LUNDS UNIVERSITET
Ekonomihögskolan
Institutionen för informatik

Att implementera säkerhetsramverk

En studie om hinder och utmaningar företag möter vid implementering av säkerhetsramverk

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik.

Författare: Måns Herlöfsson
Peter Herslow

Handledare: Odd Steen

Rättande lärare: Nicklas Holmberg
Markus Lahtinen

Förord

Vi vill börja med att tacka de tre respondenterna som deltog i intervjuerna vilket bidrog till att studien kunde utföras. Vidare vill vi tacka vår handledare Odd Steen för att ha bidragit med sin kunskap och erfarenheter vilket har hjälpt oss under arbetets gång.

Maj, 2023

Måns och Peter

Att implementera säkerhetsramverk: En studie om hinder och utmaningar företag möter vid implementering av säkerhetsramverk

ENGELSK TITEL: To Implement Security Frameworks: A Study on Obstacles and Challenges Companies Face when Implementing Security Frameworks

FÖRFATTARE: Måns Herlöfsson och Peter Herslow

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, PhD

FRAMLAGD: Maj, 2023

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 65

NYCKELORD: IT-säkerhet, säkerhetsramverk, implementering, hinder, utmaningar

SAMMANFATTNING:
Cyberbrottslighet och dess medförda skador gör IT-säkerhet till en allt viktigare del av vardagen. Företag måste ständigt arbeta för att ligga steget före cyberkriminella och förhindra eventuella skador och angrepp. En åtgärd som blir allt vanligare är implementering av säkerhetsramverk för att skapa kontroll och struktur över sin IT-säkerhet. Denna studie syftar till att identifiera hur säkerhetsramverk implementeras samt vilka hinder och utmaningar företag stöter på under implementering. Uppsatsens bakgrund redogör varför företag väljer att implementera säkerhetsramverk. I litteraturdelen görs en genomgång av IT-säkerhet och säkerhetsramverk samt vad tidigare studier kommit fram till inom området. Det empiriska resultatet består av tre intervjuer med anställda inom IT-säkerhet som tillsammans har lång erfarenhet av implementering av säkerhetsramverk. Resultatet, angående hur säkerhetsramverk implementeras, identifierade att den främsta motiveringen till varför företag väljer att implementera säkerhetsramverk var till följd av krav från partners. Gällande hinder och utmaningar vid implementering av säkerhetsramverk så är den största samt mest frekventa utmaningen ledningens engagemang och fokus inom företag. De resultat och slutsatser som presenteras i denna studie vara till nytta som underlag för företag som planerar att implementera ett säkerhetsramverk eller redan påbörjat processen.

Innehåll

Tabeller

1 Introduktion

1.1 Bakgrund

I en tid då sammankopplade nätverk innebär att all data kan exponeras har IT-säkerhet blivit en allt viktigare del av våra liv (Sanou, 2017). I takt med att cyberbrottsligheten ökar och teknik blir alltmer sofistikerad, är det viktigare än någonsin att vara förberedd på att förhindra potentiella attacker. Om det så är artificiell intelligens och alla dess innovativa applikationer, cyberattacker som utnyttjar världens ökande fragmentering, digitala supply chain- eller överbelastningsattacker; Cyberbrottslingar har en förmåga att ständigt vara innovativa och utöka sin repertoar av taktiker (Sosafe, 2023).

Cyberattacker har genom åren inneburit stora förluster för flera företag. Enligt en rapport av The Council of Economic Advisers (2018) uppskattas det att cyberbrottsenheten kostade den amerikanska ekonomin mellan 589 miljarder kronor (57 miljarder dollar) och 1 127 miljarder kronor (109 miljarder dollar) 2016. Sett ur ett globalt perspektiv är siffrorna ännu mer skrämmande. Under år 2023 menar undersökningsföretaget Cybersecurity Ventures (2022) att kostnaden för cyberbrott världen över förväntas uppgå till 83 biljoner kronor (8 biljoner dollar), vilket är den största överföringen av ekonomiskt kapital i historien. Denna enorma kostnad hotar såväl innovation som investering, och utgör betydligt större fara än vad skador från naturkatastrofer gör under ett år. Dessutom förväntas cyberbrott vara mer lönsamma än den globala handeln med alla stora illegala droger tillsammans (Cybersecurity Ventures, 2022). Framöver förväntas den negativa trenden fortsätta med fler cyberangrepp och ökade kostnader. Estimeringar gjorda av Statistas Cybersecurity Outlook (2022) visar att den globala kostnaden för cyberbrottslighet år 2027 kommer uppgå till nästan 248 biljoner kronor (24 biljoner dollar).

Kostnader för cyberbrottslighet inkluderar skada och förstörelse av data, stöld av pengar, immateriella rättigheter samt personlig och finansiell data, förlorad produktivitet, förskingring, bedrägeri, störningar i den normala verksamheten efter attacken, forensisk undersökning, återställande och radering av hackade data och system, samt skada på rykte (Cybersecurity Ventures, 2022).

För att företag inte ska hamna bakom i utvecklingen och bli en måltavla för de potentiella dataintrång och cyberattacker de ställs inför är det avgörande att vara vaksam och ha en stark säkerhetskultur samt arbeta aktivt med hantering av risker relaterade till IT-säkerhet (Sosafe, 2023). Dessvärre tyder undersökningar att det finns en brist på tillgängliga IT-säkerhetsexperter trots det stora behov som alltså finns. Detta antydande förstärks av ISACA (2022) som bekräftar besvären i en studie. Studien visade nämligen att 60 procent av respondenternas företag upplevde svårigheter att anställa kvalificerad cybersäkerhetspersonal år 2021. En ökning med 7 procent sedan 2020.

Bristen på kvalificerad cybersäkerhetspersonal ihop med det ökande hoten relaterade till IT-säkerhet gör att företag riktar sig åt andra håll och alternativa lösningar för att öka deras skydd mot dataintrång. Ett exempel är implementering och tillämpning av "Cyber Security

Frameworks" (CSF), alltså säkerhetsramverk för IT-säkerhet. Säkerhetsramverk ses som en samling policys, metoder och förfaranden som implementeras för att skapa en effektiv och strukturerad säkerhetsmiljö. Dessa ramverk ger organisationer vägledning för att skydda sina tillgångar mot cyberhot genom att identifiera, bedöma och hantera risker som kan leda till dataintrång, systemavbrott eller andra störningar. Det finns en mängd olika säkerhetsramverk, några av de allra vanligaste och mest tillämpade är NIST, ISO 27001 och ISO 27002, samt CIS Controls. Gemensamt för många säkerhetsramverk är att de erbjuder best-practise lösningar i form av checklistor. Genom att använda sig av ramverk och ha dessa checklistor som utgångspunkt i sitt arbete med IT-säkerhet får företag en tydligare säkerhetskultur genom hela organisationen vilket underlättar för företagsledningen och anställda samtidigt som det motverkar cyberbrott och dataintrång (Ryerse, 2023).

Implementering av säkerhetsramverk medför även andra fördelar som till exempel minskad kostnad, ökad vinst, förbättrad medvetenhet hos användare och minimerade risker. Företagen vägleds av ramverken i implementeringsprocessen för att uppfylla de standardkrav som finns (Taherdoost, 2022).

1.2 Problemområde

Segal (2022) nämner i sin artikel att mindre företag har tre gånger större risk att bli måltavla för en cyberattack än större företag. Bristen på anställningsbara IT-säkerhetsexperter ihop med den stora kostnaden för att anlita säkerhetskonsulter är en del av problemet. Den andra delen är den ökade mängd cyberhot som företag ställs inför. En forskning som gjordes vid säkerhetsföretaget Barracuda Networks visade att en anställd på ett företag med mindre än 100 anställda i genomsnitt kommer att uppleva 350% fler attacker än en anställd på ett större företag (Segal, 2022).

För att förbättra sin IT-säkerhet väljer många företag att blicka åt lösningar, däribland är så kallade säkerhetsramverk en frekvent förekommande åtgärd. Dessvärre påpekar Gidi Cohen (2022) i sin artikel att det förekommer problem även här då implementering och tillämpning av dessa ramverk inte kommer utan dess svårigheter och fallgropar. En fallgrop som Cohen menar ligger bakom många misslyckade tillämpningar av säkerhetsramverk är att företag stirrar sig blinda på ramverkens punktlistor och implementerar åtgärder utifrån en så kallad “checkbox mentalitet”. Företag gör det minsta möjliga för att uppfylla minimikraven hos deras ramverks olika områden vilket resulterar i en svag IT-säkerhet och hög sårbarhet för cyberbrott (Cohen, 2022). En forskning av Dimensional research visade att 95% av organisationer möter avsevärda utmaningar vid implementering av cybersäkerhetsramverk (Dimensional Research, 2016).

Ett problem som har identifierats är att det finns artiklar som refererar till källor från 2017 och tidigare som i sin tur beskriver företags utmaningar vid implementering av säkerhetsramverk. Vidare finns det vetenskapliga källor som beskriver implementationen av specifika säkerhetsramverk som till exempel: NIST eller ISO/IEC 27001, men bristen på vetenskapliga källor som beskriver generella utmaningar och hinder företag möter under processen av implementeringen av säkerhetsramverk efter år 2017 är en stor anledning till att denna studie behövs.

1.3 Forskningsfrågor

Med denna bakgrund och detta problem i fokus syftar denna rapport att svara på följande frågeställningar:

- Hur implementeras säkerhetsramverk inom företag?
- Vilka hinder och utmaningar möter företagen vid implementering av säkerhetsramverk?

1.4 Syfte

Syftet med denna studie är att identifiera de utmaningar som företag står inför när de implementerar säkerhetsramverk. Forskningen kommer att fokusera på att identifiera de faktorer som påverkar en implementering av ett säkerhetsramverk och beskriva upprepade hinder som företag stöter på under implementeringen. Resultaten av denna studie kommer att kunna användas som underlag för företag som planerar att implementera ett säkerhetsramverk eller redan påbörjat processen.

1.5 Avgränsningar

Denna studie är avgränsad till implementeringen av säkerhetsramverk. Studien kommer inte att ta upp hur företag ska välja bland ramverken utan snarare hur implementeringen ser ut hos olika företag. Vidare är studien avgränsad till att identifiera hinder och utmaningar i processen av implementering av säkerhetsramverk och inte lösningar på hur företag kan undvika de identifierade hinderna och utmaningarna.

2 Litteraturgenomgång

I denna studie används begreppen IT-säkerhet och säkerhetsramverk regelbundet. För att förstå hur dessa begrepp och områden används inom undersökningen syftar det här avsnittet till att ge en beskrivning av varje begrepp och dess betydelse för senare analys.

2.1 IT-säkerhet

Ension (u.d.) definierar IT-säkerhet på följande sätt: "IT-säkerhet ansvarar för att skydda en organisations tillgångar som information, datorer och programvara. IT-säkerhet ingår som en del i den totala säkerheten…". Begreppet IT-säkerhet anses vara vagt och missuppfattas många gånger.

Cybersäkerhet kan liknas vid IT-säkerhet. Däremot tar cybersäkerhet ett större grepp runt omvärlden, mänskliga faktorer och ledning av arbete till skillnad från IT-säkerhet (Burgess, 2010). Under senare delen av 1900-talet formades ordet cyber. Det kommer från begreppet cybernetik vilket i sin tur handlar om kontroll- och kommunikationsteorier, samt styrtekniker (Burgess, 2010). Ordet cyber används ofta tillsammans med andra ord som till exempel säkerhet.

I sin artikel definerar Craigen, Diakun-Thibault & Purse (2014) cybersäkerhet på följande sätt: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights".

2.1.1 Cyberattacker

Cyberattacker är riktade angrepp som görs av olika anledningar. Cyberbrottslingar kan bland annat utföra attacker i syfte att stjäla information för spionerі eller för att sprida propaganda. Det främsta motivet bakom varför hackers väljer att utföra dataintrång är dock för ekonomisk vinning. Attacker riktar sig då åt att stjäla pengar eller annan känslig information för att sälja den på svarta marknaden eller använda för utpressning. Andra skäl till att cyberattacker utförs är bland annat för att vandalisera och orsaka destruktiva skador. Inte sällan är hackare ute efter spänning och bekräftelse och därför kan deras angrepp mot IT-system ibland tyckas vara utförda helt utan anledning (Identity Experts, 2017). Säkerhetsramverk har skapats för att hjälpa företag analysera situationen, ta reda på hot samt vidta nödvändiga åtgärder (Alshar'e, 2023).

2.2 Säkerhetsramverk

Ett säkerhetsramverk är en samling internationella standarder och best-practice som gemensamt kallas "cybersäkerhetsramverk". Ramverk är nödvändiga för att skydda företagets information mot cyberattacker och andra säkerhetsrisker (Alshar'e, 2023).

Att välja vilket ramverk som bör implementeras är ett beslut företag bör lägga stor vikt vid för att se till att ramverket uppfyller verksamhetens krav och önskemål. För många företag räcker det med ett ramverk för att möta företagets förväntningar men företag behöver överväga ifall mer än ett ramverk behövs (Taherdoost, 2022). Vidare nämner Taherdoost (2022) att lättillgängliga standarder och ramverk är valfria vid användning. Detta betyder att företag kan implementera ramverkets olika delar för sig eller i kombination med flera delar från andra ramverk för att stärka säkerheten.

Eftersom att det finns en stor mängd säkerhetsramverk att studera om har beslutet tagits att fokusera på tre av de mest förekommande ramverken. Efter granskning av litteratur om ämnet samt efter intervjuer med anställda inom IT-säkerhet nämndes tre säkerhetsramverk upprepade gånger; NIST Cybersecurity Framework, ISO/IEC 27001 och CIS Controls. Bortsett från det faktum att de är tre väldigt vanliga säkerhetsramverk så skiljer de sig en del från varandra. ISO/IEC 27001, men även delvis NIST, har en mer teoretiskt orienterad syn när det kommer till IT-säkerhet jämfört med CIS. Detta i sin tur innebär att ISO och NIST sätter större press på de ansvariga inom säkerheten på ett företag att omsätta teori till praktik. CIS kontrollerna har en mer praktisk och prioriterad syn som därför är mer användbart som ett operationellt verktyg. Företag använder ibland en kombination av ramverk för att förbättra sin IT-säkerhet, till exempel kan användningen av CIS bidra till att företag uppfyller kraven som ställs för en ISO 27001 certifiering (Conscia, 2021).

NIST, ISO 27001 och CIS är alltså inte bara tre av de största ramverken utan deras skillnader i teoretisk och praktiskt nivå gjorde dem extra värda att studera och använda som utgångspunkt i denna studie.

2.2.1 NIST Cybersecurity Framework

National Institute of Standards and Technology Cyber Security Framework (NIST CSF) består av tre huvuddelar: kärna, nivåer av implementering och profil. Saritac, Liu & Wang (2022) berättar att kärnan består av fem funktioner. Funktionerna har i sin tur flera kategorier, där varje kategori består av specifika tekniska och ledningsmässiga aktiviteter. Aktiviteterna syftar till att täcka allt från grunderna för att utveckla ett cybersäkerhetsprogram till aspekterna av riskhanteringssystem.

Kärnans fem funktioner är definierade enligt följande:

- Identifiera (Identify): Handlar om att identifiera och hantera cybersäkerhetsrelaterade risker genom att identifiera och förstå vilka resurser som behöver skyddas, vilka sårbarheter som finns och vilka hot som kan påverka organisationen.
- Skydda (Protect): Syftar till att implementera och upprätthålla lämpliga skyddsåtgärder för att minska risken för cybersäkerhetsincidenter. Det inkluderar att etablera och genomföra policies, procedurer och tekniska kontroller för att skydda resurser och information. Det innefattar även etablering av åtkomstkontroll, ökad medvetenhet och utbildning samt träning av personal och anställda.
- Upptäcka (Detect): Denna funktion handlar om att kontinuerligt övervaka och upptäcka eventuella händelser som kan indikera en cybersäkerhetsincident. Denna funktion kräver tekniska åtgärder och processer som kan upptäcka och rapportera avvikelser eller misstänkta aktiviteter.

- Reagera (Respond): Funktionen “reagera” handlar om att ha en plan för att snabbt och effektivt reagera på en cybersäkerhetsincident när den upptäcks. Det inkluderar att ha etablerade procedurer för att hantera incidenter, att snabbt begränsa och isolera skadan samt att samarbeta med andra aktörer för att lösa situationen. Det är även viktigt att genomföra förbättringar för att motverka en liknande incident i framtiden.
- Återställa (Recover): Det är viktigt att upprätthålla planer och processer för återhämtning från incidenter relaterade till cybersäkerhet. Denna funktion handlar om att förmågan att återställa data, system, nätverk och tjänster till nivån de var innan incidenten och på så vis återgå till normal drift.

En av NIST CSF:s främsta egenskaper är att det täcker ett brett spektrum av områden och tar i beaktande många olika utfall. Dedeke (2017) nämner däremot att det finns forskare som påstår att ramverket brister inom flera områden. Den nackdelen som tycks vara mest återkommande är att CSF anses vara ett för komplicerat verktyg för ledning och styrelsemedlemmar att förstå samt att ramverket inte täcker alla olika typer av utfall. Vidare säger Dedeke att andra forskare menar att ramverkets åtgärder bör ses snarare som rekommendationer och vägledning än rena tillvägagångssätt. Alltså är det fullt möjligt för företag att själva utveckla och implementera områden och utfall de känner avsaknad av (Dedeke, 2017).

Eftersom implementering av säkerhetsramverk inte är ett engångsprojekt utan snarare kontinuerlig resa så är det viktigt att organisationer dokumenterar sitt nuvarande och framtida tillstånd. NIST föreslår att man bevakar sina framsteg med hjälp av en poängsättningsskala från 1 till 4, där 4 är högsta mognadsnivå. På så vis kan företag få indikationer och riktmärken för deras mognadsnivå och kapaciteter. Med implementeringsstadie och mognadsnivå som utgångspunkt kan organisationer så grepp om sin “profil” och därigenom bli underrättad om vilka områden som är mest kritiska och vart de således bör lägga fokus (Dedeke, 2017).

2.2.2 ISO/IEC 27001

The International Organization for Standardization (ISO) och the International Electrotechnical Commission (IEC) 27001 är en internationell standard för ledningssystem för informationssäkerhet. ISO/IEC 27001 har blivit den mest framträdande standarden inom informationssäkerhet. Standarden är möjlig att tillämpa på majoriteten av företag men inte alla, den är avsedd för företag med hög mognadsnivå (Podrecca & Sartor, 2023). Standarden ger företag, oberoende av storlek samt verksamhetens sektor, en vägledning i hur de ska upprätta, implementera, driva, övervaka, utvärdera, underhålla och förbättra sina system för informationssäkerhet. ISO/IEC 27001 har 114 kontroller i 14 domäner. Certifiering enligt ISO 27001 innebär att ett företag har visats ha implementerat ett effektivt ledningssystem för informationssäkerhet i enlighet med standardens krav. Certifieringen gäller i tre år (Razikin & Soewito, 2022).

2.2.3 CIS Controls

Center for Internet Security (CIS) Critical Security Controls är en samling prioriterade åtgärder för cybersäkerhet som ger en djupgående försvarsstrategi med konkreta och effektiva bästa praxis för att motverka de vanligaste cyberattackerna. En av de främsta fördelarna med dessa kontroller är deras förmåga att prioritera och fokusera på ett fåtal åtgärder som kraftigt minskar riskerna relaterade till cybersäkerhet (Tyas Tunggal, 2023).

CIS-kontrollerna omfattar 18 åtgärdsområden och 153 tillhörande skyddsåtgärder. De är utformade för att representera vad som krävs för god cybersäkerhet och för att stoppa, begränsa, upptäcka samt åtgärda cyberangrepp. Kontrollerna utförs antingen som tekniska åtgärder såsom att använda en aktiv skanner för att identifiera all maskinvara i ett nätverk eller som mänskliga åtgärder där någon aktivt tar ställning till något. Ett exempel är vem som har ansvar för en dator, en budget eller en affärsprocess i organisationen (Conscia, 2021).

En egenskap som särskiljer CIS-kontrollerna från andra liknande säkerhetsramverk är dess förmåga att erbjuda konkreta och praktiska lösningar som är enkla att applicera i den dagliga verksamheten. För att förhindra missförstånd för hur kontroller ska utföras finns det en CIS-guide där varje kontroll har en rubrik och en beskrivning. På så sätt behöver det inte ske personliga tolkningar och prioriteringar utan CIS-kontrollerna redogör tydligt för hur åtgärder ska utföras. Detta är viktigt då det skapar en strukturerad och trygg säkerhetsplan (Conscia, 2021).

