Examensarbete

HÖGSKOLAN I SKÖVDE

En balans mellan cybersäkerhetskrav och projektmål inom IT-konsultbranschen

A Balance Between Cybersecurity Requirements and Project Goals in the IT Consulting Industry

Examensarbete för kandidatexamen med huvudområdet företagsekonomi

Grundnivå 15 högskolepoäng

Vårtermin 2025

Studenter: Amanda Fredman

Linn Jutéus

Handledare: Annica Bragsjö Hultén

Examinator: Mikael Wickelgren

Intyg

En balans mellan cybersäkerhetskrav och projektmål inom IT-konsultbranschen
Examensrapport inlämnad av Amanda Fredman och Linn Jutéus till Högskolan i Skövde, för Kandidatexamen (BSc) vid Institutionen för handel och företagande.

2025-05-16

Härmed intygas att allt material i denna rapport, vilket inte är vårt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Amanda Fredman Linn Jutéus

Signerat: _____

√ Jag/vi har använt AI-verktyg för språkkorrigering.

√ Jag/vi har <u>inte</u> använt AI-verktyg för textgenerering i examensrapporten.

Förord

Detta examensarbete har genomförts som en avslutande del av vår utbildning inom Handelsekonomiprogrammet vid Högskolan i Skövde, och vi vill rikta ett varmt tack till alla som har stöttat oss under arbetets gång.

Vi vill särskilt tacka vår handledare Annica Bragsjö Hultén för vägledning, konstruktiv återkoppling och engagemang genom hela processen. Ett stort tack riktas även till vår examinator Mikael Wickelgren för värdefulla synpunkter som har hjälpt oss att fördjupa och utveckla vårt arbete.

Vi vill också uttrycka vår tacksamhet till de projektledare inom IT-konsultbranschen som tog sig tid att medverka i våra intervjuer. Deras insikter och erfarenheter har varit ovärderliga för studiens resultat och kvalitet.

Slutligen vill vi tacka våra nära och kära för tålamod och uppmuntran under denna intensiva period.

Skövde, maj 2025

Amanda Fredman

Linn Jutéus

Sammanfattning

I takt med digitaliseringens framfart har cybersäkerhet blivit en central fråga inom projektledning, särskilt inom IT-konsultbranschen. Syftet med denna studie är att undersöka hur nya cybersäkerhetskrav påverkar projektens grundläggande parametrar, tid, kostnad och omfattning, samt hur dessa krav kan hanteras effektivt inom agila, vattenfallsstyrda och hybridbaserade projekt. Studien bygger på kvalitativa intervjuer med projektledare inom IT-konsultbranschen, och analyseras med stöd av projekttriangeln och aktuella teorier om cybersäkerhet i olika projektmiljöer. Resultaten visar att påverkan från cybersäkerhetskrav varierar beroende på metodval, kompetensnivå och organisatorisk mognad. Kraven kan fungera både som hinder och stöd, beroende på när de integreras i processen, hur de prioriteras och vilket synsätt som råder i projektgruppen. En viktig slutsats är att cybersäkerhet inte längre kan ses som ett separat teknikområde, utan bör förstås som en strategisk och integrerad del av modern projektstyrning. Studien belyser också hur säkerhetsambitioner bör balanseras, exempelvis med stöd av 80/20-regeln, samt hur den mänskliga faktorn både kan utgöra en sårbarhet och en tillgång i projektens säkerhetsarbete.

Nyckelord

Cybersäkerhet, projektledning, IT-konsultverksamhet, agil metod, vattenfallsmodell, hybridmodell, projekttriangel, IT, säkerhetskrav

Abstract

As digital transformation accelerates, cybersecurity has become a key issue in project management, particularly in the IT consulting sector. This study aims to explore how new cybersecurity requirements affect the three core project parameters, time, cost, and scope, and how these requirements can be effectively managed within agile, waterfall, and hybrid projects. The research is based on qualitative interviews with project managers in the IT consulting industry, and the analysis is framed using the project management triangle and contemporary cybersecurity theory. Findings indicate that the impact of cybersecurity requirements varies depending on methodological approach, organizational maturity, and competence levels. These requirements can act as both barriers and enablers, depending on when they are introduced, how they are prioritized, and how well integrated they are in the project process. A key conclusion is that cybersecurity should no longer be treated as a separate technical issue, but as a strategic and embedded component of modern project governance. The study also highlights the importance of balancing security efforts, using, for instance, the 80/20 principle, and considers the human factor as both a potential vulnerability and a valuable resource in managing security within projects.

Keywords

Cybersecurity, project management, IT consulting, agile methodology, waterfall model, hybrid model, project triangle, IT, security requirements

Innehållsförteckning

1. Inledning 1
1.1. Problembakgrund 1
1.1.1. Cybersäkerhet: Risker och affärsmässiga utmaningar 1
1.1.2. Cybersäkerhetskrav och lagverk 2
1.1.3. Specifika utmaningar för projekt inom IT-konsultbranschen 3
1.1.4. Identifiering av problem och kunskapsluckor 5
1.2. Syfte 5
1.2.1. Forskningsfrågor 5
1.3. Disposition 6
2. Teoretisk referensram och tidigare studier 7
2.1. Projektstyrningsmetoder och projekttriangeln 7
2.1.1. Agila metoder 9
2.1.1.1. Aspekter på cybersäkerhet inom agila metoder 10
2.1.2. Vattenfallsmodellen 13
2.1.2.1. Aspekter på cybersäkerhet inom vattenfallsmodellen 15
2.2.3. Agila metoder vs. vattenfallsmodellen: När fungerar den ena bättre än den andra? 16
2.2.4. Cybersäkerhet i praktiken 19
3. Metod 22
3.1. Metodval 22
3.2. Analysmodell 23
3.2.1. Operationaliseringar 26
3.3. Datainsamling 27
3.3.1. Urval 27
3.3.2. Sökstrategi och urval av sökord 30
3.4. Metodkritik 30
3.4.1. Giltighet/trovärdighet 30
3.4.2. Käll- och litteraturkritik 31
3.5. Etiska överväganden 33
3.6. Kvalitetssäkring av språk 34

4. Empiri 35
4.1. Påverkan på tid, kostnad och omfattning 35
4.2. Cybersäkerhetskrav som hinder eller stöd 36
4.3. Kompetens och hantering av kunskapsbrister 38
4.4. Dataintegritet och efterlevnad av regelverk 40
4.5. Agilt och vattenfall: Likheter och skillnader i hantering 42
4.6. Strategier och framtida behov 44
5. Analys 47
5.1. Cybersäkerhetskravens inverkan på projekttriangeln 47
5.2. Hantering av säkerhetskrav i agilstyrda projekt 49
5.3. Hantering av säkerhetskrav i vattenfallsstyrda projekt 51
5.4. Hybridmodellens möjligheter och begränsningar 52
6. Diskussion 55
6.1. Reflektion och argumentation 55
6.2. Besvarande av forskningsfrågorna 58
7. Slutsats 60
7.1. Praktiska och teoretiska bidrag 61
7.2. Begränsningar 62
7.3. Förslag på vidare forskning 64
8. Referenser 65
Bilaga 1: Intervjufrågor 73
Bilaga 2: Ordförklaring 75
Bilaga 3: Individuella reflektioner 80

Figurförteckning

Figur 1 Projekttriangeln 8
Figur 2 Agil iterationsflöde 9
Figur 3 Översikt över ramverkets steg och aktiviteter 11
Figur 4 Vattenfallsmodellen 14

1. Inledning

Följande kapitel presenterar bakgrunden till studiens problemområde. I följd presenteras kunskapsluckor, studiens syfte och frågeställning. Vi avslutar kapitlet med att presentera studiens disposition.

1.1. Problembakgrund

1.1.1. Cybersäkerhet: Risker och affärsmässiga utmaningar

I dagens digitala miljö finns det risker med att använda personliga uppgifter online, vilket gör det viktigt att öka medvetenheten avseende detta. Den ökande användningen av internet och digitala enheter har bidragit till en ökad oro kring hur företag hanterar kunders personliga uppgifter. Bristen på medvetenhet kan resultera i negativa konsekvenser, exempelvis stöld av personliga uppgifter. Dataskydd samt integritet är av stor relevans eftersom personliga enheter kan äventyras i form av skadliga koder och nätfiske (Ihsan et al., 2023).

I takt med att artificiell intelligens (AI) revolutionerar affärsvärlden, står företag inför nya och komplexa utmaningar, särskilt när det gäller tilliten till att överlåta beslutsfattandet från människor till maskiner. I en studie av Balcıoğlu et al. (2024), som analyserade 263 hållbarhetsrapporter från 41 ledande amerikanska företag under åren 2014-2022, belyses både hur AI kan bidra till hållbarhetsarbete, och de risker som uppstår när företag alltmer tar stöd av beslutsfattandet till automatiserade system. Resultaten i studien visar att företag fokuserar på två huvudsakliga områden vid implementering av AI: Optimering av affärsprocesser och förbättring av hållbara metoder. Företag använder AI för att effektivisera och förbättra interna verksamhetsprocesser. Det kan innebära automatisering av uppgifter, förbättrad databehandling, effektivare resursanvändning och bättre beslutsfattande, vilket leder till ökad produktivitet och kostnadsbesparingar. AI används också för att stödja företagets hållbarhetsmål, såsom att minska koldioxidutsläpp, optimera energianvändning, hantera avfall mer effektivt och förbättra sociala aspekter, exempelvis arbetsmiljö och mångfald. AI möter dock etiska utmaningar på grund av integritetsproblem (Balcıoğlu et al., 2024).

Det finns möjligheter såväl som utmaningar att använda sig av AI, särskilt vid hantering av stora datamängder och personuppgifter. Därav är det viktigt att förordningar följs kring dataskyddstandarder och lagar, såsom ISO 27000 och GDPR för att hantering av personuppgifter är säkert och lagligt. Det finns ett behov av att ta hänsyn till olika tolkningar av lagar och förordningar, eftersom det ännu inte existerar helt etablerade standarder för användning och utveckling av AI. Detta är en svår utmaning eftersom AI är i ständig utveckling och det är outforskat hur AI kommer att påverka till exempel integritetsregler framöver (International Organization for Standardization, n.d.; Norstedts Juridik, 2024).

AI är ett effektivt verktyg att använda vid analysering och bearbetning av större mängder data, eftersom AI kan bearbeta information snabbt och identifiera samband. Det finns flera delområden inom AI, såsom maskininlärning vilket innebär att modellen hela tiden utvecklas samt har förmågan att bli bättre genom lärdomar. Ökad datatillgång möjliggör en mer avancerad utveckling av AI-system (Karlsson & Hugo, 2022).

AI-användningen väcker flera säkerhetsrelaterade frågor, särskilt när det gäller hur data hanteras. Vem har egentligen tillgång till den information som delas i AI-chattar? Varifrån hämtar stora språkmodeller (LLM) sin data? När AI-system dessutom börjar ta över arbetsmoment, utan att vara fullständigt testade, uppstår nya säkerhetsutmaningar. På längre sikt väcks även frågor om kontroll och riskhantering kopplat till artificiell generell intelligens (AGI), där AI potentiellt kan överträffa mänsklig intelligens (Adriko & Nurse. 2024; Holmlund, 2024; IBM, 2023; Mankertz, 2023).

1.1.2. Cybersäkerhetskrav och lagverk

I dagens moderna samhälle har allt flera företag genomgått en digital transformation, och deras produkter har fått avancerade digitala funktioner. Det har resulterat i att företag och produkter blivit alltmer sårbara för cyberattacker (Europeiska unionens parlament, 2022).

Under Covid-19 pandemin blev det tydligt att skydd mot cyberhot blivit avgörande för att samhället ska fungera, eftersom cyberattacker kan vara mycket kostsamma. Europakommissionen uppskattar att den årliga kostnaden för cyberbrott i slutet av 2020,

uppgick till 5,5 biljoner euro för den globala ekonomin. De ökade cyberhoten har lett till att lagstiftning har införts för att stärka skyddet av personlig integritet och hantera säkerhetsrisker (Europeiska unionens parlament, 2022).

Cybersäkerhetskrav blir alltmer omfattande och föränderliga, vilket påverkar hur företag och organisationer hanterar informationssäkerhet. Inom EU har regelverk som GDPR och NIS-direktivet införts för att stärka dataskydd och cybersäkerhet. GDPR, som trädde i kraft 2018, reglerar hur personuppgifter får hanteras, medan NIS-direktivet syftar till att säkerställa en hög säkerhetsnivå inom nätverk och informationssystem (Riksdagen, 2023).

År 2025 ersätts NIS-direktivet av NIS2, som inför skärpta krav på cybersäkerhet, rapportering och riskhantering. Direktivet kommer att omfatta fler sektorer och ge tillsynsmyndigheter ökade befogenheter för att stärka säkerheten inom både privat och offentlig verksamhet. För att möta dessa krav kan företag behöva genomföra riskanalyser och förstärka sina säkerhetsåtgärder (Myndigheten för samhällsskydd och beredskap, 2024a; Myndigheten för samhällsskydd och beredskap, 2024b; Myndigheten för samhällsskydd och beredskap, 2024c; Canea, n.d.).

För att hantera nya cybersäkerhetskrav används internationella ramverk och standarder, såsom ISO 27000-serien och NIST SP 800-30, vilket ger riktlinjer för riskhantering och informationssäkerhet. Dessa ramverk kan fungera som stöd för företag och organisationer i arbetet med att uppfylla kommande krav och skapa en mer motståndskraftig cybersäkerhetsstrategi (International Organization for Standardization, n.d.; Setiawan et al., 2017).

1.1.3. Specifika utmaningar för projekt inom IT-konsultbranschen

Den ökande användningen av AI inom olika sektorer har medfört att cybersäkerhet blivit avgörande för att skydda känsligt data. Den snabba förändringstakten och behovet av kundanpassning inom konsultbranschen kräver en effektiv implementering av cybersäkerhetskrav i projekt. Kraven som styr hur projektledare får arbeta i projektet kan till exempel röra sig om var projektdokumentation får sparas (i molnet, på egen server,

eller på egen PC) eller krav på att alla projektmedlemmar måste säkerhetsprövas. Vid projektledning behöver projektledarna säkerställa att projektet uppfyller branschspecifika standarder och kundens säkerhetskrav, såväl som att det existerar lagar som måste följas. Konsultbranschen präglas av innovation och krav på snabb anpassning till kundernas behov. Vid projektledning måste konsultbranschen navigera denna dynamik samtidigt som det kan komma uppdaterade cybersäkerhetskrav, vilket utgör en kontinuerlig utmaning för konsultföretag och projektledare att förbli konkurrenskraftiga på marknaden (Holmlund, 2024; Mankertz, 2023).

En central utmaning för företag är att kontinuerligt hålla sig uppdaterade i den tekniska utvecklingen inom cybersäkerhet. Cyberhot finns ständigt, och nya metoder för att kompromettera säkerhetssystem upptäcks regelbundet, vilket kräver att företag proaktivt och kontinuerligt anpassar och utvecklar sina lösningar (Europeiska unionens parlament, 2022; Ritter & Pedersen, 2020). Vid projekt krävs det strategier för att identifiera och hantera cybersäkerhetsrisker som kan vara till hot för projektets framgång samt företagets rykte, eftersom cybersäkerheten i deras tjänster är en nyckelkomponent i att upprätthålla förtroendet hos kunder (Holmlund, 2024).

Implementering av cybersäkerhetsåtgärder kräver en ekonomisk investering, såsom investeringar i teknik, utbildning och processer. Därav måste projektledare planera samt prioritera budgeten för att säkerställa ett projekts lönsamhet samt ser till att det stödjer verksamhetens mål. Detta resulterar i höga förväntningar på kvalitet och säkerhet i deras tjänster, där utmaningen för projektledare är att integrera nya cybersäkerhetskrav under projektets gång (Felici et al., 2015).

För att hantera dessa utmaningar behöver projektledare skapa en strategi, utifrån vald projektstyrningsmodell, som stödjer både cybersäkerhetskrav och affärsmål. Oavsett om metoden är agil eller mer traditionell, som vattenfallsmodellen, är målet att uppnå hållbara projektstyrningsmetoder samtidigt som projektets kvalitet, dvs. tid, kostnad och omfattning, balanseras (Ceyda et al., 2023).

1.1.4. Identifiering av problem och kunskapsluckor

Det finns kunskapsluckor avseende projekt och utvecklingen av cybersäkerhetskraven, vilket gör det väsentligt att analysera hur dessa krav påverkar projektets genomförande och framgång för konsultföretag (Lucky et al., 2024). Eftersom AI-teknologi utvecklas i snabb takt och integreras i allt fler verksamhetsområden, ökar behovet av en detaljerad förståelse för hur säkerhetskrav kan anpassas och hanteras i projekt (Balcıoğlu et al., 2024). Detta avser särskilt de hanteringsstrategier som tillämpas i agila respektive vattenfallsstyrda projekt, i syfte att säkerställa en effektiv projektstyrning (Ceyda et al., 2023). Att identifiera och fylla dessa kunskapsluckor är avgörande för att projekt ska kunna möta dagens- och framtida cybersäkerhetsutmaningar. Genom att förstå och hantera förändrade cybersäkerhetskrav på ett effektivt sätt kan IT-konsultföretag förbättra sin riskhantering, öka konkurrenskraften samt undvika kostsamma säkerhetsincidenter i projekt (Lucky et al., 2024). Finns det en optimal balans mellan cybersäkerhet och projektmål?

1.2. Syfte

Syftet med studien är att analysera hur nya cybersäkerhetskrav kan påverka projektets tid, kostnad och omfattning. Studien analyserar dessutom hur dessa nya krav kan hanteras effektivt av projektledare i agila respektive vattenfallsstyrda projekt. Studien fokuserar på IT-konsultbranschen, en bransch som präglas av snabb förändring och högt ställda krav på anpassningsförmåga. Resultaten syftar till att bidra med insikter som kan stödja IT-konsultföretag och projektledare i att utveckla mer hållbara och flexibla projektstyrningsmetoder för implementeringen av nya cybersäkerhetskrav.

1.2.1. Forskningsfrågor

F1: *Hur kan nya cybersäkerhetskrav påverka tid, kostnad och omfattning för projekt?*

F2: *Hur kan nya cybersäkerhetskrav effektivt hanteras av projektledare i agila respektive vattenfallsstyrda projekt?*

1.3. Disposition

Studien inleds med *kapitel 1*, där bakgrund, problemformulering, syfte och forskningsfrågor presenteras. *Kapitel 2* redogör för den teoretiska referensram som ligger till grund för analysen, med fokus på projektstyrningsmetoder, projekttriangeln och cybersäkerhet i olika projektmiljöer. I *kapitel 3* beskrivs studiens metod, inklusive metodval, analysmodell, datainsamling, metodkritik, etiska överväganden och kvalitetssäkring av språk.

Kapitel 4 innehåller empirin, där resultatet från intervjuer med projektledare i IT-konsultbranschen presenteras tematiskt. I *kapitel 5* följer analysen, där empirin tolkas och kopplas till teorin, med särskild fokus på hur cybersäkerhetskrav påverkar tid, kostnad, omfattning och hanteras i olika projektmetodiker.

Kapitel 6 består av en diskussion där resultatet reflekteras utifrån ett bredare perspektiv, inklusive reflektion kring studiens resultat och ett konkret svar på studiens forskningsfrågor. Studien avslutas med *kapitel 7*, där studiens slutsatser och bidrag, såväl teoretiska som praktiska, sammanfattas, samt begränsningar med studien och framtida implikationer.

2. Teoretisk referensram och tidigare studier

Följande kapitel presenterar studiens teoretiska referensram. Först redogörs teori om "projektstyrningsmetoder" och "projekttriangeln". Därefter presenteras "agila metoder" och "vattensfallsmodellen", samt en djupare inblick på cybersäkerhetskrav inom respektive metodik. Sedan presenteras en jämförelse mellan dessa metoder samt ett tillägg av en hybridmodell. Kapitlet avslutas med cybersäkerhet i praktiken.

2.1. Projektstyrningsmetoder och projekttriangeln

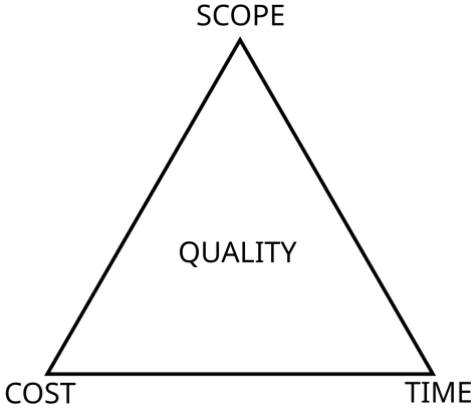
Mjukvaruprojekt är specialiserade projekt som kräver särskilda hanteringsmetoder på grund av sitt innehåll. Till skillnad från andra projekt, där slutprodukten har en fysisk form, är resultatet av mjukvaruprojekt abstrakt och baserat på intellektuella processer. Detta gör det svårare att beräkna resursanvändning och kostnader, vilket leder till en högre risk för misslyckande på grund av osäkerheter (Ceyda et al., 2023).

