Examensarbete

HÖGSKOLAN I SKÖVDE

SVENSKA VERKSAMHETERS UTMANINGAR MOT ETT CERTIFIKAT INOM INFORMATIONSSÄKERHET

En fallstudie om svenska verksamheters utmaningar för att certifiera sig enligt ISO 27001-standarden.

SWEDISH ORGANIZATIONS CHALLENGES TOWARDS A CERTIFICATE WITHIN INFORMATION SECURITY

A case studie about Swedish organizations challenges to gain a certificate according to the ISO 27001 standard.

Examensarbete inom huvudområdet informationsteknologi
Grundnivå - 30 Högskolepoäng
Vårterminen år 2023

Hanna Moffat

Handledare: Christian Lennerholt
Examinator: Mikael Berndtsson

Sammanfattning

I detta examensarbete är syftet att undersöka svenska verksamheters utmaningar i att uppnå en ISO 27001-certifiering med sitt arbete inom informationssäkerhet. Digitala medier och verktyg är numera en stor del av samhällsviktiga verksamheters tjänster samt operationer och det har bidragit till stora möjligheter såväl som stora sårbarheter. ISO 27001-certifieringar är den standard som ligger till grund för säkerhetsskyddslagen såväl som NIS-direktivet vilket gör att det är en standard som svenska verksamheter kan applicera.

Genom bakgrunden ges en inblick i vad informationssäkerhet är och hur det står i relation med cybersäkerhet. Bakgrunden innehåller även en introduktion till den svenska lagstiftningen inom informationssäkerhet såväl som ISO 27001-standarden för att belysa vad svenska verksamheter har att förhålla sig till när det kommer till sitt arbete med informationssäkerhet. I problemformuleringen lyfts de aktuella hoten och myndigheters uttalanden inom informationssäkerhet i Sverige och hur svenska verksamheter brister i dessa. Detta i kombination med den tidigare forskningen om hur utmaningar inom ISO 27001-certifieringar har tagit sitt uttryck för andra verksamheter.

Metoden redovisar hur kvalitativa intervjuer använts som verktyg för datainsamling till fallstudien men även hur det tagit sitt uttryck och beskriver processen – från förberedelse till läsbar produkt, vilket är detta examensarbete. I analysen ställs den insamlade datan i relation till tidigare forskning samt aktuella händelser för att se vilka utmaningar svenska verksamheter har för att uppnå en ISO 27001-certifiering.

Resultatet baseras på den insamlade datan då det är svenska verksamheters utmaningar som är aktuellt för fallstudien. Det resulterade i fyra utmaningar: motivation, tid och ekonomi, bransch samt komplexitet. Dessa utmaningar och dess bidragande faktorer redovisas i text såväl som figurer. Somliga av dessa utmaningar är utmaningar som lyfts i tidigare forskning, vilket gör att de även kan appliceras som utmaningar för svenska verksamheter. Uppsatsen avslutas med en diskussion där fallstudiens resultat diskuteras i olika perspektiv – samhälleliga, etiska samt vetenskapliga. Diskussion om val av metod, studiens resultat samt förslag på framtida forskning lyfts, där det diskuteras om hur lagar samt standarder inom informationssäkerhet är svåra att implementera samt förstå och om det ens är möjligt att göra det lättare.

Nyckelord: ISO 27001; ISO/IEC 27001; Informationssäkerhet; Svenska verksamheter; Säkerhetsskyddslagen; NIS-direktivet; NIS2-direktivet.

INNEHÅLLSFÖRTECKNING

1 Inledning

Digitaliseringen har gett oss oändligt med möjligheter och svenska hushåll har hakat på trenden. Internetstiftelsen (2022) senaste rapport visar exempelvis att 71% av svenskarna använder mobilt Bank-Id dagligen, 57% använder e-tjänster för kollektivtrafik samt att 85% har e-handlat det senaste året. Dessa oändliga möjligheter har i sin tur också skapat oändligt många hot. Cyberattacker är den snabbast växande formen av kriminalitet och ökar konstant när det kommer till omfattning, kostnader samt i form av sofistikation (COM(2020) 823).

ISO 27001-standarden är ett av de mest etablerade ramverken för en verksamhets arbete med informationssäkerhet och ett certifikat utfärdas för de verksamheter som klarar standardens krav (Disterer, 2013). När det kommer till Sverige visar statistiken att det inte är många verksamheter i Sverige som har en ISO 27001-certifiering (Babacus AB 2023). Rent generellt finns det brister i arbetet inom informationssäkerhet för svenska verksamheter och det baseras på Säkerhetspolisen (SÄPO) pressmeddelande från februari 2023. Där meddelade de att det finns flertalet brister inom säkerhetsskydd bland säkerhetskänsliga verksamheter inom alla områden i Sverige (SÄPO, 2023).

Detta examensarbete går ut på att undersöka vilka utmaningar svenska verksamheter har i att uppnå en ISO 27001-certifiering. Genom en fallstudie med kvalitativa intervjuer som verktyg har fyra verksamheter intervjuats – en privat verksamhet som vill uppnå en ISO 27001-certifiering, en offentlig verksamhet som arbetar utifrån vissa delar av ramverket, ett konsultbolag som hjälper verksamheter att applicera ramverket samt ett certifieringsorgan som utfärdar certifieringar för ISO 27001.

Den insamlade datan har tillsammans bidragit till fyra identifierade utmaningar för svenska verksamheter, som är baserade på olika faktorer som lyfts under intervjuerna. Tidigare forskning har fokuserat på den låga tillämpning av standarden och då med ett internationellt perspektiv där flertalet trender även går att applicera på utmaningar för svenska verksamheter att uppnå en ISO 27001-certifiering.

2 Bakgrund

I bakgrunden kommer det att ges en inblick i hur information samt informationssäkerhet definieras i denna uppsats; hot och sårbarheter för verksamheters informationssäkerhetsarbete, lagstiftningar som svenska verksamheter behöver förhålla sig till samt vad ISO 27001-standarden är och hur den tar sitt uttryck.

2.1 Informationssäkerhet och cybersäkerhet

Information finns överallt, hela tiden. Det du kommunicerar är information och det är även post it-lappar innehållandes text som sitter på en datorskärm. Vi lever ju i informationssamhället trots allt. Det som gör information svårt att definiera är just hur vi värderar den, ibland är information viktig och ibland är den mindre viktig. Pfleeger et al. (2015) argumenterar för att informationens värde inte går att definiera utan att det är baserat på vad köparen är villig att betala för den men att en avgörande roll för värdet är också när tillgången till informationen sker. Oavsett värde och pris, har alltid information skyddats.

För att verksamheter ska kunna skydda sin information finns ett antal modeller och ramverk att ta hjälp av, en av de vanligaste är den så kallade CIA-triaden som står för konfidentialitet, riktighet och tillgänglighet. Myndigheten för samhällsskydd och beredskap ([MSB], 2015) motivering till dessa ledord är att information alltid ska finnas vid behov, att informationen är korrekt samt att enbart de med behörighet har tillgång till informationen. Då MSB utgår från dessa ledord anses därmed CIA-triaden som standard och rekommenderat för svenska verksamheter.

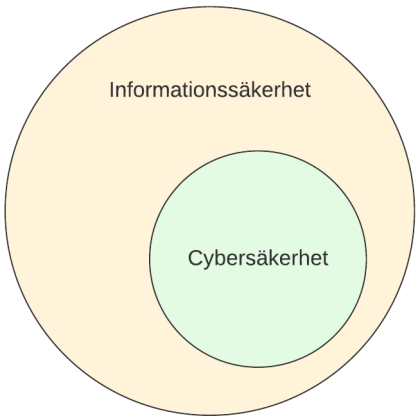
Men informationssäkerhet är ju mer än enbart CIA-triaden, det går även att argumentera för att CIA-triaden är *basic*. *Basic* innebär inte dålig i denna kontext utan CIA-triaden är bra att utgå från men det behövs mer för att bygga ett stabilt arbete kring informationssäkerhet. Lundgren och Möller (2017) argumenterar att CIA-triaden inte på ett tillräckligt effektivt sätt tar hänsyn till kontexten för brister inom informationssäkerhet och därmed blir svårt att utgå från. Definitionen är med andra ord inte tillräckligt flexibel för att tillgodose krav för olika sorters information, system eller verksamheter. Det som är största bristen är dock att den inte tar hänsyn till den mänskliga faktorn som i allra högsta grad alltid kommer att vara aktuell.

Utifrån ovanstående dras slutsatsen att konfidentialitet, riktighet och tillgänglighet är viktigt och på många sätt fortfarande är de attribut som grunden för informationssäkerhet vilar på, men det krävs mer än dessa tre attribut för att uppnå ett arbete kring informationssäkerhet som fungerar.

Informationssäkerhet och cybersäkerhet är två begrepp som ofta förknippas som ett och samma, men de bör ändå separeras då de används i liknande kontexter och inte innebär samma sak. Även vissa definitioner av begreppen är liknande men den största skillnaden mellan dem är just typen av information. Taherdoost (2022) lyfter flertalet definitioner av cybersäkerhet och informationssäkerhet men i slutändan handlar det

egentligen mest om var informationen befinner sig. Cybersäkerhet handlar om bevarandet av konfidentialitet, integritet och tillgänglighet för information i *cyberspace* och informationssäkerhet handlar om bevarandet av konfidentialitet, integritet och tillgänglighet för information. Detta innebär att om information finns tillgänglig i *cyberspace* handlar det i första hand om cybersäkerhet och om informationen finns på ett skrivbord samt att det också finns i *cyberspace*, handlar det om informationssäkerhet.

I begreppet informationssäkerhet inkluderas alltså cybersäkerhet, då det omfattar säkerhet för fysisk såväl som digital information, se figur 1. Cybersäkerhet är dock väldigt viktigt att poängtera och behålla som ett eget begrepp då *cyberspace* växer och likaså hoten mot den digitala informationen. Information lagras, transporteras eller processas digitalt inom *cyberspace* och därmed blir det viktigt att kontinuerligt se över de skydd verksamheten har för sin digitala information (Taherdoost, 2022).



Figur 1 – Cybersäkerhet i relation till informationssäkerhet

Taherdoost (2022) betonar att huvudsyftet med informationssäkerhet för en verksamhet är när verksamhetsprocesserna kan hållas i gång utan avbrott då information gör att de kan uppnå sina verksamhetsmål. Däremot är information också bland det farligaste för en verksamhet då information kan skada en verksamhets rykte och kan leda till stora förluster om informationen inte är skyddad. Ovanstående är viktigt och är såklart ett bra argument för att implementera ett ordentligt skydd för sin information. Andersson et al. (2022) lyfter även att infrastruktur, digital såväl som fysisk, numera är digitaliserad och i sin tur leder det till att samhällen också påverkas av brister i informationssäkerhet som verksamheter har. Digitaliseringen och dess integrering i samhällsfunktioner gör att verksamheter har som skyldighet att investera i informationssäkerhet.

2.2 Hot och sårbarheter inom informationssäkerhet

Informationssäkerhet är ett stort begrepp, och som tidigare fastställt, ingår även cybersäkerhet i begreppet. Hot mot informationssäkerhet kommer i flertalet olika former och utföranden. I denna delen kommer just hoten och sårbarheterna att lyftas för att ge underlag till på hur de kan agera inom informationssäkerhet. Det kommer inte att diskuteras hur dessa hot och sårbarheter ska reduceras utan den delen hanteras inom riskhantering, som inte är i fokus i denna uppsats.

Ett hot är när det finns en potentiell risk för en incident inom informationssäkerhet som kan resultera i att skada ett system eller en verksamhet samt att en sårbarhet är en tillgång eller kontrolls svaghet som exploateras så att en händelse med negativ konsekvens kan ske (ISO, 2022a).
Några av de konsekvenser som kan ske i samband med cyberrelaterade attacker är att det kan skada ett lands *image* på internationell nivå, det kan skada politiska och ekonomiska relationer för landet, det kan förstöra allmänhetens tillit, påverka religiösa/etniska trosuppfattningar, skapa internt kaos samt bilda omfattande förstörelse eller störning av de nationella cybertillgångarna (Li & Liu, 2021).

Hot och sårbarheter inom hanteringen av information kan i värsta fall leda till informationsförlust, vilka kan vara avsiktliga såväl som oavsiktliga anledningar. Så länge information finns, finns även hoten och sårbarheterna mot informationen. Hoten och sårbarheterna kan finnas internt såväl som externt för verksamheter, vilket leder till att en verksamhet bör inkludera hela verksamheten i sitt arbete med informationssäkerhet. Li och Liu (2021) lyfter att de vanligaste hoten som finns inom *cyberspace* för verksamheter är det oftast utländska, interna, mot verksamhetens *supply chain* samt brister inom de lokala resurserna. Brister inom informationssäkerhet kommer inte enbart från tekniken, som exempelvis molnbaserade tjänster eller systemintegrationer, utan det är även kopplat till mänskliga faktorn i form av avsiktliga såväl som oavsiktliga beteenden.

Den mänskliga faktorn inom informationssäkerhet är den mest oförutsägbara eftersom den inte har en kod eller utstakad väg att följa. Schaab et al. (2017) förklarar att *social engineering* innebär att en person tar information som är konfidentiell, privat eller privilegierad genom metoder som innefattar tekniska och/eller mänskliga metoder. Det kan handla om att en person genom social interaktion manipulerar eller övertygar en annan person att ge information, men det kan också handla om att någon kikar över axeln utan att någon är medveten om det och på så sätt fått tillgång till information. *Social engineering* är ständigt aktuellt och svårt för verksamheter att hantera eftersom den mänskliga faktorn inte går att kontrollera, utan bara att upplysa och informera.

Genom att öka medvetenheten kring verksamhetens policy och riktlinjer kring arbete informationssäkerhet utbildar verksamheten sin personal så att sannolikheten för oavsiktliga såväl som avsiktliga beteenden mot verksamheten (Li & Liu, 2021; Podreca et al., 2022; Andersson et al., 2021). Däremot anser Schaab et al. (2017) att en

säkerhetspolicy som behandlar *social engineering*, som är bland det mest förekommande för att få tillgång till information, inte finns. De anställda som utsätts för *social engineering* vet inte hur de ska förhålla sig eftersom de inte vet hur de ska svara på tvetydiga frågor.

Cybersäkerhet som ett eget begrepp utgör en viktig del av infrastrukturen för verksamheter och enligt Li och Liu (2021) är framgång inom cybersäkerhet även ett tecken på verksamhetens framgång och förmåga att kunna skydda interna samt kunders information mot rivaler. Men tydliga brister finns, en undersökning utförd av Ganji et al. (2019) visar att mer än 90% av de cyberattacker som drabbat verksamheter hade kunnat förebyggas om säkerhetsskyddet inom verksamheterna i fråga var aktuella och ”*up to date*” under den tid cyberattackerna utfördes.

2.3 Lagstiftningar inom informationssäkerhet i Sverige

När det kommer till lagar inom informationssäkerhet i Sverige är det dels säkerhetsskyddslagen (2018:585) och lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174), där den sistnämnda är baserad på NIS-direktivet som är förordnat av EU för dess medlemsländer där Sverige är inkluderat. Sedan den 16 januari 2023 har NIS2-direktivet ersatt NIS-direktivet från EU och medlemsländerna har fram till den 17 oktober 2024 på sig att applicera det nya direktivet inom sina nationella lagar (COM(2020) 823).