2.3 Tidigare hinder och utmaningar

Som tidigare nämnt under problemområdet så finns det en brist på vetenskapliga artiklar om generella hinder och utmaningar företag möter vid implementering av säkerhetsramverk. En tidigare relevant studie gjordes av Dimensional Research tillsammans med Tenable Network Security och Center for Internet Security år 2016. Studien innefattade 319 respondenter. Samtliga hade beslutsfattande positioner gällande IT-säkerhet på sina företag. Målet med studien var att kvantifiera mängden implementeringar av säkerhetsramverk samt undersöka hur långt företag kommit med sina implementationer (Dimensional Research, 2016).

Studien fastställde att 80% av de studerade individerna arbetade på företag som implementerat säkerhetsramverk. Det visade sig finnas fyra ramverk som var frekvent förekommande, ISO 27001/27002, CIS Controls och NIST var alla med på listan (Dimensional Research, 2016).

Gällande varför företag väljer att implementera säkerhetsramverk, fann undersökningen att den vanligaste orsaken är att det ses som best-practice. Den näst mest förekommande motiveringen var för att effektivisera efterlevnaden av regleringskrav. Andra anledningar var att det krävs enligt kontrakt eller för att förbättra den interna och externa kommunikationen (Dimensional Research, 2016).

Av de 80% som hade implementerat säkerhetsramverk på sina företag så rapporterade hela 95% att de sett positiva effekter av det. Av de 5% som inte såg några fördelar rapporterade färre än 1% att det var på grund av att ramverket inte var effektivt medan de andra konstaterade att de helt enkelt inte var tillräckligt långt komna i sin implementation. De främsta fördelarna var att implementeringen av säkerhetsramverken underlättade efterlevnad av avtalsförpliktelser, bidrog till ökad mognad och effektivitet av säkerhetsoperationer, samt medförde en mer mätbar IT-säkerhet. Ytterligare en positiv aspekt var att företagsledningen kunde få säkerhetsberedskap presenterat för sig på ett lättare och mer effektivt sätt. De fördelar som tenderade vara mest framstående var förbättrad mognad och effektivitet av säkerhetsoperationer samt efterlevnad av avtalskrav från kunder. Omkring hälften av företagen i studien kunde påvisa förbättringar inom dessa aspekter. Tydligt för alla upplevda fördelar är att de är i korrelation med tiden sedan implementeringen. Ju längre ett företag

arbetat med säkerhetsramverk desto fler positiva effekter visar det (Dimensional Research, 2016).

Studien visar dock att det allt som oftast förekommer hinder och utmaningar vid implementering av säkerhetsramverk. I 95% av fallen möter företag motgångar vid implementering. Undersökningen delar upp utmaningarna i två huvudgrupper; organisatoriska och teknologiska. Exempel på organisatoriska hinder är avsaknad av utbildad personal och bristande ledningsstöd, budget samt dåliga prioriteringar. Teknologiska hinder som identifierats är bristfällig integrering av verktyg samt avsaknad av verktyg för att automatisera och mäta effekten av kontroller och operationer. Ytterligare en utmaning är dålig rapportering. Totalt sett så är de organisatoriska utmaningarna marginellt mer förekommande än de teknologiska (Dimensional Research, 2016).

3 Metod

I följande kapitel presenteras de metoder som använts för insamling av empirisk data. Inledningsvis motiveras valet av metoder och urval gällande respondenter, för att sedan analysera datan. Slutligen diskuteras de etiska överväganden som gjordes vid planerandet och genomförandet av intervjuer.

3.1 Val av ansats

Den empiriska datan som framställs kommer till stor del att lägga grund för de diskussioner och resonemang som förs i diskussionsdelen av denna studie. Det är således av största betydelse att den genererade datan är väl anpassad för det undersökningen har som mål att komma fram till, nämligen utmaningar och hinder som finns vid implementering av säkerhetsramverk. Valet av forskningsmetod en viktig del i utformningen av en studie. Kvantitativ och kvalitativ forskning har båda olika egenskaper och anpassar sig därför åt olika undersökningar (Oates, 2022). I denna studie har kvalitativ forskning genomförts. En viktig del av denna undersökning var att erhålla data som grundar sig i människors upplevelser, erfarenheter och attityder kring området vi undersöker. För att svara på frågeställningen var det avgörande för oss att få ta del av personers åsikter och tolkningar samt att undersöka deras berättelser, tankar och känslor. Detta är information som lättast samlas in via kvalitativa forskningsmetoder, i detta fall via intervjuer (Oates, 2022). Ytterligare en anledning till att kvalitativ forskning var bäst anpassad för just denna studie är att den möjliggör för en mer flexibel och anpassningsbar datainsamling (Yin, 2013). Såväl säkerhetsramverk som utmaningarna man möter vid implementeringen av dem är komplexa ämnen. För att kunna genomföra studien på ett grundläggande och redogörande tillvägagångssätt var kvalitativ data därför av högsta essens.

3.2 Urval

För att få en nyanserad bild om ämnet fanns det under denna studie en eftersträvan om att fånga det bredaste spektrumet av synvinklar och information. Det finns olika nivåer av empirisk materialinsamling vid kvalitativ forskning, nämligen smalare datainsamling och bredare datainsamling (Yin, 2013). I denna studie studerades både enskilda respondenters tankar och attityder (smalare nivån) och hur deras företag opererade ute på marknaden (bredare nivån). Yin (2013) menar att om förhållandet mellan nivåerna tas i beaktande och fokus ligger på att förstå sambandet mellan dem så kan involveringen av den bredare och den smalare nivån ge en bättre bild om ämnet än om man bara förlitar sig på en nivå.

När det kom till att hitta möjliga respondenter så fanns det en del tillvägagångssätt enligt Yin (2013) men valet föll på att göra ett avsiktligt urval. Avsiktligt urval är det mest frekventa sättet att hitta intervjupersoner inom kvalitativ forskning och det betyder att det medvetet valdes ut vilka personer vi tog kontakt med. På så sätt kunde det i så hög mån som möjligt säkerställa att de var väl anpassade till syftet för undersökningen. Målsättningen med genomförandet av denna kvalitativa undersökning var att arbeta med de som ger den mest

användbara och relevanta data för studiens ämnesområde. Genom att göra ett avsiktligt urval kunde vi se till att de mest lämpliga personerna kontaktades (Yin, 2013).

Även om avsiktligt urval tillät oss att medvetet välja vilka eventuella intervjupersoner vi tog kontakt med så var det viktigt att intervjua de som vi anade hade olika synvinklar och åsikter om ämnet. Konkurrerande åsikter och attityder ger en mer nyanserad och icke-vinklad bild av ämnet vilket är till stor fördel enligt Yin (2013). För att undvika ett intryck av vinkling i studien var det därför viktigt att under datainsamlingsprocessen inte bara välja respondenter och källor som verifierar våra förutfattade meningar (Yin, 2013). För att få en allsidig och nyanserad bild av området valde vi därför att kontakta personer på olika delar av marknaden. Tre olika metoder användes vid sökandet efter deltagare.

Första metoden var att kontakta en lärare på Lunds universitet som utbildar inom informationssäkerhet. Då läraren inte ansåg säkerhetsramverk vara personens specialitet hänvisade hen oss vidare till en branschkollega med stor erfarenhet av IT-säkerhet och säkerhetsramverk, respondent 1.

Andra metoden var att kontakta närstående som jobbar inom IT branschen för att se om personerna hade kontakter som kunde vara intressanta att intervjua. Vi fick därigenom kontakt med flera personer som var villiga att ställa upp, varav vi valde att gå vidare med två, respondent 2 och 3.

Tredje metoden var att leta upp vetenskapliga artiklar på nätet för att kontakta skribenterna. En passande artikel hittades och vid kontaktandet med författaren så stod det klart att hen var villig att ställa upp på en intervju. Dessvärre dök personen aldrig upp trots 2 bokade intervjutillfällen. Tillslut beslutade vi oss för att inte gå vidare med respondenten då vi ansåg att den data vi samlat in var tillräcklig samt att det fanns en brist på tid.

Eftersom att IT-säkerhet kan vara ett känsligt ämne för många industrier och företag är denna studie inriktad på en bredare vy istället för en undersökning på ett specifikt företag. Detta gjorde att studien inte riskerar att skada företags säkerhet utan hjälper företag med implementeringen av säkerhetsramverk.

3.2.1 Urval av respondenter

Som tidigare nämnt valde vi att intervjua 3 personer som arbetar för olika organisationer inom IT-branschen. Samtliga respondenter har flera års erfarenhet inom IT-säkerhet och specialiserar sig på säkerhetsramverk. Respondenterna konsulterar åt företag och har således sett otaliga fall på implementering av säkerhetsramverk. Intervjuerna gav oss en djupare inblick i hur det är att implementera säkerhetsramverk samt vilka hinder och utmaningar företag tenderar att stöta på.

3.3 Litteratursökning

Vid insamling av teori användes Google Scholar samt LUBSearch för att hitta vetenskapliga artiklar. Kurslitteratur och annan litteratur har använts och lagt grunden för metoddelen. Dessa böcker fick vi tillgång till via Legimus. Vidare så användes Google för att definiera begrepp samt områden som används inom denna studie. Sökorden som användes var följande:

- Säkerhetsramverk
- Implementation
- NIST
- ISO/IEC 27001
- CIS
- IT-säkerhet
- Cybersäkerhet
- Cyberattack
- Utmaning
- Hinder
- Problem

Orden har använts i olika kombinationer samt med olika böjningar för att maximera antalet träffar. Orden har även använts på engelska i olika kombinationer.

Eftersom att flera sökningar resulterade i många träffar behövdes ett urval. Val av artiklar gjordes utefter vad som söktes efter, om artikeln nämnde områden vi letade efter, antalet citeringar och artikelns relevans. Årtalet på artiklarna hade stor betydelse då ämnet som tidigare nämnt blivit mer och mer relevant, vilket betyder att ny forskning gjorts inom området.

3.4 Datainsamling

Vilket tidigare beskrevs så föll valet på att samla in empiriska data via kvalitativ forskning i form av intervjuer. Genomförandet och planerandet av intervjuer kan skötas på olika sätt.

Vi genomförde semistrukturerade intervjuer för att underlätta flexibiliteten under intervjuerna. Detta gav oss möjligheten att ställa följdfrågor för att få en bättre förståelse för olika områden. Därutöver blev det även mer obehindrade dialoger, vilket bidrog till en tryggare och mer lättsam miljö för respondenterna (Almvide, u.d.).

Antalet genomförda intervjuer var tre. Valet att inte utföra fler intervjuer gjordes efter den sista intervjun då vi såg likheter och mönster gällande respondenternas tankar, upplevelser, åsikter och erfarenheter. Därför valde vi att påbörja sammanställningen av den data vi erhållit under intervjuerna istället för att fortsätta genomförandet av empirisk materialinsamling. Denna sammanställningen var sedan det som lade grunden för resultatet.

Den första intervjun pågick i 57 minuter, den andra i 45 minuter och den tredje i 40 minuter. Detta betyder en total intervjutid på 2 timmar och 22 minuter vilket var länge nog för att förse oss med den mängd empiriskt material som krävdes för att sammanställa ett gediget och trovärdigt resultat samt för att föra en omfattande och genomgripande diskussion.

3.4.1 Intervjuguide

Intervjuguiden för denna studie grundar sig i litteraturgenomgången samt frågeställningarna för denna studie. Guiden är uppdelad i fyra olika delar; Introduktion, Implementering av säkerhetsramverk, Arbete med säkerhetsramverk och val av säkerhetsramverk, och Övrigt. Detta upplägg gjorde att vi fick en introduktion om respondenten samt deras

kunskapsområden och erfarenheter för att sen bygga vidare till huvuddelen av intervjun. Huvuddelen av intervjuerna anses vara fas 2 och 3 i intervjuguiden.

Fas 2 och 3 skapades för att få respondenternas syn och erfarenheter angående säkerhetsramverk. Valet föll således på att ha öppna frågor då detta leder till att respondenterna kan styra intervjun i riktning till sin expertis (Alvehus, 2019).

En brainstorming av möjliga frågor gjorde att en första intervjuguide skapades. Därefter arbetades intervjuguiden ner till de frågor som ansågs vara relevanta för ämnet och frågeställningen som sedan resulterade i den använda intervjuguiden. Efter första intervjun konstaterades att frågorna fångade relevant data för att sedan kunna svara på studiens frågeställning.

Upplägget användes för samtliga intervjuer och ändrades inte mellan intervjuerna. En av intervjuerna gjordes på engelska då respondenten inte kunde flytande svenska. Samma intervjuguide användes vid intervjun dock genom en översättning till engelska. Intervjuguiden skickades till respondenterna innan intervjuerna för att respondenterna skulle ha möjligheten att förbereda sig om nödvändigt. En fördel med att ha en intervjuguide med förbestämda frågor är att jämförelsen mellan respondenternas svar lättare går att analysera (Oates, 2022).

Tabell 3.1: Intervjuguide

Tema	Frågor
Fas 1: *Introduktion*	● Vad har du för nuvarande position? ● Vad har du för utbildning/kunskap när det kommer till IT-säkerhet eller säkerhetsramverk? ● Vilka ramverk känner du till? ○ NIST Framework ○ CIS Controls ○ ISO 27000 ○ Har du något ramverk du gillar extra mycket och något du inte gillar? ● Har du varit med och implementerat ett eller flera ramverk tidigare? ○ Om ja, vad har du haft för uppgifter/roll?
Fas 2: *Implementering av säkerhetsramverk*	● Hur implementeras ramverk på ett företag generellt sätt? Från idé till färdig implementation. ● Hur mäter man om en implementering är lyckad? ● Vilka branscher använder sig vanligtvis av ramverk? ● Hur stor skillnad är/kan processen vara bland olika branscher? ○ Vilka stora delar är skillnaden? ● Vilken roll spelar organisationens kultur och ledarskap i implementeringen av ett säkerhetsramverk?

	● Hur påverkar regleringar och standarder som GDPR implementeringen av säkerhetsramverk? ● Vilka är de vanligaste hinder/utmaningar företag står inför när de implementerar ramverk? Varför? ● Är dessa hinder något som inte går att undvika? ● Hur lång tid ungefär tar det att implementera ett ramverk? ○ Skillnad på hög och låg mognadsgrad inom säkerhet? ● Vilka är några vanliga misstag som företag gör vid implementering av säkerhetsramverk? ○ Varför sker dessa misstagen?
Fas 3: *Arbete med säkerhetsramverk och val av säkerhetsramverk*	● Är det något man kontinuerligt behöver underhålla gällande ramverken? ○ Om ja, vad har företaget att göra? ● Använder företag ett ramverk eller brukar de kombinera flera? ○ Har du några preferenser? ● Vilka är några av de senaste trenderna inom säkerhetsramverk? ● Är det skillnad på små och stora företag när det kommer till ramverk? ○ Om ja, vad och varför? ● Vad är de viktigaste faktorerna att ta hänsyn till vid val av ett säkerhetsramverk för en organisation?
Fas 4: *Övrigt*	● Har du några övriga kommentarer eller något vi har missat?

3.5 Dataanalys

Vid analyserandet av den empiriska datan utgick från det tillvägagångssätt som Yin (2013) presenterar i sin bok *Kvalitativ forskning från start till mål.* Yin rekommenderar fem olika faser som utgångspunkt för analysering. De fem faserna är:

- Sammanställning
  Efter genomförandet av intervjuerna sammanställdes materialet till transkriberingar. Genom onlineverktyg transkriberades intervjufilerna till text för att sedan kontrolleras och delas upp. Transkriberingen har radnummer samt initialer på deltagarna i intervjun för att lättare kunna refereras i resultatet.

- Demontering
  Efter transkriberingen kommenterades texten via Google docs kommentarsfunktion för att hitta data som är relevant för studien. Efter att frågorna och svaren kommenterades

samlades svaren i olika listor med liknande ämne och område. Detta gjorde att en helhetsbild kunde skapas och mindre viktig data kunde uteslutas tillsvidare.

- Remontering
  Efter att alla intervjuer hade kommenterats och relevant data samlats i listor kunde en remontering göras. Detta gjordes genom att identifiera liknande tankar och åsikter hos de olika respondenterna samt olikheter i deras svar och sedan sammanställa detta i ett resultat.

- Tolkning
  Diskussionsdelen bygger på våra diskussioner och tolkningar av det remoterade materialet (Yin, 2013). Denna del av analysen handlar om att skapa ett större värde av det resultat vi framställt. Under denna fas var det viktigt att knyta det respondenterna sagt under intervjuerna till vår teori och val av problemområde (Alvehus, 2019).

- Slutsatser
  I slutsatsen besvarar vi de frågeställningar studien har genom att presentera vår slutgiltiga analys. Slutsatser är delen som avslutar analysdelen och med det även lägger slutpunkten för hela studien.

Genom att utgå från de faser som Yin presenterar har vi på ett strukturerat sätt kunnat genomföra analysdelen av vårt arbete, vilket innefattar allt från resultatet till slutsatsen (Yin, 2013).

3.6 Etiska överväganden

Forskningsetiska överväganden handlar om att hitta en rimlig balans mellan olika intressen, i detta fall våra intressen och respondenternas intressen (Oates, 2022). Vid kontaktandet av intervjupersoner tog vi hänsyn till etik och såg till att respondenternas intressen togs i beaktande. Innan genomförandet av intervjuerna var det viktigt att respondenterna hade möjlighet att avstå eller dra sig ur deltagande. Om en individ eller ett företag inte önskade att delta i forskningen så behövde de inte, oberoende av anledning. Detta gällde även om de tackat ja tidigare men av något skäl inte längre kunde eller ville delta. Vidare var det viktigt att de intervjuade i fråga fick tillräckligt med information om vad studien handlade om samt vilka frågor som vi planerade att ställa innan genomförandet av intervjuerna. Detta var dels fördelaktigt för oss eftersom vi kunde se till att respondenten hade möjlighet att komma förberedd till intervjun. Det var även en trygghet för respondenterna eftersom de fick en bild av hur intervjun var utformad vilket gav dem goda möjligheter till att förbereda sig (Oates, 2022).

Väl under intervjuerna valde vi att tidigt i den inledande fasen fråga om respondenterna önskade vara anonyma samt huruvida det var okej att spela in intervjun för att transkribera och sedan använda materialet i studien. Detta är ett tillvägagångssätt som Oates (2022) förespråkar.

Slutligen, under hela processen av intervjuerna var det en avgörande del att behandla personer med respekt. Detta inkluderade bland annat att vi inte skulle diskriminera någon, på grund av etnicitet, kön, religion m.m. (Stafström, 2017).

3.7 Studiens validitet och reliabilitet

Oates (2022) påpekar att validitet och reliabilitet är något som en skicklig forskare lägger stor vikt vid. Genomförandet av empirisk datainsamling gjordes på ett vis som medförde god validitet och reliabilitet för resultatet. Det är viktigt att vara införstådd med att reliabilitet och validitet inte är samma begrepp och används därför inte utbytbart. Reliabilitet avser huruvida forskningsresultatet är upprepningsbart. Det vill säga, om någon annan gör samma undersökning, kommer de då fram till samma resultat? Validitet, i sin tur, avser huruvida vi undersökte det vi hade som målsättning att undersöka (Alvehus, 2019).

För att försäkra att studien hade hög reliabilitet valde vi att grundligt intervjua tre personer från olika delar inom branschen. Intervjuernas genererade data analyserades och vi kunde se att åsikter, erfarenheter och attityder tenderade att delas mellan de olika intervjupersonerna. Detta var en indikation på att svaren vi fick i intervjuerna var generella inom branschen. Vilket i sin tur pekar på att undersökningen är upprepningsbar (Oates, 2022).

Vad gäller validitet så menar Oates (2022) att det finns två olika typer, intern validitet och extern validitet. Intern validitet avser i vilken utsträckning mätningarna som erhålls faktiskt undersöker det man vill undersöka. Här var det fördelaktigt för oss att ha semistrukturerade intervjuer med öppna frågor eftersom det gav dem en möjlighet att vinkla och ställa om frågor så att de var bättre ställda och undersökte rätt sak. Under intervjuerna omformulerade respondenterna några av våra frågeställningar för att frågan och svaret skulle kunna tolkas korrekt.

Studiens externa validitet avser generaliserbarheten av de resultat som vi kommer fram till (Oates, 2022). Genom att se till att urvalet av respondenter, men även intervjufrågorna, täckte ett brett spektrum av ämnesområdet kunde vi i stor mån säkerställa att resultatet vi presenterar inte är baserade på ovanliga åsikter och attityder.

4 Empiriskt resultat

Detta kapitel kommer att redovisa material från semistrukturerade intervjuer. En introduktion om vilka respondenterna är kommer att ge en förståelse för det resterande material som presenteras efter.