Faserna som en mjukvaruprodukt genomgår, från utveckling till kundanvändning, kallas för programvarans livscykel. Software Development Life Cycle (SDLC) fokuserar på processer som omvandlar krav till färdig programvara, medan Software Product Lifecycle (SPLC) inkluderar även konfigurationshantering, kvalitetskontroll samt processer för drift, underhåll, support och avveckling. Det finns ingen strikt tidsmässig ordning mellan utvecklingsprocesserna, utan livscykelmodeller såsom SDLC och SPLC skapar strukturen för processernas sekvens och interaktion (Ceyda et al., 2023).

Olika projektstyrningsmetoder kan tillämpas för att styra projekt inom mjukvaruutveckling, såsom agila metoder och vattenfallsmodellen. Valet av metod beror på faktorer som projektets storlek, produkttyp, kundens struktur och affärsområdet, och det finns ingen enskild modell som generellt accepteras som standard. Dessa modeller utgör en del av de övergripande ledningsprocesserna, vilka syftar till att styra och samordna projekt genom hela dess livscykel. Framgång i mjukvaruprojekt bedöms ofta med hjälp av projekttriangeln (Ceyda et al., 2023).

Projekttriangeln beskriver de grundläggande aspekterna av projektledning: tid (time), kostnad (cost) och omfattning (scope). En central princip i projekttriangeln är att dessa tre hörn är sammanbundna och påverkar kvaliteten (quality). Det resulterar i att en

förändring i någon av dem alltid påverkar minst en av de andra. Att hitta en balans mellan dessa faktorer för att nå framgång, utgör en av de största utmaningarna inom projektledning (Tonnquist, 2018).



Figur 1 Projekttriangeln

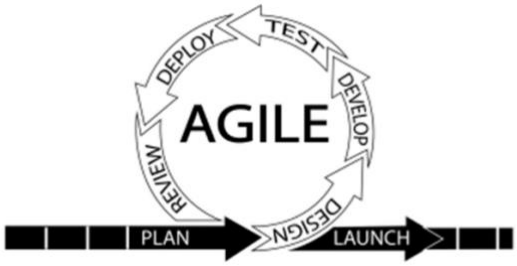
I situationer där tidsplanen behöver kortas ner och projektet ska levereras tidigare kan det krävas att resurserna förstärks, såsom att fler medarbetare sätts in. Ett annat alternativ är att minska projektets omfattning, vilket innebär att reducera antalet funktioner eller krav, för att göra arbetet mindre omfattande och lättare att slutföra innan den nya deadlinen. Att hålla sig till den planerade budgeten innebär att kostnaderna måste hållas inom ramarna. Om kostnaderna överskrider den planerade budgeten, kan åtgärder vidtas, såsom att minska användningen av resurser och undvika övertid, för att hålla kostnaderna under kontroll. I situationer där fler funktioner och krav läggs till, exempelvis att omfattningen ökar, kan det krävas en förlängning av tidsplanen, eftersom teamet behöver mer tid att genomföra det utökade arbetet. Ett annat alternativ är att utöka resurserna, vilket ökar kostnaderna. I en del projekt kan både kostnader och tidsplanen behöva justeras för att hantera den ökade omfattningen (Tonnquist, 2018).

Den fjärde aspekten i triangeln är kvalitet, vilket betraktas som triangelns mittpunkt. Kvaliteten påverkas av varje förändring i de tre hörnen. Om en förändring sker i tid, kostnad eller omfattning blir kvaliteten på slutprodukten nästan alltid påverkad. Exempelvis om tidsplanen kortas ner kan det resultera i en försämrad kvalitet, eftersom teamet haft mindre tid att genomföra noggranna tester eller detaljerad utveckling. Minskar budgeten kan det resultera i att kompromissa resurser eller använda billigare material. Detta kan påverka både produktens hållbarhet och prestanda. Ökar omfattningen utan att

tidsplanen eller budgeten justeras kan kvaliteten bli sämre, eftersom teamet kan bli överbelastade och behöva kompromissa med noggrannheter i sitt arbete (Tonnquist, 2018).

2.1.1. Agila metoder

Agila metoder är populära inom mjukvaruutveckling eftersom de fokuserar på flexibilitet genom att dela upp projektets arbete i mindre delar, vilket möjliggör kontinuerliga utvärderingar, anpassningar utifrån projektets behov och snabba leveranser. Projektet utvecklas stegvis och i återkommande cykler, där varje cykel bygger vidare på den föregående och förbättras baserat på feedback som illustreras i *Figur 2* (Ceyda et al., 2023).



Figur 2 Agil iterationsflöde

Projektteamet avgör själva hur arbetet bäst ska utföras med hänsyn till tillgängliga resurser och begränsningar, vilket främjar effektivitet och flexibilitet. De mest kritiska uppgifterna prioriteras först och projektteamet måste slutföra de tilldelade uppgifterna inom en fastställd tid för varje cykel, vilket bidrar till en smidig arbetsprocess och effektivt samarbete (Ceyda et al., 2023).

De mest typiska agila verktyg som stödjer agila metoder är Scrum, Kanban och SAFe (Dean Leffingwell, n.d; Liubimov et al., 2023). Kanban är ett system som används i syfte att hjälpa team hitta en balans mellan arbetet de behöver utföra samt tillgängligt kapital. Strukturen är uppbyggd runt Kanban-tavlor, som möjliggör att team bättre kan förstå sin arbetsbelastning samt sitt arbetsflöde. Arbetet visas i en projekttavla som är organiserad i en kolumn, exempelvis “att göra”, “pågående” och “klart”. Kolumnerna flyttas vidare tills de är slutförda (Shania et al., 2024). Scrum är en struktur i syfte att hjälpa team att samarbeta och att effektivt utföra arbete. Denna struktur ger en samlad bild över

värderingar, roller samt riktlinjer för att stödja teamet att fokusera på iterationer och ständig förbättring. Scrum genomförs vanligtvis i sprintar, det vill säga tidsbegränsade arbetsperioder, där en sprint exempelvis kan pågå i två veckor och avslutas med en förväntad leverans. Det är även vanligt med scrummöten, vilket är dagliga möten där scrumteamet samlas under 15 minuter och går igenom dagens aktiviteter. När sprinten är över organiserar scrummästaren en sprintåterblick, där teamet har möjligheter att reflektera över arbetet samt justera inför kommande sprintar (Yahya et al., 2024). Inom mjukvaruprojekt integreras design och kodning parallellt med varandra, vilket innebär att istället för att först slutföra hela designen innan kodningen startar, utvecklas designen gradvis i takt med att funktioner byggs och testas (Thummadi & Lyytinen, 2020). SAFe är en struktur som syftar till att stödja stora organisationer i att skala upp agila arbetssätt genom att samordna flera team, program och portföljer. Ramverket innehåller tydliga roller, ceremonier och arbetsflöden och bygger på principer från både Lean och agila metoder. Arbetet delas ofta in i så kallade Agile Release Trains (ARTs), vilket innebär planering och leverans i större iterationer på programnivå (Dean Leffingwell, n.d.).

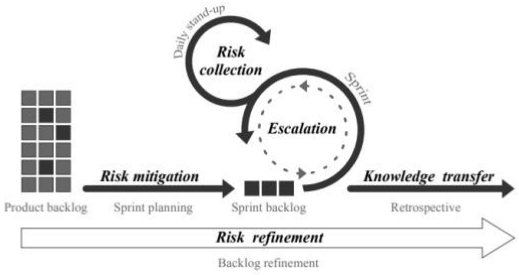
Vid projekt där agila metoder används spenderas mindre tid på att hantera krav i de tidiga faserna, vilket möjliggör snabbare cykler och en tidigare leverans av funktionella delar av produkten (Thummadi & Lyytinen, 2020). Avseende kostnad är agila metoder mycket kostnadseffektiva eftersom de fokuserar på iterativ utveckling, vilket minskar risken för kostsamma fel och gör det möjligt att anpassa sig till förändrade krav utan betydande kostnadsökningar (Thummadi & Lyytinen, 2020). Agila metoder betonar anpassningsförmåga, vilket gör det möjligt att kontinuerligt justera projektets omfattning baserat på feedback från kunder och förändrade krav. Detta säkerställer att de mest värdefulla funktionerna prioriteras (Thummadi & Lyytinen, 2020).

2.1.1.1. Aspekter på cybersäkerhet inom agila metoder

Företag måste kontinuerligt och proaktivt anpassa samt uppdatera sina säkerhetslösningar eftersom cyberhot ständigt utvecklas och nya metoder för att kompromettera säkerhetssystem regelbundet upptäcks (Europeiska unionens parlament, 2022; Ritter & Pedersen, 2020). För att implementera cybersäkerhetsåtgärder krävs ekonomiska investeringar i teknik, utbildning och processer. Företag behöver därför planera och prioritera sin budget noggrant för att säkerställa både projektets lönsamhet och att det

stöder verksamhetens övergripande mål (Felici et al., 2015). Agila metoder bygger dock på flexibilitet och kontinuerliga justeringar, vilket kan skapa en konflikt med traditionell budgetplanering, särskilt när det avser hantering och uppdatering av säkerhetskrav och riskhantering i den snabba förändringstakten i konsultbranschen (Mankertz, 2023; Salin & Lundgren, 2022).

Ett agilt ramverk för cybersäkerhetsriskhantering, illustrerat i *Figur 3,* består av fem steg, med efterföljande aktiviteter som är utformade för att stödja en iterativ och flexibel hantering av cybersäkerhetsrisker utan att överbelasta utvecklingsprocessen (Salin & Lundgren, 2022).



Figur 3 Översikt över ramverkets steg och aktiviteter

Det första steget, riskinsamling (risk collection), fokuserar på att identifiera och dokumentera nya cybersäkerhetsrisker som är aktuella i uppstartsskedet. Detta sker genom dagliga stand-up-möten, korta möten, där aktuella risker granskas. Riskobjekt skapas genom snabba bedömningar med hjälp av statiska kodanalysverktyg, det vill säga verktyg som automatiskt granskar källkod utan att köra programmet. De mest kritiska riskerna prioriteras och hela processen ska vara snabb och effektiv, vilket innebär att endast en grundläggande bedömning genomförs i detta steg, snarare än en djupgående analys (Salin & Lundgren, 2022).

Det andra steget, riskförfining (risk refinement), syftar till att genomföra en djupare analys av de identifierade riskerna och anpassa utvecklingsprioriteringarna. Detta sker som en regelbunden process där genomgångar av riskbackloggen, en prioriterad lista över potentiella risker i projektet, under backloggförädling (backlog refinement), sker antingen veckovis eller varannan vecka. Riskobjekt kan även omprioriteras efter en mer omfattande analys, och varje riskobjekt ska dokumenteras med en beskrivning samt ett

förslag på åtgärd. Dessa åtgärder ska kopplas till befintliga krav eller generera nya krav. Efter detta ska riskobjekten vara redo för sprintplanering, där teamet tillsammans planerar innehållet och upplägget för den kommande sprinten/arbetsperiod, och säkerhetskraven i backloggen ska vara uppdaterade, exempelvis genom utveckling av kod, processer eller verktyg för att stärka cybersäkerheten (Salin & Lundgren, 2022).

Det tredje steget, riskreducering (risk mitigation), omfattar att genomföra åtgärder för att minska cybersäkerhetsrisker. Detta görs genom sprintplanering, där riskrelaterade åtgärder inkluderas i sprintmålen/arbetsmålen. Dessutom genomförs de beslutade åtgärderna, såsom kodändringar, införande av nya processer och kunskapsdelning inom teamet. Varje åtgärd definieras med vad som ska göras och hur den ska testas. Vid behov genomförs även säkerhetsaktiviteter, såsom hotmodellering (en systematisk metod för att identifiera och analysera potentiella säkerhetshot mot ett system i ett tidigt skede) och kodgranskning. Efter detta har riskerna hanterats genom åtgärder och validerats genom tester för att säkerställa att de förbättrar cybersäkerheten (Salin & Lundgren, 2022).

Det fjärde steget, kunskapsöverföring (knowledge transfer), fokuserar på att sammanställa och sprida lärdomar kring cybersäkerhet inom teamet. Detta sker genom att identifiera lärdomar från genomförda riskreduceringar samt dokumentera viktiga insikter i en gemensam kunskapsbas. Dessutom kan företag arrangera och genomföra introduktioner till lågintensiv träning inom säkerhetsaktiviteter, alternativt att säkerhetsexperter bjuds in till diskussioner. Detta leder till förbättrad cybersäkerhetskompetens inom teamet och dokumenterade insikter som kan användas för framtida referenser (Salin & Lundgren, 2022).

Det femte steget, eskalering (escalation), syftar till att rapportera kritiska risker till intressenter och ledning. Detta inkluderar regelbunden rapportering av högriskobjekt minst en gång per vecka samt uppföljning av eskalerade risker för att säkerställa att resurser allokeras korrekt. Detta leder till ökad medvetenhet och bättre hantering av kritiska säkerhetsrisker samt en mer effektiv resursfördelning och riskprioritering (Salin & Lundgren, 2022).

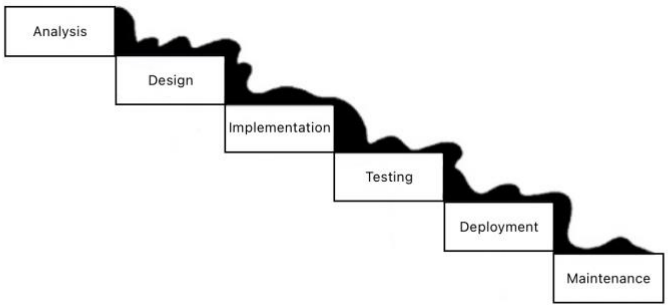
Ramverkets fem steg och aktiviteter visar hur cybersäkerhet kan integreras i agila processer utan att hämma utvecklingstakten. Genom en iterativ och strukturerad riskhantering säkerställs att säkerhetsåtgärder blir en naturlig del av arbetet, vilket stärker både systemets skydd och teamets kompetens. Dessutom möjliggör det en balans mellan flexibilitet och säkerhet i en alltmer digitaliserad och cyberhotad miljö (Salin & Lundgren, 2022).

2.1.2. Vattenfallsmodellen

Den äldsta och mest grundläggande metod inom projektledning är vattenfallsmodellen. Modellen består av att komplettera olika delar sekventiellt och därmed bilda en helhet. Efter att en fas har slutförts, övergår processen till nästa steg. I den här modellen fungerar resultatet av en fas som input till den följande, genom bland annat kravanalys, kodning, design, samt enhetstest (Ceyda et al., 2023).

Den sekventiella strukturen i vattenfallsmodellen har även lagt grunden för flera andra projektledningsmetoder som används i praktiken. En av dessa är PPS (Praktisk ProjektStyrning), en projektledningsmodell som stödjer vattenfallsmodellen och hjälper företag att planera, leda och genomföra projekt och program. Den baseras på praktiska erfarenheter, följer internationella standarder och erbjuder en helhetslösning från strategi till genomförande. Tydlig ansvarsfördelning och kommunikation är centrala delar av modellen (Utbildning.se, n.d.). En annan projektmodell som bygger på Vattenfallsmodellen är PROPS (Projekt för Projektstyrning), utvecklad av Ericsson för att skapa en mer strukturerad och effektiv projektstyrning. Modellen är fasindelad och innehåller tydliga roller, beslutsgrindar och riskhantering för att säkerställa att projekt genomförs framgångsrikt och når sina mål (Harmonit, n.d.).

Vattenfallsmodellen lämpar sig bäst för projekt där kraven är tydligt definierade från början och förväntas förbli stabila genom hela utvecklingsprocessen. Det är även fördelaktigt att använda sig av vattenfallsmodellen i långsiktiga projekt där det finns en tydlig plan och varje fas kan planeras noggrant innan det påbörjas. Ett exempel är inom statliga eller medicinska projekt där det är viktigt att varje steg måste granskas noggrant och dokumenteras (Sinha & Das, 2021).



Figur 4 Vattenfallsmodellen

Utvecklingsprocessen inom vattenfallsmodellen sker i en tydlig uppdelning faser såsom kravanalys (anaysis), design (design), implementering (implementation), testning (testing), driftsättning (deployment), och underhåll (maintenance). En grundregel i den här modellen är att varje fas ska vara avslutad och dokumenterad innan nästa kan påbörjas, vilket resulterar i en linjär arbetsgång med minimal osäkerhet (Thummadi & Lyytinen, 2020).

Modellen är framställd för att säkerställa en tydlig arbetsprocess där design och kodning separeras. Kodning får inte påbörjas förrän designfasen är färdig. Därav är vattenfallsmodellen speciellt användbar för projekt med stabila krav samt en förutsägbar utvecklingsmiljö. Den sekventiella ordningen minskar risken för att arbetsmoment hoppar fram och tillbaka, vilket annars kan leda till ineffektivitet. Styrkan i vattenfallsmodellen ligger i dess förutsägbarhet samt tydliga struktur. Dock finns det en del begränsningar, exempelvis att flexibiliteten är låg när oväntade hinder dyker upp. Detta beror på att modellen inte är utformad för förändringar och anpassningar under fortlöpande arbete (Thummadi & Lyytinen, 2020).

Vattenfallsmodellen hanterar tid på ett förutsägbart sätt, där varje fas måste slutföras innan nästa kan påbörjas, vilket skapar en tydlig tidsplan. Eventuella förändringar under pågående arbete kan dessutom leda till betydande förseningar. Kostnader i vattenfallsmodellen är ofta förutsägbara i början av projektet. Vid förändringar, särskilt efter designfasen, kan kostnader snabbt eskalera. Omarbetningar och extra arbete för att

hantera nya krav innebär ökade kostnader. Detta gör modellen mindre lämplig för projekt där förändringar är vanliga. Omfattningen av ett projekt kan förändras avsevärt om oförutsedda justeringar sker, vilket påverkar den ursprungliga planen. Nya krav kan resultera i större komplexitet och förlängda tidshorisonter (Thummadi & Lyytinen, 2020).

2.1.2.1. Aspekter på cybersäkerhet inom vattenfallsmodellen

Cybersäkerhet inom vattenfallsmodellen innebär att säkerhetsåtgärder och bedömningar integreras i varje fas av den linjära utvecklingsprocessen. Eftersom vattenfallsmodellen bygger på en strikt sekvens av aktiviteter är det av stor vikt att hantera cybersäkerhetaspekter på ett systematiskt sätt genom hela processen (Baldassarre et al., 2020).

Den första fasen, kravanalys, lägger grunden för säkerhetsarbetet. I den här fasen fastställs vilka säkerhetskrav som är kritiska för systemet baserat på lagar, exempelvis GDPR. Även analyser för att identifiera potentiella cyberhot samt risker som kan påverka projektet genomförs. För att säkerställa att säkerhetskraven kan användas som referens under design, implementering, och testning, dokumenteras dessa tydligt (Baldassarre et al., 2020).

I den andra fasen, designfasen, skapas en systemstruktur för att minska attackytor, exempelvis genom att införa nätverksdelning och använda säker kommunikation. För att upptäcka och förhindra cyberattacker används inbyggda säkerhetsfunktioner, såsom planering av funktioner som kryptering, identifiering av användare, och loggning av aktiviteter (Baldassarre et al., 2020).

Under implementeringsfasen byggs systemen. För att undvika säkerhetsproblem används säkra metoder för kodning och ramverk. I denna fas görs också regelbundna kontroller av koden för att tidigt hitta och åtgärda eventuella säkerhetsbrister (Baldassarre et al., 2020).

Under testfasen verifieras att systemet fungerar korrekt och att säkerhetskraven uppfylls. I den här fasen utförs säkerhetstester där systemet utsätts för simulerade cyberattacker för att identifiera potentiella sårbarheter. Det säkerställs även att de säkerhetsfunktioner som

kryptering och autentisering fungerar som avsett. Systemet utformas för att uppfylla krav enligt standarder som ISO 27000-serien och GDPR (Baldassarre et al., 2020; International Organization for Standardization, n.d.).

I driftsättningsfasen är det viktigt att säkerställa en smidig övergång till produktionsmiljön. Det är avgörande att systemkomponenter, både hårdvaru- och mjukvarudelar som servrar, databaser, och applikationer, är rätt inställda för att minimera säkerhetsbrister. Åtkomst till systemet bör övervakas för att skydda mot obehöriga användare. Processer används för att snabbt upptäcka och hantera eventuella säkerhetsbrister (Baldassarre et al., 2020).

Under underhålls- och uppföljningsfasen, krävs kontinuerligt arbete för att upprätthålla cybersäkerheten. Det är viktigt att identifiera och åtgärda nya sårbarheter genom exempelvis regelbundna uppdateringar. Övervakningsverktyg används för att upptäcka misstänkt aktivitet i realtid. Säkerhetsåtgärderna bör även anpassas och förbättras i takt med att hotbilden förändras (Baldassarre et al., 2020).