På grund av den ökade digitalisering skapade den svenska regeringen en ny lag för att säkerhetskänsliga verksamheter i Sverige. Den 1 april 2019 trädde den nya säkerhetsskyddslagen (SFS 2018:585) i Sverige igenom, som handlar om att Sveriges säkerhetskänsliga verksamheter är skyldiga att bedriva ett säkerhetsskyddsarbete. Utgångspunkten är att bedriva en säkerhetsskyddsanalys och att sedan utifrån analysen planera ett stabilt säkerhetsskydd där olika säkerhethetsskyddsåtgärder samverkar med varandra. Vad som däremot klassas som en säkerhetskänslig verksamhet är dock upp till verksamhetsutövaren själv, som sedan får anmäla detta till den tillsynsmyndigheten som ansvarar för verksamhetens bransch. MSB (2021) definierar en samhällsviktig organisation i Sverige som en verksamhet som är viktigare än andra i den bemärkelsen att upprätthålla samhällets funktionalitet oavsett störning.

Det befintliga NIS-direktivet från EU har visat sig vara svårt att implementera för flertalet av medlemsländerna och bidragit till stora skillnader på nationell nivå. Därför kommer NIS-direktivet nu att ersättas av NIS2-direktivet. Motiveringen till detta är att den ökade digitaliseringen har skapat stora möjligheter för verksamheter över hela världen och att med det kommer också stora risker eftersom cyberhot kan slå ut nationella ekonomier och samhällen. EU säger att cybersäkerhetsproblem har blivit ett ”*day-to-day*”-problem för EU och dess medlemsländer. Kontantlösa betalningar har underlättat arbetet för flera samhällsviktiga verksamheter såväl som för privatpersoner, men de mer sofistikerade cyberhoten i kombination med den låga tillämpningen av cybersäkerhet har gjort att det blivit mer riskfyllt att använda den här typen av

betalningsmedel. EU Agency for Network Information Security (ENISA) har rapporterat att *ransomware* och ekonomiska motiv ökat markant inom cyberhoten. ENISA utförde en undersökning där några av medlemsländerna upplever att NIS-direktivet har haft en positiv effekt, däremot finns det fortfarande stora gap mellan hur länder spenderar pengar på sin informationssäkerhet. EU har jämfört data med USA och det visade att EU:s medlemsländer spenderar 41% mindre pengar på sitt cyberförsvar än amerikanska verksamheter (COM(2020) 823).

Ovanstående har bidragit till att det befintliga NIS-direktivet ska ersättas av NIS2-direktivet. Motiveringen till detta är att det nya direktivet kommer att omfatta fler verksamheter och sektorer och därmed kommer cybersäkerheten generellt öka i medlemsländerna och vara mer långsiktigt än det befintliga direktivet. En av de största skillnaderna i det nya direktivet är gällande böter och sanktioner, där en böter maximalt kan vara på 10 miljoner euro alternativt 2% av intäkterna som en verksamhet har globalt med kravet att den summan som är högst av alternativen är den som ska tillämpas. En annan viktigt skillnad är att de som är i *senior management* för en verksamheten kan bli tillfälligt avstängda från sitt arbete, vilket leder till att verksamheter inte längre enbart ekonomiskt drabbas av en överträdelse (Long et al., 2023).

I Sverige togs ett beslut vid ett regeringssammanträdet den 23 februari 2023 som resulterade i att de tillsatt olika utredare för att på bästa möjliga sätt applicera NIS2-direktivet i svensk lagstiftning. Ett urval av de uppdrag som utredarna ska presentera svar inför regeringen 24 februari 2024:

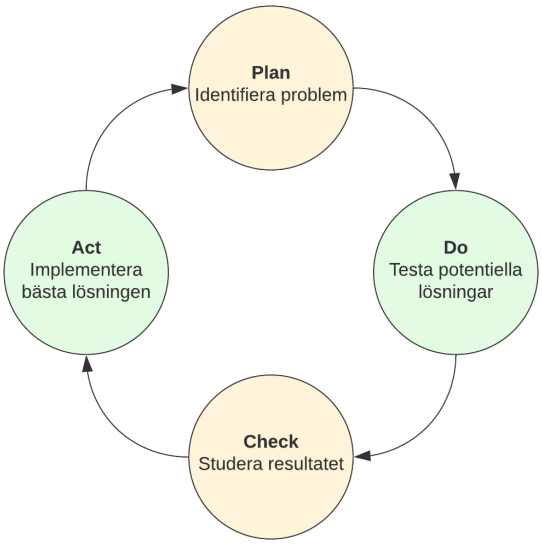
- Forskning är en av de nya sektorerna som omfattas av NIS2, utredarna ska överväga om universitet och högskolor, eller ett urval av dessa, ska ingå i det nya direktivet.
- Utse nya tillsynsmyndigheter för de nya sektorerna.
- Analysera de riskhanteringsåtgärder och incidentrapporteringar som står i direktivet och lämna förslag på hur de kan genomföras i svensk lag.
- Avgöra befogenheterna som tillsynsmyndigheterna ska ha enligt direktivet, då de är mer omfattande i det nya direktivet.
- Redogöra hur MSB kan anta en roll som nationell gemensam kontaktpunkt.
- Ta ställning till hur direktivets krav på bakgrundskontroller för anställda inom s.k. kritiska entiteter ska genomföras i svensk lag.
- Direktivet i förhållande till säkerhetsskyddslagen.
- Flera åtgärder saknar direkt motsvarighet i svensk lagstiftning, som att tillfälligt förbjuda personer i en verksamhets ledning att utöva ledningsfunktioner (Regeringens direktiv 2023:30).

Punkterna ovan leder till att det kan ske stora förändringar framöver inom informationssäkerhet och att flertalet implementeringar inom detta kommer att vara reglerade av svensk lagstiftning och därmed kommer det att ställas högre krav för svenska verksamheters arbete inom informationssäkerhet.

2.4 ISO/IEC 27001

En verksamhets arbete kring informationssäkerhet kan ske på flertalet olika sätt och det finns flera erkända metoder och ramverk, som exempelvis NIST Cybersecurity Framwork, ISO/IEC 27001, SOC2 för att nämna några. Denna rapport kommer att fokusera på standarden ISO/IEC 27001:2022, som framöver i texten kommer att refereras som ISO 27001.

International Organization for Standardization (ISO) är en organisation som i 159 länder är ledande i att utfärda internationella standarder. Tillsammans med International Electrotechnical Commision (IEC) har de tillsammans tagit fram ISO/IEC 27000-serien som handlar om informationssäkerhet. ISO 27001-standarden publicerades för första gången år 2005 och handlade då om kraven för ledningssystem för informationssäkerhet (LIS) och genom att uppfylla dessa krav kunde verksamheter uppnå en certifiering. ISO 27001 har alltid varit sett som ett ramverk, så att det ska kunna appliceras på alla sorters verksamheter utifrån deras sektor samt storlek. Typiskt för ISO 27001 är att den är baserad på ”*Plan-Do-Check-Act*” (PDCA) och därmed förespråkar ett kontinuerligt arbete med processer såväl som processernas integrering i verksamheten, se figur 2. Att planera, implementera, genomföra och kontinuerligt övervaka samt förbättra LIS:et i kombination med PDCA är med andra ord grundpelarna för ISO 27001. När det kommer till arbetet med PDCA krävs det att ledningen är engagerad för det är dom som ser till att en säkerhetspolicy utformas och är en av de viktigaste delarna för att skapa en bra grund för ett LIS (Disterer, 2013).



Figur 2 – Figur över PDCA-processen.

Det finns flertalet metoder och arbetssätt att arbeta med informationssäkerhet och det är viktigt att klargöra att ISO 27001 inte är den enda standarden att utgå från. Fördelen med ISO-certifieringar, över lag, är att de kommer med en certifiering och att det finns ett kontinuerligt verifieringsarbete kring certifikatet. I Sverige har vi MSB som kommer med stöd och rekommendationer för hur svenska verksamheter ska arbeta med exempelvis informationssäkerhet. I deras metodstöd står det tydligt att metodstödet är baserad på ISO 27001, vilket gör att ett antagande om att det ramverk ISO 27001 tillförser går att applicera såväl som redan nu appliceras på svenska verksamheter (MSB, 2015).

Verksamheter som innefattar en ISO-certifiering arbetar kontinuerligt med att upprätthålla sin certifiering och det krävs mer än en verifiering för att behålla sin certifiering. En ISO 27001-certifiering ger en verksamhet något att visa upp för sina kunder, det är alltså ett bevis på att de uppfyller de krav och kontinuerligt arbetar med att upprätthålla ett stabil arbete för informationssäkerhet. Utomstående certifieringsorgan är de som utfärdar certifieringen för verksamheter som uppfyller kraven och därmed verifierar verksamheten att de aktivt arbetar med informationssäkerhet och det kan även bli en fördel om kunder jämför verksamheter (Disterer, 2013).

Då ISO 27001:2022 implementerades 25 oktober 2022, är majoriteten av de nuvarande och relevanta artiklar med dess forskning baserade på ISO 27001:2013, som varit verksamt sedan 1 oktober 2013. Genom att redovisa skillnaderna mellan dessa utgåvor av samma standard förklaras antaganden som applicerats i denna uppsats.

De största skillnaderna mellan revisionerna 2013 och 2022 är att antalet säkerhetskontroller i Annex A har minskat från 114 st till 93 st samt att det antalet sektioner i Annex A har gått från 14 st till 4 st. Det kan låta som att det är stora skillnader, men det som har skett är att flertalet sektioner samt säkerhetskontroller har slagits samman för de är så pass lika. När det kommer till ändringarna för säkerhetskontroller i Annex A är det 11 st nya kontroller, 57 st sammanslagna, 1 st som har delats, 23 st med ändrade namn samt 35 st som inte har ändrats mellan revisionerna. Ändringarna mellan revisionerna är inget som kräver en större omställning eller på något sätt försvårar arbetet kring LIS för verksamheter. Det som ändringarna betyder för befintliga verksamheter som innehar certifieringen ISO 27001 är att det handlar om mindre ändringar i dokumentationen samt processerna. De nya kontrollerna är inte omfattande heller och utgör ingen större skillnad från hur ett LIS tidigare beskrivits (Kosutic 2022).

Skillnaderna mellan revisionerna är inte av större karaktär och därmed görs antagandet om att forskning, artiklar och annat material som handlar om ISO 27001:2013 fortfarande ligger till grund som relevant för denna uppsats och att det inte kommer göras någon skillnad i referenshanteringen kring dessa utgåvor i denna text.

En av de fundamentala delarna för att kunna certifiera sig för ISO 27001 är att en verksamhet har ett ledningssystem för sitt arbete med informationssäkerhet. Ett LIS är de processer och rutiner som styr en organisations verksamhet kring just informationssäkerhet. En stor del av ISO 27001 är att upprätta, införa, upprätthålla och ständigt förbättra ledningssystemet för informationssäkerhet. Hur ett LIS är upprättat och hur det införs är helt beroende på verksamhetens krav, mål, behov och processer baserat på verksamhetens storlek och struktur men det måste också vara anpassat för att kunna förändras med tiden då en verksamhets krav, mål, behov och processer kan ändras. Ovanstående är just utmaningen med ett LIS men det är också det som gör ett LIS bra. Genom att ständigt vara en del av verksamheten är ett LIS alltid aktuellt och på sätt också skapar ett förtroende hos intressenter genom att informationssäkerhetsarbetet ständigt är aktuellt (ISO, 2022b).

Tillämpningen av ISO 27001-standarden är svår att mäta och kontrollera eftersom verksamheter kan arbeta utifrån ramverket utan att gå mot en certifiering. Antalet utfärdade certifieringar går däremot att kontrollera och Podreca et al. (2022) skriver att år 2020 var det ungefär 45 000 st verksamheter som hade certifieringen, vilket leder till att ISO 27001 är den fjärde mest etablerade ISO-standarden. Redan år 2008 undersökte Fomin et al. (2008) varför inte ISO 27001-certifieringarna tillämpades i samma utsträckning som ISO 9000-serien, som handlar om kvalitet och ISO 14000-serien som handlar om miljö. Det som framkom ur den undersökningen var att internt spelar inte själva certifieringen för ISO 27001 någon större roll då det handlar om hur tillämpningen och arbetet med LIS:et inom verksamheten ser ut då verksamheter kan tillämpa ISO 27001-standarden utan att faktiskt certifiera sig. Däremot är inte ISO 27001-certifieringen i sig något som visat sig ha en avgörande roll gällande ekonomi, kvalitet eller förtroende, vilket gör att behovet för en certifiering inte är något som har etablerats och klassats som en självklarhet.

Tillskillnad från Fomin et al. (2008) lyfter Podreca et al. (2022) de ekonomiska fördelarna en certifiering för ISO 27001 bidrar med till verksamheter. Podreca et al. (2022) argumenterar för att de verksamheter som innehar en ISO 27001-certifiering upplever positiva resultat, exempelvis i form av lönsamhet och sälj och att det är bekräftat av flertalet verksamheter. Liksom Fomin et al. (2008) betonar Hsu et al. (2016) att det inte finns några kopplingar till att den ekonomiska vinsten i sig är utgörande för verksamheter att certifiera sig för ISO 27001. Däremot visar verksamheten i fråga att de är att lita på och framstår som mer trovärdiga. Detta beror på att en ISO 27001-certifiering innebär att verksamheten möter ”marknadens krav” och att det inte är en fördel, utan att det faktiskt är en skyldighet att arbeta med informationssäkerhet och att det därmed inte utgör en större reaktion på marknaden när de visar att de har en certifiering. Detta leder till att det är svårt att generalisera och motivera den ekonomiska vinsten en certifiering medför eftersom det har forskats inom detta i flertalet år och det finns fortfarande inget definitivt svar.

Den kritik som finns mot ISO 27001 går även att applicera på flertalet standarder inom informationssäkerhet, eftersom kritiken i sig handlar om att applicera en standard för arbetet inom informationssäkerhet (Andersson et al., 2022; Niemimaa & Niemimaa, 2016; Podreca et al., 2022). Det som just gör att standarder får kritik är att de anses för generella och att det inte går att applicera samma standard på alla verksamheter när det kommer till informationssäkerhet.
Det finns även kritik mot att framtagandet av standarder påverkas av politiska intressen samt att de som upprättar standarderna och de som är experter inom aktuellt område är i osynk. Den anledning som lyfts är att det är fler experter än företrädare från branschen som upprättar standarderna och det i sin tur påverkar processen vid framtagandet av en standard och även legitimiteten (Andersson et al., 2021; Silva et al., 2016; Niemimaa & Niemimaa, 2016).

Den mer generella kritiken mot ISO 27001-certifieringen är att det är mycket dokumentation, det kan bli dyrt då processen kan dra ut på tiden, att verksamheten kan upplevas som mindre flexibel samt att det kan bli svårt att möta specifika krav från kunder (Podreca et al., 2022).