4.1 Presentation av respondenterna

Respondent 1 önskade att vi inte skulle använda hens namn samt namnet på hens nuvarande företag. Respondenten har studerat i Danmark på University of Copenhagen och har en examen i filosofi och datavetenskap (RES1, rad 8). Efter studierna började hen jobba med en teknisk inriktning som mjukvaruutvecklare, men sedan 8-10 år tillbaka jobbar respondenten med IT säkerhet. År 2019 började hen jobba på ett danskt företag som IT security coordinator (RES1, rad 2 & 8) där respondentens nuvarande uppgifter bland annat är att implementera säkerhetsramverk (RES1, rad 4).

Respondent 2 önskade att vi inte skulle använda hens namn samt namnet på hens nuvarande företag. Respondenten har studerat i Lund på Lunds Tekniska Högskola till dataingenjör. Hen har även certifikat inom AWS (Amazon Web Services) för deras plattform kring säkerhet samt ett certifikat på sitt nuvarande företag inom säkerhet (RES2, rad 4). Respondenten jobbar som Cloud Architect på sitt nuvarande företag, där hen erbjuder säkerhet till företagets kunder (RES2, rad 2).

Respondent 3 krävde inte anonymitet men för att vara konsekventa kommer vi att hänvisa till honom som respondent 3 i resultatet nedan. Han är certifierad ISO 27001 implementer. Han har även en CDPO certifiering vilket innefattar GDPR-ramverks implementation och underhåll (RES3, rad 4). Respondentens nuvarande position är produktägare för plattformen ServiceNow (RES3, rad 10). Ramverken han är mest familjär med är delvis CIS Controls med framförallt ISO (RES3, rad 6). Till skillnad från respondent 1 och 2 som drivit flera implementationer så påpekar respondent 3 att han levererar implementationer mer än att driva dem (RES3, rad 10).

4.2 Implementering av säkerhetsramverk

4.2.1 Inledningen av implementering

Vad gäller implementering av säkerhetsramverk så finns det alltid olika anledningar bakom varför det görs. Respondent 1 och respondent 3 påpekade i sina intervjuer att företag ofta implementerar säkerhetsramverk till följd av krav från kunder och leverantörer (RES1, rad 18; RES3, rad 12). Respondent 1 påpekade att enligt sina erfarenheter så upplevde hen att organisationer sällan blir tvingade till implementation till följd av cyberattacker eller andra incidenter (RES1, rad 18). Respondent 2 hade skilda åsikter, hen upplevde att den vanligaste implementeringsprocessen var att ett företag råkar ut för någon form av incident och inser då att man bör införskaffa sig något säkerhetsramverk för att minska framtida risker (RES2, rad 36). Vidare så förklarar hen i enlighet med respondent 1 och 3 att många företag även har

kundkrav och leverantörskrav som anledning för implementering (RES2, rad 16). Respondent 2 pratar även om hur företag som implementerar säkerhetsramverk som har tillhörande certifiering gynnas. Exempelvis ISO 27000 har en certifiering som ger tillförlitlighet och skapar förtroende hos företag (RES2, rad 16). Även respondent 3 beskriver att certifiering är något som gynnar företag, framförallt på större marknader (RES3, rad 64). Däremot påpekar han att certifiering inom säkerhetsramverk kan vara för kostsamt för små företag, och då syftar han inte på själva implementationskostnaden utan istället de eventuella kostnader som kommer av att inte klara av att efterleva sin certifiering. Företag måste kunna garantera den IT- och datasäkerheten som man säger att man upplever och detta är oftast en större utmaning för mindre företag (RES3, rad 24).

Under intervjun med respondent 1 nämner hen att beslutet att implementera ett säkerhetsramverk även kan vara ett strategiskt beslut utan några direkta krav eller andra anledningar som gör det essentiellt. Detta skulle till exempel kunna vara om ett företag vill ge sig ut på en ny marknad där det av någon anledning är en konkurrensfördel att vara reglerad av ett säkerhetsramverk. Även om respondent 1 påpekar att hen aldrig sett detta, menar hen att det är fullt tänkbart (RES1, rad 18). Respondent 3 påpekar även han hur företag skulle kunna implementera säkerhetsramverk bara för att det ses som en form av best-practice, särskilt om företaget arbetar med IT-säkerhet. Han menar att certifiering huvudsakligen sker på två vis. Antingen så strävar företag efter certifiering och då blir best-practices ett resultat av implementeringen, eller så är målet med implementering att arbeta med best-practices och då kanske man får certifiering på köpet (RES3, rad 24).

Respondent 2 förklarar att enligt hen är generellt sätt ISO 27000, CIS Controls och NIST vanliga vägar in i arbetet med säkerhetsramverk. Hen fortsätter med att säga att implementering självklart skiljer sig även av lika ramverk då företag har olika förutsättningar, men att säkerhetsramverk absolut kan vara första steget i säkerhets- och ramverksarbetet (RES2, rad 36). Även respondent 3 påpekar att ISO 27000 är en bra väg in i arbetet med säkerhetsramverk. Framförallt då det resulterar i att företag enkelt kan reglera sina processer istället för att behöva "[...] uppfinna hjulet på nytt [...]" (RES3, rad 46). Respondent 1 ger en annan syn på detta. Hen menar istället att bortsett från situationer där företag blöder och konstant läcker data så är inte säkerhetsramverk rätt väg in bland ramverk. Hen rekommenderar att företag först börjar använda organisatoriskt inriktat ramverk för att få koll på deras processer och på så sätt kan arbeta med kvalitativt. För detta föreslår hen ISO 9000 som behandlar kvalitetsledning för att på så sätt bygga en grund. En grund som senare gör det lättare för företaget att implementera ISO 27000 vid behov (RES1, rad 20, 46 & 49). Detta instämmer delvis även respondent 3 om då han uttrycker att tidigare arbete med ramverk samt en förkänsla för reglerade och dokumenterade processer är hjälpsamt vid implementering av säkerhetsramverk (RES3, rad 44).

Ytterligare en sak som undersöktes i intervjuerna var huruvida olika branscher skiljer sig i implementeringen och användandet av säkerhetsramverk. Respondent 1 gör anspråk för att det inte finns någon direkt och konkret skillnad mellan branscher i sig utan det är isåfall handlar om skillnader mellan producerande företag och icke-producerande företag. Företag som producerar saker möts ofta av tekniska svårigheter vid implementering då de tenderar att ha gammal hårdvara och mjukvara. Onlineföretag kommer således alltid att ha lite lättare med implementering av säkerhetsramverk menar respondent 1 (RES1, rad 30). Respondent 2 förklarar att hen arbetar mest inom tillverkningsindustrin och kan därför inte uttala sig om några konkreta skillnader som hen upplevt gentemot tjänsteindustrin. Däremot berättar hen att det kan skilja branscher emellan gällande vilka krav som ställs. Inom hälsoindustrin nämner

hen att det finns väldigt många säkerhetsramverk eftersom de måste efterleva de krav som ställs på dem. Då är det ingen fråga om huruvida det gynnar verksamheten utan där är det allra oftast ett måste att implementera säkerhetsramverk (RES2, 20). Även respondent 3 nämner att företag ibland inte har något annat val än att implementera säkerhetsramverk. Då spelar den organisatoriska nyttan mindre roll och fokus ligger istället på att uppfylla hela certifieringar (RES3, rad 50).

Gällande skillnaden mellan branscher så beskriver respondent 3 att det snarare skiljer sig mellan marknader och dess storlekar. Företag som agerar på större marknader har mer att tjäna på att implementera säkerhetsramverk eftersom det generellt sett ställs högre säkerhetskrav på dessa företag. Större marknader är mer reglerade och IT-säkerhet hos partners kontrolleras i högre mån (RES3, rad 64 & 20). Respondent 3 menar därför att det är fördelaktigt för företag på dessa marknader att kunna hänvisa till särskilda ramverk och säga att de följer dem, alternativt att de är certifierade inom dem (RES3, rad 64).

Såväl respondent 1 som respondent 2 upplever att företag i regel använder ett säkerhetsramverk (RES1, rad 55; RES2, rad 52). Respondent 1 menar att det vanligaste är att företag belägna i USA tenderar att använda sig av NIST medan företag i Europa ofta använder och utgår från ISO standarderna (RES1, rad 55). Trots att både respondent 1 och 2 uttrycker att företag ofta väljer ett säkerhetsramverk så händer det att ramverk slås ihop. Respondent 1 arbetade tidigare på ett företag som hade två stora kunder, där en låg i USA och använde NIST och den andra låg i Europa och utgick från ISO. Företaget hen arbetade på skapade därför ett eget säkerhetsramverk där alla kontroller kunde mappas till ISO och NIST. Det visade sig vara en fördelaktig lösning för såväl företaget som för kunderna eftersom de slapp välja mellan de olika ramverken (RES1, rad 57).

Även respondent 2 berättar att kombinationer av säkerhetsramverk är möjliga. Hen beskriver att för stora företag som utgår från ISO skulle det kunna vara gynnsamt att även implementera ytterligare ett säkerhetsramverk som erbjuder ett mer praktiskt och hands-on fokuserat tillvägagångssätt, exempelvis CIS controls. Detta är dock inget hen har erfarenhet av själv men ser det som en eventuell lösning vid kombinering av flera säkerhetsramverk (RES2, 52).

Respondent 3 har en annan syn på kombinationer av säkerhetsramverk än vad de andra två respondenterna har. Han menar att företag nästan alltid implementerar flera säkerhetsramverk (RES3, rad 62). Enligt hans erfarenheter och upplevelser tenderar företag att implementera samma säkerhetsramverk som deras kunder och partners har. På så sätt kan man erhålla samma certifieringar och skapa vad respondent 3 kallar certifieringskedjor. Om kunder och partners har olika säkerhetsramverk och certifieringar kan detta alltså resultera i att företaget får implementera flera ramverk (RES3, rad 62; RES3, rad 12).

4.2.2 Arbetet efter implementering

Mätningen av hur lyckad en implementering är säger respondent 1 är svårt. Företag som har många cyberattacker i månaden kan mäta antalet attacker före och efter implementationen och på så sätt få fram resultatet. Men att mäta antalet cyberattacker före och efter implementeringen för att se hur implementeringen gick är i regel inte en bra idé (RES1, rad 28). Istället tycker hen att man bör göra riskanalyser före och efter implementeringen (RES1, rad 28). Respondent 2 tycker å andra sidan att en riskanalys före och efter implementeringen endast visar vad företaget tror om sitt system (RES2, rad 20). Hen nämner att en mätning av antalet uppfyllda punkter, i till exempel CIS, före och efter implementeringen är något som

visar hur resultatet blev på ett mer konkret vis (RES2, rad 18). Ett annat sätt att mäta hur lyckad implementeringen blev är genom att göra olika tester, som att skicka ut fejkade fishing epost och se hur många som blir träffade (RES2, rad 18). Respondent 3 är inne på liknande spår som respondent 2 vad gäller att mäta lyckad implementering genom att se hur man uppfyllt de punkter och krav man ställt (RES3, rad 18). Han menar att man innan implementeringen sätter upp ett kvalitetsmål, alltså vad man vill uppnå och vad det får kosta. Överstiger sen nyttan och värdet av den förbättrade IT-säkerheten kostnaden för implementationen så har säkerhetsramverket gett kvalitet och implementeringen ses som lyckad (RES3, rad 18 & 20).

För företag som redan arbetar ISO 9000 kommer inte att ha några större problem att arbeta med ISO 27000. Överlag så kommer företag som är vana att arbeta med ramverk och kvalitet ha större chans att lyckas i arbetet med ett säkerhetsramverk (RES1, rad 22). Respondent 2 säger, till skillnad från respondent 1, att företag inte behöver ha någon tidigare erfarenhet av andra ramverk innan man börjar arbeta med säkerhetsramverk. Hen påstår istället att exempelvis ISO 27000 och CIS Controls är vanliga vägar in i arbetet med säkerhetsramverk (RES2, rad 36).

Att följa upp och arbeta kontinuerligt med säkerhetsramverken är något som samtliga respondenter berättar är avgörande (RES1, rad 49, 51 & 53; RES2, rad 50; RES3, rad 58). Att inte följa upp ramverken kommer enligt respondent 1 resultera i att de inte är till någon nytta alls (RES1, rad 49).

Man måste alltså ha någon insatt person eller avdelning som ansvarar för ramverket. Det är otroligt mycket regleringar och krav att hålla koll på (RES3, rad 58). Respondent 3 menar att det ofta är konsulter som har hand om själva implementeringen av säkerhetsramverket men sen anställda som ansvarar för det. Dock finns det företag som är väldigt sourcade och då är det kanske mer lämpligt att ta hjälp av konsulter (RES3, rad 60). Respondent 2 påpekar likt respondent 3 att man behöver ha någon ansvarig för det. Huruvida det är en anställd eller konsult lägger hen å andra sidan inte så stor vikt vid. Däremot påpekar hen att de som bär ansvar för arbetet med säkerhetsremverket måste vara långsiktiga och ha god inblick i företaget och dess utveckling över tid (RES2, rad 60). Denna uppfattning delar även respondent 1 (RES1, rad 53).

Respondent 1 pratar om att företags mognadsnivå är en viktig del för att implementera ett säkerhetsramverk effektivt (RES1, rad 22). Allt är möjligt om ledningen i företaget hjälper till och vill göra en förändring (RES1, rad 34). Även respondent 2 och 3 benämner att ledningen har en avgörande betydelse när det kommer till en lyckad implementering av ett säkerhetsramverk (RES2, rad 16, 26, 38 & 46; RES3, rad 14, 32 & 34).

Företag som strävar efter att ha perfekt säkerhet eller implementera 100% av ett säkerhetsramverk har det svårare att lyckas med implementeringen (RES1, rad 24 & 26). Företag kommer inte komma upp i en 100% implementation av ett säkerhetsramverk på kort tid och troligtvis inte heller över en längre tid (RES2, rad 14). Respondent 2 menar även att företag som sätter en lägre ribba men uppfyller alla kraven kan ha bättre säkerhet än företag som försöker uppfylla alla kraven (RES2, rad 62). Vidare säger hen att mindre förändringar av processer kommer att gå snabbt att förändra med större, mer komplexa processer tar längre tid (RES2, rad 42). Respondent 3 berättar även han hur den organisatoriska kulturen spelar stor roll för arbetet med säkerhetsramverk. Om ett företag anser ökad IT-säkerhet vara viktigt för sin egen skull så kommer de troligtvis lägga ner större vikt vid implementeringen och

arbetandet med säkerhetsramverket än om de endast införskaffar ramverket för kunders och partners skull (RES3, rad 32 & 34).

4.2.3 Hinder och utmaningar under implementeringsprocessen

När det kommer till hinder och utmaningar vid implementering av ett säkerhetsramverk nämner respondent 1 att ett möjligt hinder är att ledningen inte är fullt medvetna om vad som behövs samt att de planerar kortsiktigt (RES1, rad 16 & 32). Detta är även något som respondent 2 pratar om. Hen tycker att det är väldigt avgörande när det kommer till implementeringen att ledningen i ett företag driver på. Att ledningen inte är aktiva och engagerade i processen kan leda till att budgeten inte räcker till (RES2, rad 26, 28 & 38). Något respondent 3 också nämner är att strukturen för implementeringen av ett säkerhetsramverk är av stor betydelse, detta då chefen eller ledningen inom ett företag kan förändras tillsammans med att målet och budgeten också förändras (RES3, rad 42).

Lång tid och många timmar krävs vid implementering samt att ta hjälp av konsulter är också något som företag inte alltid vill göra men det är något som kan krävas (RES1, rad 16). Respondent 2 berättar att mindre och enklare processer är lättare att förändra vid implementeringen av ett säkerhetsramverk medan större mer komplexa processer inom företaget tar tid och är svårare att förändra. Vilket är något som företag inte alltid förväntar sig (RES2, 42 & 48).

För företag som producerar saker är det en risk att ett hinder blir deras gamla system och processer. Medan företag som inte producerar något oftast inte har dessa utmaningar. Vidare nämner hen att företag inom hälsoindustrin oftast har mycket striktare regler vilket gör att det både tar längre tid och kan vara svårare att implementera ett ramverk (RES1, rad 30). Respondent 3 nämner att till exempel ISO standarderna har olika säkerhetsramverk beroende på vilken bransch företaget är aktivt inom, ISO 27005 och ISO 27007 är säkerhetsramverk som har fokus på samma område men för olika industrier (RES3, rad 26 & 30).

För företag med anställda som ”[…] comes to work and does what they want” (RES1, rad 32), är det omöjligt att implementera ett säkerhetsramverk. Hen nämner också att det bara går att implementera ett säkerhetsramverk om det redan finns ett kvalitetsramverk för processerna (RES1, rad 32). Människor gillar inte förändring, change management behöver finnas innan företaget implementerar någon form av ramverk (RES1, rad 42). Säkerhetsramverk gör ofta att de anställdas arbetsuppgifter blir påverkade och ibland till och med förändras. Detta är en utmaning som företag av alla storlekar påverkas av (RES2, rad 32 & 34). Respondent 3 nämner också att det är en utmaning att upprätthålla bemyndigandet genom hela implementeringsprojektet, det tappar tyngd genom tiden och fler vill hitta egna vägar för att minimera sin egen administration över tid (RES3, rad 14). Vidare säger respondent 2 att små företag har lättare att implementera ett säkerhetsramverk då det är färre anställda som behöver vara med på banan, än på större företag. Nivån på till exempel ISO är, i de fallen hen har varit med om, mycket bättre hos mindre företag jämfört med större (RES2, rad 58). Även respondent 3 påpekar att det är lättare för mindre företag att få en homogen implementation där nivån på implementationen är lika bra eller dålig. Detta är något större företag inte har lika lätt för då det kan bli större skillnader på nivån av implementationen (RES3, rad 66).

GDPR är något som ibland gör det svårt för företag att utföra sina processer vilket i sin tur leder till att implementeringen påverkas (RES1, rad 38). Detta är även något respondent 2 upplever, företag som har hand om mycket data påverkas mycket av GDPR då de behöver

hantera sin data väldigt mycket annorlunda (RES2, rad 30). Något respondent 3 nämner är att det går att ha IT säkerhet utan att ha datasäkerhet men det går inte att ha datasäkerhet utan IT säkerhet (RES3, rad 36, 38 & 40).

Något samtliga respondenter säger är att det finns en risk att företag strävar efter 100% av kraven när det kommer till säkerhetsramverk. Alla menar att detta är något som är näst intill omöjligt och inte bör göras (RES1, rad 26; RES2, rad 14; RES3, rad 16). Respondent 3 säger att detta kan leda till att företag glömmer bort varför de faktiskt implementerar säkerhetsramverk från första början, målet blir någon typ av certifiering eller delcertifiering (RES3, rad 16).

Slutligen nämner respondent 1 att det är en stor utmaning för företag med få eller inga processer att applicera ett säkerhetsramverk på. Medan företag med processer av kvalitet har det mycket enklare att implementera någon form av kontroll eller ramverk (RES1, rad 42 & 46). Även respondent 3 pratar om vikten av att ha arbetat med reglerade och dokumenterade processer före implementering av ett säkerhetsramverk. Han menar att arbetet med ett säkerhetsramverk för första gången är en inlärningsprocess och en utmaning kan vara ägandeskap i olika typer av processer, tjänster och produkter. Alltså om exempelvis produktägare, tjänsteägare, verktygsägare och processägare ska anpassa sig till nya säkerhetskrav, organisationssätt och tankegångar (RES3, rad 44).

5 Diskussion

I detta kapitel diskuteras studiens empiriska resultat i relation till litteraturen som tidigare presenterats. Syftet är att analysera och diskutera de utmaningar vi funnit från respondenterna i jämförelse med Dimensional Research (2016) som presenterar utmaningar företag mötte vid den tiden. Detta för att se hur utmaningarna har utvecklats under de senare åren samt jämföra och stödja det empiriska resultatet i denna studie.

5.1 Implementering av säkerhetsramverk

Enligt denna studiens empiriska material är det klart att saker skiljer sig i hur implementering av säkerhetsramverk sker idag jämfört med hur det såg ut då Dimensional Research gjorde sin undersökning år 2016. Något som däremot ser liknande ut är vilka säkerhetsramverk som är vanligast. Studien av Dimensional Research (2016) fann att PCI DSS var det mest frekvent använda säkerhetsramverket följt av ISO 27000, NIST och CIS Controls. Detta var även vad vårt empiriska resultat visade. PCI DSS undersöktes inte i denna studie då det är ett mer specialiserat ramverk som riktar sig åt betalningstjänster.