Genom att integrera cybersäkerhet i varje fas i vattenfallsmodellen kan säkerhetsproblem förebyggas tidigt, vilket minskar kostnader för sena korrigeringar. Modellen säkerställer att systemet uppfyller lagkrav och branschstandarder samt bygger ett robust system mot cyberhot. Vattenfallsmodellen ger en tydlig struktur för att implementera och planera säkerhetsåtgärder, men förändringar i senare faser kan vara både tidskrävande och kostsamma. Därför är en djupgående säkerhetsanalys tidigt i projektet avgörande för framgång (Baldassarre et al., 2020).

2.2.3. Agila metoder vs. vattenfallsmodellen: När fungerar den ena bättre än den andra?

I en jämförelsestudie som jämför två projektstyrningsmetoder: den traditionella vattenfallsmodellen och de agila metoderna, analyserar Krishna & Gopinath (2024) metodernas struktur, processer och effektivitet i olika utvecklingssammanhang. Studien visar hur och när respektive metod är mest effektiva, beroende på projektets krav, förutsägbarhet och förändringsbenägenhet. Vattenfallsmodellen är mest effektiv i stora och komplexa projekt där kraven är tydligt definierade från början, och där en sekventiell

och dokumentationsintensiv process säkerställer stabilitet och kvalitetskontroll. Detta gör modellen särskilt användbar i branscher med höga regleringskrav, där varje fas måste slutföras innan nästa påbörjas. Däremot är den mindre flexibel vid förändringar och kan innebära höga kostnader vid sena justeringar. Agila metoder är å andra sidan mest effektiva i dynamiska och snabbrörliga miljöer, där kundens behov och krav kan förändras under utvecklingsprocessen. Genom iterativa cykler och kontinuerlig feedback kan utvecklingsteam snabbt anpassa sig till nya krav och optimera produktens funktionalitet. Agila metoder lämpar sig därför för mjukvaruutveckling, innovationsdrivna projekt och mindre till medelstora utvecklingsuppdrag där flexibilitet och snabb leverans är centralt. En nackdel är dock att bristande struktur kan leda till svårigheter att hantera resurser och långsiktig planering, särskilt i större projekt (Krishna & Gopinath, 2024).

Rodrigues de Oliveira et al. (2023) bekräftar agila metoders effektivitet med sin studie där de undersöker hur Scrum-metoden tillämpas i sex olika universitet i Brasilien. Studien analyserar hur agila metoder påverkar projektledning inom mjukvaruutveckling i den offentliga sektorn och identifierar både fördelar och utmaningar med Scrum i dessa miljöer. Resultaten visar att Scrum bidrar till ökad kommunikation och samarbete mellan teammedlemmar och intressenter, även när teammedlemmarna arbetade på distans, vilket resulterar i förbättrad produktivitet och minskat utvecklingsarbete. 96 procent av deltagarna i studien visade på positiva erfarenheter av Scrum, vilket stärker metodens framgångsrika implementering. Scrum anses ge fördelar såsom ökad flexibilitet, snabbare leveranser och bättre anpassningsförmåga till förändrade krav. Resultaten visar även på kortare utvecklingstider och bättre hantering av resursfördelning. Utmaningar som framkommer under studien är behovet av kontinuerlig utbildning av teammedlemmar, svårigheter med att koordinera möten med slutanvändaren, speciellt i akademiska miljöer, låg teknikmognad och hög personalomsättning. Även om Scrum-metoden bidrar till ökad effektivitet och bättre hantering av osäkra projektförhållanden, kan implementering vara en utmaning på grund av de höga kraven på teknikmognad och teamstabilitet. Därför är det viktigt att ha en stark ledningsstruktur och ett strategiskt stöd från ledningen för att agila metoder ska fungera optimalt i offentlig sektor (Rodrigues de Oliveira et al., 2023).

Även Sarkar et al. (2024) nådde likande resultat i sin fallstudie, där de analyserade det asiatiska teknikföretaget *Hello Verify* och hur agila metoder och vattenfallsmodellen påverkar tidsplanering, kostnader och projektmål inom projektledning. Resultaten visar att över 70 procent av deltagarna anser att Scrum, en agil metod, är den mest framgångsrik, särskilt i en snabbt föränderlig miljö. Studien visar att Scrum blir allt vanligare inom mjukvaruutveckling. Denna preferens för Scrum kan förklaras av dess förmåga att främja kontinuerliga förbättringar, flexibilitet och bättre samarbete. Samtidigt konstateras det att vattenfallsmodellen fortfarande är användbar i projekt där stabilitet, struktur och noggrann dokumentation är avgörande (Sarkar et al., 2024).

Däremot i en annan fallstudie, skriven av Lobo Marques et al. (2023), som genomfördes inom byggindustrin i Macau, Kina, framkommer det hur vattenfallsmodellen är den mest effektiva metoden i stora infrastrukturprojekt. Studiens resultat visar att majoriteten av byggledarna föredrar vattenfallsmodellen då den möjliggör en bättre kontroll över tid, kostnad och omfattning. Vattenfallsmodellen anses som mest lämplig i projekt där det finns tydliga milstolpar, detaljerad planering och stabilitet. I studien tar det fram ett exempel av konstruktionen av ett stort hotell i Catai, där resurser som arbetskraft och material var begränsade, och en strukturerad, fasindelad strategi krävdes för att hantera dessa utmaningar. Dock framkom det att en del agila principer, såsom kontinuerlig feedback och förbättrade kommunikationsflöden, kan implementeras i specifika delar av byggprocessen för att öka effektiviteten (Lobo Marques et al., 2023).

Shimoda & Yaguchi (2024) analyserade i sin studie effektiviteten av vattenfallsmodellen jämfört med agila metoder vid utvecklingen av ett biblioteksinformationssystem. Studiens resultat visar att vattenfallsmodellen anses vara det mest lämpliga valet i de inledande faserna av systemutvecklingen, särskilt vid kravspecifikation och grundläggande design, där en helhetsbild av systemets funktioner och arkitektur är avgörande, medan agila metoder anses mest lämplig för detaljdesign och implementering, vilket är något som Krishna & Gopinath (2024) bekräftar med sin studie. Vidare tar Shimoda & Yaguchi (2024) upp ett exempel där låne- och medlemsinformation behöver en strukturerad och sekventiell strategi för att säkerställa att systemets kärnfunktioner byggs med hög noggrannhet och stabilitet. Genom detta kunde utvecklingsteamet

optimera kostnader och säkerställa en effektiv resursallokering. Även om vattenfallsmodellen är överlägsen för att hantera systemets övergripande struktur noterades att vissa agila metoder, såsom iterativa utvecklingscykler och flexibilitet vid implementering av detaljerade funktioner, kan tillämpas för att förbättra anpassningsförmågan och korta ned leveranstider (Shimoda & Yaguchi, 2024).

Shimoda och Yaguchi (2024) undersöker även hur en hybridmodell, som kombinerar vattenfallsmodellen och agila metoder, kan bidra till att balansera kostnadseffektivitet och tidig värderealisering. Resultaten visar att användning av en hybridmodellen kan minska utvecklingskostnader genom att fokusera på gemensamma och återanvändbara komponenter som kan effektivisera både den strukturerade och flexibla delen av projektet och samtidigt möjliggöra tidig leverans av funktionalitet genom iterativa cykler. Genom att strukturera utvecklingsordningen för olika delar av projektet kan kostnadsökningar minska samtidigt som värdet för slutanvändaren genomförs på ett effektivt sätt (Shimoda & Yaguchi, 2024). En hybridmodell, som kombinerar element från båda metoderna, kan vara den optimala lösningen beroende på projektets krav och förutsättningar enligt Krishna & Gopinath (2024) och Lobo Marques et al. (2023).

2.2.4. Cybersäkerhet i praktiken

Molnsäkerhet utgör en komplex utmaning för företag då nationella och internationella standarder varierar, enligt Weil (2020). I sin studie visas hur en organisation implementerade ISO 27001 i syfte att hantera molnsäkerhetsrisker. Riskbedömningen fokuserade på hybridmolnslösningar för juridiska och brottsförebyggande system, vilket innebar att ISO 27005-modellen behövde anpassas för att omfatta både scenariobaserade och tillgångsbaserade bedömningar. Implementeringen av de olika riskbedömningsmetoderna skedde genom en strukturerad process som omfattade identifiering av säkerhetskrav, analys av hotbilder och risker samt en iterativ översyn av säkerhetskontroller. Baserat på nya hot och regulatoriska krav följde organisationen en anpassad riskhanteringscykel där de regelbundet uppdaterade sina kontroller. Ett stort fokus lades på att säkerställa att riskhanteringen integrerades i de dagliga verksamhetsprocesserna genom en kombination av tekniska och organisatoriska åtgärder. Detta gjordes genom att förankra riskhanteringsrutiner i verksamhetens styrningsstrukturer och säkerställa att säkerhetskontroller blev en del av standardiserade

arbetsflöden. För att möjliggöra detta tillämpades en iterativ riskbedömningsprocess, där risker identifierades, analyserades och åtgärdades löpande genom scenariobaserade och tillgångsbaserade metoder. En central aspekt var att riskhanteringen integrerades i beslutsprocesser på olika nivåer inom organisationen, vilket möjliggjorde snabb anpassning till förändrade hot och regulatoriska krav. Vidare involverades relevanta intressenter genom interna utbildningar och riktlinjer, vilket ökade medvetenheten och säkerställde att cybersäkerhetsarbetet blev en kontinuerlig del av organisationens dagliga verksamhet (Weil, 2020).

I en annan studie beskrivs det hur en IT-konsultfirma implementerade ISO 27001 för att förstärka sin informationssäkerhet. Genom att använda en riskbedömningsram baserad på exempelvis ISO 27005 och NIST SP 800-30 kunde företaget identifiera specifika hot och anpassa sina kontroller. En stor utmaning i detta var bland annat att säkerställa att interna processer dokumenterades och implementerades på ett effektivt sätt. Implementeringsprocessen skedde i flera steg: (1) initial kartläggning av säkerhetsbehov och risker, (2) utformning av standarder och kontroller, (3) genomförande av tekniska och organisatoriska åtgärder, samt (4) kontinuerlig övervakning och förbättring.
Det var även viktigt att säkerhetsåtgärderna var anpassade efter företagets affärsmodell och att de kunde implementeras utan att kompromissa med den dagliga verksamhetens flöde och produktivitet (Kitsios et al., 2022).

Podrecca et al. (2022) menar att ISO 27001-certifiering påverkar företags finansiella resultat. Deras studie visar att företag som investerar i informationssäkerhet får ökad lönsamhet, arbetsproduktivitet och försäljningsprestanda. Däremot finns det utmaningar med operativ flexibilitet och balansen mellan säkerhet och effektivitet. Implementeringen av ISO 27001 i dessa företag följde en metodik där initiala kostnader vägdes mot förväntade vinster i form av bättre riskhantering och ökat förtroende hos kunder. Organisationerna anpassade sina strategier för att hantera de operativa utmaningarna genom att införa flexibilitet i sina säkerhetskontroller och regelbundet utvärdera om de implementerade åtgärderna gav avsedd effekt (Podrecca et al., 2022).

Sammanfattningsvis är standardiserade riskbedömningsmetoder som är anpassade efter verksamhetens specifika behov, regler och krav, väsentliga för att säkerställa en effektiv och systematisk hantering av informationssäkerhetsrisker. Dokumentation och processhantering är avgörande för en framgångsrik ISMS-implementering, det vill säga ett systematiskt arbetssätt för att hantera och skydda organisationens informationstillgångar, och kan bidra till att attrahera nya kunder genom ökad trovärdighet. Informationssäkerhet är inte enbart en defensiv åtgärd utan kan även skapa affärsnytta och differentiering på marknaden (Kitsios et al., 2022; Podrecca et al., 2022; Weil, 2020).

3. Metod

Följande kapitel presenterar studiens kvalitativa metod. Metoden bygger på semistrukturerade intervjuer samt vetenskapliga artiklar och litteratur. Avsnittet behandlar metodval, analysmodell, operationaliseringar, datainsamling, urval, och sökord, samt diskuterar metodkritik, trovärdighet, käll- och litteraturkritik och etiska överväganden. Kapitlet avslutas med kvalitetssäkring av språk där AI används för språkkorrigering.

3.1. Metodval

För att uppnå studiens syfte och möjliggöra en detaljerad analys av projektledarnas erfarenheter av cybersäkerhetens påverkan på projektledning, genomfördes semistrukturerade intervjuer som en del av den kvalitativa metodansatsen. Denna metod valdes eftersom våra forskningsfrågor handlar om "hur", vilket enligt Ghauri et al., (2020) gör metoden särskilt lämplig, för att få utförliga och detaljerade beskrivningar av projektledarnas erfarenheter och upplevelser, samt eftersom kopplingen mellan cybersäkerhetskrav och projektmål är ett nytt och outforskat område. Metoden gav utrymme för flexibla, detaljerade och utförliga svar av hur projektledare inom IT-konsultbranschen uppfattar, tolkar och hanterar cybersäkerhetskrav i sina projekt. Studien utgick från en syn på verkligheten där den inte är fast och objektiv, utan snarare något som ständigt förändras och formas av människors erfarenheter och perspektiv (Bryman & Bell, 2017; Ghauri et al., 2020; Lind, 2019).

Intervjuerna strukturerades utifrån en kombination av öppna och riktade frågor för att fånga in både generella och specifika aspekter av cybersäkerhetens påverkan på projektledning. Fokus låg på att utforska vilka utmaningar projektledarna står inför, vilka strategier de använder för att möta cybersäkerhetskraven och hur dessa krav integreras i projektens arbetsprocesser och projektledarnas projektstyrningsmetoder. Projektledarna fick berätta om konkreta uppdrag där det användes agila metoder, vattenfallsmodellen eller en kombination av metoderna (hybridmodellen), samt hur cybersäkerhetkraven påverkar projektet och hur de effektivt kunde anpassa sig till cybersäkerhetskarven (Bryman & Bell, 2017; Eriksson & Wiedersheim-Paul, 2014).

Intervjupersonerna fick frågorna via email en vecka i förväg för att kunna förbereda sig och undvika ogenomtänkta svar. En nackdel med detta tillvägagångssätt var att det kunde leda till mer strategiska svar snarare än spontana reflektioner, vilket eventuellt kunde påverka autenticiteten i intervjuerna. Samtidigt ansågs det vara fördelaktigt eftersom det gav intervjupersonerna tid att reflektera över ämnet, vilket ökade chansen att de kunde ge mer genomtänkta och detaljerade svar (Bryman & Bell, 2017; Ghauri et al., 2020). Intervjuerna bidrog till en rikare datainsamling, eftersom det möjliggjorde uppföljningsfrågor och förtydligande. En utmaning med intervjuer var att det blev en tidskrävande process för datainsamling och analys. En annan utmaning var faktorer som vårt tonfall samt formulering av frågor som kunde haft en påverkan på svaren och resultatens tillförlitlighet (Eriksson & Wiedersheim-Paul, 2014).

Alla respondenter fick identiska frågor i samma ordning, men däremot kunde det förekomma följdfrågor samt någon anpassning. Detta bidrog till en enklare jämförelse mellan svaren. Studiens empiriska del genomförde digitalt via Teams, då detta var den mest tidseffektiva lösningen eftersom det eliminerade resetid och möjliggjorde användning av Teams inbyggda transkriberingsfunktion. Det digitala genomförandet ökade även tillgängligheten för projektledarna, som ofta har fullbokade scheman och arbetar ute hos kunder, vilket förbättrade möjligheten att få intervjuerna genomförda (Bryman & Bell, 2017; Ghauri et al., 2020).

3.2. Analysmodell

Analysen av den insamlade data inriktade sig på att identifiera mönster och teman i intervjupersonernas berättelser, vad som skiljde sig och inte med intervjupersonernas berättelser. Den insamlade empirin, projektledarnas beskrivningar av utmaningar och strategier, analyserades sedan i relation till relevanta teorier, modeller och begrepp, inom projektledning och cybersäkerhet, för att skapa en mer omfattande förståelse av hur cybersäkerhetskrav påverkar projektledning i praktiken. Detta tillvägagångsätt gjorde det möjligt att analysera underliggande faktorer som påverkade projektledning inom IT-konsultbranschen samt vilka projektledarstilar som var relevanta i att navigera de utmaningar som uppstod kring cybersäkerhet i projekt (Bryman & Bell, 2017; Eriksson & Wiedersheim-Paul, 2014).

I studien användes teman i syfte att enklare kunna koda texten i analysen och identifiera mönster i det insamlade data. Genom en process där initiala teman först identifierades, och sedan bekräftades eller ändrades utifrån intervjupersonernas svar, kunde det i en andra analysnivå tolkas och sammanföra dessa koncept. Dessa teman användes sedan för att strukturera och kategorisera data, vilket möjliggjorde en mer systematisk och strukturerad analys (Ghauri et al., 2020).

Teman kopplade till teorin och empirin:

- **Cybersäkerhetskravens inverkan på projekttriangeln**
    - Detta tema är direkt kopplat till studiens syfte, eftersom det belyser hur cybersäkerhetskrav påverkar tid, kostnad och omfattning samt hur dessa krav hanteras vid införandet av nya regelverk.

- **Hantering av säkerhetskrav i agilstyrda projekt**
    - Detta tema är en central aspekt av cybersäkerhetskrav. Eftersom regelverk ofta berör skydd av data och integritet, är det relevant att undersöka hur projektledare hanterar dessa aspekter i praktiken i agilstyrda projekt och hur de påverkar projektstyrningen. Genom att undersöka hur agila metoder används i projekt och hur metoderna påverkas av cybersäkerhetskrav, kan studien bidra med insikter om hur dessa krav balanseras med projektets mål och genomförande.

- **Hantering av säkerhetskrav i vattenfallsstyrda projekt**
    - Detta tema är en central aspekt av cybersäkerhetskrav. Eftersom regelverk ofta berör skydd av data och integritet, är det relevant att undersöka hur projektledare hanterar dessa aspekter i praktiken i vattenfallsstyrda projekt och hur de påverkar projektstyrningen. Genom att undersöka hur vattenfallsmodellen används i projekt och hur metoderna påverkas av cybersäkerhetskrav, kan studien bidra med insikter om hur dessa krav balanseras med projektets mål och genomförande.

- **Hybridmodellens möjligheter och begränsningar**
    - Detta tema är en förlängning av analysen. Genom att diskutera framtida utmaningar och förbättringsmöjligheter skapas en förståelse för hur IT-konsultföretag och projektledare kan utveckla mer hållbara och flexibla projektstyrningsmetoder, en hybridmodell, för cybersäkerhets- och framtida krav. Detta ligger i linje med studiens ambition att stödja

branschen i en snabbt föränderlig bransch.

Teman Analys	Teori	Empiri
Cybersäkerhetskravens inverkan på projekttriangeln	Detta tema är direkt kopplat till teori om projekttriangeln samt case studier under "Cybersäkerhet i praktiken" samt aspekter på cybersäkerhet inom de två modellerna.	Detta tema är kopplat till resultatet från projektledarnas erfarenheter under "Påverkan på tid, kostnad och omfattning".
Hantering av säkerhetskrav i agilstyrda projekt	Detta tema är kopplat till teorin om agila metoder, cybersäkerhetskrav i agilstyrda projekt.	Detta tema är kopplat till helheten av empirin, där vi har tolkat resultatet och analyserat det i förhållande till teorin om agila metoder.
Hantering av säkerhetskrav i vattenfallsstyrda projekt	Detta tema är kopplat till teorin om vattenfallsmodellen, cybersäkerhetskrav i vattenfallsstyrda projekt.	Detta tema är kopplat till helheten av empirin, där vi har tolkat resultatet och analyserat det i förhållande till teorin om vattenfallsmodellen.
Hybridmodellens möjligheter och begränsningar	Detta tema är kopplat till vetenskapliga case studier om när den ena metoden är bättre än den andra.	Detta tema är kopplat till projektledarnas erfarenheter och åsikter under "Agilt och Vattenfall: likheter och skillnader i hantering" samt "strategier och framtida behov".

Användningen av tematiska analys möjliggjorde en rörelse fram och tillbaka mellan data och teori. Genom att kontinuerligt jämföra data med relevanta teorier kunde studien identifiera mönster, samband och avvikelser som annars kunde ha förbisetts. Detta stärkte studiens analytiska trovärdighet genom att säkerställa att tolkningarna var välgrundade och förankrade i både praktiska erfarenheter och tidigare forskning. Det möjliggjorde också en mer nyanserad analys, där teorin inte bara användes för att tolka resultaten, utan där resultaten även kunde bidra till att problematisera och vidareutveckla de teoretiska perspektiven (Ghauri et al., 2020).

3.2.1. Operationaliseringar

De teman som undersöks i intervjuerna är baserade på studiens teoretiska ramverk. En fullständig lista med intervjufrågor finns i *Bilaga 1 Intervjufrågor.*

Definition av begrepp och variabler:

Begrepp	Definition	Operationalisering (hur det utforskas i studien)
Cybersäkerhetskrav	Regelverk och standarder som påverkar IT-projekt.	Analyseras genom dokumentstudier av NIS-direktiven, andra lagkrav/standarder, och intervjuer med IT-konsulter om deras upplevelser av kraven.
Projektmål	Projektets mål utifrån tid, kostnad, omfattning och kvalitet.	Utforskas genom intervjuer med projektledare om hur de definierar och upplever projektets mål i förhållande till cybersäkerhetskrav.