3 Problemområde

COVID-19 och Rysslands militära operation i Ukraina har lett till att cyberhoten samt hoten mot informationssäkerhet har ökat och verksamheter över hela världens brister inom informationssäkerhet har exponerats. Mycket pekar på att dessa faktorer skapat fler möjligheter för attacker av digital karaktär, då cyberattacker ökat med 38% under år 2022 och medelvärdet av cyberattacker kan räknas till 1168 st per vecka (Checkpoint 2023).

Standarder och certifieringar har en stor roll i att hjälpa verksamheter att skydda deras tillgångar mot flertalet hot – interna såväl som externa (Silva et al., 2016). Informationssäkerhet måste uppmärksammas och verksamheter behöver visa att det är något som prioriteras inom verksamheten. Det faktum att kunna visa upp en ISO 27001-certifiering är en fördel som majoriteten av forskningen lyfter och är överens om (Silva et al., 2016; Disterer, 2013; Podreca et al., 2022; Andersson et al., 2022; Ganji et al., 2019). Dels är detta en internationellt erkänd certifiering, men det visar även att en verksamhet kontinuerligt och systematiskt arbetar med sitt LIS och arbete kring informationssäkerhet.

Då ISO 27001 är en internationell standard är den mesta forskningen generell och det finns ingen konkret forskning om hur svenska verksamheter förhåller sig till ISO 27001-certifieringar. Det närmsta, rent geografiskt, är Mirtsch et al. (2021) som utfört en omfattande undersökning i Tyskland för att se om det finns något samband med att tillämpningen av ISO 27001-certifieringarna inte ökat mer i samband med den ökade digitalisering. Deras resultat visade att fler verksamheter skrev att de hade en certifiering än de som faktiskt hade en certifiering för ISO 27001. Anledningen till detta var att verksamheter skrev ut att de arbetade utifrån ISO 27001-standarden utan att vara certifierade samt att deras samarbetspartners hade certifiering utan att de själva hade en. De samband som fanns hos de tyska verksamheter som var certifierade var att störst sannolikhet för certifiering fanns hos de verksamheter som var större, har hög innovationspotential samt att verksamheten är verksam inom information- och kommunikationsteknik (IKT). Deras resultat visade också att sannolikheten är som lägst om det är en äldre verksamhet. Då Mirtsch et al. (2021) undersökning är omfattande såväl som relativt ny är det relevant underlag för denna uppsats.

På grund av det aktuella läget i samhället lyfts tanken om hur svenska verksamheter står sig när det gäller ISO 27001-certifieringar inom informationssäkerhet. När det kommer till Sverige är, i skrivande stund, 80 st bolag i Sverige certifierade för ISO 27001 (Babacus AB 2023). Detta är en väldigt låg siffra och det leder till att det är svårt att veta hur svenska verksamheter arbetar och prioriterar sitt arbete med informationssäkerhet.

SÄPO (2023) gick i ett pressmeddelande ut under februari 2023 och sa att det finns flertalet brister i säkerhetsskydd hos säkerhetskänsliga verksamheter inom alla områden i Sverige, där områdena definieras som personalsäkerhet, fysisk säkerhet och informationssäkerhet. Det framkommer även att dessa brister riskerar att leda till att

uppgifter om Sveriges totalförsvarsförmåga röjs. Uttalandet från SÄPO kom efter flertalet DDoS-attacker utförda av Anonymous Sudan (inte att förväxla med hacktivist kollektivet Anonymous) tillsammans med andra ryska grupper som KillNet, MistNet och UserSec. En DDoS-attack är en slags överbelastningsattack som gör att det inte går att nå en webbsida och därmed är inte verksamhetens information till befolkningen tillgänglig (TrueSec, 2022).

Att informationssäkerheten så pass offentligt visar sina brister inför befolkningen och dessutom bekräftas av SÄPO skapar inte bara otrygghet. Det visar även att arbetet kring informationssäkerheten inte är etablerat och en självklarhet inom verksamheter, vare sig de är säkerhetskänsliga eller statliga. I ovanstående fall försvann ”tillgängligheten” i CIA-triaden. CIA-triaden har en grundläggande och viktig funktion inom arbetet för informationssäkerhet.

Nationellt center för cybersäkerhet är en fusion av Försvarets radioanstalt, Försvarsmakten, MSB samt SÄPO som skapades på uppdrag av regeringen i december 2018. Syftet med detta center är att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska cybersårbarheterna. Detta görs genom att utveckla och samordna stöd åt svenska verksamheter men också genom gemensamma analyser och lägesbilder om hot, sårbarheter och risker. En av de största brister som Nationellt center för cybersäkerhet (2020) tar upp är just svenska verksamheters avsaknad systematiskt cybersäkerhetsarbete. De definierar systematiskt cybersäkerhetsarbete som att det förutsätter att ett grundarbete genomförs som identifierar verksamhetens skyddsvärden, vilka hot och risker som riktas mot dem och identifierar vilka säkerhetsåtgärder som behöver vidtas. Av de genomförda tillsynerna och granskningarna som har gjorts uppnår inte svenska verksamheter arbetet med cybersäkerhet, då det inte finns skydd som är ändamålsenligt sett till de hot och risker som finns.

Utifrån ovanstående text går det att konstatera att svenska verksamheter har brister inom sitt arbete med informationssäkerhet och att ett mer systematiskt arbetssätt kring informationssäkerhet är i högsta grad är aktuellt. Ett sätt för svenska verksamheter att uppnå detta är att certifiera sig för ISO 27001 som dessutom verifieras kontinuerligt och integreras med verksamheten i fråga. Hsu et al. (2016) såg inte några större konkurrensfördelar i samband med ISO 27001-certifieringen i deras forskning, däremot konstaterade de att den största anledningen till det är att en ISO 27001-certifiering ses som en skyldighet och inte en konkurrensfördel.

3.1 Syfte/frågeställning

Syftet med denna studie är att den digitala världen växer och det gör även hoten mot den information som lagras, transporteras eller processas digitalt. Då ISO-standarder är den standard som genom verifiering ger certifiering samt är den standard som MSB genom sitt metodstöd rekommenderar till svenska verksamheter är ISO 27001-certifieringar det lämpligaste ramverket att kunna föra och se statistik över för svenska verksamheter. Dock är det inte många verksamheter i Sverige som innehar certifiering för ISO 27001, vilket gör att anledningen till detta bör undersökas. Utifrån tidigare forskning finns det ett tydligt samband kring vilken typ av verksamheter som väljer att certifiera sig men det framkommer att det är vanligt att arbeta utifrån ISO 27001-standarden utan att faktiskt certifiera sig. Detta är inget som satts i relation till svenska verksamheter och leder till frågan:

Vilka utmaningar finns bland svenska verksamheter för att uppnå en ISO 27001-certifiering?

3.2 Avgränsningar

Det finns flertalet erkända standarder och ramverk inom informationssäkerhet att utgå från, men denna studie kommer enbart att behandla ISO 27001-certifieringar då det är det som MSB genom sitt metodstöd rekommenderar för svenska verksamheter samt att det går att se statistik för antalet certifieringar.

Denna studie kommer inte ha genomgång av hur säkerhetsåtgärder implementeras eller diskutera riskhantering, utan det är arbetet en verksamhet arbetar kring informationssäkerhet och utmaningarna att uppnå en ISO 27001-certifiering som är av största vikt.

3.3 Förväntat resultat

Det förväntade resultat är att verksamheter idag arbetar med informationssäkerhet, men utifrån "*best practices*". Anledningen till varför det finns utmaningar till att uppnå en ISO 27001-certifiering baseras på tidigare forskning som antas i vissa situationer även kunna appliceras på svenska verksamheter. De anledningarna är att det är omständigt att implementera ett LIS, att det är en stor kostnad och att det är oklart vad en verksamhet tjänar rent ekonomiskt på en ISO 27001-certifiering. En annan anledning, som däremot inte har några belägg i tidigare forskning, är antagandet om att svenska verksamheter inte prioriterar informationssäkerheten tills de själva drabbats av ett intrång.

4 Metod

Den metod som appliceras för detta examensarbete är fallstudie, som innebär att på ett djupgående plan undersöka frågeställningen som ett fenomen i sin verksamma och naturliga miljö (Berndtsson et al., 2008). Fallstudien är uppbyggd genom kvalitativa intervjuer med verksamheter som har en viktig beståndsdel i processen för svenska verksamheter att uppnå en ISO 27001-certifiering. De olika perspektiv som intervjuerna bidrar med kommer att ge ett legitimt samt ett generellt underlag för de olika verksamheternas roll i processen.

Intervjuer har skett med en offentlig verksamhet, en privat verksamhet, ett konsultbolag som specialiserar i att hjälpa verksamheter implementera ISO 27001-ramverket samt ett certifieringsorgan som utför ISO 27001-certifieringar. Verksamheter och personer inom verksamheterna har noga valts ut utifrån kompetens och relevans för fallstudien och frågeställning, vilket gör att deras upplevelser är av högsta relevans och legitimitet.

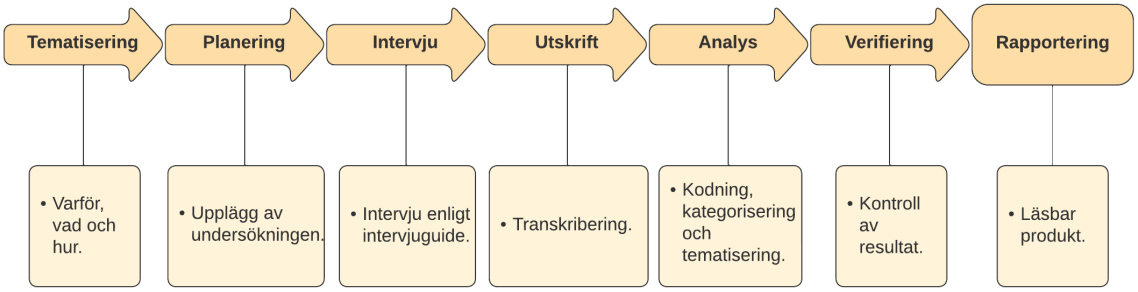
Intervjuer är även vanligt förekommande med en kvantitativ ansats, vilket på enkelt sätt innebär att den insamlade datan ska vara mätbar, kunna appliceras med siffror samt när syftet med undersökningen är att undersöka ett ämne på ”bredden” (Eliasson, 2010). En kvantitativ ansats hade varit svår att applicera på detta arbete eftersom det inte finns någon hypotes eller specifikt värde att mäta eller jämföra med. Det har inte hittats någon tidigare data angående utmaningar som svenska verksamheter har mot ISO 27001-certifieringar och därmed hade det varit svårt att veta hur frågorna skulle förberedas inför intervjuerna, som en kvantitativ ansats lägger stor tyngd vid (Eliasson, 2010). Genom den kvalitativa ansatsen som applicerats på detta examensarbete kunde frågorna anpassas efter verksamheten i fråga och respondenternas perspektiv gav en djupare förståelse om deras erfarenheter i relation till frågeställningen.

4.1 Kvalitativ intervju

Genom att kombinera kvalitativa intervjuer med en fenomenologisk teori blir svaren av respondenterna baserade på deras egna sociala fenomen utifrån deras egna perspektiv och tolkning av omvärlden (Kvale & Brinkmann, 2014). Fördelen med detta är att respondenternas svar aldrig kommer kunna tolkas som rätt eller fel utan svaren kommer att behandlas och redovisas utifrån respondenternas faktiska perspektiv. Nackdelen med detta är att det kan uppfattas som att det inte finns en vetenskaplig eller objektiv grund till svaren, men syftet med denna studie är just uppfattningen och upplevelserna från respondenterna och lämpar sig därför till denna studie. Respondenter samt verksamheter har blivit noga utvalda utifrån kompetens och relevans till frågeställningen.

För att skapa bästa möjliga förutsättningar för intervjuerna har sju stadier applicerats som ramverk för fallstudien, då intervjuerna i sig har olika karaktär och inte utgår från samma frågor. En av fördelarna de sju stadierna som verktyg har är just att det inte finns någon standardiserad procedur eller några regler för hur intervjun ska genomföras, men

stadierna ändå blir ett slags stöd genom processen. De sju stadierna är tematisering, planering, intervju, utskrift, analys, verifiering samt rapportering, se figur 3 (Kvale och Brinkmann, 2014).



Figur 3 – Bild över de sju stadierna inom intervjuerna för denna fallstudie.

Det första steget inom de sju stadierna är tematisering, där syftet med intervjuerna definierades och därmed lade grunden för hela fallstudien. Detta gjordes genom att besvara syftet med studien (varför), skaffa en förkunskap om ämnet som undersöktes (vad) samt hur kunskap från studien ska hämtas (hur) (Kvale och Brinkmann, 2014). I denna studie blir syftet med studien frågeställningen, alltså svenska verksamheters utmaningar att uppnå en ISO 27001-certifiering, förkunskap hämtades genom tidigare forskningsartiklar och rapporter om ISO 27001 samt kunskapen skapades genom explorativa intervjuer med noga utvalda personer inom relevanta verksamheter. Den explorativa karaktären av intervjuerna användes för att intervjuerna skulle vara öppna och någorlunda strukturerade eftersom respondenternas upplevelser och del i certifieringsprocessen undersöktes. Det skapade infallsvinklar där nya frågor uppstod och kunde besvaras för att undersöka respondenternas kunskap och roller i certifieringsprocessen på ett givande sätt för studien.

Planeringsstadiet grundade sig i att kunskapen som hämtades skulle vara baserad på respondenternas omvärld och upplevelser, deras perspektiv med andra ord. Den kunskap som skulle hämtas samt de moraliska och etiska aspekterna i hur detta skulle genomföras beaktades först. För att få respondenternas perspektiv med en explorativ typ av intervju så förvärvades kunskapen genom samtal. Motiveringen till detta är för att det inte skulle läggas någon värdering i egenskap av rätt och fel i respondenternas svar, utan det skulle vara helt baserat på deras perspektiv och det var det som skulle undersökas för studien skull. De etiska och moraliska aspekterna för studiens syfte var att respondenterna skulle känna sig bekväma med att delta i studien och att det genomfördes genom informerat samtycke, säkrad konfidentialitet och övervägande av konsekvenser för deltagande av studien. Samtliga respondenter gav sitt samtycke till att

delta, att spela in intervjuerna och genom anonymitet uteslöts konsekvenser som skulle kunna vara direkt kopplade till person eller verksamhet (Kvale & Brinkmann, 2014).

Intervjuguiderna för intervjuerna var olika, då varje respondent har olika roller i certifieringsprocessen för ISO 27001. Exempelvis var det inte relevant för studien att veta hur ett certifieringsorgan arbetar med sin informationssäkerhet, utan där var det relevant att veta hur de arbetar med verksamheter som vill uppnå en ISO 27001-certifiering. Eftersom intervjuerna var av explorativ karaktär var intervjufrågorna dynamiska i den form att undersöka hur, detta för att respondenterna skulle få berätta deras perspektiv och hur de uppfattar sin omvärld. Kvale och Brinkmann (2014) beskriver dynamiska frågor som ett sätt till positiv interaktion där samtalet håller sig levande. Intervjuguiderna skapades därför utifrån teman där respondenterna sedan fick svara på frågor, men det fanns bra med utrymme för att ställa ”hur”-frågor för att undersöka temat djupare utifrån respondentens perspektiv. Nedanför redovisas intervjuerna för denna studie utifrån verksamhet, tid för intervju, utförande av intervju samt vilken typ av verksamhet som intervjuades (Tabell 1).