Gällande motiveringar till varför företag väljer att implementera säkerhetsramverk så visar det empiriska resultatet på några orsaker som är vanligast. Enligt framförallt respondent 1 och 3 är den allra mest förekommande orsaken till implementering är krav från kunder, leverantörer och partners. Respondent 2 anser krav från intressenter är en väldigt vanlig orsak men påpekar att enligt hens upplevelser och erfarenheter är implementering av säkerhetsramverk vanligast till följd av någon cyberincident. Detta står i kontrast till den orsak som Dimensional Research (2016) fann vara vanligast, nämligen att företag implementerar säkerhetsramverk för att det anses vara best-practice. Detta är något som respondenterna i vår studie knappt berör vilket tyder på att detta har blivit en mindre frekvent anledning till implementering. Respondent 1 nämner att företag skulle kunna tänkas implementera säkerhetsramverk i förebyggande syfte för att det anses som best-practice men detta är något som hen aldrig har sett. Istället berättar samtliga respondenter att säkerhetsramverk är något man allt som oftast blir tvingad till att implementera. Att bara implementera det för att uppnå bättre IT-säkerhet eller någon certifiering är generellt sett för dyrt, menar vårt empiriska resultat.

Andra motiveringar till varför företag valde att implementera säkerhetsramverk år 2016 var för att efterleva regleringskrav, för att det krävs enligt kontrakt och för att förbättra den interna och externa kommunikationen (Dimensional Research, 2016). Samtliga av dessa anledningar är något som även denna studiens respondenter nämner som frekvent förekommande.

Vad gäller skillnader i hur implementering sker mellan branscher och på företag av olika storlek så är samtliga respondenter överens om att det knappt finns någon skillnad. Däremot menar respondent 1 att implementering skiljer sig mycket mellan tillverkande och icke-tillverkande företag. Tillverkande företag tenderar att ha äldre system vilket kan försvåra implementeringen av säkerhetsramverk. Icke-producerande företag har oftast system som är mer up-to-date och kommer således alltid att ha lättare med implementering menar respondent 1. Respondent 3 berättar även att det kan finnas skillnad i hur implementering sker beroende

på storleken hos företag, något som framförallt inte respondent 1 instämmer med. Respondent 3 menar att mindre företag måste vara mer försiktiga i hur mycket de implementerar och vilka certifieringar de erhåller. Detta eftersom de måste kunna leva upp till de certifieringar säkerhetsnivåer de påstår sig ha. Om företag inte klarar av att bibehålla de skydd de implementerat så kan kostnaderna bli väldigt stora. Något som respondent 3 menar att mindre företag inte har råd med. Även Respondent 2 påstår det finnas viss skillnad mellan små och stora företag vid implementering av säkerhetsramverk. Hen menar att mindre företag har lättare för att få en homogen implementering då de har färre anställda att få med på banan.

Något som alla respondenter dock tycker skiljer sig mellan branscher är varför företag implementerar säkerhetsramverk. Samtliga berättar att kraven på IT- och datasäkerhet kan se helt olika ut mellan branscher. Inom exempelvis hälso- och sjukvården menar respondenterna att det finns väldigt många säkerhetsramverk eftersom de måste efterleva de krav som ställs på dem. De är alltså tvingade att implementera och förhålla sig till säkerhetsramverk. Respondent 3 berättar även att det kan finnas skillnader i varför företag implementerar säkerhetsramverk beroende på storleken av marknaden de befinner sig på. Företag som är verksamma på större marknader har enligt respondent 3 större nytta av säkerhetsramverk eftersom det generellt sett ställs högre säkerhetskrav på dessa företag. Större marknader är mer reglerade och IT-säkerhet hos partners kontrolleras i högre mån.

5.2 Faktorer för en lyckad implementering

Något som samtliga respondenter nämner som avgörande för en lyckad implementation av säkerhetsramverk är arbetet efter implementering. Mätningen av “lyckad” implementering menar respondenterna främst görs genom att granska antalet efterlevda säkerhetsområden och punkter inom ramverket före och efter implementation. Respondent 2 berättar även att man kan utföra olika tester. Till exempel kan man skicka ut fejkade fishing e-post och se hur många som blir träffade efter implementeringen jämfört med hur det var innan.

Vid implementeringen av säkerhetsramverk är det av högsta betydelse att se det som en kontinuerlig process och inte som ett engångsprojekt. Vilket betyder att när ett företag har implementerat ett ramverk så behövs det även underhåll och ses över för att bidra med ökad säkerhet. Samtliga respondenter nämner att en implementering tar flera år och detta är något som framförallt ledning på företag måste vara införstådda med för att man ska lyckas. Cohen (2022) beskriver “checkbox mentalitet" som en vanlig fallgrop vid implementering av säkerhetsramverk. Detta är något som det empiriska materialet i denna studie också benämner. Respondenterna påpekar att det mest fördelaktiga är att primärt arbeta för att förbättra ens IT-säkerhet och processer och sekundärt försöka uppnå certifiering eller krav. Fokuserar man främst på efterlevnaden av minimikrav leder det ofta till mindre lyckad implementering. Respondent 2 beskriver även att företag som strävar efter en fullständig implementering av ett säkerhetsramverk kommer ha svårare att uppfylla hög kvalitet. Hen menar att företag bör lägga en lägre ribba och fokusera på mindre delar åt gången. Detta kommer resultera i mer kvalitativ IT-säkerhet under det långa loppet.

Att arbetet efter implementering är viktigt påpekar även Dimensional Research (2016). Deras studie konstaterade att företag tenderar att först se positiva effekter ett bra tag efter utförd implementering. Av deras 319 respondenter hade endast omkring hälften börjat se förbättringar inom olika IT-säkerhetsaspekter. Vidare visade resultatet en tydlig korrelation mellan tiden efter implementering och upplevda fördelar. Ju längre ett företag var komna i sin

implementering desto fler och tydligare blev fördelarna. Detta tyder på att deras studie, likt vår, fastställde att arbetet efter implementering är avgörande.

Denna studiens empiriska resultat framhäver ett antal aspekter som kan underlätta arbetet med implementering. Respondent 1 menar att företag som tidigare implementerat kvalitetsramverk, exempelvis ISO 9000, inte kommer att ha några större problem att implementera ISO 27000 eftersom det kräver liknande processtänk. Respondent 2 och 3 påstår däremot att företag inte behöver ha något annat ramverk innan man implementerar säkerhetsramverk utan att säkerhetsramverk som ISO 27000, CIS Controls och NIST är bra som första säkerhetsramverk eftersom de är enkla att förstå. Trots dess relativt enkla utformning menar dock samtliga respondenter att företag behöver ha någon ansvarig för säkerhetsramverken.

Slutligen är ledningsstöd en essentiell faktor för framgången av ett säkerhetsramverk. Läggs det ingen vikt vid arbetet med ramverket och processer så kommer implementeringen ha svårt att lyckas. Samtliga respondenter betonar vikten av att företag har rätt mognadsnivå och pådrivande ledning för att implementera ett säkerhetsramverk effektivt. En förändring är endast möjlig om ledningen i företaget hjälper till och vill göra en förändring. Studien av Dimensional Research (2016) visade också att om ledningen är involverad i implementeringen och arbetet med säkerhetsramverk kan de få säkerhetsberedskap presenterat för sig på ett lättare och mer effektivt sätt. En annan positiv effekt av arbetet med säkerhetsramverk som deras studie hittade var att företags mognad samt effektivitet av processer ökade. De fann även att säkerhetsramverk underlättade efterlevnaden av avtalsförpliktelser och medförde en mer mätbar IT-säkerhet (Dimensional Research, 2016). Detta var samma positiva effekter som respondenterna i denna studie nämnde.

5.3 Hinder och utmaningar under implementeringsprocessen

Implementering av ett säkerhetsramverk medför enligt Dimensional Research (2016) ofta utmaningar för företag av olika storlekar och inom olika branscher. I sin undersökning identifierade de att 95% av alla företag som implementerar säkerhetsramverk möter motgångar under processen. Även respondenterna i denna undersökning påpekar flera hinder och utmaningar som kan uppstå vid implementering av ett säkerhetsramverk. En av de största utmaningarna är bristen på medvetenhet och engagemang från ledning. Om ledningen inte förstår vad som krävs eller planerar kortsiktigt kan detta påverka budgeten negativt och göra det svårare att genomföra implementeringen. Respondent 3 nämner även att strukturen av implementeringen har en stor betydelse då chefen eller ledningen inom ett företag kan ändras med tiden vilket kan leda till att målet och budgeten förändras. Litteraturen delar upp utmaningarna i två kategorier; organisatoriska och teknologiska. En av de organisatoriska utmaningarna var, precis som respondenterna nämnde, att det kan finnas ett bristande stöd från ledningen (Dimensional Research, 2016).

Denna utmaning påverkar i sin tur andra potentiella organisatoriska utmaningar såsom avsaknaden av utbildad personal, budget samt prioriteringar (Dimensional Research, 2016). Detta är även något det empiriska resultatet visar på. Företag kan behöva ta hjälp av konsulter, vilket kan vara dyrt och något som inte alla företag är intresserade av att göra. Dessutom nämner respondent 1 att större och mer komplexa processer kan ta längre tid att förändra än mindre och enklare processer. Detta kan överraska företag som inte förväntar sig denna typ av utmaning.

Företag inom vissa branscher, som hälsoindustrin, kan också ha svårare att implementera säkerhetsramverk till följd av strikta regleringar och krav. Däremot nämner respondent 3 att ISO standarden har olika säkerhetsramverk med olika inriktningar vilket gör det anpassningsbart för olika situationer. Exempel på dessa är ISO 27005 och ISO 27007. Det är också en fördel för företag att ha ett kvalitetsramverk på plats innan de implementerar ett säkerhetsramverk. Arbetet med change management är en faktor som ger en positiv påverkan eftersom människor ofta ogillar förändringar och implementeringen kan påverka de anställdas arbetsuppgifter. Dimensional Research (2016) identifierade liknande utmaningar då två teknologiska hinder var bristfällande integrering av verktyg samt dålig rapportering.

GDPR kan också vara en utmaning för företag som hanterar mycket data, eftersom det kan påverka hur processerna utförs och kräva att företaget hanterar data på ett annat sätt än tidigare. Respondent 3 nämner att det går att ha IT säkerhet utan någon datasäkerhet men det är omöjligt att ha datasäkerhet utan att ha IT säkerhet. Med detta menar respondenten att om ett företag ska veta vilken data som finns, var och vad den består av, vem som äger den och vem som har ansvaret så måste företaget ha ett säkerhetsramverk. Detta i sin tur betyder inte att om man har ett säkerhetsramverk att man för det har koll på var data är lagrad och varför är den inhämtad samt vad den ska användas för. Det kan vara säkert ändå. Datorn vet inte om det är persondata eller finansdata eller för den delen orderdata.

En annan utmaning är att många företag strävar efter att uppfylla 100% av kraven för ett säkerhetsramverk, vilket kan vara omöjligt och inte bör vara ett mål. Att uppfylla en mindre andel krav i ett ramverk perfekt kan ge en bättre säkerhet än att försöka uppfylla alla ramverkets krav mindre bra.

Slutligen kan företag utan processer ha svårt att applicera ett säkerhetsramverk, medan företag med processer av hög kvalitet kan ha lättare att implementera kontroller och ramverk. Respondenterna i undersökningen påpekar flera utmaningar vid implementering av säkerhetsramverk, men det är viktigt att företag förstår dessa utmaningar och arbetar aktivt för att övervinna dem för att säkerställa en hög nivå av säkerhet för verksamheten. Det empiriska resultatet i denna studie har som tidigare nämnt många gemensamma hinder och utmaningar. Ett hinder som respondenterna upprepade gånger har nämnt som det största hindret vid implementering är ledningens inställning. Dimensional Research (2016) konstaterade, likt denna studie, att ledningen har ett stort inflytande över hur lyckad implementeringen blir.

6 Slutsatser

Studiens huvudsakliga syfte är att identifiera generella och upprepade hinder och utmaningar företag möter vid implementeringen av säkerhetsramverk. För att uppnå detta syfte kommer studiens frågor att besvaras nedan.

Hur implementeras säkerhetsramverk inom företag?

Det empiriska resultatet i denna studie visar att implementeringen av säkerhetsramverk har förändrats sedan 2016, även om mycket ser liknande ut. De undersökta ramverken ISO 27000, NIST och CIS Controls förblir några av de vanligaste säkerhetsramverken. Majoriteten av respondenterna anser dessa ramverk vara en naturlig och okomplicerad väg in i arbetet med säkerhetsramverk och kvalitativa processer. En respondent påpekar dock att det underlättar implementeringen om företag arbetar med kvalitetsramverk sedan tidigare.

Företag implementerar vanligtvis dessa ramverk på grund av krav från kunder, leverantörer och partners eller som ett svar på en cyberrelaterad incident. Best-practice är inte längre det primära skälet till implementering. Däremot benämner en av respondenterna att implementering skulle kunna göras i förebyggande syfte. Något som isåfall talar för best-practice som motivering.

Det är en liten skillnad i hur implementering sker mellan branscher och företagsstorlekar. Tillverkande företag kan möta ytterligare utmaningar till följd av äldre och mindre uppdaterade system. Vidare kan branscher med stränga regleringar och krav, till exempel hälsoindustrin, behöva större noggrannhet vid implementering och är ofta tvingade att arbeta med säkerhetsramverk. Vad gäller skillnaden mellan företagsstorlekar beskrivs det att små företag måste vara försiktiga med mängden implementerade kontroller som görs och certifieringarna de uppnår. Detta eftersom de kan misslyckas med underhållandet av dem, vilket kan leda till stora kostnader.

Beslutet att implementera ett säkerhetsramverk kommer, nästan alltid, från ledningen i ett företag. Ledningen har ett stort inflytande över varför, vilket, när samt hur ett ramverk ska implementeras. För att öka chansen till en lyckad implementering är det en viktig faktor att företaget har en hög kompetens och mognadsnivå, samt att ledningen stöttar processen. Vidare så är det viktigt att se implementationen av säkerhetsramverk som en process snarare än ett engångsprojekt. Något som respondenterna anser vara fördelaktigt är att implementera delar av säkerhetsramverk åt gången. Det kan resultera i högre kvalitet och mer lyckad implementering.

Vilka hinder och utmaningar möter företagen vid implementering av säkerhetsramverk?

Hinderna och utmaningarna som funnits i denna studie har likheter samt olikheter med tidigare gjorda studier. Vilket betyder att förändringar genom tider har skett men att en del utmaningar har bestått.

Den största och mest upprepade utmaningen vid implementering av säkerhetsramverk är ledningens engagemang och fokus. Företag med en ledning som inte är engagerad av implementeringen kommer att uppleva det svårare att lyckas med processen. Vidare har ledningen makten att ändra budgeten samt resurserna för en implementering. Detta är två

relaterade faktorer som påverkar implementeringen av ett säkerhetsramverk. Det kan leda till att implementeringsprocessen fallerar och att företag inte når de mål som satts upp i början av projektet. Ledningen har även ett stort inflytande i hur de anställda ställer sig inför en förändring. Saknaden av change management ökar risken att de anställda går tillbaka till de gamla rutinerna med tiden och inte utför processerna enligt ramverkets krav.

Slutligen, underhållandet av ramverket efter implementeringen har en stor betydelse för hur ramverket kommer att hjälpa med att förbättra säkerheten. Företag som ser implementeringen som en "fit-and-forget" eller att de endast vill se attraktiva ut för intressenter kommer att uppleva att säkerhetsramverket inte bidrar med den potentiella säkerheten.

6.1 Vidare forskning

Som tidigare nämnt finns det ett begränsat antal vetenskapliga artiklar som forskar kring generella hinder och utmaningar vid implementering av säkerhetsramverk. Därför anser vi att mer forskning behövs för att säkerställa vårt resultat och slutsatser. I denna studie intervjuades tre personer med bakgrund inom IT säkerhet vilket gav oss en grund att stå på samt information som bidrog till att frågeställningarna kunde besvaras på. Däremot skulle fler intervjuer med personer eller företag från olika sidor av implementeringen möjliggöra en bredare analys om ämnet.

Slutligen kan forskning som studerar hur företag kan kringgå nämnda hinder och utmaningar i denna studie bidra till att företag i framtiden minskar risken att misslyckas med implementeringen av säkerhetsramverk.

Appendix

Appendix A - Transkription intervju 1

Medverkande personer:

Peter Herslow (PH)

Måns Herlöfsson (MH)

Respondent 1 (RES1)

Datum och tid: 2023-04-21 14:00 - 14:57

#	**Person**	**Fråga/Svar**
1.	PH	First question then, what is your current position?
2.	RES1	My current position is right now it's called IT security Coordinator, so that’s the current title that I have.
3.	PH	Okay and what's your ehh responsibilities on a daily, daily work?
4.	RES1	I'm security specialist and I'm primary responsible for incident management, implementing security framework controls, doing risk analysis and so on. You might imagine a season for one factory or something like that. So it's on that level, like being a season, but but not for an organization but for an isolated factory.
5.	PH	OK.
6.	RES1	Full stack, more or less.
7.	PH	OK, what education or knowledge do you have when it comes to IT security and security frameworks?
8.	RES1	Have many many years of experience. I’ve worked as a software programmer with in cryptographics and security for many many years. Embedded Linux being a software architect. But then I moved into security. I don’t know, 8-10 years ago. Well, my first position was security whatever was that called? Security System engineer I think handling system engineering. Very good NIST standards for system engineering as well. I can recommend those if you’re bored one day. And and so I sort of started that way as a programmer of the very heavy technical background. And before that, of course I have some formal education and then I have had several security positions after that. You’re welcome to find me on LinkedIn if you’re curious. I have my CV there. Then I had another security position and another security position. And then four years ago I was hired in XXX, and

		I'm very happy to be here today. Academically, I've started at the University of Copenhagen back in the days. I actually have a bachelor's degree in philosophy, and I've started computer science as well on University of Copenhagen. So that's sort of the background. Formally I have, but then of course I've extended tons of classes and courses and some vacations and shit. But but my formal, my formal education is a PA from the University of Copenhagen and Philosophy and Computer Science. My final I did my thesis on open software and hacker ethics just for your information. But that was actually that was handed in on and the faculty of philosophy. But with the computer science angle, there was a little bit out-of-the-box.
9.	PH	Okay, okay okay. So which security framework are you familiar with?
10.	RES1	Yeah, quite a lot. You mentioned NIST. I know the NIST standards. I worked a lot with them. I had previous experience in the, what is it called, Airplane industries in the aero aeronautics and in that area and the new standards especially with with American customers that is sort of golden framework. And I also work with European producer of airplanes, a large European producer of airplane airplanes and they preferred the ISO standards. So I have worked with those, but here in XXX we're using mostly corporate internal standards. But in my experience we you can can map most of the standards. In one of my previous positions we we worked with a couple of proprietary closed standards. I kind of reveal the names of them but with some frameworks that were proprietary and the confidential of course. But we were able to map all the controls to ISIS standards and new standards. So that in my experience that is possible for many standards, but I work with several. Including NIST and ISO 27000.
11.	PH	Yeah, perfect. Okay. So you have been involved with implementing them as well, I can imagine?
12.	RES1	Yeah, yeah. I've done it in at least two companies. Three maybe. Yeah, something like that, yeah.
13.	PH	What has been your role in the implementation part?
14.	RES1	Security specialist, mostly understanding the requirements. I've been process engineering, writing processes, setting up controls, physical controls. It controls all kinds of IT security. So yes, full stack more or less controlling and handling incidents, selling the idea to the customer, documenting. Yeah, a little bit of everything. Okay. Generally in leading projects in security framework implementation and also handling daily operation well.
15.	MH	In general, how is a framework implemented from like the first idea to the finished implementation? If you could say, is it that a company comes to you and ask you?
16.	RES1	And in my experience, no company will do this unless they're forced

		to. That's the. That's the starting point. There must be some external force demanding or recommending this. I haven't seen many companies, at least not in Denmark, that implements high security just because they want to do the right thing. I haven't seen that you only do it when you're forced to. If you can see that it has a competitive advantage or something like that, then then you might you might consider it, then typically it'll start in the. The technical department or in a system engineering department or something like that, where they realize there's a need and first of all you will need management, understanding and backup. So as always, the first step will be awareness, making your management and senior management aware that this is a need and we need to allocate resources and and plan ahead. Because it's no matter what framework you choose to implement, it'll take a long time. It'll cost them a lot of money, a lot of hours. And you use consultants and so on and nobody wants to do that unless it's required. So that's sort of the starting point in my opinion. From a practical perspective, I don't know if that answers your question.
17.	MH	Yeah. And just like the first part, is it due to that they are in some form of incident or that they're hacked or something like that or is it just like they feel that they want it??
18.	RES1	It's typically requirements from customers and partners. So let's say you want you want to sell a products or to a regulated industry, it could be. I work with the the train industry before with Siemens and I work with the urinal industry with copham. That's public information. You can see it on my CV and when you enter negotiations with a controls industry. The industry with with some kind of going through a regulated industry, that's the right way regulated industry. Then as a soft supply you will be forced, they will ask you so how do you, how do you take care of your security, what framework have you implemented? And then typically a company will say, yeah, but we have something really smart and we have full control, OK show me all the controls and and how you monitor them and how it's how it's implemented on what standard are you living up to. Then suddenly people start running around and getting very hectic. We don't have a framework and then probably the the company will realize it. It could also be a strategic decision. If this was a wise company, I haven't seen it, but it could be a strategic decision. We want to enter this new market and if you do your analysis correctly, you'll find out if you want to be a player in this market. It could be some kind of regulated industry, could bank sector, it could be XXX, the training industry or. There's no medical industry then it's a regulated industry and if we want to go there, new requirements will be put on us. Then you could then you could realize it in advance. But in my experience it it's it's a sudden, a sudden vision that management suddenly gets Oh yeah, we we are going to do business with with somebody that requires us to follow a standard. So that's my experience.