Riskhantering	Strategier och processer för att identifiera och hantera cybersäkerhetsrisker.	Undersöks genom att analysera hur intervjupersoner beskriver sina arbetsprocesser, beslutsfattande och utmaningar i att hantera risker.

3.3. Datainsamling

Utöver semistrukturerade intervjuer användes vetenskapliga artiklar och litteratur för att ge en detaljerad kontext och stärka analysen genom att integrera tidigare forskning samt teoretiska perspektiv (Bryman & Bell, 2017; Eriksson & Wiedersheim-Paul, 2014). Användning av denna typ av data var effektivt eftersom det sparade både resurser och tid. Det här bidrog även till ett bredare perspektiv genom att ge tillgång till information från flera olika källor, vilket möjliggjorde identifiering av mönster och fenomen som annars hade varit svårt att upptäcka. Vetenskapliga artiklar och litteratur var även en värdefull resurs inom forskningen och analysen, eftersom det var en kostnadseffektiv tillgång till information (Bryman & Bell, 2017).

Utmaningar med vetenskapliga artiklar och litteratur var samtliga begränsningar. Exempelvis kunde information vara inaktuell och irrelevant för det aktuella arbetet. Variabler, urval och metoder kunde skilja sig från vad som initialt söktes eftersom data samlats in för ett annat syfte. Kvaliteten och tillförlitligheten kunde även vara utmanande. Källorna granskades noggrant genom att kritiskt analysera deras ursprung, syfte och metodologi, eftersom vi själva inte samlat in den data, exempelvis kunde en rapport vara vinklad för att gynna ett företags intressen (Bryman & Bell, 2017).

3.3.1. Urval

Studien avgränsades till IT-konsultbranschen, där automatiserade system har blivit allt vanligare, vilket i sin tur har lett till en ökad exponering för cyberhot. Som en följd av detta har nya cybersäkerhetskrav och regelverk utvecklats, vilket IT-konsultföretag måste

följa samtidigt som de behöver anpassa sig till kundernas krav. Detta skapar en komplex situation, särskilt vid införandet av nya regelverk, såsom NIS2-direktivet som ska verkställas 2025, då företagen både måste säkerställa efterlevnad och bibehålla flexibilitet gentemot sina kunder. De avgränsningar som gjordes i specifika säkerhetskrav i förstudien var ISO 27001, NIS-direktivet, NIST SP 800–30 och GDPR. Detta eftersom dessa regelverk ansågs relevanta till studiens syfte utifrån de säkerhetskrav och lagverk som exciterade eller skulle verkställas inom snar framtid.

IT-konsultbranschen är särskilt utsatt eftersom konsulter arbetar direkt med IT-lösningar och förväntas vara flexibla utifrån kundens behov. Samtidigt måste de även anpassa sig efter nya lagkrav inom cybersäkerhet, vilket ställer högre krav på projektstyrning. Frågan blir därför hur projektstyrningsmetoder kan utformas för att möjliggöra en smidig och effektiv anpassning till förändrade säkerhetskrav. Projektets kvalitet mäts i tid, kostnad och omfattning (projekttriangeln), därför utgår studien ifrån projekttriangeln för att mäta cybersäkerhetens påverkan på projektets kvalitet.

Tabellen redovisar projektledarnas befattning, tillhörande företag, projekt samt intervjutid:

Projektledare	Företag	Befattning	Projekt	Intervjutid
A	1	VD, projektledare	IT- projekt och förändringsprojekt	50 min
B	2	Projektledare, teknisk expertis	OT-projekt	45 min
C	3	Projektledare/ produktägare, service level manager	Implementerings-projekt inom IT	40 min
D	4	Projektledare, verksamhetsutvecklare	Projekt i offentlig förvaltning	40 min
E	3	Projektledare, product manager	Agil utveckling av digitala produkter	50 min
F	2	Projektledare, CDO	Utvecklingsprojekt med produkter	45 min

G	3	Projektledare	Business transformation, SAP, ERP, IT och business development-projekt	35 min
H	5	VD, projektledare	Utvecklingsprojekt, stora utredningsprojekt	60 min

Vi använde oss av vårt kontaktnät inom IT-konsultbranschen när intervjupersoner valdes. Intervjupersonerna valdes strukturellt baserat på att de var seniorkonsulter samt deras arbetsroll och kompetens inom området för att säkerställa att de kunde ge detaljerade och relevanta svar. De valda intervjupersonerna var projektledare i småföretag, IT-konsultföretag, som arbetar med olika projekt. De projekt som studien fokuserar på tillhör IT-branschen, eftersom AI är en aktuell och växande fråga inom denna sektor, där framtida utmaningar kring cybersäkerhet förväntas uppstå. Andra projekt hade inte varit lika applicerbara för denna studie (Ghauri et al., 2020).

Intervjupersonerna i studien valdes av deras erfarenhet av olika projekt, vilket kunde ge insikter om hur cybersäkerhetskraven påverkade projektens genomförande och hur olika projektstyrningsmetoder tillämpades (Bryman & Bell, 2017). För att ge ett mångsidigt perspektiv valdes åtta projektledare inom IT-konsultbranschen som intervjupersoner i studien. Detta ansåg vi vara tillräckligt, med stöd av Ghauri et al. (2020) som beskriver att kvalitativa studier främst fokuserar på att intervjua rätt personer för studien med insikt i forskningsproblemet och kan bidra till att besvara forskningsfrågorna, snarare än att inkludera ett stort antal respondenter. Genom att välja intervjupersoner med direkt erfarenhet av cybersäkerhetskravens påverkan i projekt säkerställdes att studiens data var relevant och tillförlitlig (Bryman & Bell, 2017; Ghauri et al., 2020).

Studien fokuserade på projektledare i IT-konsultföretag i Göteborg/Malmö. Anledningen till att projektledare för IT-konsultföretag valts som studieobjekt var för att projektledare

har en nyckelroll i att leda och hanterar komplexa projekt samtidigt som tekniska, organisatoriska och affärsmässiga faktorer samverkar. Eftersom vi befann oss i västra- och södra Sverige, var valet av IT-konsultföretag i Göteborg/Malmö av praktiska skäl.

3.3.2. Sökstrategi och urval av sökord

För att identifiera relevanta vetenskapliga artiklar till studien användes databaser som är tillgängliga via Högskolan i Skövdes bibliotekstjänst LibSearch. Biblioteket tillhandahåller en omfattande samling databaser, bland annat Scopus, ACM Digital Library och JUNO Bas. Valet av sökord baserades på studiens syfte och centrala begrepp.

Vi kombinerade sökord relaterade till projektledning och projektmål (t.ex. Project management, Project time, Project cost, Project scope, Project quality, Project triangle, Project success), projektmetoder (t.ex. Agile method, Scrum, Kanban, SAFe, Waterfall model, PROPS), och cybersäkerhet (t.ex. Cybersecurity, Cybersecurity requirements, Risk management, GDPR, ISO 27000, NIS-directive, NIS2-directive, NIST SP 800-30).

Vid behov inkluderades även kompletterande sökord som Artificial intelligence och IT consulting för att identifiera kontextspecifika perspektiv och trender inom IT-branschen. På svenska användes ibland begrepp som PPL (Praktisk Projektledning) för att hitta relevanta svenska källor och ramverk.

Sökord:

Agile method, Agile methods vs waterfall models, Artificial intelligence, Cybersecurity, Cybersecurity requirements, GDPR, ISO 27000, IT consulting, IT projects, Kanban, NIS-directive, NIS2-directive, NIST SP 800-30, PPL, Project cost, Project management, Project management methods, Project quality, Project scope, Project success, Project time, Project triangle, PROPS, Risk management, SAFe, Scrum, Waterfall model.

3.4. Metodkritik

3.4.1. Giltighet/trovärdighet

Den metodiska processen beskrivs noggrant i studien och hur resultatet identifierades för att säkerställa att studien var lätt att förstå och transparant. Detta gör det möjligt för

läsaren att enkelt följa forskningsgången och förstå hur studiens slutsats framkom (Bryman & Bell, 2017).

För att säkerställa att datainsamling och analys genomfördes systematiskt följde forskningen den beskrivna processen. För att öka tillförlitligheten användes en metod för jämförande analys, där den insamlade empirin från intervjuerna ställdes i relation till tidigare forskning. Majoriteten av de granskade studierna var publicerade inom de senaste fem åren, vilket bidrog till att resultaten kunde sättas i ett relevant sammanhang och att återkommande mönster och teman kunde identifieras (Bryman & Bell, 2017).

Metodiken dokumenterades noggrant, vilket gjorde studien granskningsbar. Studien granskades även av opponenter, handledare och examinator, vilket bidrog till kvalitetssäkra processer och minskad risk för metodologiska brister, som gjorde studien pålitlig (Bryman & Bell, 2017).

I studien diskuterades hur resultaten kunde appliceras hos likande förtag inom IT-konsultbranschen för att öka studiens överförbarhet. I studien analyserades företag av samma storlek med liknande verksamhetsfokus. Detta gjorde att det inte enbart kunde dras slutsatser som begränsade sig till de specifika fall som undersöktes, utan även kunde ge insikter för andra aktörer inom branschen (Bryman & Bell, 2017).

3.4.2. Käll- och litteraturkritik

För att styrka trovärdigheten hos intervjupersonerna presenterade de konkreta bevis från sina uppdrag. Projektledarna svarade på liknande sätt, vilket tydde på en samstämmighet i deras upplevelser och erfarenheter. Detta skulle kunna stärka trovärdigheten i resultaten och indikera att projektledarna delade en gemensam syn på uppdragens krav och utmaningar. Samtidigt fanns en risk att detta snarare var en konsekvens av en relativt homogen urvalsgrupp. En bredare geografisk spridning eller inkludering av fler företag hade möjligtvis kunnat ge en mer varierad bild av hur cybersäkerhetskrav hanteras i olika IT-konsultföretag. Vidare kunde en viss bekräftelsebias förekomma, då vi kunde ha tolkat samstämmiga svar som en styrka utan att ifrågasätta om oliktänkande perspektiv saknades. Eftersom endast vissa befattningar inom konsultföretagen intervjuades innebär detta en begränsning, då andra roller inom IT-konsultverksamheten inte inkluderades i

studien och därmed inte återspeglas i resultatet, exempelvis ekonomiansvarig och företagets kunder kunde ha bidragit med ytterligare perspektiv på cybersäkerhetskravens påverkan (Eriksson & Wiedersheim-Paul, 2014).

Resultatens tillförlitlighet kan påverkas av att endast åtta projektledare intervjuades, vilket innebär ett begränsat urval. Dock bestod samtliga respondenter av seniorkonsulter med lång erfarenhet inom projektledning, vilket stärker tillförlitligheten i deras svar. Även om de var verksamma i olika typer av projekt visade deras svar en hög grad av samstämmighet, vilket bidrar till studiens trovärdighet (Ghauri et al., 2020). Samtidigt hade tillförlitligheten kunnat stärkas ytterligare om respondenterna varit verksamma inom mer liknande projektkontexter, eftersom detta hade minskat variationer kopplade till skilda organisatoriska och metodmässiga förutsättningar.

I studien användes även vetenskapliga artiklar som var peer-reviewed, rapporter och publikationer från myndigheter samt andra etablerade källor med hög trovärdighet, såsom Norstedts Juridik och liknande juridiska och branschspecifika resurser. Dessa kompletterades med metod- och studielitteratur för att ge en teoretisk grund och säkerställa att informationen var både relevant och tillförlitlig. Genom en systematisk granskning bedömde vi källornas trovärdighet utifrån flera kriterier. Vi kontrollerade författarna i de vetenskapliga artiklarnas akademiska eller professionella bakgrund, såsom deras institutionella tillhörighet, tidigare publikationer och/eller expertis inom ämnesområdet. Det säkerställdes att författarna till de vetenskapliga artiklarna som användes i studien var verksamma vid erkända universitet eller forskningsinstitut. För rapporter från myndigheter, juridiska källor, såsom Norstedts Juridik, och övriga källor, säkerställde vi att de var publicerade av auktoritativa organisationer med expertis inom området.

I studien användes flertal källor inom samma område, där majoriteten var från de senaste fem åren, eftersom cybersäkerhetskrav inom projektledning är ett område i ständig utveckling, där nya regelverk, teknologier och säkerhetsutmaningar kontinuerligt påverkar praxis. Genom att använda nyare källor kunde studien spegla de senaste förändringarna och ge en relevant analys av hur cybersäkerhetskrav implementeras i

projektledning. Eftersom källorna utgick från samma grund skapades det en stor trovärdighet, då flera oberoende källor utgav liknande information. Detta betydde däremot inte nödvändigtvis att slutsatserna var allmängiltiga eller fria från bias.

Det fanns en möjlighet att källorna utgick från liknande metodologiska tillvägagångssätt eller baserades på samma datakällor, vilket kunde begränsa variationen i perspektiv och därmed påverka bredden i den insamlade kunskapen. För att identifiera och hantera detta granskades studiernas metodval och datakällor noggrant, där fokus låg på att undersöka om forskningen utgick från olika kontexter, branscher och forskningsmetoder.

Vidare kunde en publikationsbias förekomma, där studier med positiva resultat hade större sannolikhet att publiceras än sådana som visade utmaningar eller motsägelsefulla slutsatser. För att säkerställa en mer balanserad förståelse jämfördes forskningsartiklar med rapporter från myndigheter och IT-branschen, vilka ofta inkluderar både framgångsfaktorer och svårigheter vid implementeringen av cybersäkerhetskrav, samt val av projektstyrningsmetod. Genom att analysera både enighet och avvikelser i materialet skapades en mer nyanserad bild av forskningsfältet och de faktorer som påverkar projektledning inom IT-konsultbranschen.

Även om källorna till stor del var aktuella (från de senaste fem åren) kunde äldre forskning fortfarande vara relevant, särskilt inom områden där teoretiska ramverk eller etablerade principer inte förändrats snabbt. För att få en mer nyanserad bild av forskningsområdet kunde analysen i studien stärkts ytterligare genom att inkludera kritiska studier som ifrågasätter eller motsäger deras resultat (Eriksson & Wiedersheim-Paul, 2014).

3.5. Etiska överväganden

Etiska överväganden, inklusive konfidentialitet och nyttjande av insamlade data, beaktades noggrant för att intervjuerna skulle genomföras på ett ansvarsfullt och respektfullt sätt, och för att undvika att intervjupersonerna drabbades negativt av sin medverkan. Alla intervjupersoner gav sitt samtycke att delta i studien, och de informerades via email om syftet med forskningen och frågorna som skulle ställas samt hur deras svar skulle användas. Intervjupersonerna fick även möjlighet att ställa frågor

om studien innan de gav sitt samtycke att delta. Intervjupersonerna gav sitt samtycke att intervjun fick spelas in via Teams och transkriberades automatiskt. Dessutom informerades de om att inspelningen och den okorrigerade transkriberingen skulle raderas när transkriberingen hade granskats och korrigerats av oss. Om känslig information nämndes under intervjun ersattes den med en kod, exempelvis en siffra eller bokstav, i transkriberingen i syfte till att skydda respondentens anonymitet. Intervjupersonerna fick även möjlighet att granska transkriberingen efter intervjun (Ghauri et al., 2020; Vetenskapsrådet, 2024).

Intervjupersonerna (projektledarna), IT-konsultföretagen och deras kunder hölls anonyma för att skydda affärskritiska uppgifter och känslig information. Anonymiseringen syftade till att skapa en trygg intervjumiljö där deltagarna kunde tala öppet utan oro för negativa konsekvenser för sina företag eller kundrelationer. Samtidigt fanns en viss begränsning i anonymiseringsprocessen, eftersom det i vissa fall kan vara möjligt att indirekt identifiera personer eller företag utifrån specifika citat eller kontextuell information, även om inga namn eller direkta identifierande uppgifter nämns. Medvetenheten om denna potentiella risk beaktades i analysen genom att formulera resultat och citat på ett sätt som minimerade identifieringsmöjligheterna, samtidigt som vi bibehöll en korrekt och trovärdig representation av intervjupersonernas svar (Ghauri et al., 2020).

För att ytterligare skydda deltagarnas rättigheter och bekvämlighet gavs de möjlighet att när som helst avbryta intervjuerna utan att behöva ange någon anledning. Intervjuerna genomfördes via Teams, i en miljö där deltagarna uppmuntrades att fritt dela sina tankar och upplevelser utan någon form av press eller påverkan. Deltagarna var bemötta med full respekt, och hade samma möjlighet att bidra till studien (Ghauri et al., 2020).

3.6. Kvalitetssäkring av språk

För att säkerställa en hög nivå av grammatik och språklig korrekthet i denna studie har artificiell intelligens (AI) använts för att genomföra språkkorrigering. Detta har gjorts för att underlätta för oss och effektivisera arbetsprocessen, vilket sparade tid.

4. Empiri

Följande kapitel redovisar resultatet från de kvalitativa semistrukturerade intervjuerna. Resultatet har delats upp i relevanta teman utifrån studiens syfte.

4.1. Påverkan på tid, kostnad och omfattning

Cybersäkerhetskrav har en påtaglig påverkan på projektens tre grundläggande parametrar: tid, kostnad och omfattning. Ett exempel på detta är den påverkan som låg organisatorisk mognad kan ha. Projektledare B lyfte särskilt fram hur bristande intern kompetens inom cybersäkerhet ofta leder till att externa experter behöver anlitas. Detta kan resultera i betydande kostnadsökningar och i vissa fall generera nya, separata projekt som måste drivas parallellt. Även när cybersäkerhetsarbetet är mer integrerat i projektet påverkas resurserna avsevärt. Enligt Projektledare A introduceras cybersäkerhetskraven ofta tidigt i projektets livscykel och hanteras löpande. Projektledare A menar att ”ju fler krav som ställs desto mer tid krävs, vilket också innebär högre kostnader och en större omfattning”. Behovet av noggrannare planering, fler tester samt ökad dokumentation medför enligt respondenten en tydlig resursförstärkning, både i form av tid och budget.

Tidspåverkan lyfts som en återkommande konsekvens av cybersäkerhetskrav. Projektledare E och F, framhöll att cybersäkerhetskrav ofta förlänger projektens ledtider. Exempelvis nämndes hur ett projekt blev tre veckor försenat i väntan på godkännande för att använda produktionsdata i testmiljö. Projektledare F noterade även att krav på utbildning, säkerhetsvalidering och samordning bidrar till att projektens omfattning och kostnadsbild påverkas negativt initialt. Samtidigt betonades att dessa investeringar kan minska risken för framtida incidenter, stärka dokumentationens kvalitet och därmed bidra till lägre kostnader över tid. En annan dimension som belystes var cybersäkerhetens långsiktiga kostnadseffektivitet. Projektledare D betonade vikten av att förstå cybersäkerhet som en investering snarare än en kostnad, då frånvaro av tillräckliga säkerhetsåtgärder kan medföra betydligt högre utgifter längre fram. Projektledare D menar att, ”På kort sikt kan cybersäkerhet verka dyrt, men i ett långsiktigt perspektiv är det betydligt mer kostnadseffektivt.”

Projektledare C illustrerade denna påverkan med ett konkret exempel där en ransomware-attack mot en molnbaserad lösning orsakade ett produktionsbortfall på tre månader, och

där även FBI var inblandad. Händelsen krävde omfattande och kostsamma efterkontroller i form av säkerhetsgranskningar och systemtester. Trots den allvarliga incidenten menade respondenten att företaget ändå klarade sig relativt lindrigt, men underströk samtidigt allvaret: ”Det här var verkligen ett exempel på när det blir allvarligt – när det fallerar i IT-säkerheten.”

Hur cybersäkerhetskrav påverkar projekt kan också variera beroende på organisationens struktur och interna ansvarsfördelning. Projektledare D och G menar på att i större organisationer är det ofta speciella avdelningar som ansvarar för cybersäkerhet. Den direkta påverkan på projekten kan därför uppfattas som indirekt, men projektledarna var överens om att påverkan ändå är betydande, särskilt vad gäller tid och kostnadsramar.

Projektledare H framhåller att säkerhetsarbete alltid handlar om avvägningar. Inom cybersäkerhet kan skyddsnivån höjas till en viss gräns, men det är inte realistiskt att uppnå ett fullständigt skydd. Som ett illustrativt exempel hänvisar projektledaren till 80/20-regeln, där 80 procent av säkerhetsbehoven kan täckas med cirka 20 procent av resurserna, medan de återstående 20 procenten kräver oproportionerligt mycket, upp till 80 procent av resurserna. Detta väcker frågan om hur mycket som faktiskt bör investeras i att täcka de sista och mest resurskrävande delarna. Projektledaren menar att en ambition att nå 100 procents skyddsnivå riskerar att leda till kraftiga förseningar och ökade kostnader, då projekten i praktiken aldrig blir färdiga under sådana förutsättningar.