Tabell 1

Fallstudiens insamlade data genom intervjuer.

Verksamhet	**Yrkestitel**	**Tid**	**Utförande**	**Typ av verksamhet**
V1	IT-chef	15:50 min	På plats	Offentlig
V2	IT- och säkerhetschef	32:57 min	Digitalt	Privat
V3	Affärsområdeschef	36:36 min	På plats	Certifieringsorgan
V4	Head of Information Security	35:31 min	Digitalt	Konsultbolag

Då samtliga respondenter gav sitt samtycke till att spela in intervjuerna, transkriberades dessa för att få den insamlade datan i skriftspråk såväl som talspråk. Motiveringen till detta är för att skriftspråk gör det lättare att analysera och koda datan som utgör underlaget för denna studie. För att säkerställa samtliga respondenters konfidentialitet har direkt identifierande uppgifter som namn på personer såväl som verksamheter uteslutits i skriftspråket.

Analysen av den insamlade datan för studien har utförts med inspiration från en kvalitativ innehållsanalys med en induktiv ansats. Det innebär att det den insamlade datan har gått igenom kodning, kategorisering samt placerats i ett tema. Kodning har i den här studien utförts genom att markera de uttalanden från intervjuerna som är av relevans, både i form av enstaka ord och meningar. Dessa har sedan kategoriserats, då vissa meningar och ord har samma alternativt liknande innebörd i de olika intervjuerna

och därmed tillsammans skapa en kärna. I de fall kategorierna enbart består av en kod, har det blivit kärnan för kategorin. Temat för den här studien är problemformuleringen och är därför den röda tråden för samtliga kategorier (Klingberg & Hallberg, 2021).

När det gäller verifieringen av den insamlade datan har reliabiliteten och validiteten granskats. I denna kontext innebär reliabilitet om datan kan reproduceras vid andra tidpunkter utifrån samma frågor, alltså om respondenterna ändrar svar utifrån intervjuare. Validitet i den bemärkelsen att sanningshalten och riktigheten i den insamlade datan för studien. Reliabilitet och validitet är svårt att kontrollera på kvalitativa studier som applicerats med en fenomenologisk teori, då det är personens egna perspektiv och omvärld som granskas. I ett bredare perspektiv går det däremot att validera kvalitativa studier till den grad som observationerna speglar de fenomen eller variabler som är av intresse, vilket var fallet för denna studien. Utifrån tidigare forskning och karaktärerna av de personer som valts för att delta i studien anses validiteten och reliabiliteten av den insamlade datan som hög och därmed lämplig för denna studie (Kvale och Brinkmann, 2014).

4.2 Etiska aspekter

Integritetsskyddsmyndigheten (IMY) fastställer att personuppgifter är all slags information som direkt eller indirekt kan knytas till en person som är i livet, som exempelvis namn, telefonnummer eller digitala ljudinspelningar. För att kunna använda personuppgifterna för denna studien krävs alltså ett samtycke. Ett samtycke ska vara ett fritt och genuint val och blir ogiltigt om någon har utsatts för en påverkan (IMY, 2022a).

Detta innebär att ett samtycke måste ha upprättats innan intervjun påbörjats för att kunna ha rätt till att spela in intervjun för att sedan transkribera och behandla materialet. Det är också viktigt att berätta för personen att det är lika lätt att återkalla ett samtycke som det är att lämna det (IMY, 2022b). Detta kompletteras med Kvale och Brinkmann (2014) riktlinje att alltid tydligt informera respondenterna om syftet med intervjuerna, hur resultatet kommer att redovisas samt att inget som kan återkopplas till dem som person, eller verksamhet, kommer att publiceras utan deras samtycke.

Samtliga respondenter informerades om ovanstående etiska aspekter utifrån IMY samt Kvale och Brinkmann (2014) och de valde att ge sitt samtycke till detta examensarbete under dessa förutsättningar. Ingen av respondenterna har under arbetets gång återkallat sitt samtycke.

5 Analys

Denna fallstudie är baserad på fyra stycken kvalitativa intervjuer där alla är en del av processen för en verksamhet att uppnå en ISO 27001-certifiering. I analysen kommer den insamlade datan att jämföras och analyseras med befintlig forskning. Den insamlade datan kommer att refereras till utifrån nedanstående tabell (Tabell 2).

Den första sektionen som analyseras är själva processen för ISO 27001-certifieringar, detta för att redovisa hur svenska verksamheter förhåller sig till processen och hur den ter sig utanför forskningen. I den sektionen är det mest bidrag från V3 samt V4, då de har varit involverade i flertalet certifieringsprocesser och har en bred branschkunskap. I den andra sektionen ges en kort presentation om V1 samt V2, hur de bedriver sitt nuvarande arbete inom informationssäkerhet, hur de resonerar kring det och vilka lagar de har att förhålla sig till i Sverige. I den tredje sektionen lyfts trender inom ISO 27001-certifieringar för att se om det skiljer sig mellan svenska verksamheter och den tidigare forskningen. I den sista och avslutande sektionen finns en sammanfattning av samtliga sektioners analys.

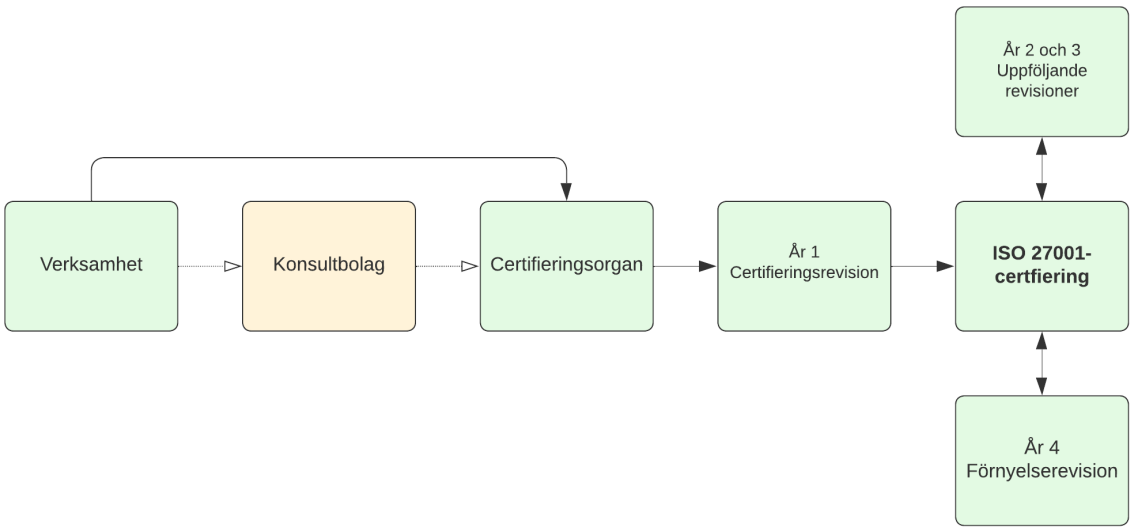
Tabell 2

Referensförteckning över insamlad data från intervjuer.

Verksamhet	**Yrkestitel**	**Typ av verksamhet**
V1	IT-chef	Offentlig
V2	IT- och säkerhetschef	Privat
V3	Affärsområdeschef	Certifieringsorgan
V4	Head of Information Security	Konsultbolag

5.1 Processen för ISO 27001-certifiering

Eftersom ISO 27001 är ett ramverk finns det ingen process som visar exakt hur den ska appliceras inom en verksamhet, men för att kunna få en certifiering måste en verksamhet först klara att gå igenom certifieringsprocessen och sedan underhålla certifieringen med hjälp av revisioner. Processen börjar med att en verksamhet har tagit beslutet för att gå mot en ISO 27001-certifiering. En verksamhet kan antingen välja att applicera ramverket själva i verksamheten eller att ta hjälp av ett konsultbolag. Då det inte är obligatoriskt men vanligt förekommande att en verksamhet tar hjälp av ett konsultbolag är den markerad som orange (Figur 4).



Figur 4 – Övergripande process över aktörer inblandade mot ISO 27001-certifiering.

V3 samt V4 uttryckte under intervjuerna att rent teoretiskt kan en verksamhet själva kontakta ett certifieringsorgan och genomföra certifieringen i egen regi, men det händer sällan då:

- Ledningssystem är komplexa att implementera själva utan experter.
- Riskanalyser och riskbedömningar är svåra då verksamheten inte ser alla potentiella risker.
- Få verksamheter har ISO 27001-experter som kan granska och följa upp arbetet internt.
- Det är ett stort projekt som tar tid och kostar mycket pengar, bättre att få det rätt från början.

V4 beskriver det som att när en GAP-analys genomförts och de pratat med verksamheten kan det ta mellan 3 månader upp till 1 år för en verksamhet att implementera ISO 27001-ramverket. V3 beskriver att det är antingen verksamheten i fråga eller det konsultbolag som verksamheten anställt som kontaktar dom när LIS:et är

klart. Ofta kontaktas flera certifieringsorgan som sedan får räkna på hur mycket det skulle kosta att genomgå certifieringen, där det blir en kombination av siffror direkt från standarden samt verksamhetens egna kostnader. V3 beskriver det som att det finns många olika parametrar att ta hänsyn till men att samtliga certifieringsorgan i slutändan ska ha räknat ut samma tidsåtgång då det är baserat på standarden. Det som i slutändan skiljer certifieringsorganen åt är dagspriset. V3 säger att: *"sen vill ju vi tro att vi är bra på det vi gör och att dom inte bara väljer oss för att vi har det mest attraktiva priset men att vi också har ett bra upplägg och ehm, omtyckta, att vi gör ett bra jobb där ute".*

När en verksamhet sedan har accepterat en offert från ett certifieringsorgan planeras certifieringsrevisionen in och datum bestäms mellan verksamhet och certifieringsorgan. Certifieringsrevisionen sker i två steg där V3 beskriver det som: *"Steg 1 handlar ofta ganska mycket om eh.. dokumentrevision där man då går igenom dokumentation då och.. sånna grejer och sen då så tittar man mer på processerna då steg 2.. Och ehm, sen leder det oftast till men inte alltid men oftast till ett antal förbättringsförslag då och troligen också några avvikelser. Och sen så får ju kunden jobba med att stänga dom avvikelserna då helt enkelt"*. När en verksamhet sedan har åtgärdat eventuella avvikelser så avslutas certifieringsrevisionen och certifieringsorganet utfärdar där ett ISO 27001-certifikat.

När en verksamhet fått ett ISO 27001-certifikat måste detta underhållas och det görs andra och tredje året i form av uppföljande revisioner, dessa är inte lika omfattande som certifieringsrevisionen och görs för att säkerställa att verksamheten underhåller sitt arbete med ramverket. Det fjärde året görs en förnyelserevision, som V3 beskriver som större och mer omfattande än de uppföljande revisionerna men inte lika omfattande som själva certifieringsrevisionen. V3 beskriver processen med revisionerna som en certifikatscykel som sträcker sig över 3 år eftersom uppföljande revisioner startar igen när en förnyelserevision är genomförd. Disterer (2013) beskriver certifieringsprocessen likadant som V3, men lyfter att om det framkommer avvikelser från kraven under uppföljande revisioner kan det leda till att certifieringsorganet kan göra att verksamhetens certifikat antingen suspenderas eller i värsta fall ta tillbaka det. Om ett certifieringsorgan tar tillbaka ett certifikat måste verksamheten på nytt genomgå en certifieringsrevision.

Disterer (2013) samt V3 bekräftar att ett ISO 27001-certifikat kräver kontinuerligt underhåll inom verksamheten och det räcker inte med att enbart ha klarat certifieringsrevisionen för att verksamheten ska få ett permanent certifikat. Hsu et al. (2016) undersökning visade dock att verksamheter inte alltid utför det arbetet som beskrivs i det som LIS:et fastställts, exempelvis var det en verksamhet som fortsatte att använda USB-stickor trots att det gick emot LIS:et. Detta är något som även bekräftas av V4 som betonar att en ISO 27001-certifiering nödvändigtvis inte påverkar en verksamhets arbete med informationssäkerhet. V1 har tidigare arbetat inom verksamheter som har haft en ISO 27001-certifiering och beskriver det som att det tenderar till att bli en pappersprodukt. Detta leder till en konflikt i processen eftersom det är konstaterat att det råder delade meningar om hur LIS:et och upprätthållandet av

certifieringen ser ut i verksamheterna. V4 riktar en viss kritik mot certifieringsorganen genom att säga: ”*En problem till exempel dom som gör ISO-audits.. Ehm, det finns skillnader. Kvalitativt. Eh, och ibland olika åsikter om hur man ska eh.. tolka en ISO-clause. Och det kan jag tycka leder till frustration hos våra kunder*”.

Ovanstående uttalande tyder på att det ändå finns oenigheter även bland certifieringsorganen om hur de ska tolka vägledningarna i standarden eftersom det varierar baserat på vem som utför revisionen för verksamheten. Detta bildar frustration mellan verksamhet, konsultbolag och certifieringsorgan. V3 uttrycker även*: ”Eh, äsch, det kan vara den här 1 men.. vi skriver 5 sidor på policies och så finns det 1 mening ”om ni anpassar er och lägger till 2 ord då är det ISO-komplett, men om ni.. utan dom här 2 ord då är ni inte ISO-compliant. Ish-nivå. Jag är lite mer.. hands on. Det här gör ingen skillnad för säkerheten vi har varför måste det vara så, varför måste det vara så petigt i vissa fall..”.* Disterer (2013) belyser att ett ISO 27001 är ett ramverk, för att det lätt ska gå att anpassa oavsett verksamhet och storleken på verksamheten. Trots att det låter bra teoretiskt bildar det ju också problem då det inte är tydligt med hur ramverket ska implementeras och det kan alltså uppstå meningsskiljaktigheter mellan de parter som är inblandade i processen just för att det beror på hur ramverket tolkas.

Att processen för ISO 27001-certifieringen är omfattande och komplex är alla intervjupersoner såväl som forskningen eniga om. V3 säger att dom som certifieringsorgan kan lyfta moment inom standarderna till svenska institutionen för standarder (SIS) och därmed kan standarder ändras och formuleras om så att det blir lättare men också bättre i praktiken när det kommer till vissa implementeringar inför revisionerna. Detta är dock inte vanligt inom internationella standarder som ISO 27001 är. Andersson et al. (2022) lyfter att framtagandet av standarder inom informationssäkerhet, som ISO 27001, ska inkludera personer från olika branscher och att utvecklingen av en standard ska ske genom delaktighet, frivillighet samt intressentstyrning. SIS ska i Sverige säkerställa att så många relevanta intressenter som möjligt bjuds in för att delta i dessa möten, ISO har samma ansvar fast på internationell nivå. Detta ger alltså förutsättningarna för att standarder ska kunna skapas utifrån intressenter som är i verksamheter som standarden i fråga ska kunna appliceras på och därmed utgöra ett ramverk som ska gå att applicera på så många olika typer av verksamheter som möjligt. Andersson et al. (2022) beskriver dock att så är inte fallet utan att under dessa möten är det oftast enbart 2–3 personer som lyfter sina åsikter och normen är att övriga personer inte motsätter sig till detta. Det är en slags auktoritet hos de företag som är störst, som exempelvis IBM och Microsoft, samt att det är mycket politiska intressen som styr besluten.