19.	MH	And that's not a good thing, right? You would prefer that it was like a standard to implement those security frameworks, right?
20.	RES1	Not not, not necessary. It all depends on the company you are and the the threat scenario and the risks you face. And in general, I like this, a very famous drawing with with if you imagine, can I can I do a drawing here? I think I can. It's one of the new features. I'm sure it's here. OK, that doesn't matter. I can explain it. If you imagine you have an XY matrix. And then you see quality going up overtime. That's what we want, right? Security going up, quality going up overtime. Then there's a very famous drawing where you sort of put in a triangle that will force you to go from point A to point B by using a standard. I don't know if you've seen that. But it's it's one of the ways you can sort of use it as a a lifting rock to lift up your standards. So if you are on this level and you want to go to somewhere higher, how can we get there? And one of the best and easiest way to come from point A to point B is to implement some kind of standard to to to go there. So if if you think you want to improve then a security framework a standard could be a very good idea. But I think it's ridiculous if you implement a very strict security standard. If it's not needed then it's a waste of money. I have I have a different security standard at home than when I'm at work because there's another threat scenario and the risks are different. So you have to have something that fits first of all fits the threat scenario and and the assets that you want to protect. But what is even more important? Is that you need to understand the mature, the process maturity level of the organization you work within. Are you familiar with the CMMI model? CMMI? Yes, you will look it up on Wikipedia afterwards. I know that CMMI is a very, very nice model that describes how mature an organization is in regards to processes. When I when I do my laundry at home, there are hardly no processes. Everything is done ad hoc. So I just sort of do it and then next time maybe I do it differently and if a problem comes, then I'll solve it, right? That's my laundry at home. It works. It's it's a good process maturity. If we do things in XXX where we implement, let's say a billion dollar production line then. Use another another maturity. Things have to follow specified process and we try to foresee problems. We do risk analysis in advance and so on because it fits the the threat scenario and the way the organization works. In the same way, it would be quite stupid if I told my old parents to implement ISO 27000 at their home, because they wouldn't be, they wouldn't be ready for it. Right, They don't have the underlying basic frameworks to implement this. So if you have zero quality system, if you have zero incident management, if if you don't have any of these things in advance, if you have no processes at all in your company like my laundry at home, I have no processes for it. But if you have 0 processes, trying to implement strict security framework will be very bad idea. You you have to find a security framework that matches the maturity level of the organization. Do you understand it? And that is actually one of the highest paths. That is persuading management that

		your basic quality framework needs to be in order. If you have a ISO 9000, you know that general ISO quality standard thing if you have a normal ISO 9000 and you're doing as you're supposed to do. 27000 is very, very easy. Yeah, seriously, it it is not difficult because it's sort of the same mindset that things has to be measurable. They have to to happen in fixed processes and so on. But if everybody's just acting ad hoc like they do in small companies or companies that are faced with the new challenges. Then it's it's the wrong in place to implement a strict security framework. So we have to find a maturity level of the organization that fits a security framework. I hope it makes sense. It's a pattern point for me because people keep talking, don't you want to implement? And then some very advanced security control and I'll say I would love to. It would be amazing, but in this area of the production or this area of our development, we don't have the underlying processes to support that. For example, I was in a, I was in another company, won't mention any name, but there was a big discussion about penetration tests, physical penetration tests and and electronic penetration tests and the company. Was really considering should we do these pen tests, it would be so exciting. But we were not there. We were not ready for it because we knew already that there was so many open gaps everywhere and we had no process to to catch. If we had some findings, how would we solve them? We had no controls that we could fine tune. So you need to build up something first, some kind of process level, some kind of maturity this CMMI model and then you can build on that. With no underlying quality framework, you cannot implement a security framework.
21.	MH	OK, And would that suggest that larger businesses are more keen to implement those security frameworks? Because smaller companies don't really have that.
22.	RES1	Not not necessarily large or small, but regulated. Non regulated. So if you're if you're working in a regulated sector like banking or producing medicine or making. Anything that can kill people, basically cars or automobile pills or anything. If you if you work in any industry where you can kill people then it's a lot easier because then you're already used to to quality mindset and you have an underlying quality framework. So it's not about size in in my opinion, it's about the the CMMI, the process maturity level where you are already and if you have 0 processes for anything. Then start with getting a good firewall and yeah and teach people not to use use P sticks instead, right. It's probably probably better.
23.	MH	And is the goal always because we looked at NIST and we saw that there are the four like implementation tiers. It’s like the CMMI maturity level. Is the goal always when you implement the security framework to reach the highest level of security or no?
24.	RES1	No, definitely not. I worked on a project in a company where we

		aimed to have an ISO 27000 like implementation. We we concluded from the beginning that we would not go for certification, but we wanted to establish processes that were similar. So. We don't necessarily want to achieve it. You can still use the framework to get results. So and also just to get inspiration and maybe you say these areas we have a low process maturity. It's very hard for us to implement controls in this area. On the other hand on that area there or that department or something in that area, we can implement stricter controls, hopefully risk based, so we say. Where is the biggest risk and where is the the the, the price maturity able to cope with this? And then you can implement parts of of of a standard or be inspired by it or make your own standard or something. The only reason I see to implement a strict standard like 27000 on this standard or I work with all the weird standards from the from the industry. But the only reason to implement that is if you are forced to so to speak, you you you have a business. Application or very business motive to do it. If you understand, it'll cost your money. If you don't do it and you'll earn more if you do it, then then suddenly things happen, right?
25.	MH	And do you have any examples of you being in a company where the aim was to reach the highest level and did you so in that case like accomplish it?
26.	RES1	No, I will not say that I've never, I've never been in the company that. That want imperfect security. I think any company trying, any any company trying for that will fail. But I of course, I've worked with with different ambitions and different level of ambitions, but normally it's based on the regulating industry and the authorities regulating that area. So you try to meet the demands and the requirements.
27.	MH	You mentioned failure there. How do you? Because that's a topic we have discussed a lot. How do you measure, like the implementation, if it's successful or if it's a failure? Because it's kind of hard to say that: OK, we didn't have a cybersecurity attack in the last two years, so our security has to be really good.
28.	RES1	No, no, that's bullshit. You you can only measure. Yeah, I looked at that question as well and I was wondering what to answer. And. Of course, of course you can't measure it on incidents that would be stupid. Yeah, and unless you you you have incidents. Let's say you have a website and it's hacked 8 * a month and then you implement the security framework and now it's no longer hacked. OK, you have evidence, right? But in most cases it's based on fear or risk analysis. So what What I recommend and and the way I work is long way to do a risk analysis. That shows that the cause of missing controls or inferior controls, the risk is too high. Then afterwards when the control is implemented, I'll, I'll do a similar risk analysis and show that either the the impact of an incident or the the likelihood of an incident has lowered, right. You know that normally when we talk about risk, it's the product of likelihood and impact. Are you aware of

		that? Great, Great. You read the textbook. Fantastic. The risk is the product of likelihood and impact. And if I can demonstrate that by using this security control, the impact is lower, then I've succeeded. So let's say I implement a good bag of strategy and now I can tell the company if our servers are nuked. They're hacked, they have virus or whatever. At least we have a good backup and we can recall in one day that'll only cost us 10 million chroma and it will not bankrupt the entire company. Right then I have a good risk analysis. I can show the impact is now lower because I implemented backup. I can also say that if all my ports on my computer is open towards the Internet and I never patch my Windows computers, then I estimate that there is a very, very high likelihood. This machine will be compromised somehow. And after I implemented the control, I can say the likelihood is probably lower now, and then the risk analysis will show the efficiency of the control. Does it make sense? Yeah. Yeah. OK, great. Because that is exactly the way I work here in XXX. That is by doing formal risk analysis of our controls and estimating them before and after we implement. 2 controls or improve our controls.
29.	MH	Super. And how does implementation differ from different industries? So let's say the healthcare industry or the like, the car industry, it's the implementation any different?
30.	RES1	It's the same stuff. I see, I see basically there's one big difference that is. From production companies to non production companies, every every company that is producing stuff is typically hit by a lot of technical depth, meaning old hardware, old software, old Plcs, old systems. So production facilities and production companies will typically lag behind, let's say an online web business. Because they're used to living in an isolated area, and especially if it's a regulated industry, it might take 10 years to get a regulated facility approved. In XXX, it can take 10 to 20 years, maybe 15 years or so, to have a facility approved by all the healthcare authorities everywhere in the world. And because of that, things are planned and designed in the past. When put into production today and it's sometimes very, very difficult to change the science in production companies because it's regulated and you can't just change the design of this server on that robot because then you have to go through all this validation again. So in production companies we're typically behind and regulated production companies it's even worse. So I'm we were doing our best. We're trying all we can but. Production company will always be a little bit behind because of the way things are and it's just it's terrible what you see in the from industrial supplies is is crazy. We're getting office office that we refuse but we're getting offices on system based on Windows 9 to 5 and 97 and things like 98 or whatever it's called things from back in the days. They and these systems are being sold to the industry today because they were developed years and years ago and they still sort of work constantly and and they have proven to be very stable and so on. But they are just completely insecure and not maintained anymore. And that's what you see in the in the real world

		in the in the industry and you will not see that in a .com company working only online. But when you start dealing with huge industrial robots and things like that, production lines, then suddenly you are 15 - 20 years behind because it takes a long time to have them certified and the suppliers are from from a different time. I don't know if that was what you asked for.
31.	MH	Yeah, it was good and leads kind of to the next question as well. We had a question that was like what role do organizational culture and leadership play in the implementation, if that can hinder it sometimes?
32.	RES1	Yeah, absolutely, absolutely. Awareness is always number one and if you work the security awareness goes in two directions, at least downwards and upwards, right. So one of my most important task is to constantly inform our senior management and make them aware. The situation that we are in and and what are the pitfalls? Where could it go wrong? What are the potential risks? So if there's no culture in the company to to be proactive, If there's no culture to have Also talking about CMMI and process maturity. If there's no culture for by having strict processes and doing things after, I repeat doable control way. Then it's impossible. You can't implement a security framework in a company where everybody just comes to work and does what they want. It's simply not possible. You can only implement the security framework if there's a basis for it, a layer of basic quality framework, basic processes. So if you have, if you have no process for how you hire people, then you can't put in in in with failing for example, where you do background checks and everything. You need, you need sort of that basis and if you have no basis for how to handle passwords, it's very difficult to say. We have a password complexity requirement now. So you need if everybody just makes their own passwords on the servers and there's no control, there's no monitoring, there's nothing and people are not used to asking anybody. There are no written rules, there are no guidelines, there's nothing. Some companies work like that and. Especially small companies in not unregulated industries, but startups especially. Everybody is just sort of technician and they all work together and yeah, we'll just hang it. But a company like that will be absolutely impossible to implement formal security framework in in my in in my deepest belief, it'll be impossible. You will fail before you started. So the the the quality mindset. The idea that you have to work after repeatable processes, if that is not in the company, you'll never ever be able to implement the security framework.
33.	MH	OK, makes sense. And have you seen that? Is that something that happens usually?
34.	RES1	Yeah, no, not usually. But it it happens. Yes, everything, everything is possible if management supports it. Everything is possible, right? And if you have funding and if you have good people, then of course everything is possible. But you might have to start with something

		else, building up a basic quality framework before you can do a security framework. So, so yeah, that's sort of my answer.
35.	MH	Yeah. OK. And moving on to GDPR, is there any. Complications with that?
36.	RES1	No. No. it's fun and games.
37.	MH	Yeah. No, but regarding the implementation, is there like some special parts of the security frameworks that is regulated especially by the GDPR that makes it kind of hard in some businesses to implement?
38.	RES1	GDPR is extremely difficult. It's just it's it's very, very difficult. I I usually say it as a private person and as a European data subject, I'm very, very happy about GDPR. Think it's wonderful. Finally my privacy is protected and I'm I'm so proud that the European Union is able to do something like this because it's a dramatic change in the data regulation in EU. On the other hand, as a representative of of industry and and commercial interests, I'll say that this is absolutely crazy and it's not possible to implement it and you cannot, you cannot run a business with these stupid laws. Don't. I'm sort of, I'm sort of caught between these two positions and it is very, very difficult. And I think one of the reasons that it's very difficult is that that how can I say it, it's nothing new. We've had very similar data regulation laws in Denmark before GDPR. So in theory there's really almost nothing new. The new thing is that the fines and the consequences are. Astronomers, you know that you, you, you, you can have a file of how much is it 4% of your global revenue or global something. It's it's absolutely crazy. It could it could be billions and billions for normal notice, right. So the the the fines and the consequences are huge. Because of that companies have to do something about it, right? But again, if you don't have, if you don't have a quality framework for your data in place. Already then it's extremely difficult. So I would say for for certain industries, GDPRs, no issue. I'll be so bold to say a company like Facebook, they can easily do it because they are handling personal information. That's what they do. That's what they that's the entire business model, an insurance company or bank or something like that. They're used to handling this kind of information. They know how to structure it. But for a company that is not normally handling personal information in any way, No, not. Of course they're handling it, but they're not. They haven't built processes around it. They don't have a a quality mindset on how to handle personal data at all. It's very difficult because how can they build a control? You know the GDPR has the right to be forgotten, for example, right? So I can call a company and say hello, you have some data on me. Please delete it, then the company should do what I said right? In theory, if they have no basic control of their data, it'll be huge problem. Facebook implemented something in how much was it a few months and now you can just press a button and you get all your data and that's it. If you trust them of course, but they they were able to

		implement it really really fast. But for a small company. With everything in Excel files and there's some docks on a few servers here and there and a little bit in the cloud and and things like that, they don't have a quality framework to handle GDPR, so how will they be able to do it? So in a way, in a way, I think GDPR is hitting the wrong kind of people because it was meant politically to control the really, really big online players like Twitter, like Microsoft, like Google, like Facebook, those the intention. But in real life I think it might be harder hitting on small companies with no basic quality framework in place. And just imagine you're having a small restaurant and people are calling in booking tables and things like that. Suddenly you have to be very aware how you handle this information. The way you store it and what about that cloud solution we got for free from Russia? How is is a complete new way of thinking but if you're already used to handling personal data then it's just yes, expanding that, changing that framework. So again it's it's all about the quality basis. What do you have in to attach it to if you have nothing to attach it to How can you if I write a nice process? But I don't have a quality framework where sort of can attach it. So I can, I can write a process. Every time Peter is getting coffee, he has to check this and that. OK, I can write it on a piece of paper. Now I have a nice process. But if you don't have anything to control that process, if there's no training in place, if there's no quality assurance department that checks. How would I implement it? I can write it on a piece of paper, but implementing it in real life is impossible without sort of the basic quality framework in the organization.
39.	MH	Speaking of that, when you come to a company, do you make the like the current state of the IT security or is that something you get from the company? So like for example when you're working with NIST you have like the the current States and future states? And you always look at those twins each other, right. So do you make that assessment of their current state or is that something that you get when coming to the company?
40.	RES1	Depends a lot, depends a lot. There's no simple answer in in XXX I'm doing a lot of the the risk assessments myself together of course with the system experts and. All kinds of quality insurance and process people. And so it's it's a teamwork. You have to involve all the right subject matter, experts and externals. Sometimes you have to hire external resources for good risk analysis, and sometimes you might want to do a pen test or something like that, vulnerability assessment. Sometimes you hire external people to help deal with that. But it it, it completely depends on what you're trying to assess. Some risks will be easy to assess and you can easily make an assessment. But other things, it's very, very complicated and hard to assess. So it depends a lot also on the organization, the size of the organization. In some organizations you have 100 people doing risk assessments all the time, constantly, and in other organizations it's a part time job. You might be able to spend a few hours every week. So it it depends on the

		organization how it's done and but again it has to fit the general level of process maturity in the company. So yeah, long answer again, I'm not sure I answered what you asked for, but I tried.
41.	MH	That's good. Yeah, that's good. And just to sum this implementation part of the interview up. What are the most common obstacles and challenges that companies meet when implementing frameworks? Like, these three or these five hinders come up all the time.
42.	RES1	Yeah, and of course there's always pushback. People, people don't like change. Change management is extremely important and that's a textbook thing as well. And you you need to understand this resilience and this push back from people. Whenever you change people's way of work, they will be pushing back. So that's one thing. And again, I have to mention this about the quality mindset and the quality system. If you cannot attach your processes to anything, it's impossible. So if if you are not. You don't have a process to to review your log files. For example, if you don't have a process to review your log files in place, it's very hard to establish an an annual review. So if you already, if you're already reviewing your log files every month for other things, it could be quality related, then it'll be easy to also review your log files for security incidents if you're already. Doing background check for some parts of your employees, then it's easier to do background check for us, right? So it it, I think the difficult thing is to to go into Greenfield where there's nothing built. So if you go into an in space where there are no processes already, so if there's no quality framework to attach to, then it's extremely difficult to implement any. Formal controls or regulated controls? And every security framework is all about having standard regulated controls, right? So you need, you need this framework to attach it to. I can come up with all the good processes and all the good ideas I have, but if there's no nothing to attach it to, if there's no process in place already, then it's it's very, very difficult.
43.	MH	And these obstacles are avoidable, right? It's kind of easy if if the organization works, to try to mitigate them?
44.	RES1	Yeah. But it's easier if people are used to having processes, if people are used to. When I do this, I have to work according to this and that. If people already have that culture in the company, that whenever we do certain things it has to happen in a special way. And we had to document what we do if if that culture is already implemented and if you have processes for that. Then it's a simple task to implement another procedure, a security procedure. It's nothing. It's just another procedure. But the hardest part is going into Greenfield, going into an area where there's no regulation and no process and nothing and trying to establish a framework or some kind of any kind of security. Actually, that's the biggest obstacle in my president.
45.	MH	And lastly, approximately how long does it take to implement the

		framework to the grade that you want to implement it?
46.	RES1	So you know my answer already. It depends on on what what you're building upon. If you're building upon a good company with with a lot of quality frameworks already, as I said, if you have ISO 9001, if you have ISO 9001 already in place, you're certified. Then you can sort of just take 17, what is called 27000 and just attach it. It's it's so it's plug and play. You can just attach it to the controls you already have and and expand them and it can be implemented in in months. If if you're if you're working on a Greenfield in a company or an organization with with no process framework and no quality framework, then it'll take years because you have to change the entire. The company way of working the the mindset and and the way you look upon quality and things like that. For some, for some companies quality is we earn money. For some companies quality is nobody dies today. But for for other companies quality is something measurable that we have to do. You can imagine how it is to produce medicine that people inject in their body. For us quality is very measurable. We have to constantly measure quality in all parts of the organization and all, and because of that it is possible to also attach new security procedures whenever that is needed. But try in your first startup to implement the security framework and it will be absolutely impossible.
47.	MH	OK
48.	PH	OK, so moving on to when. Companies work with the frameworks. Is there something regarding the frameworks that the companies have to maintain and yeah, maintain continuously?
49.	RES1	All of it? I'm saying it doesn't make sense to do this as a one time exercise because security is about a process framework. It's basically a quality framework in regards to IT security. So. If you have, if you implement security controls and you don't monitor your controls, they have zero value. So if you implement a firewall or an anti malware protection or any security technical security control, if you don't monitor it, it has zero value because you can't trust it. You don't know if it's working. You have no idea so. You you in, my in my opinion, you cannot implement any security measures or any security controls without constantly measuring them and constantly following up. So it doesn't make sense to use, you know, not even $1 on on any security initiative if you don't plan to follow up because it's worthless. So you you have to constantly follow up and you have you need this quality mindset. And work closely together with quality experts to ensure that the controls that you say you have are actually working. And if you're not measuring your controls over and over constantly, constantly, constantly, then that's just a waste of time and money. So and then if you implement one security framework and you are now on this level right then. And you think this is good. Now we have here, but we want to be even higher. So now we found a new security framework or a new security standard and we want to go there. Then it will be