4.2. Cybersäkerhetskrav som hinder eller stöd

Cybersäkerhetskraven kunde ses som hinder och som stöd i projektverksamheten, beroende på om fokus ligger på kortsiktiga eller långsiktiga mål. Projektledare B beskrev cybersäkerhetskrav som försvårande, särskilt i organisationer med låg mognadsgrad inom området. Utifrån detta perspektiv blir cybersäkerhetskraven en utmaning, eftersom organisationens grundläggande nivå inte alltid motsvarar det som projektet anser vara en nödvändig lägstanivå.

Projektledare F och H instämde i att cybersäkerhetskrav initialt kan försvåra projektets gång, särskilt med avseende på tid och effektivitet, men är särskilt viktig i en organisation där känsliga journaler hanteras. Att leverera utan att ta hänsyn till säkerhetsaspekter kan

verka enklare på kort sikt, men medför betydande risker. Istället argumenterade Projektledare F för att dessa krav, när de hanteras systematiskt, kan bidra till tydligare och mer effektiva arbetsprocesser, genom standardisering och strukturering av hur säkerhet ska integreras genom hela projektet. Projektledare E delade denna uppfattning, att cybersäkerhetskraven är nödvändiga, trots att de kan vara resurskrävande i utvecklingsfasen. Enligt Projektledare E är dessa krav avgörande för att uppnå långsiktig stabilitet och säkerhet i systemen, och måste därför beaktas som en investering i projektets framtida hållbarhet.

Projektledare G anser däremot att kraven varken förenklar eller försvårar arbetet för den som har erfarenhet och förståelse för dem. För den som är ny i rollen kan det vara värdefullt att förstå vad kraven innebär, men med erfarenhet blir det en naturlig del av arbetet. Projektledare G ser cybersäkerhet mer som ett arbetssätt för att säkerställa att saker görs på rätt sätt och att viktig företagsinformation skyddas, snarare än något som enbart skulle påverka projektets utmaningar eller resultat negativt. Projektledare C uttryckte en liknande uppfattning, där cybersäkerhetskraven betraktas som en självklar och nödvändig del av modern projektverksamhet. Dessa krav ökar projektens komplexitet och ställer högre krav på leverans och kompetens. Cybersäkerhetskrav ses som ytterligare en parameter att ta höjd för, de måste integreras tillsammans med övriga funktionella och icke-funktionella krav.

I linje med detta betonade andra respondenter vikten av att betrakta cybersäkerhet som en integrerad del av projektarbetet. Projektledare A beskrev cybersäkerhetskraven som en integrerad men komplicerad del av projektarbetet. De kan ibland upplevas som hinder eftersom de kan stå i konflikt med andra användarkrav, såsom funktionalitet eller tillgänglighet. Ofta blir kraven och deras komplexitet tydliga först senare i processen, vilket kan leda till förändringar under projektets gång. Dock lyfter Projektledare A att om cybersäkerhetskrav, som exempelvis GDPR, tydliggörs tidigt i projektet, kan det förenkla arbetet och bidra till att bygga lösningar med högre kvalitet redan från början.

Projektledare D delade en likande syn, att cybersäkerhetskrav inte nödvändigtvis försvårar projekten, utan snarare kräver ett nytt synsätt. Det handlar om att alla inblandade

behöver lära om och bygga upp ny kompetens. När kraven träder i kraft tar det tid för företagen att anpassa sig, men med ökad förståelse och kompetens kan det på sikt leda till ökad kostnadseffektivitet. Cybersäkerhetsarbetet ses därmed mer som en omställning än ett hinder.

4.3. Kompetens och hantering av kunskapsbrister

För att hantera de snabbt föränderliga krav och utmaningar som cybersäkerhet ställer på projektledning, lyfter flera projektledare fram vikten av kontinuerlig kompetensutveckling och anpassning. Projektledare A betonar hur svårt det kan vara att förutse exakt vilka cybersäkerhetsbehov som kommer att uppstå i ett projekt. Därför är det viktigt att både planera för och förbereda resurser i förväg, men också vara beredd att hantera eventuella kunskapsgap löpande under projektets gång, särskilt när agila metoder används. Detta innebär att vissa säkerhetskrav kan behöva hanteras genom löpande utbildning eller certifieringar, men även att projektmedlemmarna måste vara flexibla och öppna för att adressera säkerhetsfrågor som dyker upp under arbetets gång. Samtidigt poängterar Projektledare B vikten av att säkerhetsmedvetenheten inte bara är något som är kopplat till experterna, utan att det är en grundläggande del av hela projektteamets arbete. Både driftteknikker och verksamhetsanalytiker bör ha ett säkerhetstänk, även om deras huvudsakliga uppgifter kanske inte direkt relaterar till cybersäkerhet. Som Projektledare B förklarar, är det lätt att förlita sig på att tekniska system "bara fungerar", men ofta fallerar säkerheten vid förvaltningen, där rutiner för uppföljning och underhåll inte alltid är tillräckliga. Därför måste alla teammedlemmar förstå vikten av att kontinuerligt säkerställa att deras arbete följer de säkerhetskrav som gäller.

För andra projektledare, som Projektledare E, handlar det om att organisera expertisen på ett mer centraliserat sätt. Projektledare E delar synen att det är svårt att utbilda hela projektteamet i cybersäkerhet, och istället väljer de att låna in externa experter som kan fokusera på säkerheten under projektets gång. Denna modell gör det möjligt att få högspecialiserad kompetens i kritiska faser utan att belasta projektet med omfattande utbildningar för alla teammedlemmar. Samtidigt pekar Projektledare E på att det är viktigt att ha en tydlig ansvarsfördelning inom projektet, där de som är ansvariga för cybersäkerhet har ett klart mandat att ta beslut och driva säkerhetsåtgärder.

Projektledare F betonar att det inte bara handlar om att ha experter för säkerhetsfrågor, utan att säkerheten måste vara en integrerad del av hela projektverksamheten. Genom att involvera alla i projektet i cybersäkerhetsarbetet, även om de inte är experter, kan projektteamet säkerställa att säkerhetsaspekterna är en naturlig del av varje beslut och varje process. Projektledare F påpekar att alla medlemmar i tvärfunktionella team bör genomgå en grundläggande säkerhetsutbildning för att få en gemensam förståelse för risker och åtgärder. Vid behov kan vissa medarbetare få vidareutbildning eller specialiserade kurser, men den grundläggande säkerhetsmedvetenheten ska finnas på alla nivåer.

Projektledare D reflekterar över hur säkerhetsfrågor ofta hanteras i projektteam. Projektledaren beskriver att det i många fall finns en säkerhetsspecialist som ansvarar för cybersäkerheten, men att resten av projektteamet inte alltid lyssnar på eller förstår säkerhetsfrågorna. För att ett projekt ska kunna agera optimalt krävs det att gruppen har en god dynamik och att alla känner sig trygga att dela sina tankar, även när det handlar om säkerhet. Detta betyder att säkerhetsansvaret måste vara tydligt och att det är viktigt att alla i projektteamet förstår och respekterar expertens roll, samtidigt som expertens perspektiv tas med i alla beslut. Även om Projektledare G inte har arbetat direkt med projekt där cybersäkerhet är den centrala frågan, understryker Projektledare G av att ständigt anpassa säkerhetspolicys för att möta nya hot och förändringar. Detta visar på en gemensam insikt bland många projektledare om behovet av att vara proaktiv och flexibel i hur säkerheten hanteras, oavsett om det gäller att anpassa strategier eller att involvera expertkompetens under projektets gång.

Cybersäkerhet utvecklas snabbt, men kompetensen hänger inte med. Hoten har gått från tekniska brister till avancerade AI-baserade attacker och riktade sociala manipulationer. Människan har blivit den svagaste länken, och cybersäkerhet är nu lika mycket en mänsklig som en teknisk utmaning, berättar Projektledare H. Projektledare H betonar vikten av att fokusera på den mänskliga faktorn i cybersäkerhet. Medan många projekt fokuserar på tekniska lösningar, glöms ofta den mänskliga svagheten bort. Kriminella utnyttjar detta genom att manipulera människor för att komma åt systemet. Ett exempel är hot och utpressning riktat mot chefer för att få tillgång till företagsinformation.

Projektledare H nämner också hur enkelt det är att bli lurad, som i ett fall där studenter betalade för en lägenhet som inte existerade. Detta belyser hur lätt det är att manipulera systemet och skapa falska identiteter. Projektledare H påpekar att säkerhetsbrister ofta inte rapporteras och att företag kan bli utsatta för attacker utan att allmänheten får veta. För att motverka detta krävs ett kontinuerligt arbete med att förbättra cybersäkerheten. Problemet är att det inte finns tillräckligt många experter inom området och att de kriminella hela tiden utvecklar nya metoder för att utnyttja svagheter.

4.4. Dataintegritet och efterlevnad av regelverk

En gemensam strategi för att säkerställande av dataintegritet och efterlevnad av regler vid användning av AI och tredjepartsdata i projekt är att integrera cybersäkerhetskrav tidigt i projektet. Detta innebär att säkerställa att alla lösningar och system som utvecklas från början möter specifika säkerhetskrav och följer relevanta regelverk, såsom GDPR och andra internationella lagar. Projektledare A betonar att cybersäkerhetskrav inkluderas som en del av kravhanteringen i projektet och att det sker en löpande uppföljning. Om det uppstår situationer där krav inte kan uppfyllas fullt ut, görs avvikelsehantering och godkännande begärs från styrgruppen. Detta är ett sätt att hantera och förmedla risker inom projektet, särskilt i komplexa miljöer där flera krav kan krocka med varandra.

För att säkerställa att data används på ett korrekt sätt och inte bryter mot lagar som GDPR, används metoder som anonymisering och syntetiskt data. Projektledare E förklarar hur datakvalitetskontroller och kryptering av data både i vila och under överföring används för att skydda känslig information. Användningen av syntetiskt data är också en åtgärd för att minska beroendet av verkligt data under utveckling och testning. Detta kan bidra till att säkerställa att dataintegriteten inte äventyras och att inga oavsiktliga läckor av känslig information sker under utvecklingsprocessen.

En annan viktig aspekt som framkommer är hanteringen av tredjepartsdata. Projektledare A och E lyfter att det finns risker med att dela eller använda tredjepartsdata utan korrekt kontroll, vilket kan innebära att skyddad information kan bli åtkomlig för AI-lösningar. För att hantera detta är det viktigt att verifiera att AI-lösningar inte kommer åt eller använder skyddat data. Projektledare A påpekar också att AI inte alltid är felfritt och att

det fortfarande råder osäkerhet om vem som är ansvarig när AI gör misstag. Detta innebär att en kontinuerlig uppföljning av hur AI-system interagerar med data är nödvändig för att säkerställa att de följer både interna och externa regelverk.

Projektledare D påpekar även att den tekniska utvecklingen har gått snabbare än lagstiftningen, vilket gör att behovet av cybersäkerhet och efterlevnad av lagar har blivit mer tydligt på senare tid. Trots att IT-säkerheten bör vara en inbyggd del av alla system, likaså som användarupplevelse, user experience (UX), är det fortfarande nödvändigt att säkerställa att IT-säkerheten granskas för att förebygga säkerhetsproblem.

När det gäller AI, påpekar Projektledare D att användningen av AI i offentlig förvaltning är strikt reglerad och att det finns utbildning för att säkerställa korrekt användning och efterlevnad av regler. AI-verktyg får inte användas fritt utan kontrolleras noggrant för att garantera att de kommer från etablerade och säkra leverantörer. Projektledare D framhåller också att AI kan effektivisera processer, såsom dokumenthantering, men att dessa system måste byggas på rätt sätt från början och att det är upp till varje aktör att implementera tekniken ansvarsfullt och i enlighet med lagar. Projektledare H påpekar att AI har enorm potential för gott, till exempel inom medicin och forskning, men när den börjar tolka regler själv uppstår risker. Generativ AI kan utveckla egen vilja, vilket gör kontroll och reglering avgörande. Tekniken måste styras, annars kan den lika lätt skada som hjälpa.

För att säkerställa att alla åtgärder efterlevs och att inga säkerhetsrisker uppstår, är det också avgörande att involvera säkerhetsexperter och att det finns en strikt uppföljning av säkerhetsåtgärder. Projektledare B understryker att säkerhetslösningar implementeras med hjälp av externa säkerhetsexperter, och att säkerheten hanteras enligt både nationella och internationella standarder, vilket ger en grundläggande nivå av skydd mot intrång och dataförluster.

Säkerställandet av dataintegritet och efterlevnad av regler vid användning av AI och tredjepartsdata innebär att integrera cybersäkerhetskrav i hela projektets livscykel, implementera rätt tekniska lösningar som kryptering och anonymisering, samt att

kontinuerligt övervaka och hantera säkerhetsrisker som kan uppkomma under projektets gång.

4.5. Agilt och vattenfall: Likheter och skillnader i hantering

En kombination av agila och vattenfallsbaserade metoder är vanligt förekommande. Flera projektledare beskrev hur de använder vattenfallsmodellen som ett strukturerande ramverk för att definiera tidsramar, budget och scope i början av projektet, medan agila metoder används för att ge flexibilitet i genomförandet. Denna kombination gör det möjligt att hantera förändringar, till exempel nya cybersäkerhetskrav, utan att förlora kontrollen över projektet.

Projektledare H kombinerar både agila och vattenfallsmetoder beroende på projektets behov. Agilt fungerar bra i utvecklingsfaser, men kan vara ineffektivt om det inte tillämpas rätt, som när en testledare använde Scrum men förlorade 30 procent av arbetstiden på planering. Projektledare H föredrar att använda vattenfallsmodellen i början för struktur, och agilt under utveckling för flexibilitet. I byggprojekt fungerar agila metoder inte alls, eftersom det krävs strikt planering och standarder. Byggbranschen är mer förutsägbar, medan IT-projekt har många lösningar för samma problem, vilket gör planeringen svårare och mer flexibel. Projektledare H betonar att metoden måste anpassas efter projektets natur.

Detta instämmer Projektledare G med, där deras arbetsmetod ofta är en blandning av vattenfall och agilt arbete. De använder vattenfallsmodellen för att skapa en övergripande tidsplan, men inom varje fas arbetar de mer agilt för att kunna hantera förändringar och iterationer. På detta sätt får de det bästa av båda metoderna. Detta är också något som Projektledare D betonade när de beskrev hur det agila arbetssättet styr själva arbetsprocessen, men att en övergripande tidsplan inspirerad av vattenfall fortfarande är viktig för att hålla projektet på rätt spår.

Projektledare C underströk att den senaste trenden har varit att använda mer agila metoder, även om inslag av vattenfall fortfarande finns kvar, särskilt vid striktare deadlines eller externa krav som lagändringar. Detta kan ibland tvinga fram en mer linjär

och strukturerad arbetsgång, även om projektet annars är agilt. Projektledare B reflekterade över samma sak och betonade att för mer komplexa projekt där många system och aktörer är involverade, är agila metoder mest effektiva för att hantera iterationer och tester. Agilitet gör det möjligt att kontinuerligt testa och justera innan produktionen påbörjas.

När det gäller cybersäkerhet är det tydligt att alla projektledare ansåg att säkerhetstänkandet måste vara närvarande genom hela projektet, oavsett om projektledaren använder agila metoder eller vattenfallsmodellen. Projektledare E beskrev hur cybersäkerhet ofta integreras i det agila arbetet genom att säkerhetskraven läggs som egna stories i backloggen, det vill säga som specifika arbetsuppgifter eller funktioner som ska hanteras och prioriteras i utvecklingsteamets löpande arbete. Detta gör att de hanteras från början och är en naturlig del av utvecklingen. För att säkerställa efterlevnaden av säkerhetsstandarder i agila projekt använder Projektledare F en liknande metod genom att ha "Security Champions" i projektteamet, som kontinuerligt bevakar säkerhetsfrågor och ser till att alla krav uppfylls.

Projektledare B betonade att agila projekt är bra på att hantera förändringar i krav, vilket kan vara särskilt viktigt inom områden som OT (Operational Technology), där säkerhetskrav ofta är striktare. Här kan säkerhetskrav dock vara en utmaning, även i agila miljöer, då det kan krävas försiktighet och noggrant övervägande innan nya säkerhetskrav implementeras. Detta är något som Projektledare D också pekade på, då de nämnde att säkerheten i deras agila arbetssätt hanteras genom kontinuerlig dialog och konsultation med IT-säkerhetsavdelningen för att säkerställa att alla krav uppfylls utan att påverka projektets leveranstid eller kvalitet negativt.

Projektledare A, som hade en mer strukturerad syn på metodkombinationen, förklarade att de använder vattenfallsmetoden för att etablera ett tydligt scope och tidsramar inför projektstart. Inom de operativa faserna av projektet tillämpas dock agila metoder för att hantera krav som utvecklas och förändras under projektets gång. Denna kombination gör det möjligt att balansera mellan struktur och flexibilitet, vilket är särskilt viktigt när nya cybersäkerhetskrav dyker upp under projektets gång.

Samtliga projektledare bekräftade att en hybridmodell, där både agila metoder och vattenfallsmodellen används, är vanlig. Denna metodik gör det möjligt att anpassa arbetsprocessen till projektets specifika behov och krav. Projektledare G förklarade att detta innebär att de ofta planerar enligt vattenfallsmodellen men arbetar agilt inom varje fas, vilket gör att de kan hantera osäkerheter och förändringar utan att tappa kontrollen över projektets övergripande mål. Projektledare A berättade om sin vana att använda vattenfall för projektets (långsiktiga) planering, genomförande, rapportering och leveranser gentemot externa intressenter (som styrgrupp och mottagare av resultat) och agil metodik, ofta scrum, för det dagliga arbetet inom projektet. På så sätt användes en hybridmodell, där projektets interna (kortsiktiga) planering, genomförande och uppföljning följde agila principer inom teamet. Arbetsmoment för den externa projektplanens förvaltning hanterades i en backlog. Detta omfattade även mer projektadministrativa delar som till exempel beredning rapport eller demo till styrgruppsmöten, även om tyngdpunkten i backloggen låg på aktiviteter kopplade till projektets målsatta leveranser (vanligen implementering av tekniska och funktionella krav i ett IT-system).

4.6. Strategier och framtida behov

Inom cybersäkerhet betonas ett starkt behov av att anpassa sig till det snabbt föränderliga digitala landskapet. Projektledarna belyser hur säkerhet inte längre enbart kan hanteras som en separat funktion utan måste integreras i projektens alla faser och på alla nivåer. Projektledare A beskriver hur införandet av AI påverkar möjligheten att planera och styra projekt på traditionellt sätt. Tidigare har arbetet byggt på tydliga riktlinjer, tydligt definierade mål och förväntade resultat.

Detta behov av anpassning återkommer hos flera projektledare, inte minst i relation till cybersäkerhet. Projektledare B understryker att säkerhetsspecialister borde vara en självklar del i alla projekt, oavsett inriktning. Att omge sig med personer som har djup kompetens inom detta område ses som avgörande för projektens långsiktiga hållbarhet. Projektledare E delar denna syn, men beskriver en modell där expertis istället organiseras centralt i ett "center of excellence" och lånas in vid behov. Enligt Projektledare E är detta

en kostnadseffektiv lösning som möjliggör hög kvalitet i kritiska skeden, särskilt under utvecklingsfasen, samtidigt som resurser används smartare under underhållsfasen.

Projektledare F vidgar perspektivet ytterligare och lyfter fram vikten av att hela projektverksamheten har en grundläggande säkerhetsmedvetenhet. Enligt Projektledare F räcker det inte längre med att bara vissa har specialistkunskap, utan alla involverade behöver en grundläggande förståelse för cybersäkerhet. Projektledare F menar att denna kompetens bör ses som en kärndel i hur projekt organiseras framåt, i en tid där hotbilden ständigt förändras och kraven blir fler.

Samtidigt pekar Projektledare C på att det fortfarande finns strukturella begränsningar inom vissa organisationer. Projektledare C beskriver en situation där strategiska beslut och säkerhetskrav formuleras centralt, ofta av säkerhetsavdelningen, och där projektledare snarare förväntas anpassa sig än att vara delaktiga i strategiarbetet. Denna uppdelning mellan operativt och strategiskt arbete innebär att de som befinner sig i projekten ibland saknar inflytande över de ramar de behöver förhålla sig till, vilket kan försvåra ett proaktivt säkerhetsarbete.

Projektledare D ger uttryck för ett liknande utifrånperspektiv, men utifrån en mer reflekterande position. Projektledaren D beskriver sig själv som relativt ny i rollen och relaterar till hur nya lagkrav och regleringar nu får direkt påverkan på projektarbetet, något respondenten inte tidigare behövt hantera. Projektledare D ser också en framtid där sådana krav kommer att öka i takt med samhällets digitalisering, vilket i sin tur ställer krav på kontinuerlig kompetensutveckling hos alla yrkesverksamma inom området. Denna syn delar Projektledare E och menar på att:

> "Företaget vill alltid vara bättre än lagarna, så att när en lag kommer så tittar de på den och lägger på 25 procent. De försöker alltid vara bättre än vad kraven är, dels för att de är smarta och inser att kraven kommer att gå upp, men också för att de vill vara en ansvarstagande spelare på marknaden".