Detta leder till att det finns problematik i framställningen av en standard såväl som i hur ramverket appliceras på en verksamhet. I Culot et al. (2021) undersökning visade det sig att hela 68% av forskningsartiklarna inom komplikationer med ISO 27001-certifieringarna handlade om problem i samband med implementeringen av ramverket. Teoretiskt sätt ska det inte vara några problem, då ramverket ska vara flexibelt och

anpassningsbart utifrån verksamheten i fråga och en standard ska just vara en standard. Dock visar intervjuerna såväl som forskningen att det är svårare i praktiken än i teorin. V4 lyfte att det ett slags ”ISO 27001-light” borde finnas: *”Jag ser ett behov i marknad för ett certifikat som har mindre omfattande än ISO 27001, som ett ISO 27001 light eller vad man ska kalla det. Ehm, det finns vissa krav är.. som jag tycker är superviktig, men det finns andra krav som är krångligt”*. V3 belyser att det finns andra ISO-standarder som har blivit lättare att implementera sedan start på grund av uppdateringar och moderniseringar, men att ISO 27001 på ett sätt är en klass i sig då den är väldigt omfattande och att det inte är något som går att uttala sig om huruvida den kommer att bli enklare att implementera. Efterfrågan av ett mindre komplext ramverk som ger certifiering styrks även av V1 som har vissa delar av ISO 27001-ramverket implementerade i sitt arbete med informationssäkerhet men valt att inte gå för certifiering på grund av omfattningen.

5.2 Hur svenska verksamheter arbetar med informationssäkerhet idag

V1 beskriver arbetet inom IT i en offentlig verksamhet som att de är ett ”eget” IT-företag åt verksamheten då de har sin egna ekonomiska enhet och andra förvaltningar köper IT-relaterade tjänster av dem, exempelvis drift, datorer och telefoner. De har ingen specifik avdelning för information- eller cybersäkerhet utan det ansvaret hamnar på IT-avdelningen. Anledningen till det är att det är svårt att få igenom när verksamheten är politiskt styrd. V1 uttrycker det som: *”Det finns en tydlig struktur i vår informationssäkerhetspolicy i hur det här ska fungera, eh, sen är det ju ett naturligtvis pågående ständigt arbete att hålla på med det här och tänka runt det vid upphandling, införande av olika system och sånt där”.*

För V2 som är en privat verksamhet fungerar arbetet lite annorlunda med informationssäkerhet. Verksamheten arbetar mot telekom-, energi- samt fastighetsbranschen, deras interna IT-avdelningen är liten och de har ingen specifik avdelning för just information- och cybersäkerhet. De har även tagit in konsulter för att stötta verksamheten i deras arbete inom säkerhet, där mest fokus varit just på personalsäkerhet. V2 upplever att ledningen är engagerad inom arbetet med informationssäkerhet och är väldigt måna om att det är en viktig del i verksamhetens arbete. V2 säger att deras kunders kravställningar på informationssäkerhet har eskalerat det senaste halvåret och att de märker att det är mer krav och bevis från deras sida som ska visas upp i samband med beställningar och upphandlingar. De har en pågående säkerhetsanalys av verksamheten under intervjun som inte är fastställd än. V2 beskriver deras nuvarande utgångsläge som: *”Det faller ju på vår lott att bevisa att vi jobbar lika bra eller bättre som ISO 27000. Det kräver ju både kompetens från vår sida och från beställarens sida att kunna verifiera det då”.*

När det kommer till de anställda skickar V1 ut mejl med minikurser var tredje vecka och sedan kör de ibland workshops och V2 skickar ut liknande varannan vecka. V1 upplever att media bidragit till att de anställda tänker mer på informationssäkerhet som privatpersoner och därmed även tar med sig det beteendet till sin arbetsplats. De har

inte haft några större incidenter, utan det kan handla mer om att en anställd blivit kapad på sina privata användarkonton och haft samma lösenord på arbetsplatsen och därmed har åtgärder vidtagits. Det vanligaste försöken till cyberintrång för både V1 och V2 handlar om phisingmejl såväl som att genom ökad aktivitet påverka servrarna från utlandet. Phisingmejl informerar de sina medarbetare om i största möjliga mån samt att de använder sig av geoblockering för att hindra utländska aktörer. När det gäller deras största utmaning inom informationssäkerhet uttrycker V1: *"Man försöker hela tiden effektivisera och slimma organisationer och eh, i det sammanhanget är det ju så att i och med att vi har ett har ett välfärdsuppdrag där vi är ålagda att utföra vissa saker så kan vi inte välja bort att utföra vårt grunduppdrag. Och i det sammanhanget kan det ju bli så att informationssäkerhetsarbetet kanske inte blir den högsta prion hos medarbetarna".* För V2 är den största utmaningen nu att förhålla sig till sina kunders krav inom informationssäkerhet eftersom kunderna har svårt att veta vad de ska begära då det är mycket kring säkerhetsskyddslagen.

Både V1 och V2 omfattas av säkerhetsskyddslagen (2018:585) och arbetar utifrån de lagstiftade kraven där som inkluderar krav på säkerhetsskyddsanalys. V2 har däremot flertalet tillsynsmyndigheter eftersom de är verksamma inom flera sektioner. V1 omfattas däremot av lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174) som är baserad på NIS-direktivet. MSB (2021b) skriver att verksamheter som berörs av båda lagarna måste se över om lagarna överlappar helt eller delvis, exempelvis kan NIS-regleringen beröra de delar som inte omfattas av säkerhetsskyddslagen eller delar som berör säkerhetsskyddslagen är borttagna från NIS-regleringen. För att göra det ännu mer komplicerat är det inte heller nödvändigt att hela organisationen omfattas av ovanstående regleringar, utan det kan vara delar av verksamheten som enbart berörs. Eftersom det är upp till en verksamhet att själv avgöra om de omfattas av säkerhetsskyddslagen och sen anmäla detta hos en tillsynsmyndighet råder det mycket förvirring. V2 nämner ett fall med en verksamhet inom telekombranschen som fick en sanktionsavgift på 12.5 miljoner svenska kronor där det var uppenbar förvirring som låg till grunden.

Post- och telestyrelsen ([PTS], 2023) har i sitt beslutsunderlag skrivit att verksamheten i exemplet från ovanstående stycke anser att lagstiftningen är svår att förstå, för det finns väldigt lite vägledning och det saknas praxis för privata verksamheter samt inom sektorn elektronisk kommunikation. I beslutsunderlaget står det att verksamheten inte ansåg att de omfattades av säkerhetsskyddslagen i första säkerhetsskyddsanalysen PTS krävde, däremot ansåg de att de omfattades i den andra säkerhetsskyddsanalysen som PTS begärde. I samband med att verksamheten implementerade de åtgärder som var nödvändiga inom ramen av säkerhetsskyddslagen bedömdes det ändå att de gjort en överträdelse av säkerhetsskyddslagen och en av få sanktionsavgifter utfärdades. Robertsson & Linde (2023) har undersökt hur tillsynsmyndigheter har hanterat ärenden med överträdelser inom säkerhetsskyddslagen sedan dessa myndigheter fick större befogenheter när lagen skärptes december 2021. På bara 2 månader hade antalet ärenden ökats med 45% och Robertsson & Linde (2023) bedömer att det kommer vara

en fortsatt ökad trend i antalet ärenden. Det som deras undersökning dock visade var att det enbart är en sanktionsavgift som har utfärdats vid överträdelse av verksamheterna i undersökningen. Vanligast var att ärendet avslutades med ett föreläggande utan vite. Det råder stor skillnad i hur dessa tillsynsmyndigheter hanterar ärenden och hur de delar ut viten, sanktionsavgifter och avskrivningar. Det som är tydligast är att tillsynen blivit mer effektiv, däremot har det inte blivit mer likvärdigt eftersom det är extrema skillnader mellan liknande fall.

Svenska verksamheter har två lagar inom informationssäkerhet att förhålla sig till, där det är stora skillnader i hur tillsynsmyndigheter arbetar och tar beslut i eventuella överträdelser och konsekvenserna av detta. Det är inte ens säkert att verksamheten i fråga ens omfattas av regleringarna vilket gör att svenska verksamheter generellt sätt har ett ganska flexibelt sätt att arbeta med sin informationssäkerhet. Mirtsch et al. (2021) säger att verksamheters fokus på de regulatoriska kraven gör att verksamheter anser att de har genomfört det arbete som krävs inom informationssäkerhet och därmed inte är i behov av en certifiering. I kontrast till Mirtsch et al. (2021) uttrycker V4 sig som att det är svårt för verksamheter att egentligen bry sig om och ta åt sig av de befintliga lagstiftningarna inom informationssäkerhet som finns i Sverige just nu, då en böter eller sanktionsavgift egentligen inte är något en verksamhet drabbas så mycket av. V4 lyfter dock att NIS2-direktivet antagligen kommer ge verksamheter bättre ansvarstagande inom verksamhetens arbete med informationssäkerhet, då ledningen kan drabbas av en ”*time out*” om de inte tar ansvar och då mer konkret blir direkt ansvariga för eventuella brister. I sin tur bidrar detta till att en överträdelse blir mer personlig och personers inkomst och livsstil påverkas mer direkt. I Regeringens direktiv 2023:30 står det att de tillsatt utredare på hur detta ska gå att applicera i svensk lag eftersom det inte finns något stöd för en sådan konsekvens i dagens lagstiftningar och regleringar.

Viktigt att belysa är att NIS-direktiven och säkerhetsskyddslagen i stora drag är baserade på ISO 27001-standarden, vilket innebär att om en verksamhet har en ISO 27001-certifiering även håller sig inom de föreskrifter som dessa regleringar innebär. Det i sin tur innebär att om verksamheten omfattas av dessa regleringar även arbetar utifrån ISO 27001 ”*best practices*” i den mån de vill. Detta blir fallet för både V1 och V2 eftersom båda verksamheterna omfattas av lagarna och därmed jobbar utifrån delar av ISO 27001-standarden.

En av anledningarna till varför V2 ska påbörja processen med en ISO 27001-certifiering är för kunder och investerares skull eftersom under upphandlingarna blir det en konkurrensfördel med ett certifikat. Det blir tydligt att de arbetar kontinuerligt och systematiskt med sin informationssäkerhet och har koll på säkerhetsskyddslagen såväl som NIS-direktiven som i stora drag är baserade på just ISO 27001. I kontrast till detta så belyser Podreca et al. (2022) att många verksamheter har svårt att möta kunders och investerare krav, just för att ISO 27001-standarden kan anses som oflexibel vilket leder till att verksamheter förlorar upphandlingar och kunder då en verksamhet kan ha svårt att anpassa sig efter kundens krav. I Sverige anses dock ett ISO 27001-certifikatet som

en konkurrensfördel eftersom lagstiftningarna är baserade på standarden och därmed blir mer utav en säkerhet än något oflexibelt.

När frågan om ISO 27001-certifiering var aktuellt för V1 blev svaret däremot: *”Eh, nej, eh.. däremot så anammar vi ju som sagt mycket av det som finns i ISO 27000 när vi jobbar med vårt egen informationssäkerhetsarbete. Men vi har inte haft någon ambition om att certifiera oss”.* Detta är det vanligaste inom svenska verksamheter enligt V4 som säger att många verksamheter är nöjda med att jobba enligt ISO 27001-ramverket utan att gå för certifiering eftersom investeringen och kostnaden i sig får många att backa som inte har krav från kunder och investerare. Fomin et al. (2008) bekräftar att det är vanligt att arbeta utifrån standarden utan certifiering, men att det är svårt att veta hur många verksamheter som gör det. Däremot anser Fomin et al. (2008) att det bekräftas genom att antalet sålda standarder är betydligt fler än utfärdade certifieringar. V4 lyfter också att han tycker att ISO 27001-ramverket är det bästa för svenska verksamheter, men att han också förstår de verksamheter som inte väljer att gå mot en certifiering och anser att det är de verksamheter som behöver konkurrensfördelen som är de som bör investera i certifikatet. Genom att sätta detta i V1 och V2:s kontext blir det tydligt att V1 inte behöver ett certifikat som konkurrensfördel, utan det passar deras verksamhet att enbart arbeta utifrån ramverket i sig. Podreca et al. (2022) säger dock att det är vanligt att offentliga- samt statliga verksamheter däremot ställer krav på att verksamheter under upphandlingar ska ha en ISO 27001-certifiering. Tillskillnad från V1 ser V2 konkurrensfördelen som en viktigt aspekt och är den främsta faktorn till certifiering. V3 uttrycker sig däremot: *”Jag tror att börjar man jobba efter och börja jobba efter.. ehm.. standarden om man säger så ehm, då tror jag att man har för avsikt att tillslut gå efter en certifiering just för att kunna tala om för omvärlden att man är certifierade annars är det ju.. om man inte.. eh.. då får du ju inte med dig det värdet om man säger så. Sen så själva arbetet i sig har ju ett lika stort värde om du gör det utan att certifiera dig eller inte för, för.. bolaget i sig själva. Eh så absolut för en del tror jag att det börjar där.”*

Utifrån dessa utlåtanden är samtliga verksamheter överens med att det börjar genom att ramverket appliceras till viss grad inom verksamheter, sen råder det dock delade meningar om hur och varför de väljer att gå mot en certifiering eller inte. Hsu et al. (2016) lyfter att verksamheter som innehar en certifiering anses som mer trovärdiga, vilket gör att ur det perspektivet spelar det inte någon roll huruvida verksamheten arbetar utifrån standarden eller inte utan att det är certifikatet i sig som är det viktiga med ISO 27001

V3 samt V4 bekräftar också att det har blivit en slags ”boom” och att efterfrågan för verksamheter att gå mot ISO 27001-certifieringar har ökat och ökar fortfarande, främst i samband med cyberattacken mot Coop, COVID-19 samt Rysslands invasion av Ukraina. Detta har enligt V3 skapat en brist av kompetent personal för både certifieringsorgan och konsultbolag: ”*Missförstå mig rätt när jag säger kompetensbrist. Det är inte en brist på kompetenta personer men det finns för få kompetenta personer eh, och det är inte bara när det gäller certifieringssidan utan det är hela informationssäkerhetssidan även på*

konsultsidan så skulle det behövas med tanke på att det efterfrågas mer och mer så behövs det mer folk in i den branschen.". Ovanstående uttalande går även att sätta i verksamheters perspektiv, då det inte är vanligt förekommande att ha intern personal inom informationssäkerhetsarbetet och de vänder sig till konsultbolag såväl som certifieringsorgan för rådgivning och hjälp vid implementering. Det är inte heller helt ovanligt att det inkommer samtal i panik till konsultbolag såväl som certifieringsorgan när verksamheter har drabbats av ett intrång och vill åtgärda deras arbete med informationssäkerhet så fort som möjligt. V4 uttrycker det som att dessa samtal kan delas i två olika riktningar – de som absolut inte vill gå igenom ett intrång igen och har inställningen att det får kosta, de kan inte gå igenom det här igen och vill gå mot certifiering. Andra frågar mer för att förstå hur det kunde ske från första början, de vill veta hur deras tidigare investeringar inom informationssäkerhet har brustit och hur de ska tänka utifrån deras nuvarande utgångspunkt.