		relatively easier because then you have the foundation in place already. So my recommendation would always be start with something quality wise. Start with an ISO 9000 and get your basic shit in place so you know about quality so you have processes in place for how things are done in your company. After that we can talk security. If you're bleeding data, OK, go buy a firewall and some antivirus or something. But if you're not bleeding data and you have no incidents, then start by implementing a good quality mindset and a quality framework and build on top of that. But by the way, if you don't measure your stuff, how will you know if you have incidents, right? So.
50.	PH	OK, so you have to have people who work with the frameworks or like a checklist or some sort.
51.	RES1	Yeah, but if you implement I said 27000, I've done that a few times. Then it's about engineering and modifying your processes. You have to build on the process framework sometimes it's called what is called SIEM. Security information or something seem recorded seem sometimes or. Something else I don't remember, but you you have to implement a process framework. That's important Word the process framework where you can where you can attach your processes again. If I wrote this process on a paper, a piece of paper, when Peter goes to coffee, he has to check the Windows Phone or whatever. If if I can't attach it to something, then it won't work, and if I don't monitor it afterwards it doesn't work. And if Peter's not writing in the logbook. I went for coffee, I checked for burgers, no burgers found. Then I cannot monitor it. I cannot see if the controls are performed. That is worthless. So in every case you need to follow up, your controls needs to be living, it has to be a quality mindset and so on. And what was the question again? I'm afraid I forgot.
52.	PH	If you have to have hired people who always work with the frameworks?
53.	RES1	Yes, yes, you need. And that could be internal or external resources. For some companies, it doesn't make sense to have your own IT security department or quality quality assurance department. And some companies can hire that outsource it in some ways. So it doesn't have to be your own employees, so to speak. But you will need you don't need somebody to monitor your controls. If you don't monitor your controls, then why have them?
54.	PH	Okay. Do you tend to see that companies use one framework or they tend to use multiple or some parts of a framework?
55.	RES1	I tend to see that companies will typically use one framework at a time. So a company will use let's say ISO standard or new standard or something like that. In case like normal, we have our own internal security standards that we try to live up to, right? They are heavily

		influenced by the ISIS standards, heavily influenced, but they are not one to one copies of ISIS standards. What I see is that American companies, they tend to look towards NIST, European companies used to they tend to look at ISIS standards and then in different industries you will look at the industry specific standards if such exists. So if you work in certain industries there will be. Sometimes closed and confidential frameworks that you have to live out to, but it might be very specific.
56.	PH	OK, do you have any, do you have any preferences on which framework you like or have used the most?
57.	RES1	Yeah, I love the NIST standards myself and I think there's yeah, I think NIST standards are wonderful and they're public and you can read them without paying for them. I think the ISIS standards are expensive. I think they're quite good. It's ISO 27000, at least it's good. But I really hate the idea that it's a close proprietary standard that you cannot even obtain a copy of. If you two guys want a copy of it, you have to pay for it. I think it's ridiculous. It's a it's a bad business model. So that's my personal opinion. It's not XXXs opinion, it's my personal opinion and I think it's wrong. And you should not support a business model like that. But the standard itself is fine, it works perfectly. I think some of the new standards have very well developed explanations and theoretical parts. I remember first time I read the new standards about system engineering. I can highly recommend those. I don't remember the names anymore, but when I read the new standards about system engineering. Was the first time I really understood what an IT system was and it was like, wow, I've read so many books at university and everywhere and now they explained it. They're so mature. The mid standards are from developed originally in the 50s or something like that in the by the, by the US military, right. They've been built upon and built upon and developed and developed and they are so mature and they are really there's some. There's some thoughts in these standards that are they they're so work through, they're they're so mature, these standards. So I really, I really love these documents, but they're not heavily used in Europe. That's my impression. But if if you're just going to implement this good standard, go follow the ISO, it's easy and you can easily get a consultant to help you and a company to to certify you and so on. So that would be the natural choice. The company like XXX and we had to live up to multiple standards because of the multiple health and what is it called the medical authorities all around the world. So we might have certain requirements from the Turkish government, certain certain requirements from the American government and so on. And we will have to combine those into one. I worked previously worked with the company. We had two major customers, one was in US, they used the NIST standard, one was in Europe, they used the ISO standards. And what we did was we established our own framework and then we made sort of a reference so you could see that we would cover those standards and and that made both of them happen that we

		had, we had our own framework but all our controls could be mapped. 2 controls in this standards and ISO standards. And they loved it because then we didn't have to choose.
58.	PH	Perfect, perfect. Is there a big difference between small companies and large companies when it comes to the frameworks, when implementing them and working with them?
59.	RES1	No, I wouldn't say that. It's about how regulated you are and it's about the process maturity again. And some small companies are heavily regulated. You can have a small company that does some kind of business in an area where you need to be able to explain every breath you take and every comma you put in a code every; Because you're working in a certain industry. In a company like that, security controls are generally simpler to implement. So it's not about size, it's about cost, maturity, and. If you're working in a regulated area already.
60.	PH	OK, OK, I think you mentioned it a little bit earlier, but what is the most important factors when considering choosing a framework?
61.	RES1	Don't waste your money. Don't waste your time, that's it. Get banks for the buck. Do what you need to do. Do it based on. A professional risk assessment and not based on smart sales people and have somebody help you do a professional risk assessment so you find out what do we need, what are the actual risks here, what are we trying to protect here And don't implement the framework just because it sounds good or it looks good on the paper and that's that's the wrong way of looking at a security framework. A security framework is there to help you to implement. The controls that you need, but you need to control to protect your assets and to prevent threats. So start with your assets, find out what are we going to protect, do a risk analysis, is there any threats that could harm our assets and then go from there and choose the appropriate. So it all depends what are we trying to protect and then find the appropriate way of doing that based on risk analysis.
62.	PH	Perfect. Perfect. Yeah. Yeah.
63.	RES1	I hope it makes sense.
64.	PH	Yeah, absolutely, Absolutely. So we're basically done. But do you have any other comments or something you want to add or something we missed?
65.	RES1	How is your thesis going along? Have you interviewed a lot of people or?
66.	PH	No we are going to interview one on Tuesday and then we have to book one more, so at least at least three.
67.	RES1	All right. Yeah, if if you if your thesis is public, you're very welcome

		to send me a copy. I would love to read it. I think it's an extreme. It's an extremely interesting topic and it's happening everywhere. One one thing finding common could be I I often compare safety to security. You know the difference. Safety is personal safety. Think about personal safety in a production facility 200 years ago people literally died in normal. We're aiming for zero accidents, zero sick days based on on the accidents related to personal safety. Think about all the regulation today, if you open a business what you allowed to do with your employees. How much you have to protect them? All the regulations about their personal safety? Then think security. Think IT security, personal security, data security. Think how new IT is and imagine in 10 years, 50 years, imagine the amount of regulation that will be put into security as well. It'll be exactly the same journey and we will see more and more more regulation using. Increased regulation from authorities and from from other companies if you want to do business with them. So we've only started regulating IT and data security. And I think if we look at personal safety, then we have something to compare with. Just just think about that, give it a thought that people were actually dying in factories 100 years ago. Because nobody can. We could just hire some new workers and nobody cares what kind of paint a painter would use. Just 20 years ago they had brain damage and their eyes fell out or something because they used toxic paint. All that is gone today and we have moved so much in regards to to personal safety and environmental safety as well, but especially personal safety. So much has happened and I think we will see the same kind of evolution. In in security and security frameworks. But we will see even faster because it's it's a new industry and things are moving even faster. So my expectation is within 20 years you'll see a completely different landscape where all big organizations and corporations are using internationally acknowledged frameworks or their own frameworks or. Somehow being able to document that their data security and personal security, data security and IT security and so on is on par with the rest of the world. So think about this. I think that's a good idea.
68.	PH	Perfect. Thank you for participating.
69.	MH	Thank you so much.
70.	RES1	Good luck.

Appendix B - Transkription intervju 2

Medverkande personer:

Peter Herslow (PH)

Måns Herlöfsson (MH)

Respondent 2 (RES2)

Datum och tid: 2023-04-25 13:00 - 13:45

#	Person	Fråga/Svar
1.	PH	Vad har du för nuvarande position här på företaget?
2.	RES2	Min officiella titel är Cloud Architect. Sen är vi lite flytande med titlarna så ibland är det Cloud Security Architect eller Senior och så att. Men men jag sitter och driver ett team där vi liksom erbjuder säkerhet till våra kunder där vi ofta redan har ett driftavtal. Vi jobbar med AWS, primärt AWS Cloud. Så det är mycket säkerhetsfokus och erbjudanden där. Men också ren arkitekt och vilken teknik vi använder och hur vi bygger våra lösningar.
3.	PH	OK, vad har du för utbildning eller kunskap när det kommer till IT säkerhet och säkerhetsramverk?
4.	RES2	Vi har några kurser från. Vad det gäller säkert så har jag läst några på LTH. Jag läste treårig dataingenjör sen har jag är jag certifierad inom AWS har ett en certifiering för sin plattform kring säkerhet och som är och sen finns det även här som heter Security plus som är, minns inte vad de heter som har den men den den generell sådana här brett säkerhetscertifiering.
5.	PH	Perfekt. Vilka ramverk känner du till? Vi skriver just nu om NIST, CIS Controls och ISO 27001.
6.	RES2	De känner jag ju till. Sen finns det ju en helt annan, ja men plattform vi jobbar med AWS, de har ju en hel del egna ramverk alltså. De har ju sina egna ramverk och så det finns ju även liknande plattformar.
7.	PH	Ja, ja och vad vet du om de vi har nämnt här?
8.	RES2	NIST är någonting jag inte jobbat med konkret, men jag har tittat en del på det de har. Det är väldigt detaljerat och där finns ju väldigt mycket om den här färdiga, typ policies och sånt man kan som är kopplat till det som man kan sno i princip, så jag har tittat på lite på sånt för inspiration och så, CIS använder vi mycket. Vi har, dels så är det vårt go-to när vi kommer till en kund som inte har ett eget ramverk, de jobbar utifrån och som säger för att ha någonting att jobba utifrån att se vad, vad behövs, vad är viktigt och så så är det

		CIS vi ofta använder. Och sen ISO 27000 har vi, vi har varit certifierade, vi jobbar. Vi är inte certifierade längre, men vi jobbar utifrån samma processer som vi blev certifierade på. Så det har vi jobbat med internt här också. Så jag är väl ganska ganska väl medveten om alla dem.
9.	PH	Perfekt, har du varit med och implementerat ett eller flera ramverk? Och i så fall, vad var din roll i de processerna?
10.	RES2	Ja vi, jag har, mot en kund så jag har implementerat ett. De har sitt eget ramverk med, men det är till 90 % CIS och där har ju varit med om att, där sitter jag och driver det hela. I princip att de har sin och sen har jag tagit den och så driver jag på sig att vi deras miljö uppfyller de här kraven. ISO 27000 har jag varit med internt. Det har ju inte varit. Det har ju varit mer. Ja en del en del rådgivande och så, men inte inte lika centralt i vår värld.
11.	MH	Alltså finns det något speciellt med CIS Controls som ni alltså tycker är extra bra liksom för det är väl mer praktiskt än typ som ISO som är lite mer tolkningar?
12.	RES2	Och det är lite just det du säger om att det är lite mer praktiskt. Det ger mindre utrymme för feltolkningar. ISO är väldigt. Såhär, beroende på hur hur mycket du själv bryr dig eller den som sitter med plånboken bryr sig så så kan så kan någon som uppnår de här certifieringarna och någon annan har helt olika nivå på den faktiska säkerheten. Och det är väl det som CIS tycker jag att gör det lite mer konkret, lite enklare och liksom faktiskt. Man vet att om två företag uppfyller samma krav så är de troligtvis närmare varandra än de här ramverken.
13.	MH	Och är det alltså billigare att implementera CIS? För det blir lite mindre typ eller än typ ISO.
14.	RES2	Ja det är så jag har. Dels har ju varit med och implementerat ISO här på det här på det vid ett företag på ungefär drygt 20 anställda. Jag har också pratat med folk som implementerat ISO på företag med upp till 2000 anställda. Det är nog svårt att säga att att en implementation av ett ramverk har särskilt pris. Det handlar väldigt mycket om just hur du väljer att göra de här tolkningarna. Vilken tidslinje du lägger det på. Den viktigate aspekten av de här ramverken är ju att. Allting bygger på att du kommer inte vara. Det kommer inte upp i 100% av kraven. I alla fall inte de första åren och troligtvis inte i längden ofta, utan det handlar ju om att. Man gör avvägningar det här, det här är viktigt. Det här ska vi lösa nu. Det här är viktigt. Men vi kanske får vänta något år och vissa saker bara inte är värt pengarna, för det är ofta där det handlar när man pratar om privatägda företag så är det ju en fråga om att. Ja, men är det billigare att alltså om man ska vara cynisk. I vissa fall är det billigare att ta böterna för att göra fel eller smällen mot infrastrukturen som de blir, ransomware eller vad det är,

		än att faktiskt betala för en lösning på det här problemet. Så att, jag har lite svårt att säga om den ena är billigare eller dyrare.
15.	MH	Och till implementering, generellt sett. Hur går det från idé? Ett företag har en idé om att vilja implementera någonting till att de faktiskt har något implementerat liksom. Vad är processen där?
16.	RES2	Det blir ju också väldigt annorlunda. Och det jag kan prata med i vårt företag där ISO 27 och där handlar det om där var det ju en, ett initiativ från ledning som sa att OK, men vi ser att det är värdefullt för oss. Både att öka vår säkerhet, men det kan det också potentiellt ge förtroende hos kunder eller vara ett krav som kunder har att deras leverantörer ska vara certifierade. Sen vet jag ju inte deras jobb som konsult mot andra företag. Jag vet inte exakt hur jag. Jag är ju aldrig inne när beslutet tas utan det är först efteråt som de blir intresserade av att ta in någon potentiell att jobba med, så där har jag svårt att säga. Men generellt sett så måste det nästan vara någon ledningsfråga om man har antingen ledning eller om man har en separat. Om man är väldigt stor och har en separat organisation för just compliance och säkerhet så kan det vara ett initiativ därifrån också.
17.	MH	Och hur mäter man att en implementering är lyckad? För att liksom vi har snackat en del om att även om du inte är med om en cyberattack och får stora förluster där liksom så kan man ju inte på det sättet säga att man har en jättebra säkerhet.
18.	RES2	Och det är ju en jätteintressant fråga då. Det har ju vi vi som då vill sälja säkerhetstjänster till kunder. Det är intressant fråga för oss OK, men hur visar vi att detta har ett värde? Ett enkelt sätt är ju att bara mäta på OK, men här är här är 50 compliance punkter. När vi började uppfyllde vi 4, nu uppfyller vi 35 liksom, grafer går uppåt. Det är positivt, det är ju den enklaste så. Sen, man kan ju också ta annan data och titta på om man implementerar tekniska lösningar kan vi få data för hur mycket spam email har man hindrat eller man kan göra övningar i form av. Mm så här att man skickar ut fejkade fishing epost och sådant och så ser man vilken träff rate har jag på det här före vi börja implementera och när vi nu har utbildade folk och liksom höjt nivån i organisationen har vi en lägre träff rate, sa jag att man det finns inget lätt sätt att säga det för att för att du kommer inte ha samma händelser både före och efter. Men det är väl de sätt jag har sett.
19.	MH	Och och är det ofta liksom eller är det nästan alltid att man kollar risker före och sen risker efter implementation?
20.	RES2	Ja alltså det. Det blir det väl lite och alltså det. Jag vill någon kolla när det finns kollar risks rakt av, för alltså om man tittar på en riskanalys så kan ju klart man kan göra en sådan före och efter och men i mina ögon så att göra en sådan efter handlar ju bara om att den stora förändringen där är vad, vad tror du om dina egna system? Om

		vi har riskanalys och jag tror att det här löser det bra. Det är ju inte faktiskt ett test av det. Men nej, men jag tror att i många fall så har man compliance ramverk just för compliance. Alltså, du har krav på det för att du sysslar med hantera en viss typ av data, då ska du vara compliant med viss typ av ramverk typ hälso industrin har ju har ju väldigt mycket sådana ramverk där måste vara det för att få kunna göra det arbete du vill göra och då är det ingen fråga om saken. Då skulle man uppnå det. I andra fall så så kan det vara för oss som leverantör till exempel. ISO är någonting som bevisar att vi har ett visst tänk att vi har en viss rutiner och då och det kan vara någonting som krävs så att. Ramverk av den här typen handlar inte alltid om säkerhet. I vad ska man säga mer på mer detaljnivå.
21.	MH	Och du nämnde hälsovården där, men alltså vilka specifika branscher använder sig av ramverk? Eller är det jätteolika liksom alltså?
22.	RES2	Det, och nu pratar jag på säkerhetsramverk specifikt då det skulle jag väl säga vi vi jobbar ju inom IT. Våra kunder jobbar inom, det väldigt mycket tillverkningsindustri. Och där finns ju. Jag ser inte någon tydlig skillnad mellan branscher. I fråga om om man använder sig av ramverk. Däremot ser jag skillnad i vilket ramverk man använder sig av, alltså till exempel. Vad vad har mycket höga krav på vissa saker.
23.	MH	Och typ tillverkande branscher, typ kan det vara till bilbranschen och så alltså den som tillverkar en produkt liksom. Är det någon skillnad mellan de branscherna och typ hälsovården då som inte tillverkar något utan det här mera typ, andra krav?
24.	RES2	I stort, alltså mycket av det här om man utgår från de här ramverken vi pratar om så är det ju väldigt generella så att. Men till exempel ett ISO 27000 är ju väldigt. Det måste du ju anpassa väldigt mycket till en organisation. Och då blir det ju givetvis antagligen någon skillnad i bottomline. Att vad blir det? Konkreta implementationen kommer bli olika beroende på vad ditt företag gör.
25.	MH	Vilken roll spelar organisationens kultur och ledarskap in i implementationen om den gör det liksom?
26.	RES2	Väldigt avgörande för att ha har du inte en ledning som driver på det som säger att det här ska vi göra, då kommer du inte få en budget till det. Så att det det är ju helt avgörande. Och det är likadant att du kan ha en IT avdelning eller en säkerhetsavdelning som säger att, nej men nu ska vi införa det här ramverket och för att vi vi tror på detta. Men, men om du inte får resten av organisationen med på det, då , men då kommer inte få OK att göra sådana här tester av dem eller att förändra rutiner för att göra det säkrare du, du måste ju ha allting med dig och då måste du ha ledningen med dig så att.
27.	MH	Har du varit med om någon gång det blev motstånd typ?
28.	RES2	Ja alltså, vad ska vi säga? Det blir väl en, det är alltid någon jag. Jag

		har aldrig varit med om att allting bara var go och och grönt på allting för att det blir alltid en prioriteringsfråga. När ska det här genomföras i det här med i årets budget? Eller så kan man lägga in nästa års budget eller? Är den här ändringen OK att göra eller? Eller kommer ni att skapa skapa problem för ett annat projekt som vi prioriterat och då för det där så att. Det är ju alltid en fråga om att hur. Om att man prioriterar med detta med mängd andra saker.
29.	MH	Och alla de regleringar som finns tillhörande till exempel GDPR och så här liksom är det något som påverkar implementeringen av säkerhetsramverk?
30.	RES2	Det blir det ju. I det att. Om de till exempel till exempel har data klassificering som en vanlig del av många den här ramverken så blir det ju en typ av data då som du måste hantera väldigt annorlunda. Sen, sen så vet du inte om det direkt krockar så mycket för de pratar ju lite olika saker så att du kan ju implementera det ena det andra eller båda utan att det blir bra. Sen ska vi också säga att vi vi är ofta inte med i mycket GDPR diskussioner då vi sysslar med infrastruktur och ofta inte anses vara en data processor som det heter alltså, vi har inte ansvar för kunden kunders data så att där är vi inte ofta så involverade.
31.	MH	Och vilka är de vanligaste hinderna som man står inför om man ska implementera ett säkerhetsramverk? Vilka är de vanligaste motgångarna man kan få liksom?
32.	RES2	Alltså, det är väl att säkerhet är jobbigt. Det är att att mycket av de här ramverken säger att inte bara att du ska skriva ner en process för hur jag söker utan den här processen ska innehålla vissa grejer som. Som gör arbetet svårare. Du måste, du måste fylla i en särskild blankett eller du måste göra någonting på ett visst sätt för att uppnå säkerhetsrutinerna. Och det blir mer jobb än att bara låta bli och den typen av att hur, hur implementerar man en rutin som är säker, men som folk faktiskt använder och vill uppskatta liksom.
33.	PH	Men kan det bli ett motstånd där bland alla medarbetare att de inte riktigt vill ha den förändringen utan vill ha det som alltid varit?
34.	RES2	Ja men det blir det ju så, sen och sen beror det ju också mycket på. Det är en väldigt kontrast mellan ett litet företag som vi. Som sysslar med det är många tekniska har en viss förståelse av just säkerhet på på det planet där där är det mycket enklare att införa någonting för att enklare få folk att köpa idéerna bakom medans pratar man en stor koncern eller någonting, då är det ju ett helt annat. Då är det ju den som implementerar det här ramverket tar de här besluten och då är det ju väldigt långt från den här människan som som blir påverkade av den där förändrade rutinen potentiellt och då är det mycket svårare att få de här människorna att förstå att det här är viktigt.

