossey-Bass.

Walliman, N. (2006). *Social Research Methods.* London: Sage Publications.

Weber, R. P. (1990). *Basic Content Analysis.* Thousand Oaks: Sage Publications.

Wellington, J., & Szczerbinski, M. (2007). *Research Methods for the Social Sciences.* London: Continuum International Publishing.

Yavari, A. (2013). Compatibility Equations of Nonlinear Elasticity for Non-Simply-Connected Bodies. *Archive for Rational Mechanics and Analysis, 209*(1), 237-253.

Bilaga A Intervjuguide

Denna bilaga innehåller den guide som används vid intervjuerna i studien. Då intervjuerna är av semi-strukturerad kvalitativ form, ska frågorna i guiden ses mest som riktlinjer. Utformningen och ordningen på frågorna kan improviseras fram under intervjuns gång.

Intervjuns inledning

Först ges en kort presentation av studiens och intervjuns syfte och form. Respondenten underrättas om att hans/hennes svar kommer att hanteras konfidentiellt men inte anonymt. I praktiken innebär detta att det i rapporten kommer att framgå vilka respondenter som har deltagit i intervjustudien, medan det inte kommer att framgå vilka respondenter som gett vilka svar. Respondenten meddelas möjligheten att när som helst avbryta intervjun. Respondenten meddelas även hur lång tid intervjun beräknas ta och att intervjun spelas in.

Intervjuguide brukare

Denna del utgör det underlag som används vid intervjuer med brukare.

Om respondentens relation till standarderna

Vilka av de standarder som tagits fram i kommittéerna ISO/TC 223 och ISO/TC 262 har du arbetat med? (räkna upp vilka dessa standarder är)

Vilken roll har du haft i arbetet med dessa standarder?

Vilka av dessa standarder anser du dig vara väl insatt i?

Om aspekter i standarderna

Hur viktiga är dessa aspekter för att standarderna ska vara kompatibla? (ange värde mellan 0 och 5) (här tas de aspekter som hittills identifierats i studien med.)

Finns det några andra aspekter som du anser vara viktiga ur ett kompatibilitetsperspektiv? (även dessa aspekter graderas av respondenten på samma sätt som i föregående fråga).

Kompatibilitet

Anser du att standarderna i ISO/TC 223 överlag är kompatibla med standarderna i ISO/TC 262?

Finns det något som inte är kompatibelt mellan standarderna i ISO/TC 223 och standarderna i ISO/TC 262?

Vilka problem har du stött på i arbetet med dessa standarder?

Upplever du att dessa standarder bidrar till en större samsyn mellan olika aktörer?

Anser du att aspekt x i standard x är kompatibel med aspekt x i standard y? (Viktiga aspekter väljs ut efter hur respondenten svarat i tidigare frågor.)

Intervjuguide utvecklare

Denna del utgör det underlag som används vid intervjuer med brukare.

Om respondentens relation till standarderna

Vilka av de standarder som tagits fram i kommittéerna ISO/TC 223 och ISO/TC 262 har du arbetat med? (räkna upp vilka dessa standarder är)

Vilken roll har du haft i arbetet med dessa standarder?

Vilka av dessa standarder anser du dig vara väl insatt i?

Om aspekter

Vad gör ni för att säkerställa kompatibiliteten mellan de standarder ni tar fram i en kommitté och de standarder som tas fram i andra kommittéer?

Vad är problematiskt i sådana processer?

Vad tror du skulle kunna göras för att lösa dessa problem och förbättra arbetet med att göra standarder mer kompatibla?

Vilka aspekter beaktar ni i dessa processer?

Hur viktiga är dessa aspekter ur ett kompatibilitetsperspektiv?: (ange värde mellan 0 och 5) (här tas de aspekter som hittills identifierats i studien med, inklusive de aspekter som respondenten nämnde i föregående fråga)

Finns det några andra aspekter som du anser vara viktiga ur ett kompatibilitetsperspektiv? (även dessa aspekter graderas av respondenten på samma sätt som i föregående fråga).

Kompatibilitet

Anser du att standarderna i ISO/TC 223 överlag är kompatibla med standarderna i ISO/TC 262?

Finns det något som inte är kompatibelt mellan standarderna i ISO/TC 223 och standarderna i ISO/TC 262?

Upplever du att dessa standarder bidrar till en större samsyn mellan olika aktörer?

Anser du att aspekt x i standard x är kompatibel med aspekt x i standard y? (Viktiga aspekter väljs ut efter hur respondenten svarat i tidigare frågor.)