5.3 Trender inom svenska verksamheter som väljer att certifiera sig för ISO 27001

Det som framkom tydligt under intervjuerna är att det är vissa branscher som är mer benägna att certifiera sig än andra. V3 och V4 nämnde följande branscher:

- IKT-verksamheter
- Finansbranschen
- Hälso- och sjukvården

Mirtsch et al. (2021), Culot et al. (2021) samt Podreca et al. (2022) bekräftar i sin forskning de branschtrender som V3 och V4 lyfter under intervjuerna, vilket tyder på att det är en internationell trend såväl som svensk. Anledningen till certifieringarna är dock olika. IKT-verksamheter certifierar sig främst för certifikatets skull eftersom det ger en konkurrensfördel och gynnar upphandlingar som är fallet för V1 som befinner sig i den typen av verksamhet. V4 säger att finansbranschen generellt sätt har ett bra befintligt arbete kring informationssäkerhet då det finns många regulatoriska krav, men att dom drabbas hårt av brister inom informationssäkerhet eftersom det kan leda till konkurs. Litar inte kunder på sin bank, byter dom helt enkelt och då står banken utan kunder och får lägga ner sin verksamhet.

En annan tydlig trend är att det är bolag som redan har andra ISO-certifieringar, främst ISO 9001 men även ISO 14001, som väljer att även certifiera sig för ISO 27001. V3 och V4 instämmer i denna trend och V4 uttryckte det som: *"Jaja, det går hand i hand. Absolut. Dom bolag som redan är 9000-certifierat för kvalité dom är.. dom behöver man inte övertyga att det är en fördel att bli ISO-certifierat. Eh och dom förstår redan att det finns redan vissa processer på plats som vi kan använda igen. Eh, non conformity.. eh, avvikelseprocessen, non confirmity, ledningsgenomgång.. så dom är redan "Aja, men okej det här låter allt bekant och.. så för dom brukar det vara.. Aa, absolut.. Då är det bara next step. Yes. Det tycker jag".* Detta går i linje med V2, som har andra ISO-certifieringar och upplever att styrelsen har sett ISO 27001-certifieringen som en självklarhet och är

insatta i hur arbetet kring ISO-standarder fungerar. Podreca et al. (2022) och Culot et al. (2021) har i sina undersökningar sett ett tydligt samband i att verksamheter som går mot ISO 27001-certifieringar har andra befintliga ISO-certifieringar i verksamheten.

V3 som även utfärdar certifikat för ISO 9001 och ISO 14001 sa: ”V*id första anblicken tror många att kunder att.. nämen har vi 9 och 14 kan vi addera 27, men så är det inte riktigt. För 27 är betydligt mer komplex. Eh åh.. Det kanske är andra människor på företaget man pratar med i större utsträckning än vad det är inom 9 och 14. Ehm, det är andra processer, det är.. ehm, ja det är mer komplext. Eh och… Tittar man på vid första anblicken kanske man tror att det är ganska likt 9 och 14 men man djupdyker djupare på ett annat sätt skulle jag säga”.* V3 bekräftar att det finns ett samband, men att det inte är lika självklart att gå mot ISO 27001-certifieringen eftersom den är mer komplex och mer arbete behöver läggas ner jämfört med övriga ISO-certifieringar.

Mindre bolag har oftast inte de ekonomiska förutsättningarna att gå mot en ISO 27001-certifiering, vilket leder till att det oftast är större bolag som väljer att certifiera sig. V4 nämner att många mindre bolag är intresserade men backar väldigt fort när de hör prisuppgifterna. V3 upplever dock inte att det är bolagets storlek som brukar avgöra om en verksamhet går mot en certifiering utan tycker mer att det är faktorn vilken typ av verksamhet som bedrivs, som IKT-verksamheter. Där upplever V3 att det är etablerade verksamheter såväl som nya bolag. Mirtsch et al. (2021) har i sin sammanfattning skrivit att i deras undersökning var det en tydlig trend att det var nyare bolag som är mer måna om att certifiera sig för ISO 27001.

ISO 27001-certifikaten är internationella, vilket innebär att de finns i hela världen och är därför vanligt förekommande i andra länder. Framför allt i Taiwan, Singapore och Indien eftersom de ser certifieringar som en del av produkten de säljer och kopplar samman det med kvaliteten (Podreca et al. 2022; Mirtsch et al. 2021; Fomin et al. 2008). V4 säger att vanliga frågor från deras kunder är hur de kan implementera ramverket och samtidigt förhålla sig till andra länders lagkrav, just för att verksamheten i fråga kan ha utländska kontor.

5.4 Sammanfattning av analys

En verksamhets arbete inom informationssäkerhet är lättare att implementera i teorin än i praktiken. Trots att det finns standarder och lagar som upprätthåller en viss praxis, är det många verksamheter som ändå har svårt att implementera och upprätthålla de krav som krävs. Det börjar redan i framställningen av en standard där Andersson et al. (2022) indikerar att det inte är så pass demokratiskt och inkluderande som det ska vara och som det framställs. Själva implementeringen är det som de flesta verksamheter har svårt för och det kan ibland uppstå meningsskiljaktigheter inom tolkningen av standarden mellan verksamheten, eventuellt konsultbolag samt certifieringsorganet. Detta skapar en frustration som gör att processen tar längre tid, kostar mer pengar och även skapar konflikter. V3 lyfter att det råder kompetensbrist i Sverige när det kommer

till informationssäkerhet i den aspekten att det finns för få som arbetar med implementeringslösningar såväl som revisioner.

I Sverige finns det enbart lagar och regler inom informationssäkerhet för de verksamheter som bedriver en verksamhet som är viktigare än andra i den bemärkelsen att upprätthålla samhällets funktionalitet oavsett störning (MSB, 2021a). Detta är dock upp till verksamheterna själva att avgöra, sedan ska de rapportera till den tillsynsmyndighet som deras sektion tillhör. Detta har skapat mycket förvirring för de verksamheter som omfattas av säkerhetsskyddslagen såväl som stora skillnader i hur tillsynsmyndigheter hanterar överträdelser av lagen.

Majoriteten av de utmaningar svenska verksamheter har bekräftas även i tidigare forskning som inte är specificerad för svenska verksamheter. Däremot har det inte forskats mycket i form av konkreta faktiska utmaningar utan mer hur en ISO-certifiering påverkar en verksamhet ekonomiskt samt anledningar till en låg tillämpning av ISO 27001-standarden. Däremot har det hittats anledningar och motiveringar från flertalet forskningsartiklar som sedan har sammanställts i detta arbete.

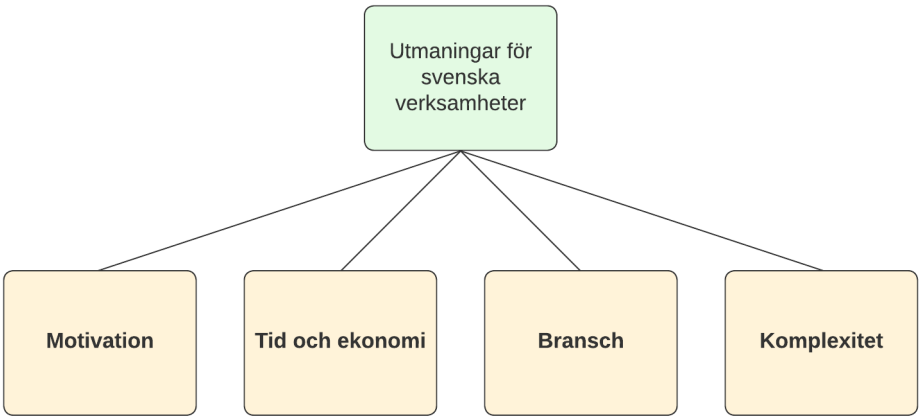
En av de tydligaste indikationerna från forskningen såväl som fallstudiens data är att det finns en tydlig branschtrend. Branschtrend i den bemärkelsen att det finns branscher som har högra tillämpning av ISO 27001-standarden än andra.

6 Resultat

Resultatet av denna fallstudie är baserad på analysen av den insamlade datan, som tillsammans ska besvara frågan:

Vilka utmaningar har svenska verksamheter för att nå en ISO 27001-certifiering?

Ur analysen hittades fyra stycken utmaningar som i sin tur är uppbyggda av faktorer som lyftes under intervjuerna, se figur 5. Eftersom det inte är många svenska verksamheter som har en ISO 27001-certifiering finns det uppenbara utmaningar för verksamheter att applicera ramverket på sin verksamhet.



Figur 5 – Forskningsfrågans övergripande resultat.

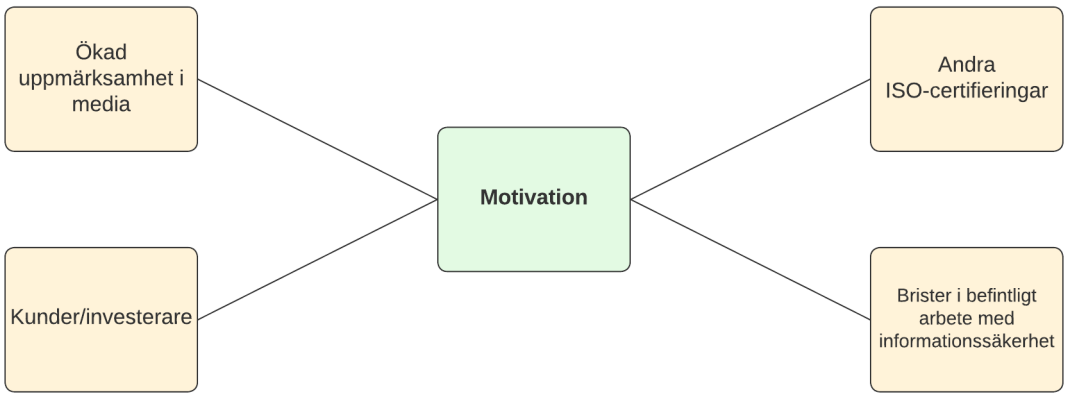
6.1 Utmaning 1: Motivation

Den första utmaningen för verksamheter för att certifiera sig mot ISO 27001 handlar om vad som motiverar verksamheten att certifiera sig. V2 uttryckte att det börjar komma in mer krav från kunder för verksamheten att certifiera sig, vilket direkt påverkar verksamheten som helhet och blir därmed en motivation till att ta en certifiering. V1 uttryckte det som att de inte har något behov av en certifiering, alltså har de ingen motivation till att ta verksamheten mot en ISO 27001-certifiering. V1 är även en politiskt styrd verksamhet, vilket gör att beslut inte kan tas lika lätt som i privata verksamheter.

V2 som arbetar mot en certifiering inom ISO 27001 har även andra ISO-certifieringar inom verksamheten, vilket har gjort det lättare att få med ledningen i processen utan vidare diskussioner, varit mer självklart och mer utav en fråga om när. Detta går i linje med V3, V4, Podreca et al. (2022) samt Culot et al. (2021) som bekräftar ett tydligt samband i att verksamheter som går mot en ISO 27001-certifiering har andra befintliga ISO-certifieringar i verksamheten. De har erfarenhet av hur ett ISO-certifikat har påverkat verksamheten inom andra områden och har sett den utdelning som ett certifikat ger.

V3 och V4 uttryckte att efterfrågan ökar hela tiden och att de ser ett starkt samband med cyberattacken mot Coop, COVID-19 samt Rysslands invasion av Ukraina. Den ökade uppmärksamheten i media har lett till att många verksamheter i preventivt syfte vill genomgå en certifiering eller att de faktiskt har utsatts för ett intrång alternativt intrångsförsök och därmed upplever brister i sitt befintliga arbete inom informationssäkerhet.

Ovanstående redovisas i Figur 6, just för att se hur ovanstående faktorer bidrar till utmaningen ”Motivation”.



Figur 6 – Bidragande faktorer till utmaningen ”Motivation”.

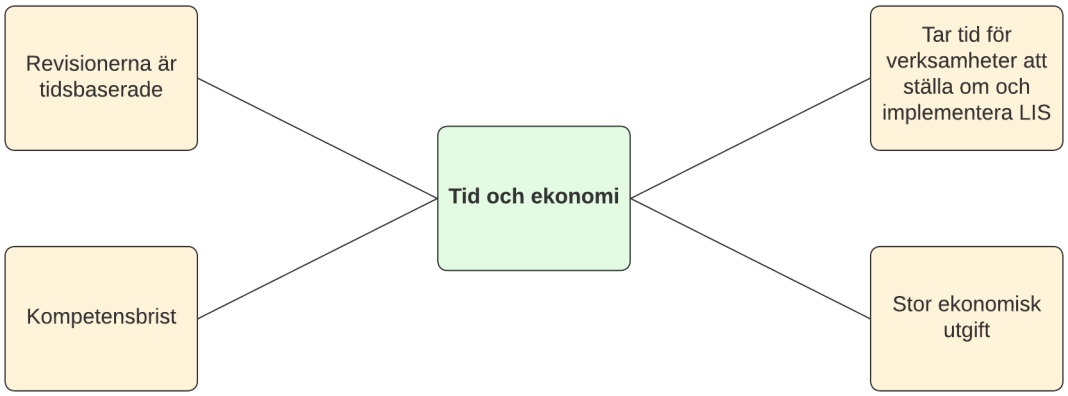
6.2 Utmaning 2: Tid och ekonomi

En utmaning som forskning såväl som fallstudien är överens om är just en verksamhets tid och ekonomi. Dels kräver det mycket tid från verksamheter eftersom de behöver anpassa verksamheten efter LIS:et såväl som medarbetare som ska arbeta med omställningen. När LIS:et är fastställt och certifieringsorganet sedan kan påbörja revisionerna tar det i sin tur också mycket tid, så sammanlagd tid tar generellt sätt minst ett år. Vill en verksamhet anställa ett konsultbolaget för att skapa LIS:et blir det en stor ekonomisk utgift, som vissa verksamheter är villiga att ta men alla har inte dom finansiella förutsättningarna att göra detta. Utöver konsultbolaget blir det även en kostnad mot certifieringsorganet vilket gör att ISO 27001-certifieringarna blir en stor ekonomisk utgift oavsett om de väljer att ta hjälp av ett konsultbolag eller inte.

V4 sa att det är många verksamheter som hör av sig och är intresserade av en ISO 27001-certifiering men att många backar när de inser hur mycket tid och pengar de måste lägga ner på certifieringen. Denna anledningen är även vanlig förekommande i tidigare forskning om ISO 27001-certifieringar, Podreca et al. (2022) skriver att det dessutom är svårt att veta hur stor den ekonomiska utgiften totalt blir eftersom en certifieringsprocess kan dra ut på tiden vilket gör att både tid samt ekonomi påverkas.