Genom att ligga steget före lagstiftningen positionerar sig företaget inte bara som proaktivt och ansvarstagande, utan skapar också handlingsutrymme i projektarbetet. Ett

sådant förhållningssätt stärker projektens motståndskraft och säkrar framtiden både kompetens och leverans, i en tid där regelverken inte längre enbart utgör något att förhålla sig till, utan i allt högre grad formar själva förutsättningarna för projektgenomförande.

Vikten av att ständigt ligga steget före hotaktörer betonas av flera respondenter, inte minst i beskrivningen från Projektledare H, som reflekterar över cybersäkerhetens begränsningar och krav på proaktivt tänkande:

> "Man kan bara skydda sig så mycket som kompetensen ger dig, den tekniken som finns idag och det du vet. Utmaningen för säkerhetsavdelningar är att ständigt ligga steget före de kriminella aktörerna. När någon utvecklar en ny metod att angripa system skapas hål och sen gäller det att snabbt sprida kunskap. Det gäller att tänka framåt - vad kan bli nästa steg i säkerhetsaspekten. Hur stoppar man hot mot människor?"

Projektledare H refererar till en incident från 2000-talet, känd som "Love Letter", där en hög chef mottog ett e-postmeddelande som till synes kom från en trainee. Meddelandet visade sig dock vara ett skadligt program skapat av en hackare, vilket ledde till att angriparen fick tillgång till chefens kontaktlista, en särskilt allvarlig konsekvens med tanke på chefens höga position och omfattande nätverk inom företaget. Denna händelse fungerar som en tidig påminnelse om hur social manipulation kan användas för att kringgå tekniska skydd, en sårbarhet som fortsatt är relevant i dagens digitala landskap. Om ansvarsfördelningen i projekt inte hade varit formellt uttalad eller personbunden, skulle det kunna försvåra för de kriminella att kartlägga beslutsvägar och manipulera specifika roller för att få tillgång till känslig information. I takt med att AI utvecklas och används både inom försvar och angrepp, blir behovet av proaktivt säkerhetsarbete och stärkt motståndskraft mot nya typer av hot, som hot mot människor, alltmer avgörande för framtida projekt och samhällens långsiktiga resiliens.

5. Analys

Följande kapitel presenterar en analys med hjälp av studiens teoretiska referensram och empiri. Analysen är strukturerad på ett sätt som syftar till att besvara studiens forskningsfrågor.

5.1. Cybersäkerhetskravens inverkan på projekttriangeln

Projekttriangeln, bestående av tid, kostnad och omfattning, tydliggör det ömsesidiga beroende som präglar planering och genomförande inom projektverksamhet. Enligt Tonnquist (2018) innebär en förändring i ett hörn av triangeln en oundviklig påverkan på minst ett annat hörn, med konsekvenser för projektets totala kvalitet. Denna dynamik visas tydligt i resultatet, där samtliga projektledare beskriver hur nya cybersäkerhetskrav påverkar både resurstilldelning och genomförandetakt.

Resultatet pekar på att cybersäkerhetskraven ofta medför ökad tidsåtgång. Till exempel att krav på godkännanden, utbildningar och samordning lett till förseningar, i ett fall med upp till tre veckors fördröjning. Detta överensstämmer med Tonnquist (2018) beskrivning av hur nya krav (ökad omfattning) ofta kräver justering av tidsplanen för att kunna hanteras. Kostnadsmässigt uppstår påverkan främst genom behovet av extern kompetens och utökade resurser. Projektledarna nämner att bristande intern mognad inom cybersäkerhet kräver att företag anlitar externa experter, vilket lett till ökade kostnader och i vissa fall till att nya projekt fått startas parallellt. Detta illustrerar hur cybersäkerhetskrav, när de tillkommer utifrån snarare än integreras tidigt, kan skapa oplanerade utgifter, vilket riskerar att spräcka budgetramar. Om detta sker, enligt Tonnquist (2018) och projektledarna, krävs det omfördelning av resurser eller minskad omfattning på andra delar av projektet.

När nya cybersäkerhetskraven tillkommer under projekts gång beskrivs det av projektledarna som en förändring av projektets omfattning. Fler krav innebär fler aktiviteter, exempelvis mer dokumentation, fler tester och noggrannare planering. Denna ökade omfattning förutsätter i sin tur större resursinsats, vilket påverkar både tid och kostnad, i linje med projekttriangelns princip om ömsesidig påverkan (Tonnquist, 2018). Däremot enligt Kitsios et al. (2022) och Weil (2020) är dokumentation och

processhantering avgörande för en framgångsrik ISMS-implementering och kan bidra till att attrahera nya kunder genom ökad trovärdighet. Cybersäkerhetskraven bör därför ses som en långsiktig investering snarare än en kortsiktig kostnad. Detta bekräftas av Podrecca et al. (2022), som i sin studie visar att företag som investerar i informationssäkerhet får ökad lönsamhet, arbetsproduktivitet och försäljningsprestanda. Detta perspektiv lyfter ett centralt dilemma: även om krav på cybersäkerhet (omfattning) initialt kan leda till högre kostnader och förlängd tid, enligt projekttringeln (Tonnguist, 2018), kan det samtidigt bidra till att minska risken för framtida incidenter. Ett exempel på en sådan incident är en ransomware-attack som, enligt en projektledare, orsakade ett produktionsbortfall på tre månader i ett projekt. I ett sådant scenario är kostnaden för förebyggande åtgärder betydligt lägre än de kostnader och produktionsbortfall som uppstår vid en faktisk säkerhetsincident, vilket också rör projektets kvalitet i form av tillförlitlighet och långsiktig robusthet. Företagens struktur och ansvarsfördelning påverkar hur cybersäkerhetskrav påverkar projekten. I större organisationer är säkerhetsansvaret ofta centraliserat, vilket kan skapa en illusion av att påverkan är indirekt. Men påverkan på tid och kostnad är ändå tydlig, även om den inte alltid hanteras inom projektets kärnteam.

Enligt Kitsios et al. (2022) kan företag identifiera specifika hot och anpassa sina kontroller genom att använda en riskbedömningsram baserad på exempelvis ISO 27005 och NIST SP 800-30. I resultatet framkommer det dessutom att det anses fördelaktigt att ligga steget före gällande lagstiftning. När nya krav införs ses det som en god strategi att addera en säkerhetsmarginal på cirka 25 procent. Företag bör sträva efter att överträffa minimikraven, både utifrån att regelverken sannolikt kommer att skärpas över tid och för att agera som en ansvarstagande aktör på marknaden. Däremot betonas en vikt av att göra medvetna och realistiska avvägningar i projekt. Det går att bygga säkerhet till en viss nivå, men den kommer aldrig kunna skyddas till 100 procent. I praktiken handlar det om att identifiera en rimlig skyddsnivå som står i proportion till projektets resurser och mål. Ett användbart angreppssätt är den så kallade 80/20-regeln: ofta kan 80 procent av säkerheten uppnås med endast 20 procent av resurserna, medan resterande 20 procent kräver oproportionerligt stora insatser. Den avgörande frågan blir därför hur mycket tid och budget som faktiskt bör avsättas för att nå nära full säkerhet, något som riskerar att

spräcka tidsramar och göra projektet ekonomiskt ohållbart. Att acceptera att viss risk alltid kommer att finnas är därför en förutsättning för att kunna fatta kloka beslut och driva projekt framåt, med andra ord, enligt Tonnquist (2018), att finna en optimal balans mellan tid, kostnad och omfattning.

5.2. Hantering av säkerhetskrav i agilstyrda projekt

Agila metoder kännetecknas av flexibilitet, snabb återkoppling och iterativ utveckling. Denna struktur möjliggör kontinuerlig anpassning av projektets omfattning och prioriteringar, vilket också skapar utrymme för att integrera cybersäkerhetskrav successivt under projektets gång (Ceyda et al., 2023; Thummadi & Lyytinen, 2020). Resultatet visar dock att dessa krav både kan uppfattas som stödjande och hindrande beroende på organisatorisk mognad, kompetensnivå och hur tydligt kraven är förankrade i projektets arbetsprocess. Flera projektledare beskriver hur cybersäkerhetskrav initialt kan upplevas som resurskrävande och försvårande, särskilt i utvecklingsfasen. Detta bekräftar den teoretiska problematik som Mankertz (2023) och Felici et al. (2015) beskriver: att agila projekt kan ha svårt att balansera behovet av snabbhet med säkerhetsrelaterade investeringar i utbildning, teknik och processer. Samtidigt visar resultatet att när cybersäkerhetskrav integreras systematiskt och iterativt, kan de bidra till ökad struktur och kvalitet i projektarbetet. Till exempelvis hur säkerhetsaspekter kan standardiseras och struktureras genom hela projektets cykler, vilket överensstämmer med Salin & Lundgrens (2022) ramverk för agil riskhantering.

Det agila ramverket visar att cybersäkerhetsrisker kan hanteras effektivt genom att prioriteras och åtgärdas i sprintar, dokumenteras i backloggen och följas upp genom återkommande sprintplanering och kunskapsöverföring. Detta arbetssätt återfinns också i resultatet, hur säkerhetskrav inkluderas som stories i backloggen eller hanteras av särskilda "Security Champions" i projektteamet, något som möjliggör löpande anpassning utan att bromsa utvecklingstakten. En ytterligare aspekt som framträder genomgående i resultatet är vikten av relevant kompetens. Det krävs ett nytt synsätt och ökad förståelse inom hela projektteamet för att cybersäkerhetskrav ska bli en naturlig del av det agila arbetet. Detta ligger i linje med det fjärde steget i Salin & Lundgrens (2022) ramverk, kunskapsöverföring, där lärdomar från tidigare sprintar systematiskt sprids inom projektteamet. Det visar sig också att erfarenhet spelar en avgörande roll. För

projektledare med erfarenhet blir säkerhetskrav snabbt en självklarhet, medan mindre erfarna ofta upplever dem som hinder, ett perspektiv som speglar vikten av långsiktig kompetensuppbyggnad inom agila projekt.

Resultatet visar att i agila projekt, trots sin flexibilitet, också har vissa begränsningar. Cybersäkerhetskrav hamnar ibland i konflikt med användarkrav, vilket kan skapa komplexitet i prioriteringsarbetet, där kompromisser ofta behöver göras. Cybersäkerhetskrav i agila projekt kan hanteras effektivt om de integreras tidigt, förankras i projektteamets arbetsprocess och kombineras med kontinuerlig kompetensutveckling. Kraven uppfattas då inte som hinder, utan som ett stöd för ökad kvalitet, struktur och riskminimering.

En aspekt som bör beaktas är att den mänskliga faktorn kan få ökad betydelse i agila projekt där roller och ansvarsfördelning inte alltid är tydligt definierade, vilket Krishna & Gopinath (2024) också lyfter. Resultatet visar att otydlighet kring vem som bär ansvar för olika säkerhetsrelaterade beslut kan skapa sårbarhet, särskilt vid bedrägeri eller andra mänskligt riktade hot. Om det är oklart vem som ska skyddas eller vem som kan påverkas, ökar risken för att sådana hot inte upptäcks eller hanteras i tid. Samtidigt kan denna flexibilitet också vara en styrka om projektteamet har en gemensam förståelse för säkerhet och förmåga att snabbt anpassa sig. Detta understryker vikten av att även i agila miljöer arbeta med tydlig kommunikation, rollfördelning och kontinuerlig medvetenhet kring säkerhetsfrågor.

Ur ett externt perspektiv, visar resultatet att otydliga roller i agila projekt även kan innebära en viss fördel ur ett cybersäkerhetsperspektiv. När ansvarsfördelningen inte är formellt uttalad eller personbunden, kan det försvåra för externa angripare att identifiera nyckelpersoner att rikta sig mot genom exempelvis bedrägeri. Bristen på tydliga kontaktpunkter gör det svårare att kartlägga beslutsvägar och att manipulera specifika roller för att få tillgång till känslig information. Detta visar att flexibilitet och distribuerat ansvar i vissa fall kan fungera som ett skydd, även om det samtidigt ställer höga krav på intern transparens och koordinering för att undvika säkerhetsluckor internt.

5.3. Hantering av säkerhetskrav i vattenfallsstyrda projekt

Vattenfallsmodellen kännetecknas av sin linjära och fasindelade struktur där varje moment i projektet bygger vidare på det föregående. Denna sekventiella ordning erbjuder tydlighet och förutsägbarhet, vilket gör modellen särskilt lämplig i projekt med väldefinierade och stabila krav (Thummadi & Lyytinen, 2020). Denna struktur möjliggör en systematisk integrering av cybersäkerhetskrav, under förutsättning att kraven är kända tidigt i projektets livscykel. Resultatet visar dock att denna styrka också kan utgöra en sårbarhet när säkerhetskrav förändras eller tillkommer sent i processen. Flera projektledare lyfter vikten av att identifiera cybersäkerhetskrav tidigt. När kraven kommer in sent i ett vattenfallsstyrt projekt riskerar det att skapa omfattande omarbetningar, vilket kan bli både kostsamt och tidskrävande. Detta överensstämmer med Thummadi & Lyytinen, (2020), som betonar att förändringar efter designfasen ofta leder till ökade kostnader och fördröjningar. Exempelvis beskrivs hur krav som GDPR, om de inte är kända från start, kan bidra till större förändringar senare i processen, något som kan påverka hela projektets struktur negativt.

Resultatet visar att vattenfallsmodellen erbjuder goda möjligheter till strukturerad säkerhetsplanering. Tydliga processer och ansvarsfördelning gör det möjligt att hantera säkerhetskraven metodiskt, särskilt om experter kopplas in i rätt fas. Detta ligger i linje med Baldassarre et al. (2020), som beskriver hur cybersäkerhet bör integreras i varje fas av vattenfallsmodellen, från kravanalys till underhåll. I kravfasen fastställs de grundläggande säkerhetsbehoven, i designfasen införs tekniska lösningar för att minska attackytor, och i testfasen används simulerade attacker för att utvärdera skyddsnivån. Flera projektledare uttrycker också att cybersäkerhetskrav inte nödvändigtvis är ett hinder i sig, utan snarare kräver rätt kompetens och planering. Detta bekräftar vikten av kontinuerlig kunskapsuppbyggnad i projektteamet, särskilt i projekt där struktur och dokumentation är centralt. Denna typ av projekt ställer höga krav på att rätt kompetens finns på plats i rätt fas, något som också framhålls i resultatet, där cybersäkerhetsexpertis tillförs vid kritiska punkter snarare än att spridas över hela projektteamet.

Det framgår av Sinha & Das (2021) att vattenfallsprojekt, till skillnad från agila projekt, inte har samma flexibilitet att iterativt testa och justera säkerhetslösningar, som även bekräftas i resultatet. Därför blir det särskilt viktigt att cybersäkerhetskrav är tydligt definierade, dokumenterade och godkända i kravfasen. Projektledarna beskriver hur krav från externa regelverk eller hos kund ibland formuleras centralt utan att de själva är involverad, vilket kan skapa en klyfta mellan beslutsfattande och operativt genomförande. Detta kan leda till ineffektivitet och ökade risker om säkerhetskraven inte är tillräckligt integrerade från början. Enligt Sinha & Das (2021) kan vattenfallsmodellen vara effektiv för att hantera cybersäkerhetskrav, men bara under förutsättning att dessa krav identifieras och förankras tidigt, vilket även framkommer i resultatet. Den linjära strukturen möjliggör en noggrann planering och uppföljning av säkerhetsaktiviteter genom hela projektet, men skapar också begränsningar när förändringar behöver genomföras i senare faser. Därför blir det avgörande att investera i tidig säkerhetsanalys, dokumentation och tydlig ansvarsfördelning, för att undvika att cybersäkerhet blir en kostsam flaskhals i slutet av projektet.

I vattenfallsstyrda projekt, där roller och ansvarsfördelning ofta är tydligt definierade, kan den mänskliga faktorn utgöra en säkerhetsrisk. Resultatet indikerar att hot som riktar sig mot individer, exempelvis genom “Love Letter”, bedrägeri eller utpressning, riskerar att förbises i miljöer där kommunikation sker främst genom formell dokumentation snarare än löpande dialog. Detta understryker vikten av att inte enbart fokusera på tekniska lösningar, utan även inkludera mänskliga och organisatoriska sårbarheter i den tidiga säkerhetsanalysen.

5.4. Hybridmodellens möjligheter och begränsningar

Hybridmodellen, en kombination av agila och vattenfallsbaserad projektstyrning, beskrivs av projektledarna som ett vanligt förekommande tillvägagångssätt. Flera projektledare framhåller att en hybridmodell möjliggör både struktur och flexibilitet. Den övergripande projektplanen utformas ofta enligt vattenfallsmodellens logik, där tid, budget och omfattning definieras tidigt, till kund. Samtidigt tillämpas agila principer inom respektive fas eller leveranscykel, inåt i teamet, vilket gör det möjligt att iterativt anpassa sig till förändrade krav, exempelvis när nya cybersäkerhetsaspekter uppstår.

Detta överensstämmer med fallstudierna i teorin om hybridmodellers styrkor, där struktur från vattenfall kombineras med agilitetens reaktionsförmåga (Krishna & Gopinath, 2024; Lobo Marques et al., 2023; Shimoda och Yaguchi, 2024). I projektmiljöer där osäkerhet råder eller där omfattande regelverk måste följas, exempelvis inom IT, offentlig verksamhet eller teknikområden relaterade till AI erbjuder en hybridmodell ett flexibelt ramverk för att hantera både långsiktiga krav, via vattenfall och kortsiktiga justeringar, via agilt.

I resultatet framkommer det att cybersäkerhetskrav ofta hanteras just genom denna kombinerade metodik. Säkerhetskrav i agila faser integreras som stories i backloggen och därmed hanteras kontinuerligt, medan det finns ett tydligt ramverk för ansvarsfördelning och mål enligt en vattenfallsstruktur. På detta sätt kan säkerhetskrav både planeras in från början och justeras längs vägen. Detta speglar teorin från Baldassarre et al. (2020) betonar vikten av att integrera säkerhet på ett strukturerat sätt i linjära projektmodeller, medan Salin och Lundgren (2022) visar hur detta i en hybrid kontext kompletteras med agila inslag, såsom riskhantering i sprintformat och dagliga stand-up-möten. En styrka med hybridmodellen, enligt flera projektledare, är att den möjliggör prioritering av säkerhetsaspekter utan att förlora kontrollen över projektets omfattning och leveranser. Agila metoder kan vara nödvändiga för att hantera förändringar, men att vissa externa krav (exempelvis lagkrav) kräver en mer linjär och strukturerad arbetsgång. Hybridmodellen blir då ett verktyg för att balansera dessa behov.

Enligt Shimoda och Yaguchi (2024) kräver en hybridmodell tydlig kommunikation, ansvarsfördelning och koordinering mellan olika arbetssätt. Hybridmodellen fungerar särskilt bra när cybersäkerhetskraven är både stabila och föränderlig, vissa krav kan definieras och implementeras strukturerat, medan andra måste hanteras iterativt i takt med att ny teknik introduceras, vilket exemplifieras i resultatet med användningen av AI och molntjänster. Kombinationen av fasta faser och flexibel utveckling gör det möjligt att möta både regelverk och marknadsdrivna behov, men kräver att organisationen har tillräcklig mognad och kompetens för att hantera komplexiteten i kombination av metoder.

I hybridmodellen, där projektarbetet växlar mellan strukturerade faser och iterativa moment, kan den mänskliga faktorn ta sig olika uttryck beroende på var i processen ett hot uppstår. Resultatet visar att just växlingen mellan agilt och vattenfall kan skapa otydlighet kring vem som ansvarar för säkerhetsrelaterade beslut i olika faser. I praktiken kan detta innebära att informationsöverföring mellan delmoment brister, vilket öppnar upp för sårbarheter, särskilt vid bedrägeri eller bedrägeriförsök riktade mot specifika individer. För att begränsa denna typ av risker behövs en klar ansvarsfördelning mellan olika arbetssätt, i kombination med ett gemensamt säkerhetstänkande som genomsyrar hela projektets livscykel.

6. Diskussion

Följande kapitel ger en subjektiv reflektion kring studien resultat. Kapitlet avslutas med att ge ett kort konkret svar på studiens forskningsfrågor.

6.1. Reflektion och argumentation

Vi ser att cybersäkerhetskrav inte längre kan betraktas som en separat del av projektarbetet, utan som en integrerad och strategisk komponent i samtliga projektfaser, oavsett vald projektstyrningsmetod. Cybersäkerhet utvecklas därmed från att vara ett tekniskt specialistområde till att bli en strategiskt viktig del av organisationen, med påverkan på både projektens strukturer och den övergripande organisationskulturen.