35.	MH	Och enligt din liksom så här erfarenhet måste man ha haft någon form av regelverk, kanske till och med säkerhetsramverk innan du implementerar typ ISO eller CIS eller något så här liksom?
36.	RES2	Nej, alltså då jag menar de här är ju ofta det man börjar med. Jag ser ju att det vanligaste är väl att man går från att inte ha någonting. Till att man har en incident och sen inser man att oj då vi behöver nu tänka på säkerhet och sen så hittar man någonting och det är ju de har ofta då man hittar om man bara söker efter säkerhetsramverk så är de här de mest populära. Så jag skulle väl snarare säga så att det här är det här är insteget till att jobba med ramverket. Sen finns det ju också. Sen kan man ju också ha sina egna mindre. Det kan jag tänka mig att många mindre företag som ändå vill vara lite medvetna är att man börjar sätta upp lite regler kring dig. Alltså vilken data du skickar, epost eller nånting, alltså här småsaker som de börjar bygga sitt egna ramverk. Men jag kan kan inte tänka mig att man gör det i så stor utsträckning innan man inser att ok, det är nog tacksamt att någon annan har gjort det här jobbet från backen.
37.	MH	Och och de hinderna, typ såhär med motstånd och så här liksom. Om det skulle vara så att man märker att det inte riktigt går så bra att implementera det är det ofta då liksom kört? Eller kan man liksom något sätt arbeta kring de motstånd typ?
38.	RES2	Alltså återigen så handlar det här om att man måste ha ledningen med sig. Man måste ha någon uppifrån som kan säga att detta är viktigt, detta är prioriterat. För för att annars kommer aldrig kunna förändra en organisation. Det är ju egentligen oavsett vilken förändring du vill göra.
39.	MH	Och till typ såhär tid på implementation är det för alltså olika eller finns det någon mönster man kan se att typ en organisation som aldrig har haft ett sådant här tar den här tiden att implementera det?
40.	RES	Det, det beror nog lite på vad du menar att någonting är implementerat?
41.	MH	Ja, men om vi säger alltså du vill ha typ av 18 åtgärder i CIS så vill du upp nå 8 för det är ett krav?
42.	RES2	I mina ögon, så det finns ju en en. En punkt till det du börjar jobba med ramverket om man om man tar ISO till exempel då är det att när ni implementerar ett ledningssystem för att följa upp det här när du börjar lägga in de här rutinerna, att det är OK ser den avvikelse ska du rapportera det här etcetera. Där ser jag alltså den tiden. Den sträckan kan ju vara ganska kort. Sen har du ju ISO där du kan bli certifierad och och där. Det är ju beroende på organisation men säg att du kanske du kanske certifierar det året efter första gången eller så har du här din första audit året efter sen blir certifieringen i. Jag tror det är andra, du göra 2 eller 3 audits för att faktiskt få certifieringen

		så att då pratar man tid på två/tre år. Men att faktiskt, att uppnå högre procent av compliance med till exempel CIS. Det är ju, det är ju ett. Det, det är ju ingenting. Det är ju ingenting som har sett ett datum på på det sättet, så som jag ser det utan det handlar om att det här är någon förändring och hur vi arbetar kontinuerligt framöver. Så att det är mycket svårare att säga någon slags när, vad. När jag, ur erfarenhet när jag har jobbat ute hos kunder och har sagt OK, nu ska vi börja jobba utifrån det här. Det går väl snabbt i början och höja compliance och sen så alltså så här att OK, men vi behöver en rutin för det här så vi skriver några meningar, då har vi en rutin, då har vi uppfyllt detta eller vi behöver ha en vi, vi får inte exponera oss mot internet, det måste skyddas. I vissa fall kan vara enkelt bara stänga ner vissa saker och så är du där och sen så finns det här projektet. Kraven som OK, det här är någonting som som vi behöver jobba behöver flera år för att det här är en fundamental förändring av hur vi jobbar.
43.	MH	Och typ så här när företag vill ha ett sådant säkerhetsramverk, vill man då ofta ha ett totalt fullt, liksom alla punkter inom ISO eller alla punkter inom CIS och uppnå allt. Eller är det ofta att du typ ha bättre koll på den här delen av det liksom.
44.	RES2	Ofta, jag får bilden av att man. Det handlar mer om att man. Man vill förbättra säkerheten snarare ut något särskilt mål. Det ISO är ju speciellt rätt och det är ofta att man vill bli certifierad och då är det väldigt tydligt vad målet är. Medans CIS eller NIS, då gör man ju mer utifrån att OK, vi vill bli bättre på detta. Och då är det ofta en, en acceptans av att vi kommer inte vara 100%. Vi vill sikta dit, men saker förändras konstant. Så att även om det börjar närma dig 100 så helt plötsligt så köper man upp ett mindre företag eller man man gör en stor förändring inom organisationen som gör att: Ojdå, nu måste vi backa på allt det här för att nu inte längre liksom ja.
45.	MH	Och och slutligen i implementeringsdelen, vilka är de vanligaste misstagen som företag gör? Finns någon mönster liksom att det här brukar förekomma ofta?
46.	RES2	Bra fråga. Spontant vet jag inte om jag har något. Men det det är väl återigen. Jo, det jag ska säga är väl just det här att man måste, det är en satsning från företaget. Det är inte en säkerhetskonsult som ska liksom okej, nu ska den här människan fixa vårt säkerhetsramverk. Utan det här kommer ju handla om att organisationen måste vara med på den. Att inte vara beredda på det från början skulle jag väl säga är ett fundamentalt misstag men som är rätt lätt att göra.
47.	MH	Och finns det brukar det finnas en övertro, liksom att det är lättare alltså? Man tror att det är lättare än vad det blir?
48.	RES2	Ja, jag jobbar ju inom IT då tror alla alltid allting är lättare faktiskt i praktiken, men. Men ja. Alltså det. Jag vet inte om jag har ett bra svar på det jag gör. Jag vet inte riktigt där. Vad kunden har förväntat. I vårt

		fall så var det väl kanske lite svårare än vi förväntade oss, men men det var ändå inte, det var inte helt. Det var ungefär det vi förväntade oss fortfarande.
49.	PH	OK, så går vi vidare till arbete med med ramverken och så där och du nämnde att det är ingenting man implementerar utan man jobbar lite med det hela tiden. Och vad är det då man behöver kontinuerligt arbeta med när det kommer till olika ramverk?
50.	RES2	Alltså det handlar ju. Det handlar ju. Det viktigaste är att man följer upp i grunden. Att du tittar på vad är jag och vad gör jag för att förbättra? Vad är nästa steg för att kunna förbättra det här? Vad behöver vi göra? För att gör du det så ser du ju allt annat som du då behöver ordna. Så det. Det är väl viktigt att du faktiskt följer upp det löpande.
51.	PH	Och sen tenderar du att se att företag använder ett ramverk eller vill man kanske ha flera eller vill man ta del av olika ramverk och bygga ett eget nästan?
52.	RES2	Det sättet är väl ofta att man man utgår från i större organisationer så utgår man från ett av de här ramverken och sen så kan man med att lägga till sina egna regler där om om man om man säger att någonting företagsspecifikt att ja, men okej, men i lösenords policyn så har vi de här extra kraven för att typ ja, men du ska inte använda företagsnamnet, ditt företags namn. Så att man man utgår ofta från att justera, men sen så. Av de här 3 som vi pratar om primärt så ser vi att man ofta väljer en. Möjligtvis då att man utan att man skulle kunna om man har ett väldigt stort företag både ha typ ISO 27000 plus att man har ett mer av de här hands-on som man jobbar utifrån. Men de överlappar väldigt mycket så så jag ser inte jättemycket mening i och jobba detaljerat utifrån flera av dem.
53.	PH	Och vad hade du föredragit om du fick oändliga med resurser och så där så? Har du valt att kombinera? Eller gå strikt på ett istället?
54.	RES2	Alltså, när jag jobbar med teknik så tycker jag helt klart mest om CIS för att den är väldigt hands-on. Den är väldigt tydlig på på ett bra plan. (mötet avbröts av kollegor)
55.	PH	Har du sett några trender nu de senaste? Men när det kommer till ramverket att man kanske är mer följer ISO och eller man mer för något annat eller är det specifikt per bransch eller land kanske?
56.	RES2	Svårt att säga. Det har ju, jag jobbar ju inte med så många olika branscher och så. Så många företag samtidigt så att jag kan nog inte säga att det finns något mer än en generell trend av att säkerhet är mycket mer på tapeten nu än vad det var för några år sedan, så att men det finns ett mer allmänt intresse av den här typen. Men, men att det skulle vara någon särskild kan jag inte svara på.

57.	PH	Ja och jag tror du nämnde det lite grann innan. Är det någon skillnad på små och stora företag när det kommer till både arbete och implementering med ramverken?
58.	RES2	Jo, men det blev det ju alltså. Dels blir det ju ett. Alltså bara bara då egentligen små stora företag funkar väldigt olika för på grund av att de behöver funka olika på grund av storlekarna och den skillnaden kommer ju givetvis överföra sig hur man jobbar med ramverk. Det är. Det är mycket enklare att implementera ett ramverk på ett litet företag för du har. Jag men i vårt fall då, vi är ungefär 20 pers då behöver du få med 20 pers på banan. Istället för 20000 pers. Det är ju en helt annan skillnad, så jag tror att det känns som att jag har pratat med folk som har varit med och implementerat i sådär ISO på mycket större företag som sagt att. En, som är anställd här tidigare, som gick ett annat företag som också var som sa att: Nej, nej, alltså, det här är ju en helt annan grej. Nivån på vår ISO var mycket högre. För att vi kunde liksom få med alla och så medans på det här andra företaget, då var det ju mycket mer att. Nej, men vi vill ha den här fina stämpeln på vår hemsida ungefär så vi ska absolut minimum. Och det kan jag tänka mig är en generell trend att som ett litet företag så så blir det ju. Alla kommer bli mycket mer påverkad av ramverk medans på ett stort företag så blir det ju kanske att ja, det finns ett. Det finns ett system för att registrera en avvikelse. Men det är kanske 1 på 10 som använder varje år eller någonting medans är vi 1 på 10 här som använder det så har ju hela syftet försvunnit.
59.	MH	Och så här behöver man ha någon anställd, liksom på företaget som konstant jobbar med ramverket och ser till att det följs och så här liksom. Eller behöver man inte det eller behöver man ska man ha en konsult som fixar det?
60.	RES2	Alltså du måste, du måste ha någon särskilt om jag minns rätt så har väl till och med ISO explicit sagt att du ska ha någon. Alltså, det är en del av ramverket, du måste ha någon som ansvarar för vissa typer av aktiviteter. Och de andra har väl kanske inte det explicit så, men men jag menar för att du du behöver någon som följer upp det. Och det är ju en klar fördel om de är långsiktiga i alla fall. Sen huruvida det är en anställd eller konsult kan ju vara i praktiken vara väldigt. Alltså en konsult kan ju sitta flera år, då blir det ju väldigt nära en anställd. Det handlar ju mer om att behöva ha förståelse för det här företaget och liksom hur det utvecklas över tid.
61.	PH	Vilka tycker du är de viktigaste faktorerna när man ska välja ramverk?
62.	RES2	Allra viktigaste är väl att alltså det ska vara. Det ska vara någonting man kan jobba med. Det ska vara något som man kommer få effekt av. Alltså du om du väljer att implementera CIS och säger att nu ska vi implementera det här till 100 procent. Då är risken att du kanske inte lyckas, medans du sätter mycket lägre ribba men ändå kan få

		någonting som kan få genomslag i det så kan det vara mycket, mycket mer säkert i praktiken. Alltså att. Så det det det känns ju som att. Hitta rätt nivå att att förstå vad ramverken gör och hitta det där du uppfyller det du behöver. CIS mycket med hands-on, ISO mycket mer. Vad ska man säga? Processorienterat och ledningsfokuserat. NIST har jag ju inte alls jobbat med lika mycket, men blir min bild där är att det har ju väldigt mycket bra material, men annars är det ganska löst och det är ju det är mer intressant om man om man är aktiv i USA.
63.	PH	Har företag en tendens att välja fel för att du nämnde innan att företag vill se bra ut för kunden, kanske med en certifiering eller eller något annat så. Är det så att företag ibland kanske väljer fel för att de vill se bra ut då?
64.	RES2	Ja och nej alltså det. Det beror lite så här. Väljer fel utifrån vad? För är målet att vara mer säker? Då kommer antagligen vilket av de här ramverken som helst hjälpa dig. Men det är klart att man kan. Ja, men att du potentiellt till exempel väljer ISO då för att få en certifiering av dem här. Sen känns väl ISO inte som fel val generellt så, men men om du väljer ISO i kombination med att du inte lägger tiden på att faktiskt. När du då skriver de här interna dokument och rutiner och etcetera för ISO att faktiskt tänka hela vägen ut, då hade det kanske varit bättre att ta ett ramverk som CIS som ger mer från början gratis. Så det skulle möjligtvis vara det.
65.	MH	Slutligen då, har du någonting som du vill kommentera eller något du tycker att vi har missat som är viktigt liksom?
66.	RES2	Bra fråga. Nej, det är väl möjligtvis lite det här att jag ser. Jag ser de här ramverket som att göra väldigt olika i alla fall, CIS och ISO. Att de de jobbar väldigt olika nivåer. Så det. Det är väl lite möjligtvis i hur frågorna var. Frågor kan ha varit lite för generella. Sen vet ju inte exakt vad ni vad ni vad ni söker så att det kan ju fortfarande vara rätt frågor utifrån det.
67.	MH	Ja för ISO är väl mer typ övergripande och tolkningsbart liksom och CIS mer…
68.	RES2	CIS handlar ju mer om IT, ISO handlar organisationen. Säkerhet är väldigt brett begrepp. I den här allmänna certifieringen jag tog så var det till exempel frågor om brandsläckare på övningsuppgifterna för att. I det säkerhet som du kan till exempel skydda någon server eller någonting. Det var frågor om om sådana här fysiska hinder för att ta sig in. Alltså såna här passerkort och så vidare. Den typen av grejer är ju på en helt annan nivå än att prata IT säkerhet. Så men men det. Men det är ju så och men jag märker ju även folk ute i branschen som som har svårt att liksom skilja på det här. Så det är inget konstigt så. Men men det gör det ju lite så det gjorde lite svårt för mig att förstå var jag skulle lägga nivån på svaret.

69.	MH	Tack så mycket du.
70.	PH	Tusen tack.

Appendix C - Transkription intervju 3

Medverkande personer:

Peter Herslow (PH)

Måns Herlöfsson (MH)

Respondent 3 (RES3)

Datum och tid: 2023-05-08 11:00 - 11:40

#	**Person**	**Fråga/Svar**
1.	PH	Vad har du för nuvarande position?
2.	RES3	Produktägare
3.	PH	Produktägare ja, och vad har du för utbildning eller kunskap när det kommer till IT-säkerhet eller säkerhetsramverk?
4.	RES3	Jag är certifierad ISO 27001 implementer. Och så har jag en CDPO certifiering. Det vill säga en GDPR ramverks implementation och underhåll.
5.	PH	OK, vilka ramverk känner du till? Vi skriver för tillfället om NIST och CIS Controls och ISO 27001.
6.	RES3	CIS Controls och men framför allt ISO.
7.	PH	OK, har du något ramverk som du gillar extra mycket eller något du inte gillar överhuvudtaget?
8.	RES3	Nej, alltså i konsultverksamhet så får man ju gå efter kundens val och i mångt och mycket så alltså. Syftet med dem är ju ett och samma. Men för mig i bank och finans har det hittills varit ISO certifieringar.
9.	PH	Ja, har du varit med och implementerat ett eller flera ramverk tidigare?
10.	RES3	Ja jag är ju en del av det, det vill säga jag jobbar ju sällan heller med själva ramverks integrationen. Men jag levererar flera olika delar till de. Jag är produktägare för ServiceNow plattformen. Och ServiceNow levererar ju till elevorganisationen. Oavsett om det handlar om scoops om det handlar om riskhanteringen eller om det handlar om bara över det nu incident problem och request och allting. Det ja de flesta hanterar ju tjänster i ServiceNow. Och när vi

		gör det så levererar vi med andra ord implementationer men driver inte implementationen, men levererar till dem på alla olika nivåer och tjänst.
11.	MH	Du nämnde det här med bank och finans, och ISO, är det något som är speciellt bra för just dem?
12.	RES3	Nej, det handlar nog i slutändan tror jag om kunderna, alltså kunderna till bankerna eller andra partners till bankerna. Och då vill man ju gärna ha ett delat regelverk. Mer om så att säga certifieringarna följer med så att säga så man inte bryter så att för er certifieringskedjorna. Och då kanske det är så att ISO är det som är mest använt. Som ändå går till stora data leverantörsbolag. Så är de ofta ISO certifierade.
13.	MH	OK, och genom implementering om säkerhetsramverk, finns det något mönster i hur det går från idé till färdig implementation startar?
14.	RES3	Ja, det gör det väl. Det går som det flesta andra typer av implementationer för ramverk. Att man, det fattas ett beslut att det ska göras och så bemyndigas det beslutet. Men det är svårt att upprätthålla bemyndigandet genom implementationsprojekt. Det tappar liksom tyngd när tiden går och fler vill hitta sina egna vägar för att minimera sin egen administration över tid. Och då är det ju viktigt att man fångar upp det. Jag tänker så här, det vore trevligt om det inte var så om man liksom från början kunde plocka in rätt typer av stakeholder och rätt typ av bemyndigande och också finansiera hela implementationer. Men man måste nog också förstå att det är inte riktigt så det fungerar om man har ansvarsfördelning och resultatkrav och olika delar i en organisation. Och organisationen då implementations ska bära sina egna kostnader så är det såklart att då flyttar man ju också över ett ansvar. Där kanske man viktar olika helt enkelt. Så det jag tänker att det är kanske något att hoppas på att man kan göra en plan som håller från a till ö. Det viktiga är nog snarare förhålla sig till verkligheten och titta långsiktigt och förstå att det är det första jobbet att certifiera sig kan vara enkelt, men allt typ av organisations hantering utgår ifrån människorna och det får man vara beredd på att det tar tid. Och det måste, arbetet som utförs måste vara tydligt värdeskapande för alla som är inblandade.
15.	MH	Är det ofta så att man tänker att det ska implementeras totalt, men så fort man uppnår sin certifiering så läggs det lite på is?
16.	RES3	Ja precis man glömmer ju bort alltså. Målet blir någon typ av certifiering eller del certifiering eller en process genomlysning eller så har man glömt bort varför man faktiskt gör arbetet. Det vill säga, det är liksom som att plugga för tenta och glömmer bort att någonstans i det här så är det ju faktiskt kunskapen som är värdet.