V3 lyfte även att det finns en kompetensbrist i Sverige när det kommer till informationssäkerhet. Inte att det finns personer med för lite kompetens, utan att det finns för lite personer med just kompetens i branschen. Detta i kombination med den ökade efterfrågan leder till att revisorer får fler uppdrag samtidigt som det inte går att anställa revisorer i samma takt. Flertalet svenska verksamheter har inte heller interna informationssäkerhetsspecialister utan antingen förläggs arbetet på den befintliga IT-avdelningen eller så anlitas ett konsultbolag. Detta tillsammans bidrar till att tiden och ekonomin är en stor utmaning för verksamheter som vill gå mot en ISO 27001-certifiering.

Ovanstående redovisas i Figur 7, just för att se hur ovanstående faktorer bidrar till utmaningen ”Tid och ekonomi”.



Figur 7 – Bidragande faktorer till utmaningen ”Tid och ekonomi”.

6.3 Utmaning 3: Bransch

Under intervjuerna framkom det att det är tydligt vilka branscher som väljer att certifiera sig och dessa bekräftas även av forskning, vilket tyder på att det är en svensk såväl som internationell trend när det gäller ISO 27001-certifieringar.

V1 är en politisk styrd organisation utan andra ISO-certifieringar bekräftar datan från övriga intervjuer. De har inga andra ISO-certifieringar och har svårt att prioritera informationssäkerhet i den aspekten att gå mot en ISO 27001-certifiering.

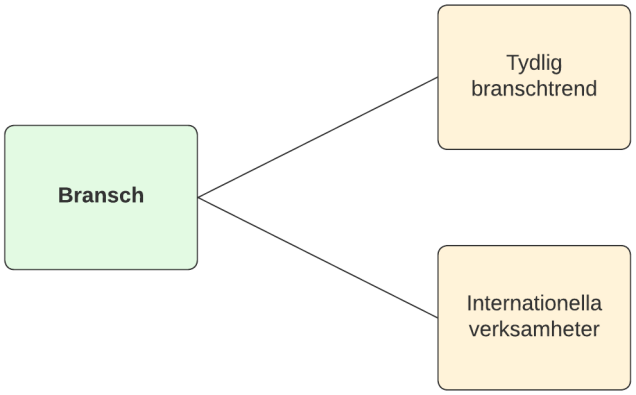
De trender som kom från fallstudien var:

- Verksamheter inom finans, hälso- och sjukvården samt IKT.
- Andra ISO-certifieringar.
- Internationella verksamheter.

Värt att nämna är däremot Mirtsch et al. (2021) samt V4 som poängterar att det är främst större bolag som har bättre ekonomiska förutsättningar som väljer att certifiera

sig för ISO 27001, däremot säger V3 att de inte upplever en verksamhets storlek som en trend utan att det mer handlar om de ekonomiska förutsättningarna.

Ovanstående redovisas i Figur 8, just för att se hur ovanstående faktorer bidrar till utmaningen ”Bransch”.



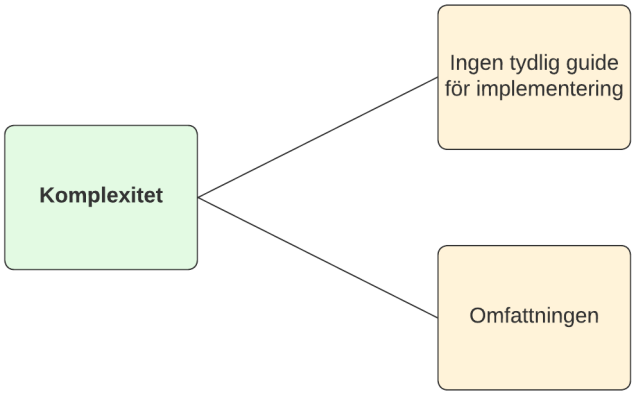
Figur 8 – Bidragande faktorer till utmaningen ”Bransch”.

6.4 Utmaning 4: Komplexitet

Komplexiteten bygger främst på att det inte finns någon tydlig guide i hur standarden ska appliceras i en verksamhet samt omfattningen som ramverket bidrar med. Att det inte finns någon tydlig guide är för att standarden ska vara flexibel eftersom det är ett ramverk, för att den ska kunna anpassas efter verksamheten i fråga. Det ska inte heller vara baserat på en verksamhets storlek men omfattningen gör att det inte är många mindre verksamheter som väljer att genomföra certifieringsprocessen. Som Culot et al. (2021) lyfte visar 68% av artiklar med svårigheterna inom ISO 27001-certifieringar just att implementeringen är där verksamheter stöter på mest problem. Implementeringen är en huvuddel i processen och utan den blir det ingen certifiering för verksamheten i fråga.

Omfattningen och den bristande tydligheten för implementering av ramverket gör att verksamheter ofta applicera delar av ramverket och arbetar utifrån *”best practices”.* Fomin et al. (2008) säger att det är tydligt genom antalet sålda ISO 27001-standarder i kontrast till hur många verksamheter som har en ISO 27001-certifiering. V3 upplever dock att de verksamheter som börjat med att arbeta utifrån *”best practices”* sedan ser nyttan i att arbeta mot en certifiering eftersom det befintliga arbetet fungerar bra och de ser nyttan i att ha ett certifikat för det arbetet de lagt ner. V4 tycker att det i stället borde skapas någon form av ”ISO 27001-light” som ska ge ett certifikat, just för att skala ner omfattningen och behålla de allra viktigaste kraven i ramverket och därmed också underlätta implementeringen.

Ovanstående redovisas i Figur 9, just för att se hur ovanstående faktorer bidrar till utmaningen ”Komplexitet”.



Figur 9 – Bidragande faktorer till utmaningen ”Komplexitet”.

7 Slutsats

Fallstudiens resultat bildade fyra utmaningar som baserades på faktorer från samtliga intervjuer. Motivation är en viktig drivkraft till att en verksamhet ska gå mot en ISO 27001-certifiering eftersom det är omfattande, komplext, tidskrävande samt en stor ekonomisk utgift som verksamheter investerar i för att till slut få sitt certifikat.

Att det är just certifikatet som lockar är en av de huvudsakliga anledningarna till att verksamheter väljer att certifiera sig för ISO 27001, det är ett resultat av verksamhetens informationssäkerhetsarbete (Silva et al., 2016; Disterer, 2013; Podreca et al., 2022; Andersson et al., 2022; Ganji et al., 2019). Verksamheterna i fallstudien hade alla olika ställningstagande till ISO 27001-standarden – V1 såg det som en pappersprodukt i den bemärkelsen att det egentligen inte bevisar hur en verksamhet faktiskt arbetar med sitt informationssäkerhetsarbete, V2 såg det som en självklarhet då kunder, investerare såväl som ledning är införstådda i fördelarna med det, V3 såg det som en självklarhet då det är en erkänd ISO-standard och V4 såg det som ett bra ramverk, men att det finns stor potential till förbättringar i form av korrigeringar av vissa krav.

Rent generellt går det att applicera mycket av den tidigare forskningen mot svenska verksamheters låga tillämpning av ISO 27001-certifieringar. Det kan ses som en generell bekräftelse att ISO 27001-standarden inte är så pass flexibel som den är menad att vara. Mycket av den tidigare forskningen håller dock inte samma linje, utan kan ibland säga motsatsen om samma dilemma. Exempelvis betonar Podreca et al. (2022) att verksamheter som har ISO 27001-standarden upplevs som mindre flexibla mot kunder då de har ett ramverk att förhålla sig till och Disterer (2013) argumenterar för att det flexibla ramverket gör det lättare för verksamheter att möta kunders krav. Ovanstående leder till att det finns en viss generell bild av ISO 27001-standarden inom forskningen men att det också finns en hel del meningsskiljaktigheter.

Det är svårt att veta hur verksamheter i Sverige ska samt bör bedriva sitt informationssäkerhetsarbete. De befintliga lagarna i Sverige är inte konkreta nog för att verksamheter ska veta om de omfattas av lagarna eller inte. Det är stor skillnad i hur tillsynsmyndigheter hanterar överträdelser av säkerhetsskyddslagen och ISO 27001-standarden är skapad som ett flexibelt och anpassningsbart ramverk för det ska kunna passa alla typer av verksamheter, men det skapar också oklarheter. Det är alltså lättare sagt än gjort för verksamheter att bedriva sitt informationssäkerhetsarbete i enlighet med svenska lagar såväl som ISO 27001-standarden.

8 Diskussion

Diskussionen för detta examensarbete handlar om hur arbetet står i relation till samhälleliga-, vetenskapliga- samt etiska aspekter. Utöver detta diskuteras även metodvalet, studiens resultat samt förslag på framtida forskning.

8.1 Samhälleliga aspekter

En av de viktigaste och mest oförutsägbara förändringarna i svensk lagstiftning är just NIS2-direktivets påverkan. Regeringen har vidtagit åtgärder i form av att utredare ska undersöka hur det går att implementera ändringarna som NIS2-direktivet kräver i förhållande till svenska lagar. NIS-direktivet är idag grunden för lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174) och om den lagen kommer försvinna eller utökas återstår att se eftersom det är fler krav som måste appliceras utifrån NIS2-direktivet. Två tänkbara scenarion är att antingen väljer fler verksamheter att certifiera sig för ISO 27001 och därmed får en bekräftelse av ett certifieringsbolag att de arbetar utifrån standarden och därmed uppfyller lagkrav. Det andra scenariot är att NIS2-direktivet kommer leda till att verksamheter ställer om sitt arbete inom informationssäkerhet och blir medvetna om hur lagen fungerar och därmed anser de att *”best practices”* är tillräckligt eftersom de följer de lagar som finns och upplever inte att ett certifikat direkt påverkar verksamheten. Det som är värt att lyfta är att NIS2-direktivet kommer att påverka mycket och med största sannolikhet kommer att bli en drivkraft för just ledningen i verksamheter eftersom NIS2-direktivet möjliggör att de personligen kan hållas ansvariga för en verksamhets brister inom arbetet med informationssäkerhet.

En annan viktig aspekt är bristen av kompetenta personer inom informationssäkerhet i Sverige. MSB (2021c) lyfte i en förstudie om kompetensbrist inom information- och cybersäkerhet i Sverige och att den ökade digitaliseringen riskerar att på sikt leda till en ”generellt undermålig säkerhetsnivå”. Det officiella yrkesregistret (SSYK) har skapat underlaget för MSB:s kartläggning av kompetensbristen, men det är svårt att utgå från eftersom det är en stor skillnad utifrån MSB:s undersökning. Exempelvis så har SSYK 2300 registrerade personer verksamma som IT-säkerhetsexperter i hela Sverige som blir en tydlig kontrast när 200 av de verksamheter som svarat på MSB:s enkät har angett att de har 4000 anställda som primärt arbetar med IT- alternativt informationssäkerhet. MSB (2021c) redovisar även resultat från en internationell undersökning som besvarats av 489 cybersäkerhetsexperter där resultatet visade att kompetensbristen har påverkat 57% av verksamheterna, 95% uppger att kompetensbristen och dess konsekvenser inte har förbättrats det senaste året samt att 44% uppger att det även har blivit värre. I Sverige har det hittills varit svårt att hitta en undersökningsmetod som speglar det faktiska läget, men MSB konstaterar att det råder kompetensbrist i Sverige såväl som på global nivå när det kommer till personer inom informationssäkerhet.

8.2 Vetenskapliga aspekter

Den befintliga forskningen är långt ifrån överens när det kommer till ISO 27001-standarden. Somliga anser att det inte går att applicera en standard på en verksamhets arbete inom informationssäkerhet eftersom det finns för många aspekter som inte går att anpassa och få skräddarsydda att passa verksamheten i fråga (Andersson et al., 2022; Niemimaa & Niemimaa, 2016; Podreca et al., 2022). I kontrast till detta finns de forskare som anser att en standard är det som är bäst att utgå från eftersom det skapar en kartläggning för att etablera, implementera, underhålla samt kontinuerligt förbättra en verksamhets LIS med hjälp av PDCA (Ganji et al., 2019; Culot et al., 2021). Detta gör att det ibland kan vara svårt att hitta en generell bild av hur forskningen kring ISO 27001-standarden tidigare har sett ut. Däremot fanns det likheter såväl som skillnader för svenska verksamheter i kontrast till tidigare forskning och därmed kunde vissa utmaningar bekräftas. Svenska verksamheters utmaningar och faktorer blir dock förstärkta inom vissa aspekter, exempelvis trenden att verksamheter med andra ISO-certifieringar är mer benägna att även gå mot ISO 27001. Detta stämde in på V1 samt V2, då V2 har ambitionen att utöka sin ”ISO-familj” med ISO 27001 i kontrast till V1 som inte har någon ISO-certifiering i verksamheten och inte motiveras till att gå mot ISO 27001.

8.3 Etiska aspekter

En verksamhet behöver nödvändigtvis inte ha ett dåligt arbete informationssäkerhet trots att de inte är certifierade, men det underlättar såklart att ha en certifiering som bevis för att man har ett systematiskt arbete kring informationssäkerhet. På samma sätt innebär det att en verksamhet som har en certifiering nödvändigtvis inte heller ha ett bra informationssäkerhetsarbete. Hsu et al. (2016) lyfter i sin forskning att de såg certifierade verksamheter gå emot sitt egna LIS, i det här fallet att de anställda använde USB-stickor trots att det inte längre var tillåtet inom verksamheten. Fomin et al. (2008) såg ett samband i antalet sålda standarder och utfärdade certifikat, vilket indikerar på att fler verksamheter applicerar ramverket utan att faktiskt certifiera sig. Det är också värt att nämna att det finns många andra bra ramverk och standarder inom informationssäkerhet som inte ger ett certifikat, däremot blir det svårt att veta i vilken grad dessa är implementerade då det inte går att validera på samma sätt som ISO 27001-certifikat.

Det som också skapar ett etiskt dilemma inom informationssäkerhet är att de som blir utsatta för cyberattacker är offer. Dom är just offer, vilket innebär att skulden inte ska läggas på dem som blir utsatta för intrång. Det skapar en balansgång som är ganska svår, dels för att det är viktigt att implementera och arbeta kring informationssäkerhet inom verksamheten men samtidigt är det också viktigt att komma ihåg att det ska fungera. Som privatperson litar man på att en verksamhet förvaltar personuppgifter efter bästa möjliga förmåga vilket leder till att antagandet att de har ett säkert informationssäkerhetsarbete implementerat. I takt med att cyberattacker blir alltmer sofistikerade är det viktigt att verksamheter framöver ser över och kontinuerligt går igenom deras befintliga informationssäkerhetsarbete.

8.4 Metodval

För denna uppsats har en fallstudie genomförts där kvalitativa intervjuer genomförts. Kvale och Brinkmann (2014) lyfter att standardkritiken mot kvalitativa intervjuer är:

- Att det inte är vetenskapligt, utan mer baserat på sunt förnuft samt för personberoende.
- Att det enbart är kvalitativt och inte kvantitativ.
- Att datan byggs på subjektiva intryck, alltså att den inte blir objektiv och att därmed inte blir valid.
- Svårt att prova en hypotes, då kvalitativa intervjuer är mer utav en explorativ karaktär.
- Att datan inte blir tillförlitlig eftersom den bygger på ledande frågor.
- Att det inte går att generalisera den insamlade datan, eftersom det aldrig kommer att finnas tillräckligt många personer att intervjua.