En central reflektion är att cybersäkerhetskrav upplevs olika beroende på organisationens mognadsgrad, projektmetod och individens erfarenhet. Medan kravuppfyllelse i agila projekt kan ske iterativt och integreras i sprintplaneringar, krävs i vattenfallsmodellen att säkerhetskraven är väldefinierade redan från början. I praktiken innebär detta att samma krav kan uppfattas som stödjande i en agil kontext, men som hämmande i vattenfallsstyrda projekt, särskilt om de uppstår sent i processen. Här synliggörs också ett viktigt argument: att metoden i sig inte avgör hur effektivt säkerhetskrav hanteras, utan hur bra de är anpassade till organisationens struktur, resurser och kompetens. Vi tolkar det som att hybridmodellen framstår som ett verklighetsnära svar på komplexiteten. Genom att kombinera förutsägbarheten i vattenfall med den anpassningsförmåga som finns i agila metoder, ges bättre förutsättningar att hantera cybersäkerhetskrav av både stabil och dynamisk karaktär (Shimoda och Yaguchi, 2024). Men detta ställer i sin tur krav på tydlig ansvarsfördelning, god kommunikation och inte minst, säkerhetskompetens, både centraliserad och spridd i projektverksamheter.

En annan viktig aspekt är tidsperspektivet. Diskussionen om cybersäkerhetskrav som hinder eller stöd knyts ofta till om fokus ligger på kortsiktiga leveranser eller långsiktig hållbarhet. Flera projektledare betonar vikten av att se cybersäkerhet som en investering snarare än en kostnad, vilket även bekräftas av Podrecca et al. (2022), som i sin studie visar att företag som investerar i informationssäkerhet får ökad lönsamhet, arbetsproduktivitet och försäljningsprestanda. Detta perspektiv utmanar traditionella sätt att se på projektmål, där fokus ofta ligger på att optimera tid, kostnad och omfattning i

närtid, snarare än att bygga robusta lösningar över tid (Tonnquist, 2018). Här finns en spänning mellan projektekonomi och strategisk riskhantering, där cybersäkerhet utgör en bro mellan dessa två perspektiv. Företag som lyckas integrera cybersäkerhet på ett naturligt och värdeskapande sätt, har ofta gemensamma kännetecken, de har etablerade arbetssätt för att hantera krav, tydliga roller och ansvar samt en kultur där säkerhetsfrågor inte bara är något för experterna, utan för hela projektteamet. Detta sker inte per automatik, det krävs aktiva insatser i form av utbildning, kunskapsöverföring och inte minst, ledarskap som ser cybersäkerhet som en central del av verksamhetsutvecklingen. Genom att använda en riskbedömningsram baserad på exempelvis ISO 27005 och NIST SP 800-30 kan företag identifiera specifika hot och anpassa sina kontroller (Kitsios et al., 2022).

Ytterligare en aspekt som väcker frågor är den mänskliga faktorn. Det kan diskuteras om medlemmar i ett projekt bör hållas anonyma för allmänheten av säkerhetsskäl. Genom att inte offentliggöra, via sociala medier eller andra plattformar, vilka individer som är involverade i ett projekt kan risken för riktade cyberattacker, som exempelvis bedrägeri eller nätfiske, minska. Samtidigt uppstår en avvägning mellan öppenhet och säkerhet, särskilt i projekt där samverkan och extern kommunikation är centrala. Det kan därför vara relevant att överväga rutiner för hur synlig projektorganisationen bör vara, beroende på projektets känslighet och risknivå.

I agila projekt uppmuntras det att arbeta öppet, exempelvis genom projekttavlor, stand-up-möten och aktiv närvaro i digitala samarbetsytor. Denna öppenhet kan skapa sårbarheter om individers identiteter och arbetsroller kan exponeras i för stor utsträckning, särskilt i projekt med hög känslighetsgrad eller säkerhetskrav. Vi ser att projektledare behöver balansera öppenheten som är grundläggande för det agila arbetssättet med säkerhetsrutiner som skyddar individens och projektets integritet. Det kan handla om att begränsa vilka uppgifter som delas externt, att anonymisera roller i offentliga sammanhang, eller att ha tydliga policyer för vad teammedlemmar får publicera.

I mer traditionellt vattenfallsstyrda projekt kan projektledare i högre grad styra hur och när information om projektets organisation kommuniceras, samt säkerställa att personuppgifter hanteras enligt etablerade säkerhetsprotokoll. Samtidigt är det vanligt att kunden sätter ramarna för vad som får delas externt, särskilt i upphandlade projekt eller projekt som omfattas av sekretess. Vi ser att projektledare därför har ett operativt ansvar att samordna intern kommunikation och informationshantering i enlighet med både interna riktlinjer och externa krav. Dock kan även dessa projekt vara utsatta om medarbetares roller eller kontaktuppgifter görs synliga i exempelvis rapporter, samarbetsverktyg eller kommunikationsplaner som delas utanför organisationen. Det ställer krav på tydliga rutiner och en medveten strategi för hur projektorganisationens synlighet hanteras, även i strukturerade och regelstyrda sammanhang.

I hybridmodellen, där element från både agila och vattenfallsstyrda arbetssätt kombineras, ser vi att det uppstår en särskild utmaning när det gäller att hantera den mänskliga faktorn. Här varierar graden av öppenhet och dokumentation beroende på projektets fas, delprojekt eller teamstruktur, vilket kan skapa otydlighet kring vilka säkerhetsrutiner som ska gälla. I vissa delar av projektet kan ett agilt arbetssätt dominera, med hög transparens och täta avstämningar, medan andra delar är mer formella och styrda enligt vattenfallsprincipen. Något som vi har reflekterat över är att detta ställer krav på att projektledare inte bara anpassar informationshanteringen utifrån metod, utan även aktivt bedömer risknivån i olika delar av projektet. Det kan exempelvis innebära att införa selektiv öppenhet, där viss information är tillgänglig för interna team men begränsas externt, eller att utforma differentierade kommunikationsrutiner beroende på känsligheten i det aktuella arbetspaketet. En viktig roll för projektledare i hybridprojekt blir därför att identifiera när öppenhet bidrar till effektivitet och samverkan, och när den behöver begränsas till förmån för integritet och säkerhet. Vi anser därför att det krävs både metodkompetens och en förståelse hos projektledare, för hur projektets olika delar interagerar med varandra organisatoriskt, tekniskt och kommunikativt.

Det väcks frågor kring framtiden: Hur säkerställer konsultföretag kontinuerlig kompetensutveckling i takt med nya lagkrav och teknikutveckling? Hur kan cybersäkerhet integreras redan i projektinitieringsfasen utan att skapa överarbete eller

förlamning? Och hur förflyttar sig synen på cybersäkerhet från reaktiv krishantering till proaktiv affärsstrategi? Hur kan den mänskliga faktorn hanteras som en säkerhetsrisk i framtidens projekt? Det finns inte en universell lösning, men genom att ha ett medvetet och systematiskt förhållningssätt, där metodval, kompetens och kommunikation samspelar, är avgörande för att möta framtidens cybersäkerhetskrav i projektverksamheten.

6.2. Besvarande av forskningsfrågorna

F1: Hur kan nya cybersäkerhetskrav påverka tid, kostnad och omfattning för projekt?

Studien visar att nya cybersäkerhetskrav påverkar projektets tre grundparametrar, tid, kostnad och omfattning, på ett ömsesidigt och dynamiskt sätt. Kraven tenderar att introducera fler aktiviteter (ökad omfattning), vilket i sin tur kräver mer tid och ökade resurser. Om kraven inte integreras i ett tidigt skede riskerar de att skapa oplanerade omarbetningar och kostnadsökningar. Däremot ses kraven också som en långsiktig investering som stärker kvaliteten och minskar risken för framtida incidenter. Hur mycket dessa krav påverkar projektets parametrar beror dock i hög grad på hur omfattande skydd projektet väljer att implementera. I enlighet med 80/20-regeln kan en stor del av riskerna hanteras genom relativt begränsade insatser, medan en ambition att uppnå fullständig säkerhet ofta kräver oproportionerligt stora resurser. Projektledaren har därför en viktig uppgift i att avväga ambitionsnivån, så att säkerhetsåtgärderna förblir proportionerliga i förhållande till projektets mål, riskbild och tillgängliga resurser.

F2: Hur kan nya cybersäkerhetskrav effektivt hanteras av projektledare i agila respektive vattenfallsstyrda projekt?

I agila projekt hanteras cybersäkerhetskrav bäst när de integreras löpande i sprintar och backlogg, samt när projektteamet har ett gemensamt säkerhetsmedvetande. Agilitet möjliggör anpassning, men kräver struktur och säkerhetskompetens. Projektledare behöver etablera tydliga riktlinjer för vilken information som delas, var och hur, exempelvis genom att begränsa personlig identifierbar information i digitala samarbetsytor och skapa gemensamma rutiner för vad teammedlemmar kommunicerar externt.

I vattenfallsstyrda projekt krävs att säkerhetskraven definieras och dokumenteras tydligt i kravfasen, då sena förändringar blir kostsamma och tidskrävande. Här bör projektledare, i nära dialog med kunden, upprätta en detaljerad kommunikationsplan som specificerar ansvar, godkända informationskanaler och hantering av projektorganisationens synlighet. Genom att styra informationsflödet tidigt kan säkerheten integreras i både dokumentation och samverkan med externa parter.

Genom att kombinera struktur, exempelvis tid och budget, externt till kund, med anpassningsförmåga exempelvis arbetsprocessen, internt i teamet, inom varje fas skapar hybridmodellen förutsättningar för att hantera både stabila och föränderliga krav, förutsatt att roller, ansvar och kommunikationsvägar är tydligt definierade. Förutsättningen är att projektledare tydligt definierar roller, ansvar, kommunikationsvägar och säkerhetsrutiner för varje del av projektet. Vi anser därför att informationshantering bör anpassas efter metod, men styras utifrån en sammanhållen strategi som prioriterar både säkerhet och effektivitet.

Oavsett projektstyrningsmetod är det avgörande att ligga steget före kraven genom proaktiv planering, kontinuerlig kompetensutveckling och tidig involvering av säkerhetsexpertis. Effektiv hantering förutsätter inte bara tekniska lösningar, utan också ett strategiskt synsätt där cybersäkerhet ses som en integrerad och affärskritisk del av projektets genomförande, inklusive hur och när projektorganisationen exponeras öppet utåt.

7. Slutsats

Följande kapitel presenterar en slutsats i form av praktiska och teoretiska bidrag, samt begränsningar med studien. Kapitlet avslutas med förslag på vidare forskning inom området.

Studien syftade till att undersöka hur nya cybersäkerhetskrav kan påverka projektmål i form av tid, kostnad och omfattning, samt hur dessa krav kan hanteras av projektledare inom IT-konsultbranschen beroende på om projekten bedrivs enligt agila metoder, vattenfallsmodellen eller en hybridmodell. Studien har belyst vilka utmaningar och möjligheter som uppstår när säkerhetskrav integreras i projektstyrningen, och därigenom skapat förutsättningar för ökad förståelse för hur projektledare kan balansera krav på säkerhet med projektets övriga mål.

Resultatet visar att cybersäkerhetskrav påverkar projekt i varierande grad, och att effekten beror på faktorer såsom metodval, organisatorisk mognad och projektledarens kompetens. Det finns ett samband mellan hur väl kraven integreras i projektets processer och upplevelsen av projektets framgång. När säkerhetsaspekter hanteras som en naturlig del av projektets planering och genomförande, exempelvis genom att läggas in som stories i backloggen i agila projekt, ökar möjligheten att upprätthålla både säkerhet och leveransprecision. Samtidigt visar resultaten att projektledare ofta upplever cybersäkerhetskrav som ett hinder när de introduceras sent i projektet eller när kraven är otydliga eller motstridiga.

Studien visar också att det inte finns en generell lösning som passar alla projekt, utan att hanteringen av cybersäkerhetskrav måste anpassas till kontexten. Exempelvis tycks agila projekt gynnas av kontinuerlig kompetensutveckling och nära samverkan mellan team och säkerhetsexperter, medan vattenfallsstyrda projekt kräver tydlig kravspecifikation i tidiga faser. Hybridmodellen framstår som en möjlig väg för att kombinera strukturell tydlighet med flexibel anpassning, men förutsätter en hög grad av medvetenhet och metodkunnande hos projektledaren.

Slutsatserna stöder tidigare forskning (t.ex. Salin & Lundgren, 2022; Weil, 2020) som visar att cybersäkerhet inte enbart är ett tekniskt eller juridiskt krav, utan en strategisk aspekt av projektledning som kräver integrerade arbetssätt, tydlig kommunikation och organisatorisk anpassningsförmåga. Det krävs mer än att uppfylla regler, projektledare behöver stödja en kultur där cybersäkerhet ses som en gemensam angelägenhet. Därmed blir även frågor om ansvar, utbildning och prioritering centrala i utvecklingen av framtidens projektmetoder inom IT-branschen.

7.1. Praktiska och teoretiska bidrag

Studien har undersökt hur nya cybersäkerhetskrav påverkar projektverksamhetens grundläggande parametrar, tid, kostnad och omfattning, samt hur dessa krav kan hanteras effektivt inom olika projektmetodiker. Genom att analysera erfarenheter från projektledare i IT-konsultbranschen framträder en tydlig bild av att cybersäkerhet har gått från att vara en specialiserad funktion till att bli en central och integrerad del av projektledning.

En av studiens centrala slutsatser är att cybersäkerhetskrav påverkar alla delar av projekttriangeln. När kraven introduceras sent i processen, särskilt i vattenfallsstyrda projekt, leder de ofta till fördröjningar, ökade kostnader och omarbetningar. I agila projekt kan samma krav hanteras mer flexibelt, men kräver kontinuerlig anpassning och säkerhetskompetens i hela projektteamet. Hybridmodellen erbjuder välbalanserad metod för att kombinera planerad struktur med agilitet, vilket skapar goda förutsättningar för att hantera både stabila och föränderliga cybersäkerhetskrav. Dock kräver detta tydlig ansvarsfördelning, god kommunikation och en viss organisatorisk mognad.

Ur ett praktiskt perspektiv visar studien att kompetens är en avgörande faktor. Projekt som lyckas hantera cybersäkerhetskrav effektivt har ofta säkerhetsexpertis nära projektteamet, exempelvis genom access till ett “center of excellence”. Ett annat framgångskriterium är att hela teamet, inte bara experterna, delar ett grundläggande säkerhetsmedvetande. Detta stärker möjligheterna till snabb anpassning, särskilt i agila projekt där kraven ofta förändras under arbetets gång. Samtidigt blir den mänskliga faktorn en viktig aspekt att beakta, både som en resurs för samverkan och som en potentiell säkerhetsrisk vid bristande kommunikation eller otydlig ansvarsfördelning.

Ett intressant teoretiskt bidrag från studien är att cybersäkerhetskrav inte enbart bör ses som externa regelverk eller riskreducerande åtgärder, utan också som en strategisk möjlighet. Företag som aktivt ligger steget före i sin säkerhetsstrategi kan skapa handlingsutrymme, affärsnytta och stärkt förtroende på marknaden. Vissa företag väljer därför medvetet att lägga sig över gällande regelverk, exempelvis genom att tillämpa säkerhetsåtgärder som överträffar lagens minimikrav med god marginal. Detta grundar sig dels i en strategisk förståelse för att kraven kommer att skärpas över tid. Sådana proaktiva säkerhetsstrategier fungerar även som ett sätt att positionera företaget långsiktigt. Däremot visar studien också att säkerhetsambitioner behöver balanseras i linje med exempelvis 80/20-regeln, då majoriteten av riskerna ofta kan hanteras med en begränsad del av insatserna, medan fullständig säkerhet kan kräva oproportionerligt stora resurser.

Detta visar att cybersäkerhet i allt högre grad blir en del av företagets positionering och värdegrund, inte bara en fråga om teknisk efterlevnad. Här bidrar studien till att nyansera förståelsen av cybersäkerhet som både ett operativt krav och ett strategiskt verktyg. Denna studie belyser vikten av att anpassa projektmetodik, kompetensutveckling och organisatoriska strukturer för att möta växande cybersäkerhetskrav. För projektledare innebär detta inte bara ett ökat ansvar, utan även nya möjligheter att driva innovation, kvalitet och förtroende i en digitalt föränderlig omvärld.

7.2. Begränsningar

Vad avser denna studies resultat finns det vissa begränsningar som påverkar dess trovärdighet. En av de mest påtagliga begränsningarna är att endast åtta projektledare intervjuades, vilket innebär ett relativt litet urval. Även om samtliga respondenter hade lång erfarenhet som seniorkonsulter och därmed besitter djupgående kunskaper om projektledning, går det inte att bortse från att resultatet endast speglar ett begränsat antal perspektiv. Hade studien inkluderat fler projektledare, eller projektledare med mindre erfarenhet, exempelvis juniorkonsulter, är det möjligt att andra uppfattningar kring cybersäkerhetskravens påverkan på projektmål hade framkommit. Det kan exempelvis

tänkas att nyexaminerade projektledare, som utbildats i en tid där cybersäkerhet är mer integrerade i kursplaner, hade haft andra tankesätt eller förhållningssätt.

En annan begränsning ligger i att respondenterna var verksamma i olika typer av projekt och organisationer. Denna variation har bidragit till ett rikt empiriskt material, men har också inneburit att svaren ibland varit svåra att jämföra direkt. Det har i vissa fall varit oklart om skillnader i upplevelser beror på organisationens interna processer, kundernas krav, projektmetod eller individens egna arbetssätt. Det kan därmed inte uteslutas att vissa upplevelser är unika för den kontext som respondenten befinner sig i, vilket påverkar resultatets tillämpbarhet.

Ytterligare en faktor som kan ha påverkat studiens trovärdighet är att intervjuerna genomfördes digitalt via Teams. Även om det gav flexibilitet och underlättade deltagande, fanns det i vissa fall en viss distans i samtalet. Det går inte att utesluta att icke-verbal kommunikation gick förlorad, eller att vissa nyanser i resonemangen inte fångades på grund av teknikens begränsningar. Att intervjufrågorna skickades ut i förväg kan dessutom ha påverkat graden av spontanitet i svaren. Även om syftet var att ge respondenterna tid att reflektera, finns risken att svaren blev mer genomtänkta och strategiska, snarare än ärligt reflekterande i stunden.

En sista aspekt som påverkar studiens giltighet och tillämpbarhet över tid är att cybersäkerhetsområdet utvecklas snabbt. Nya teknologier, lagkrav och hotbilder tillkommer kontinuerligt, inte minst genom utvecklingen av artificiell intelligens. Detta innebär att det som i dag upplevs som en utmaning eller ett hinder i projektledning, om några år kan vara fullt integrerat i både projektmodeller och verktyg. Vissa projektledare uttryckte även att de inte själva kände sig fullt insatta i cybersäkerhetskrav, utan snarare förlitade sig på externa cybersäkerhetsexperter i projektteamet. Det innebär att deras svar bygger mer på upplevelse än på djup teknisk förståelse, vilket kan ha påverkat hur frågorna tolkats och besvarats.

Sammantaget bör därför resultaten i denna studie betraktas som en ögonblicksbild av hur ett urval av erfarna projektledare förhåller sig till cybersäkerhetskrav inom olika projektmiljöer, snarare än en allmängiltig sanning bestående över tid.

7.3. Förslag på vidare forskning

Då cybersäkerhetskrav fortsätter att utvecklas i takt med digitalisering, AI och nya regulatoriska ramar, finns ett behov av ytterligare forskning kring hur dessa krav påverkar samarbete, beslutsfattande och ansvarsfördelning i projektverksamheter. En intressant riktning vore att undersöka hur verksamheter i olika branscher bygger upp en säkerhetskultur, och vilken roll projektledarens förmåga att navigera mellan teknik, regelverk och mänskliga faktorer spelar. Det skulle också vara intressant att undersöka hur säkerhetskrav inverkar på organisationers innovationskapacitet och deras förmåga att genomföra en agil omställning, särskilt i miljöer som präglas av hög komplexitet och snabb förändring. Framtida forskning med ett större och mer varierat urval, eller en tydligare avgränsning till en viss projektkontext eller projektmodell, skulle kunna bidra till att fördjupa analysen av projektledarens roll i implementeringen av cybersäkerhetsåtgärder.