17.	MH	Och gällande lyckad implementering, för det är ett begrepp som ofta dyker upp. Hur skulle du säga att man kan mäta en lyckad implementering?
18.	RES3	Jag skulle säga ja, för det första, en lyckad implementering definieras ju av utrulladets acceptans krav. Helt enkelt det är där man sätter sin kvalitetsnivå. Och uppnår man den kvalitetsnivå som man har sagt då har man ju en lyckad implementering. Men en lyckad implementering kan ju vara mycket olika saker. Och riktigt lyckad implementering betyder ju att man har penetrerat en process övertid. Att man också 5 år senare har processer som stödjer lifecycle på det som man har implementerat. Och då i så fall måste det ju om det ska det ske, så måste ju den funktionen, som man adderar i ert fall nu, säkerhetsramverk, de måste ge ett värde. Det måste vara bra.
19.	MH	Och kvalitetsnivå, hur mäter man det? Är det typ hur många områden av till exempel ISO då man uppfyller typ?
20.	RES3	Ja precis kvalitetsnivån, det är ju lika med pengar. Så man måste ju bestämma. Vad får det kosta? Och vad ger det i slutändan liksom? Det är lätt att tro att någonting som är bra är kvalitativt. Det behöver det ju inte vara. Det är väl så enkelt att man får bestämma vad kvalitet är för en själv kvalitet är ju när den när nyttan och värdet överstiger kostnaden och och resurserna som krävs för att implementera och upprätthålla. Då har man ju en bra kvalitet.
21.	MH	Och vilka branscher brukar använda sig av sådana här säkerhetsramverk vanligtvis?
22.	RES3	Det gäller framför allt bolag som är agerar på en större marknad. Och i en kontext där det ger värde där man kan gå in i en affär och säga att om ni gör affärer med oss så vet ni att vi upprätthåller ett ramverk för, ni lämnar en garanti. Och att vi uppfyller ett ramverk. Och det som händer är att nästa person som gör och nästa organisation som gör affär med den kan säga att vi upprätthåller vårt väg. Nej, vår struktur och det gör också våra partners.
23.	MH	Och kan det vara skillnad på stora och små företag?
24.	RES3	Absolut småföretag som, sen ska vi säga så här det kan ju också vara så att man är ett företag som jobbar specifikt med ett säkerhet till exempel. Skulle man ju kunna tro att det är ett det ökar behovet för en certifiering inom området, men det kanske det inte alls gör. En certifiering lutar sig mot en good practice. Och det kanske är så att man utvecklar best practice. Certifieringen kanske kommer på köpet. Men det kanske inte är det som man kollar på, man kanske det, men det kanske är så att man utvecklar certifieringen och därför kanske man inte ens kan uppfylla den. Och när det gäller små företag så är det oftast för kostsamt. Skulle jag säga. Och man, och

		då tänker jag inte att det kanske alltid är så kostsamt att införliva processen. Men det finns ju en liability mer. Du garanterar ju något och om någonting då händer så är du också ansvarig för det så att säga. Man kommer att, om du har data breach eller något informationssäkerhet någonting händer och du har lovat att det inte ska ske och certifiera det för att det inte ska ske. Men det sker ändå. Den som du då har skrivit kontrakt med kommer ju gå till dig såhär skulle ju inte hända. Men så det är ett ansvar som man har accepterat och det kommer det. Det är bra i försäljningen, men om det ska utverkas så är det inte alls roligt. Men det är ju bara bättre att säga att vi böjer oss för er certifiering till exempel. Vi använder ert och preciserar det i vår organisation, men vi går under eran certifiering. Tar man inte det ansvaret då.
25.	MH	Och rent implementeringsmässigt kan den skilja sig mellan olika branscher och storlekar på företag? Typ tillverkande företag och icke tillverkande företag.
26.	RES3	Ja, det skiljer ju sig. Det skiljer sig ju också i standarderna liksom. De är ju anpassade till olika till olika branscher.
27.	MH	ISO standarden? Hur då?
28.	RES3	Det är olika bibliotek för informationssäkerhet och för tillverkande säkerhet.
29.	MH	Alla är en del av samma typ ISO 27001?
30.	RES3	Ahh precis men sen så är det ju 27005 och det är 27007 och det ja, det ena med det andra olika appendix för olika typer av verksamhet. Så det skiljer.
31.	MH	Vilken roll spelar organisationskultur och ledarskap in när man implementerar det?
32.	RES3	Jag ska ju säga att all förändring som man genomför utgår ifrån personerna i en organisation. Det är där det sker. Har man en organisationskultur där man bara vill uppnå ett mål och inte funderar så mycket, varför. Där man har lättare att man kanske inte jobbar under governance som i finans man har liksom finansinspektion eller liknande. Så är det stor skillnad det är. Jag skulle säga det avgörande skillnad i hur du måste gå igenom implementationen, oftast så syns det redan i din stakeholder eller liksom på den nivån man har fattat beslutet har man fattat beslutet därför att man är därför att man ser det här som är en underlättande väg framåt för sin organisation. Så ser implementationen ut på ett sätt, men om man har fattat beslutet därför att man ska uppfylla någon annans skallkrav och bara därför så ser det inte så ser du väldigt olika ut.
33.	MH	Har du varit med om det någon gång?

34.	RES3	Ja, ja, absolut, jag har varit med om jag skulle säga att om man hållit på ett tag så har man sett och väldigt det hela skalan. Hela skalan representerar sig sen i om man jobbar med större företag. Också i, inom organisationen. Vissa kommer bara tycka att det här är skittråkigt och det kommer ledas av team som säger så här ni måste göra det, men ni får inga pengar. Och det kan man ju förstå då om man har liksom en organisations ledning eller ett ben som säger att det här måste ni göra för att någon annan har sagt då en vi stödjer det inte. Så det är såklart att det kommer se annorlunda ut den. Eller några som förstår ett annat värde av.
35.	MH	Och du nämnde innan att du har kunskap inom GDPR, är det någonting inom implementering av säkerhetsramverk som blir påverkat av GDPR specifikt?
36.	RES3	Jag tänker svara på det med mitt standardsvar är det är ju att du kan ha IT säkerhet utan att ha datasäkerhet, men du kan aldrig ha datasäkerhet utan att ha IT säkerhet.
37.	MH	Och det menas med det då?
38	RES3	Det menas med att om. Ja, då ska du veta vilken data som finns, var och vad den består av, vem som äger den och vem som har ansvaret för en och hur den datan transfererar sig inom en organisation och inom produkter. Då måste du ha IT säkerhetsramverk som hanterar vilken typ av data och hur rör den sig etcetera. Men det betyder att har man ett IT säkerhetsramverk så betyder ju inte det att man för den delen har koll på vilken data är det vad vi står den och varför är den inhämtat? Vad ska den användas för? Det kan ju vara säkert ändå. Men datorn vet ju inte om det är persondata eller finansdata eller orderdata. För det är ju en annan fråga, men har man vill man ha koll på GDPR så måste det ju också ha koll på system.
39.	MH	Nej, men är det någonting som kan hjälpa med GDPR att implementera typ ISO 27001?
40.	RES3	Absolut, du kan omöjligt upprätthålla en datahantering om du inte har en IT säkerhetshantering, det är omöjligt. Det, men det går att göra tvärtom. Du kan ha säker IT kultur utan att ha saker datastruktur, men du kan inte ha säkert datastruktur utan säkerhetskultur.
41.	MH	Och till hinder och utmaningar, vilka är de vanligaste hinder och utmaningar företag stöter på när de implementerar det?
42.	RES3	Det är att man inte tar de kostnader och man tar inte hand av lifecycle. De tänker att det fit and forget, och det är det inte. Det är det varken i själva verktygen eller själva värdera som man gör eller i upprätthållandet över tid. Det är liksom varken i varken med personerna som jobbar med det eller verktygen är fit än forget. 2 månader eller 2 år senare så kommer det sitta en annan chef med

		annat mål. Eller en annan budget. Som kommer att utmana den struktur som då har byggt ut. Och då måste den strukturen vara så bra och väl implementera det organisationerna att den motstår det, det vill säga att det måste vara själv upprätthållande, vara enkel att hantera och det måste bidra med ett värde.
43.	MH	Är det bättre om man har haft ett ramverk sen innan så man vet hur det är att jobba med regleringar på sådant sätt?
44.	RES3	Ja, det är klart att vi bedöms. Det är ju en det är en inlärning som jag ser det ju mer man är van med att jobba med reglerade processer och dokumenterade processer och ägarskap i olika typer av processer och tjänster och produkter. Ja då har man ju möjlighet att hantera det om själva tanken är om själva tanken att man har liksom en produktägare och en verktygägare eller en processägare och en tjänstägare om sådana typer krav, tankegångar och, eller liksom organisationssätt är nya för dig. Då blir det ju svårt såklart.
45.	MH	Men vad skulle du säga att typ ISO 27000 är en bra väg in i arbetet med säkerhetsramverk och ramverk överlag?
46.	RES3	Det är ju därför man har dem höll jag på att säga, det är ju inget, det är ju inget som säger att man blir säkrare av att följa ett ramverk och man vet vad man håller på med. Ett ramverk ger ju den som, då behöver man ju inte uppfinna hjulet på nytt. Det är ju rätt som håller på med det en manual hur det ska hanteras. Det är en bricklista liksom. Täcka av. Det är en ganska diger, men det är fortfarande vad det är.
47.	MH	Och du nämnde det här med att man behöver underhålla det. Om företags stöter på hinder med till exempel, att man har för liten budget är det ofta då att skiter sig eller är det något som går att undvika och förebygga då?
48.	RES3	Det där får du ta igen.
49.	MH	Om man stöter på hinder, till exempel att man har för liten budget eller att man inte klarar underhållande det. Går det att lösa då eller brukar det vara att man OK, då blir det inte någon certifiering eller brukar man lösa det då?
50.	RES3	Det är alltså antingen så. Man måste ju också fundera på om certifieringar eller om hela certifieringar är det som man vill uppnå. Är det det man behöver? Och är det det som man behöver så har man ju förmodligen ett behov. Och är det behovet hållbart? Ja, då ska man ju uppfylla det. Alltså, då ska ju inte pengar. Det är klart. Du måste ju vara värd, det måste ju vara värdeskapande. Det kan ju vara så att man inte får lov att göra affärer om man inte har ett ramverk. Och jag menar då spelar det inte så stor roll vad det kostar. Men det är antingen, får du eller så får du inte liksom. Ja, jag tror att

		när man börjar böja sig för att man bara ska leverera ramverket för att få certifikatet på grund av att pengarna är för korta, då får man nog göra ett omtag. Det var inte så att man bara kan fuska. Det är bättre att bedöma situationen på riktigt och liksom hantera det som det problem det är. Om man inte gör det, då tänker jag att det är ja då blir det problem med slutändan i alla fall.
51.	MH	Och sista frågan gällande implementeringen, hur lång tid brukar det ta att implementera från att man kommer på idén tills man är nöjd med där man är liksom?
52.	RES3	Ett par 3 år kanske.
53.	MH	Och skiljer det sig då? Kan det skilja jättemycket? Kan någon klara det på ett år och någon tar det 10 år?
54.	RES3	Ja, vill du säga att det kan nog också att det tar 10 år för en del. Ingen bör klara det på ett år man bör ta certifieringssteg och man bör då ha audits med ett lagom mellanrum och ett lagom mellanrum brukar vara att man gör liksom en delaudit ett halvår och sen ett halvår senare så gör man det lite större audit. Och så tänker man att man har flera avdelningar så eller flera områden. Plus att man får nog vara beredd på att auditen den inte lyckas. Ja. Så ja, man är inte 2 år tänker man inte på en 2 års plan. Då tror jag att man ska fundera lite vad man tänker på. En del tycker jag också att det ska gå snabbt och enkelt om man ska göra det och men då blir det ju en topp down implementation. Och så uppfyller man kravet så möjligtvis misslyckas man alltså lyckas man, men man har inte gjort någon förändring i organisationen. Och den, den kommer inte att hålla. Utan det gäller att få alla förstå. Varför är det här viktigt att inte hoppa över viktiga steg som. Ja. Och hålla reda på känslor och produkt.
55.	MH	Är det ett vanligt misstag som förtag alltså företag gör att de har någon övertro på sig själva?
56.	RES3	En sak är väl kanske att man har en ledningsperson som ska utföra detta och den personen vill nog gärna bli klar inom en kort tid, inom en bestämd tid. Och det. Vi kan sätta en icke kvalitativ process eller press på implementationer.
57.	PH	OK nu går vi vidare till arbetet med ramverken och val av ramverk. Du nämnde det innan att företag måste underhålla säkerhetsramverk. Vad är det mer specifikt då de behöver underhålla eller göra?
58.	RES3	Ja först behöver man någon som är ansvarig för själva ramverket. Vad händer med ramverket för ramverket uppdateras ju också. Så någon behöver liksom vara ansvarig för själva ramverk. Men sen så måste ju de olika, alla måste vara anses. Alla måste ha reda på vem som äger, vilka tjänster och produkter. Då återkommer vi till liksom,

		det vill säga. En tjänst använder jag oftast flera produkter och en produkt ofta använt sig av ofta av flera tjänster. Men den som är ansvarig för en produkt måste ju bara ser ju för hur säkerhetsramverket appliceras på produkten och likadant för den som applicerar på tjänster och sen så avrapporterar man att man är att man då har compliance på sina saker till den som är IT säkerhetsramverksansvarig.
59.	PH	OK brukar man då ha anställda eller brukar man köpa in konsulter som har hand om det?
60.	RES3	Det vanligaste är att man har konsulter till implementation och inhämtning av kunskapen och liksom uppsättandet av ramverk och kanske konsulter till att stödja den som är ramverksansvarig. Men det här ska ju komma som ett arbete som är en del av det är väldigt vanliga arbete och där ska det ju inte, det beror på om man är en väldigt sourcad organisation så blir det ju konsulter såklart eller leverantörer eller liknande. Men de konsulterna är ju inte där för att jobba med ramverket det blir ju bara en sak till att hålla reda på en till bock i ett system eller något eller ja.
61.	PH	Ja och använder företag ett ramverk eller brukar de använda flera ramverk i kombination?
62.	RES3	Nej, man använder flera stycken i kombination med varandra, de flesta organisationer som har behov så brukar detta växer också organiskt. Du vill säga att man får lägga sig med sig när man köper andra bolag.
63.	PH	OK, ja du nämnde innan här. Är det någon skillnad på små och stora företag när det kommer till ramverk liksom vad och varför i så fall?
64.	RES3	Då vi kom ifrån naturligt tillverka den produkt som säljs och den som köper den produkten har, ställer krav eller en myndighet ställer krav. Så det är så klart att om det inte. Jobbar man på en väldigt liten marknad så minskar ju kraven. Om det inte råkar vara så att just din produkt är liksom under ett under luppen av en eller någon orsak. Men varje gång som man säljer sin produkt till en större organisation eller till den till den kontrollerad marknad så kommer frågan att komma upp, då kan man. Ja antingen kan man svara, på frågan om hur hanterar i din data? Hur hanterar din säkerhet? Vad händer om någonting händer? Vem har ansvar för att upprätthålla det? Vem ser till så att ni har rätt typ bra protokoll och kontroller och så de frågorna kommer ju alltid komma. Antingen så är de nya för en varje gång eller så, säger man. Vi följer det här ramverket.
65.	PH	OK och om ett litet företag implementerar samma ramverk som ett stort företag. Blir det någon skillnad på kvaliteten av implementeringen? Att dom mindre företag företagen har mindre anställda, så det blir kanske på något sätt bättre implementerat.

66.	RES3	Det är svårt att faktiskt, och det finns små företag som gör det jättebra. Det finns små företag som är jättedåligt och likadant på stora företagssida. Möjligtvis kan man väl säga att mindre företag har lättare att få en homogen implementation, det vill säga att de är lika bra eller dåliga över hela organisationen. Medan det i större företag kanske så för några jättestarkt implementering i en del och en svag på en annan del.
67.	PH	Och vilka är de viktigaste faktorerna att ta hänsyn till när man ska välja ett ramverk?
68.	RES3	Ja att det hanterbart och hanterbart över tid och att det är relevant för dina kunder eller din marknad.
69.	PH	Och företag brukar inte ha en tendens att kanske välja fel då?
70.	RES3	Nej, nej, det är det inte. Man jobbar i de branscherna och där men befinner sig liksom, så att det brukar inte vara ett problem. Men det händer ju såklart.
71.	PH	Ja det var egentligen alla frågor, är det någonting du vill kommentera eller något vi har missat tycker du?
72.	RES3	Nej, jag tycker det var bra frågor. Kan vara väldigt spännande och jobba med detta. Det blir ganska komplext ganska snart. Men det är också det som gör att man behöver ett ramverk. Och ramverken är smarta höll jag på att säga, de kan alltid göra komplexitet.
73.	MH	Men stort tack så jättemycket.
74.	PH	Tusen tack.

Referenser

Almvide, S. (u.d.) ‘Intervjuteknik - att effektivt använda intervjuer vid kravinsamling’, Qestit. Tillgänglig online: https://www.qestit.se/inspiration-kunskap/intervjuteknik-att-effektivt-anvanda-intervjuer-vid-kravinsamling [Hämtad 12 april 2023].

Alvehus, J. (2019) Skriva uppsats med kvalitativ metod: en handbok. Andra upplagan. Stockholm: Liber AB.

Alshar’e, M. (2023) ‘CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001’, Applied computing Journal, pp. 245–255. Tillgänglig online: https://doi.org/10.52098/acj.202364 [Hämtad 5 april 2023].

Burgess, J.P. (ed.) (2010) The Routledge handbook of new security studies. London ; New York: Routledge (Routledge handbooks).

Cohen, G. (2022) Why Cybersecurity Frameworks Alone Won’t Stop The Next Major Breach, Forbes. Tillgänglig online: https://www.forbes.com/ [Hämtad 11 april 2023].

Conscia. (2021) CIS Controls. Tillgänglig online: https://conscia.com/se/ [Hämtad 12 april 2023].

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014) ‘Defining Cybersecurity’, Technology Innovation Management Review, 4(10), s. 13–21. Tillgänglig online: https://doi.org/10.22215/timreview/835 [Hämtad 30 mars 2023].

Cybersecurity Ventures (2022) 2022 Official Cybercrime Report. Tillgänglig online: https://s3.ca-central-1.amazonaws.com/ [Hämtad 3 april 2023].

Dedeke, A. (2017) ‘Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles’, IEEE Security & Privacy, 15(5), s. 47–54. Tillgänglig online: https://doi.org/10.1109/MSP.2017.3681063 [Hämtad 20 april 2023].

Dimensional Research (2016) CYBERSECURITY FRAMEWORKS AND FOUNDATIONAL SECURITY CONTROLS. Dimensional Research, s. 11. Tillgänglig online: https://static.tenable.com/whitepapers/Tenable_CIS_Survey_Report___Nov_4_2016.pdf [Hämtad 4 maj 2023].

Ension (u.d.) CYBERSÄKERHET, IT-SÄKERHET OCH INFORMATIONSSÄKERHET, Ension. Tillgänglig online: https://ension.se/ [Hämtad 12 april 2023].

ISACA (2022) State of Cybersecurity 2022. Schaumburg: ISACA, s. 40. Tillgänglig online: https://www.isaca.org/ [Hämtad 6 april 2023].

Oates, B.J., Griffiths, M. & McLean, R. (2022) Researching information systems and computing. Andra upplagan. Thousand Oaks: SAGE Publications Ltd.

Podrecca, M. & Sartor, M. (2023) ‘Forecasting the diffusion of ISO/IEC 27001: a Grey model approach’, The TQM Journal, 35(9), pp. 123–151. Tillgänglig online: https://doi.org/10.1108/TQM-07-2022-0220 [Hämtad 25 april 2023].

Razikin, K. & Soewito, B. (2022) ‘Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework’, Egyptian Informatics Journal, 23(3), pp. 383–404. Tillgänglig online: https://doi.org/10.1016/j.eij.2022.03.001 [Hämtad 20 april 2023].

Ryerse, J. (2023) Top 11 cybersecurity frameworks in 2023, CONNECTWISE. Tillgänglig online: https://www.connectwise.com/blog/cybersecurity/11-best-cybersecurity-frameworks [Hämtad 11 april 2023].

Sanou, B. (2017) Global Cybersecurity Index (GCI) 2017. ITU, s. 65. Tillgänglig online: https://www.itu.int/dms_pub.pdf [Hämtad 28 mars 2023].

Saritac, U., Liu, X. & Wang, R. (2022) ‘Assessment of Cybersecurity Framework in Critical Infrastructures’, in 2022 IEEE Delhi Section Conference (DELCON). 2022 IEEE Delhi Section Conference (DELCON), New Delhi, India: IEEE, pp. 1–4. Tillgänglig online: https://doi.org/10.1109/DELCON54057.2022.9753250. [Hämtad 20 april 2023]

Segal, E. (2022) Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report, Forbes. Tillgänglig online: https://www.forbes.com/sites/edwardsegal/ [Hämtad 28 mars 2023].

Sosafe (2023) Cybercrime Trends 2023. Cologne: SoSafe, s. 33. Tillgänglig online: https://lp.sosafe.de/ [Hämtad 6 april 2023].

Stafström, S. (2017) GOD FORSKNINGSSED. Stockholm: Vetenskapsrådet, s. 81. Tillgänglig online: https://www.vr.se/God-forskningssed_VR_2017.pdf [Hämtad 12 april 2023].

Taherdoost, H. (2022) ‘Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview’, Electronics, 11(14), s. 2181. Tillgänglig online: https://doi.org/10.3390/electronics11142181 [Hämtad 14 april 2023].

The Council of Economic Advisers (2018) The Cost of Malicious Cyber Activity to the U.S. Economy. The Council of Economic Advisers, s. 60. Tillgänglig online: https://trumpwhitehouse.archives.gov/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf [Hämtad 26 mars 2023].

Tyas Tunggal, A. (2023) ‘What are the CIS Controls for Effective Cyber Defense?’, UpGuard. Tillgänglig online: https://www.upguard.com/blog/cis-controls [Hämtad 6 april 2023].

Yin, R. K. (2013). Kvalitativ forskning från start till mål. Första upplagan. New York: The Guilford Press.