Ovanstående kritik kan såklart vara befogad men eftersom denna fallstudie har applicerats med en fenomenologisk teori är det just intervjupersonernas upplevelser som varit i fokus. Denna fallstudie utfördes just för att litteraturen och forskningen inom ISO 27001-certifieringar lyfter samma kritik och fördelar, därför var just syftet att få en mer subjektiv bild av hur situationen i Sverige är och därmed se hur utmaningarna faktiskt ter sig i praktiken. Fler personer att intervjua hade såklart varit bättre men då konsultbolaget såväl som certifieringsorganet träffat hundratals med verksamheter att hjälpa att arbeta utifrån ISO 27001-certifiering känns deras input som valid eftersom de varit med verksamheter från början till slut. De kunde alltså ge en generell såväl som valid input för hela ISO 27001-processen såväl som fallstudien i sin helhet.

Intervjuerna och planeringen för intervjuerna gick som planerat. Varje intervju fick en egen skräddarsydd ram av frågor eftersom verksamheterna i fråga är med i olika delar av processen för ISO 27001-certifieringar, detta baserat på att samma frågor inte hade varit relevant för fallstudien. Det skulle ju ha varit bra att ha med en verksamhet som faktiskt har genomfört en ISO 27001-certifiering just för att se hur deras utmaningar såg ut och för att få veta om de upplevde att det var värt allt arbete. Anledningen till att det inte blev aktuellt var dels för att fokus just skulle vara på utmaningarna, inte på hur verksamheten nu arbetar och om arbetet var värt det i slutändan. Utan det relevanta var just utmaningar som sker från början till slut av processen och inte hur verksamheterna upplever sitt arbete med en ISO 27001-certifiering. Den andra anledningen är att konsultbolaget såväl som certifieringsorganet har erfarenhet från hundratals olika verksamheter som de hjälpt just från början till slut och därmed kunde ge en uppriktig samt samlad bild av hur utmaningar kan se ut längs hela processen.

8.5 Studiens resultat

Studien resulterade i fyra stycken utmaningar – motivation, tid och ekonomi, bransch samt komplexitet. Det som är viktigt att komma ihåg är att det är utmaningarna verksamheterna har att förhålla sig till och inte dem som verksamheterna har skapat. Det är mycket oklarheter i hur en standard framställs vilket leder till att det inte är konstigt att det också bidrar till oklarheter i samband med implementeringar.

En tanke som lyftes när resultatet var klart var just att det kanske är fel att leta efter generella utmaningar för ISO 27001-certifieringar utan att varje del i processen har sin utmaning för verksamheten och det leder till att certifieringsprocessen i sig är en utmaning. Det som framkom under intervjuerna var att samverkan mellan verksamhet, konsultbolag och certifieringsbolag kan ta uttryck på olika sätt då alla har sina egna tolkningar av ISO 27001-standarden och ska hitta en lösning som passar alla involverade. Verksamheten vill ha ett certifikat, konsultbolagen vill implementera bästa möjliga LIS och certifieringsorganet vill utfärda certifikat – de spelar alla olika roller och det är inte konstigt att de har olika syn på hur processen ska ta sitt uttryck.

Anledningen till varför det var ISO 27001-standarden som var av intresse för studien var att för att det är den standarden som ger certifikat och det går att se statistik över hur dessa utfärdas. En annan anledning är att MSB rekommenderar verksamheter att applicera ramverket på sina verksamheter och det är i enlighet med de befintliga svenska lagstiftningarna inom informationssäkerhet. En annan tanke som lyftes var just att ett certifikat inte är tillräckligt mycket utav en motivation för svenska verksamheter? Det är ett så pass stort jobb för de verksamheter som omfattas av lagarna att ställa om verksamheterna efter lagarna att man inte tänker att ett certifikat är värt det utifrån tid och ekonomi. Det som framkom var just att ett certifikat kräver mycket tid och ekonomi, vilket många verksamheter inte nödvändigtvis har.

En annan trend som framkom var att verksamheter med andra ISO-certifieringar är mer benägna att gå mot ISO 27001-certifieringar än andra verksamheter vilket också går att applicera på V1 och V2. Dock är tillverkningsindustrin en sådan bransch där verksamheter har andra ISO-certifieringar, däremot är det extremt ovanligt att de går mot ISO 27001. En anledning till detta kan vara att de anser att de inte behöver det utan att de i stället ställer krav på sina underleverantörer och därmed anser att de säkrar certifieringar i andra led som direkt påverkar deras arbete och därmed ”har” en certifiering. Detta var något som Mirtsch et al. (2021) lyfte i sin undersökning, att verksamheter som arbetar mot andra verksamheter med ISO 27001-certifiering anser att de indirekt också har certifieringen.

Detta examensarbete gick som planerat från början till slut, det var inga direkta avvikelser eller ändringar som påverkade arbetet i sin helhet. Det mest spontana som skedde var att efter intervjun med V3 togs ett beslut att kontakta V4 med anledning av att efter den intervjun upplevdes det som att de kunde bidra med mer information från verksamheters perspektiv under ISO 27001-processen, vilket de också gjorde.

8.6 Framtida forskning

Det pågår mycket förändringar inom informationssäkerhet som sektor i Sverige men även globalt. EU och dess medlemsländer håller på att ställa om lagar och regelverk för att applicera NIS2-direktivet och samtidigt pågår det oroligheter där cyberattacker är ett av de vapen som används. Det kommer med hög sannolikhet att bli mer fokus på informationssäkerhet och det kommer att skapa diskussioner om hur, vad och varför åtgärder bör implementeras.

Detta skapar många intressanta vinklar i den framtida forskningen utifrån detta examensarbete. NIS2-direktivet kommer att röra om i grytan när det kommer till verksamheters arbete inom informationssäkerhet. Det vore intressant att se om fler verksamheter väljer att certifiera sig för ISO 27001 eftersom det säkrar att fler verksamheter uppfyller de krav som kommer från direktivet. Det kan också resultera i motsatt effekt, alltså att verksamheter inte anser att de behöver certifiera sig för ISO 27001 för att de arbetar utifrån NIS2-direktivet och därmed uppfyller de krav som förväntas av dem inom deras arbete med informationssäkerhet. Av den anledningen vore det intressant att se hur verksamheter tänker kring NIS2-direktivet i kombination med ISO 27001-certifieringar.

En annan vinkel hade varit att se hur svenska verksamheter upplever att ISO 27001-certifieringar har påverkat verksamhetens arbete inom informationssäkerhet och hur utmaningarna i detta examensarbete har påverkat deras process mot en ISO 27001-certifiering. Det är något som med fördel hade kunnat genomföras med en kvantitativ ansats för att se hur utmaningarna tar sitt uttryck i en bredare skala. Det hade också varit intressant att veta hur ISO 27001-certifieringen har påverkat dem som verksamhet – har det varit en konkurrensfördel? Är de nöjda med sitt LIS?

Detta examensarbete kan ses som en språngbräda till att gå vidare inom flera aspekter av hur verksamheter i Sverige arbetar med informationssäkerhet.

Referenser

Andersson, A., Hedström, K., & Karlsson, F. (2022). ”Standardizing information security – a structurational analysis”. *Information & Management*, 59 (2022), 103623. https://doi.org/10.1016/j.im.2022.103623.

Babacus AB (2023). Statistik. https://www.certifiering.nu/ecomedia/stat/basic.aspx?type=1&lang=sv-SE [2023-01-27].

Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B. (2008). Thesis Projects – A Guide for Students in Computer Science and Information Systems. Andra upplagan. London: Springer Verlag London Limited.

Checkpoint (2023). 2023 Cyber Security Report. https://research.checkpoint.com/2023/2023-security-report-cyberattacks-reach-an-all-time-high-in-response-to-geo-political-conflict-and-the-rise-of-disruption-and-destruction-malware/ [2023-02-10]

COM(2020) 823. *The NIS2 Directive - A high common level of cybersecurity in the EU.* Europeiska unionen. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

Culot, G., Nissimbeni, G., Podreca, M. & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, 33, 7(2021), pp. 76-105. https://doi.org/10.1108/TQM-09-2020-0202

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 4 (2013). 92-100. http://dx.doi.org/10.4236/jis.2013.42011

Eliasson, A. (2010). Kvantitativ metod från början. Andra upplagan. Lund: Studentlitteratur AB.

Fomin, V., de Vries., H. & Barlette, Y. (2008). ISO/IEC 27001 information systems security management standard: Exploring the reasons for low adoption. *Proc. 3rd Eur. Conf. Manage. Technol*., (2008), 1–13.

Ganji, D., Kalloniatis, C., Mouratidis, H. & Malekshahi Gheytassi, S. (2019). Approaches to Develop and Implement ISO/IEC 27001 Standard – Information Security Management Systems: A Systematic Literature Review. *International Journal on Advances in Software*, 12, 3 &4 (2019), pp. 228-238.

Hsu, C., Wang, T. & Lu, A. (2016). The Impact of ISO 27001 Certification on Firm Performance. *49th Hawaii International Conference on System Sciences (HICSS)*, (2016), pp. 4842-4848. https://doi.org/10.1109/HICSS.2016.600

Integritetsskyddsmyndigheten (IMY) (2022a). Vad är personuppgifter? https://www.imy.se/privatperson/dataskydd/introduktion-till-gdpr/vad-ar-personuppgifter/ [2023-02-20]

Integritetsskyddsmyndigheten (IMY) (2022b). Samtycke. https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/samtycke/ [2023-02-20]

International Organization for Standardization. (2022b). Informationssäkerhet – Cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav (ISO 27001:2022). https://www.iso.org/standard/27001

International Organization for Standardization. (2022a). Informationssäkerhet, cybersäkerhet och integritetsskydd – Vägledning om riskhantering inom informationssäkerhet (ISO 27005:2022). https://www.iso.org/standard/80585.html

Internetstiftelsen. (2022). *Svenskarna och internet 2022.* https://svenskarnaochinternet.se/app/uploads/2022/10/internetstiftelsen-svenskarna-och-internet-2022.pdf

Klingberg, G. & Hallberg, U. (2021). Kvalitativa metoder helt enkelt!. Första upplagan. Lund: Studentlitteratur AB.

Kosutic, D. (2022). ISO 27001 2013 vs. 2022 revision – What has changed? Advisera [blogg], 25 oktober. https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/ [2023-02-02]

Kvale, S. & Brinkmann, S. (2014). Den kvalitativa forskningsintervjun. Tredje upplagan. Lund: Studentlitteratur AB.

Li, Y. & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7 (2021). 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Long, R.M.W., Cuyvers, L., Bruynseraede, M. & Oates, E. (2023, 19 juni). EU Publishes New NIS2 Cyber Directive Imposing Liability and Obligations on Senior Management. Sidley. https://datamatters.sidley.com/2023/01/19/eu-publishes-new-nis2-cyber-directive-imposing-liability-and-obligations-on-senior-management/

Lundgren, B. & Möller, N. (2017). Defining Information Security. *Science and Engineering Ethics*, 5 (2019), 419-441. https://doi.org/10.1007/s11948-017-9992-1

Mirtsch, M., Kinne., J. & Blind, K. (2021). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions on Engingeering Management*, 68, 1 (2021), 87-100. doi: 10.1109/TEM.2020.2977815

Myndigheten för samhällsskydd och beredskap. (2015). Detta är informationssäkerhet. https://www.informationssakerhet.se/om-informationssakerhet2/vad-ar-informationssakerhet/ [2023-02-13]

Myndigheten för samhällsskydd och beredskap. (2021a). Identifiera samhällsviktig verksamhet. https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/samhallsviktig-verksamhet/identifiera-samhallsviktig-verksamhet/ [2023-04-03]

Myndigheten för samhällsskydd och beredskap. (2021c). Kompetens inom informations- och cybersäkerhet – en förstudie om kompetensförsörjning för samhället. https://www.informationssakerhet.se/siteassets/kompetensutveckling/kompetens-inom-informations--och-cybersakerhet---en-forstudie-om-kompetensforsorjning-for-samhallet.pdf

Myndigheten för samhällsskydd och beredskap. (2021b). NIS-regleringen och säkerhetsskyddslagen. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/lag-forordning-och-foreskrifter/definiation-av-nis-regleringen-och-sakerhetsskyddslagen/ [2023-05-08]

Nationellt center för cybersäkerhet. (2020). Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden. https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nationellt-center-for-cybersakerhet/rapport-cybersakerhet-i-sverige-2020--hot-metoder-brister-och-beroenden.pdf

Niemimaa, E. & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems*, 26, (2017), 1-20. https://doi.org/10.1057/s41303-016-0025-y

Pfleeger, C.P., Pfleeger, S.L. & Margulies, J. (2015). Security in Computing. Femte uppl., Massachusetts: Pearson Education, Inc.

Podreca, M., Culot, G., Nassimbeni, G. & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, 142 (2022), 103744. https://doi.org/10.1016/j.compind.2022.103744

Post- och telestyrelsen (PTS). (2023). http://pts.se/sv/nyheter/telefoni/2023/telenor-ska-betala-sanktionsavgift-enligt-sakerhetsskyddslagen/ [2023-03-01]

Regeringens direktiv 2023:30. *Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft: Regeringens direktiv 2023:30.* https://www.regeringen.se/contentassets/77a6664e7064451c8616caef98fd6961/gen

omforande-av-eus-direktiv-om-atgarder-for-en-hog-gemensam-cybersakerhetsniva-i-hela-unionen-och-eus-direktiv-om-kritiska-entiteters-motstandskraft.pdf

Robertsson, V. & Linde, S. (9 februari, 2023). Ett år med de nya sanktionerna i säkerhetsskyddslagen – så såg tillsynsarbetet och besluten ut. *Aktuell Säkerhet*. https://www.aktuellsakerhet.se/ett-ar-med-de-nya-sanktionerna-i-sakerhetsskyddslagen-sa-sag-tillsynsarbetet-och-besluten-ut/

Schaab, P., Beckers, K. and Pape, S. (2017). Social engineering defence mechanisms and counteracting training strategies. *Information and computer security*, 25:2 (2017), 206-222. https://doi-org.libraryproxy.his.se/10.1108/ICS-04-2017-0022

SFS 2018:585. Säkerhetsskyddslag. Stockholm: Justitiedepartementet.

Silva, L., Hsu, C., Backhouse, J. & McDonell, A. (2016). Resistance and power in a security certification scheme: The case of c:cure. *Decision Support Systems*, 92 (2016) 68-78. http://dx.doi.org/10.1016/j.dss.2016.09.014

Säkerhetspolisen (SÄPO) (2023). Försämrat omvärldsläge. Stockholm: Säkerhetspolisen. https://sakerhetspolisen.se/om-sakerhetspolisen/publikationer/sakerhetspolisens-arsberattelse/sakerhetspolisen-2022-2023/sammanfattning/forsamrat-omvarldslage.html

Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, 215 (2022), 483-487. https://doi.org/10.1016/j.procs.2022.12.050

TrueSec. (2022). Anonymous Sudan Threat Intelligence Report. Stockholm: TrueSec.