8. Referenser

Vetenskapliga artiklar

Adriko, R., & Nurse, J. R. C. (2024). Does Cyber Insurance Promote Cyber Security Best Practice? An Analysis Based on Insurance Application Forms. *Digital Threats: Research and Practice, 5*(3), 1–39.
https://doi.org/10.1145/3676283

Balcıoğlu, Y. S., Çelik, A. A., & Altındağ, E. (2024). Artificial Intelligence Integration in Sustainable Business Practices: A Text Mining Analysis of USA Firms. *Sustainability, 16*(15), 6334.
https://doi.org/10.3390/su16156334

Baldassarre, M. T., Barletta, V. S., Caivano, D., & Scalera, M. (2020). Integrating security and privacy in software development. *Software Quality Journal, 28*(3), 987–1018.
https://doi-org.libraryproxy.his.se/10.1007/s11219-020-09501-6

Ceyda Ünal, Elçin Nur Demirkol Öztürk, & Aşkın Demirag. (2023). Analysis and Comparision of Waterfall Model and Agile Approach in Software Projects. *Online Academic Journal of Information Technology, 14*(54), 183–203.
https://doi.org/10.5824/ajite.2023.03.002.x

Felici, M., Wainwright, N., Bisogni, F., & Cavallini, S. (2015). What's New in the Economics of Cybersecurity?: Observational and Empirical Studies. *IEEE Security & Privacy, 13*(5), 12–15.
https://doi-org.libraryproxy.his.se/10.1109/MSP.2015.105

Ihsan, S. N., Abd Kadir, T. A., Ismail, N. I., Yuan, K. Z., & Jie, Y. S. (2023). Implementation of Serious Games for Data Privacy and Protection Awareness in Cybersecurity. *2023 IEEE 8th International Conference On Software Engineering and*

Computer Systems (ICSECS), 330–335.
https://doi.org/10.1109/ICSECS58457.2023.10256329

Karlsson, R. U., & Hugo, L. (2022). AI och myndigheters registerförfattningar: rättsliga utmaningar och hinder. *Juridisk Publikation, 1*, 73–103.
https://urn.kb.se/resolve?urn=urn:nbn:se:miun:diva-45762

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability (Switzerland), 14*(3).
https://doi-org.libraryproxy.his.se/10.3390/su14031269

Krishna, V. V., & Gopinath, G. (2024). Software Development Life Cycle for Web Application by Using Traditional Methodology vs Agile Methodology. *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, 1–6.
https://doi-org.libraryproxy.his.se/10.1109/ICONSTEM60960.2024.10568596

Liubimov, O., Turkin, I., Pavlikov, V., & Volobuyeva, L. (2023). Agile Software Development Lifecycle and Containerization Technology for CubeSat Command and Data Handling Module Implementation. *Computation, 11*(9), 182.
https://doi.org/10.3390/computation11090182

Lobo Marques, J. A., Bragança dos Reis Morais, J. J., Alves, J., & Gonçalves, M. (2023). Effectiveness Analysis of Waterfall and Agile Project Management Methodologies - a Case Study from Macau's Construction Industry. *Journal of Management Analysis / Revista Gestão Em Análise, 12*(1), 23–38.
https://doi-org.libraryproxy.his.se/10.12662/2359-618xregea.v12i1.p23-38.2023

Lucky, B., Ayodeji, A., Prisca, A., Mayokun, A. & Kudirat, A. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances, 19*(02),

134-153.
https://doi.org/10.30574/gjeta.2024.19.2.0084

Mankertz, T. (2023). IT consulting leaders need to level-up in 2023 to meet the big challenges of the talent arms race. *Strategic HR Review, 22*(6), 182–185. https://doi-org.libraryproxy.his.se/10.1108/SHR-08-2023-0043

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

Sarkar, T., Rakhra, M., Sharma, V., Singh, A., Jairath, K., & Maan, A. (2024). Comparing Traditional vs Agile Methods for Software Development Projects: A Case Study. *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, *7*, 221–227. https://doi-org.libraryproxy.his.se/10.1109/IC3I61595.2024.10829321

Salin, H., & Lundgren, M. (2022). Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams. *Journal of Cybersecurity and Privacy, 2*(2), 276–291. https://doi-org.libraryproxy.his.se/10.3390/jcp2020015

Setiawan, H., Putra, F. A., & Pradana, A. R. (2017). Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute. *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*, 251–256. https://doi-org.libraryproxy.his.se/10.1109/ICITSI.2017.8267952

Shania, M., Handayani, P. W., & Harahap, N. C. (2024). Evaluation of Kanban Implementation in an Information Technology Service Provider. *2024 International*

Conference on Information Management and Technology (ICIMTech), 218–223. https://doi-org.libraryproxy.his.se/10.1109/ICIMTech63123.2024.10780920

Shimoda, A., & Yaguchi, K. (2017). A Method of Setting the Order of User Story Development of an Agile-Waterfall Hybrid Method by Focusing on Common Objects. *2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI),* 301–306. https://doi-org.libraryproxy.his.se/10.1109/IIAI-AAI.2017.149

Ritter, T., & Pedersen, C. L. (2020). Digitization capability and the digitalization of business models in business-to-business firms: Past, present, and future. *Industrial Marketing Management*, *86*, 180–190. https://doi.org/10.1016/j.indmarman.2019.11.019

Rodrigues de Oliveira, E., Cabral Ribeiro, P. C., Picinini Méxas, M., & Barbará de Oliveira, S. (2023). Scrum method assessment in Federal Universities in Brazil: multiple case studies. *Brazilian Journal of Operations & Production Management, 20*(1), 1–14. https://doi-org.libraryproxy.his.se/10.14488/BJOPM.1496.2023

Thummadi, B. V., & Lyytinen, K. (2020). How Much Method-in-Use Matters? A Case Study of Agile and Waterfall Software Projects and their Design Routine Variation. *Journal of the Association for Information Systems*, *21*(4), 864–900. https://doi.org/10.17705/1jais.00623

Weil, T. R. (2020). Standards for Cloud Risk Assessments - What's Missing? *2020 IEEE Cloud Summit,* 11–17. https://doi-org.libraryproxy.his.se/10.1109/IEEECloudSummit48914.2020.00008

Yahya, N., Abdul Salam, A. M., Maidin, S. S., & Awang Abu Bakar, N. S. (2024). Hybrid Agile Model, the Synergy of Waterfall Model and Scrum in a Software Project. *2024 9th International Conference on Information Technology and Digital Applications*

(ICITDA), 01–08.
https://doi-org.libraryproxy.his.se/10.1109/ICITDA64560.2024.10809639

Myndigheter

Europeiska unionens parlament. (2022, 3 november). *Kampen mot cyberbrott: Så funkar EU:s nya lagar om cybersäkerhet*. Europeiska unionens parlament. https://www.europarl.europa.eu/topics/sv/article/20221103STO48002/kampen-mot-cyberbrott-sa-funkar-eu-s-nya-lagar-om-cybersakerhet

Myndigheten för samhällsskydd och beredskap (MSB). (2024a). *Cybersäkerhetskonferensen 2024*. Hämtad den 22 januari 2025 från https://www.msb.se/sv/aktuellt/kalender/2024/oktober/cybersakerhetskonferensen-2024/

Myndigheten för samhällsskydd och beredskap (MSB). (2024b). *Det här är NIS 2-direktivet*. Hämtad den 22 januari 2025 från https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/krav-och-regler-inom-informationssakerhet-och-cybersakerhet/nis-direktivet/det-har-ar-nis2-direktivet/

Myndigheten för samhällsskydd och beredskap (MSB). (2024c). *Om NIS-direktivet*. Hämtad den 22 januari 2025 från https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/krav-och-regler-inom-informationssakerhet-och-cybersakerhet/nis-direktivet/om-nis-direktivet/

Riksdagen. (2023). *Behandling av personuppgifter*. https://www.riksdagen.se/sv/om-webbplatsen/behandling-av-personuppgifter/

Vetenskapsrådet. (2024, november 25). Etik i forskningen och god forskningssed. *Vetenskapsrådet.* Hämtad den 19 mars 2025 från https://www.vr.se/uppdrag/etik/etik-i-forskningen.html

Övriga artiklar

Canea. (n.d.). *Hur NIS2-direktivet påverkar din verksamhet*. Hämtad 27 januari 2025, från https://www.canea.se/blogg/hur-nis2-direktivet-paverkar-din-verksamhet

Dean Leffingwell. (n.d.). *SAFe in Five Minutes.* Scaled Agile, Inc. Hämtad den 6 maj 2025 från https://framework.scaledagile.com/presentations-and-videos

Holmlund, David. (2024, 7 mars). *Så skapar du en effektiv AI-policy*. Digitalist. Hämtad den 22 januari 2025 från https://www.digitalist.se/blogg/sa-skapar-du-en-effektiv-ai-policy

IBM. (2023, 2 november). *What are large language models (LLMs)?* IBM. Hämtad 31 mars 2025 från https://www.ibm.com/think/topics/large-language-models

International Organization for Standardization. (n.d.). *ISO/IEC 27001: Information security management*. Hämtad den 22 januari 2025 från https://www.iso.org/standard/27001

Harmonit. (n.d.). *Projektmodell PROPS*. HarmoniT. Hämtad 1 april 2025, https://harmonit.se/projekt/projektmodeller/projektmodell-props/

Norstedts Juridik. (2024, September 13). Juridiska utmaningar i AI-projekt. *Norstedts Juridik.*
https://www.nj.se/nyheter/juridiska-utmaningar-i-ai-projekt

Utbildning.se. (n.d.). *PPS - Projektledning och projektstyrning*. Utbildning.se. Hämtad 1 april 2025
https://www.utbildning.se/kurser/pps/

Böcker

Bryman, A., & Bell, E. (2017). *Företagsekonomiska forskningsmetoder* (3:e uppl.). Liber.

Eriksson, L. T. & Wiedersheim-Paul, F. (2014). *Att utreda, forska och rapportera* (10:e uppl.). Liber.

Lind, R. (2019). *Vidga vetandet: Teori, metod och argumentation i samhällsvetenskapliga undersökningar*. (2 Uppl.). Studentlitteratur.

Ghauri, P., Grønhaug, K. & Strange, R. (2020). *Research methods in business studies* (5:e uppl.). Cambridge University Press.

Tonnquist, B. (2018). *Projektledning* (7:e uppl.). Sanoma Utbildning.

Figurer

Figur 1 Projekttriangeln
Tonnquist, B. (2018). *Projektledning* (7:e uppl.). Sanoma Utbildning.

Figur 2 Agil iterationsflöde

Ceyda Ünal, Elçin Nur Demirkol Öztürk, & Aşkın Demirag. (2023). Analysis and Comparision of Waterfall Model and Agile Approach in Software Projects. *Online Academic Journal of Information Technology, 14*(54), 183–203. https://doi.org/10.5824/ajite.2023.03.002.x

Figur 3 Översikt över ramverkets steg och aktiviteter
Salin, H., & Lundgren, M. (2022). Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams. *Journal of Cybersecurity and Privacy, 2*(2), 276–291.
https://doi-org.libraryproxy.his.se/10.3390/jcp2020015

Figur 4 Vattenfallsmodellen (Modifierad version av modell)
Ceyda Ünal, Elçin Nur Demirkol Öztürk, & Aşkın Demirag. (2023). Analysis and Comparision of Waterfall Model and Agile Approach in Software Projects. *Online Academic Journal of Information Technology, 14*(54), 183–203. https://doi.org/10.5824/ajite.2023.03.002.x

Bilaga 1: Intervjufrågor

Bakgrund och allmänna frågor:

- Vad är din nuvarande befattning och vilka är dina huvudsakliga ansvarsområden?
- Hur länge har du arbetat med projekt inom IT-konsultbranschen?
- Vilka typer av projekt arbetar ni främst med?

Cybersäkerhet i projekt:

- Hur hanterar ni nya cybersäkerhetskrav i era projekt?
- Vilka är de största utmaningarna med AI-utvecklingen avseende cybersäkerhet?
- Hur påverkar cybersäkerhetskrav projektets tidsram, kostnad och omfattning?
- Ser du cybersäkerhetskrav som en faktor som förenklar eller försvårar projektleveransen? Varför?
- Finns det en optimal balans mellan hänsynstagande till cybersäkerhet och projektets mål? Om ja, hur uppnås den?
- Hur säkerställer ni att projektmedlemmarna har relevant kunskap inom cybersäkerhet? Inkluderar detta individuell säkerhetsprövning och kontinuerlig kompetensutveckling?
- Hur rekryterar ni cybersäkerhetskompetens till era projekt? Finns det specifika kompetenser inom cybersäkerhet som är svåra att hitta eller rekrytera?

Datahantering och integritet:

- Vilka rutiner har ni för att säkerställa dataintegritet och skydd av känsliga data i projekt?
- Hur säkerställer ni att AI-lösningar följer gällande lagar och regelverk (t.ex. NIS2, GDPR, NIST SP 800–30)?
- Hur hanterar ni säkerhetsrisker kopplade till användning av tredjepartsdata och externa AI-modeller?

Projektstyrning och metodik:

- Använder ni agila metoder eller vattenfallsmodellen i projekt? Eller en kombination?
- Varför har ni valt denna projektstyrningsmetod? Eller när använder ni respektive metod?

Om ni använder agila metoder:

- Hur påverkar säkerhetsåtgärder projektets kvalitet, omfattning och leveranstid?
- Vad har ni för strategier för att integrera cybersäkerhetskrav i agila projekt?

Om ni använder vattenfallsmodellen:

- Hur integreras cybersäkerhetskrav i de olika faserna av projektet? (Till exempel vid planering skapas en kommunikationsplan om hur information skyddas och delas, vid beredning undersöks vilka resurser som får finnas inom säkerhetsskopet osv.)
- Upplever ni att säkerhetskraven skapar utmaningar vid övergången mellan faser?
- Vad har ni för strategier för att integrera cybersäkerhetskrav i vattenfallsprojekt?

Framtid och förbättringar:

- Ser du ett behov av att förändra hur cybersäkerhet hanteras i projekt? Om ja, på vilket sätt?
- Vilka åtgärder eller verktyg tror du skulle underlätta integreringen av cybersäkerhet i projektstyrningen?

Bilaga 2: Ordförklaring

Agil metod - Ett arbetssätt inom projektledning och systemutveckling som bygger på flexibilitet, kontinuerlig förbättring och nära samarbete med kunden.

Agile Release Trains (ARTs) - Ett centralt begrepp inom SAFe (Scaled Agile Framework) och representerar ett tvärfunktionellt team av agila team som samarbetar för att leverera värde i koordinerade, regelbundna releaser.

Artificiell intelligence (AI) - System som uppvisar intelligent beteende genom att analysera sin miljö och vidta åtgärder, med viss grad av självständighet, för att uppnå särskilda mål

Artificiell generell intelligence (AGI) - En typ av artificiell intelligens som har förmågan att förstå, lära sig och utföra vilken intellektuell uppgift som helst som en människa kan utföra.

Automatiserade system - System som kan utföra uppgifter självständigt utan mänsklig inblandning, ofta med hjälp av datorer, sensorer och mjukvara.

Backloggen - En lista över allt arbete som behöver göras i ett projekt eller produktutveckling, vanligtvis inom agil metodik som Scrum eller Kanban.

Backloggförädling - En återkommande aktivitet i agila team där man granskar, förbättrar och prioriterar innehållet i produktbackloggen.

Center of excellence - En enhet eller grupp inom en organisation som samlar och fokuserar på expertkunskap.

Cybersäkerhet - Att skydda datorer, nätverk, system och data från digitala hot, såsom hackerattacker, skadlig kod och dataintrång.

Cyberattack - Ett angrepp där hackare försöker skada, störa eller få obehörig åtkomst till datorer, nätverk eller data. Dessa attacker kan drabba företag, myndigheter och privatpersoner.

Generativ AI - Artificiell intelligens som kan skapa nytt innehåll, som text, bilder, musik eller kod.

General Data Protection Regulation (GDPR) - En dataskyddsförordning som gäller inom hela EU och syftar till att skydda individers personuppgifter och ge dem större kontroll över hur deras data används.

Hybridmodell - Ett samlingsnamn för en metod, strategi eller struktur som kombinerar två eller flera olika modeller för att dra nytta av styrkorna i varje del.

Information Security Management System (ISMS) -implementering - En systematisk process för att införa ett ledningssystem som syftar till att skydda en organisations information genom att hantera risker relaterade till informationssäkerhet.

International Organization for Standardization (ISO) 27001 - En internationell standard för informationssäkerhet. Den hjälper organisationer att skydda känslig information genom att införa ett ledningssystem för informationssäkerhet.

IT-projekt - Ett tidsbegränsat arbete med målet att utveckla, förändra eller införa en IT-lösning, till exempel ett nytt system, en app, ett nätverk eller en databas.

Kanban - En metod för visuell projektledning och en typ av agil arbetsmetodik som hjälper team att hantera och förbättra arbetsflödet.

Lean - Ett arbetssätt som fokuserar på att förbättra processer genom att eliminera onödiga steg, optimera flöden och ständigt förbättra verksamheten.

Mjukvaruprojekt - Projekt i att utveckla en programvara eller en applikation, och det innefattar alla de steg som krävs för att planera, skapa, testa och distribuera programmet.

Molnsäkerhet - Att skydda data, system och tjänster som lagras eller körs i molnet, alltså på servrar som tillhandahålls av företaget.

National Institute of Standards and Technology Special Publication (NIST SP) 800-30 - En del av NIST:s 800-serie, som består av vägledningar kring cybersäkerhet och informationssäkerhet.

Network and Information Security Directive (NIS-direktivet) - En EU-lagstiftning som syftar till att stärka cybersäkerheten inom EU.

Network and Information Security Directive 2 (NIS 2-direktivet) - En uppdaterad version av EU:s NIS-direktiv som syftar till att stärka cybersäkerheten inom EU. Det antogs 2022 och ska börja gälla i medlemsländerna från oktober 2024.

Nätfiske - En form av bedrägeri på internet.

Operativ teknik (OT) - Teknik och system som används för att övervaka, styra och automatisera fysiska processer i exempelvis industrier, energisystem och infrastruktur.

Praktisk ProjektStyrning (PPS) - En projektstyrningsmodell som används för att strukturera, leda och följa upp projekt på ett tydligt och effektivt sätt.

Projekt för Projektstyrning (PROPS) - En projektstyrningsmodell som togs fram av Ericsson. Den används för att strukturera och genomföra projekt på ett systematiskt sätt, särskilt i större, tekniskt komplexa organisationer.

Projektledare - Den person som har det övergripande ansvaret för att leda och driva ett projekt från start till mål.

Projektstyrningsmetoder - En metod eller struktur som används för att planera, genomföra, följa upp och avsluta projekt på ett organiserat och effektivt sätt. Exempelvis agila metoder och vattenfallsmodellen.

Projekttavla - En projekttavla enligt kanban-metodiken är ett visuellt styrverktyg som används för att planera, följa upp och kontinuerligt förbättra arbetsflöden i projekt- och linjeorganisationer. Tavlan är indelad i kolumner som representerar arbetsprocessens olika steg (t.ex. Att göra, Pågår, Klar). Varje arbetsuppgift visualiseras som ett kort som flyttas horisontellt över tavlan i takt med att den fortskrider.

Projektteam - Ett team (en grupp människor) som arbetar tillsammans inom ett specifikt projekt med ett gemensamt mål, ofta under en begränsad tidsperiod.

Projekttriangeln - En klassisk modell inom projektledning som visar projektets kvalitet baserat på balansen mellan tre grundläggande faktorer (tid, kostnad och omfattning).

Ransomware-attack - En cyberattack där filer eller system låses av hackare som kräver en lösensumma för att återställa åtkomsten.

Scaled Agile Framework (SAFe) - Ett ramverk för att skala upp agil metodik till hela organisationer, inte bara enskilda team. Det används ofta i stora företag som vill arbeta agilt men har många team, produkter, affärsområden eller komplexa strukturer.

Scrum - Ett ramverk för agil projektledning som används för att organisera och hantera mjukvaruutveckling, men kan tillämpas på andra typer av projekt också.

Scrummästare - En facilitator och coach inom ett Scrum-team som ansvarar för att säkerställa att Scrum-processen följs och fungerar effektivt.

Security Champions - Personer inom ett team eller en organisation som har särskilt ansvar för att främja och stödja cybersäkerhet, utan att själva vara säkerhetsexperter på heltid.

Sprintar - En tidsbegränsad arbetsperiod, vanligtvis 1–4 veckor lång, där ett team arbetar fokuserat för att färdigställa ett visst antal uppgifter eller leverera en fungerande produktinkrement.

Sprintplanering - Ett möte där teamet planerar arbetet för en kommande sprint (en tidsbegränsad arbetsperiod, ofta 1–4 veckor).

Stand-up-möten - Korta, dagliga möten där teammedlemmar snabbt uppdaterar varandra om vad de gjort, vad de ska göra, och om det finns några hinder.

User experience (UX) - Användarens totala upplevelse av en produkt eller tjänst.

Vattenfallsmodellen - En traditionell projektlednings- och utvecklingsmetod som följer en linjär och sekventiell process, där varje fas måste vara klar innan nästa påbörjas.

Bilaga 3: Individuella reflektioner

Amanda Fredman

Att arbeta med detta examensarbete har varit en lärorik och utmanande process där jag både har fördjupat min teoretiska förståelse och utvecklat nya praktiska färdigheter. Eftersom jag parallellt har gjort praktik inom ett IT-konsultföretag, kunde jag snabbt relatera många av våra teoretiska resonemang till den verklighet jag själv befinner mig i. Det har gjort lärandet mer konkret och relevant för mig.

En stor del av min personliga utveckling har handlat om att förstå cybersäkerhetens praktiska konsekvenser för projektledning, inte bara som ett teknikområde utan som en central komponent i hur projekt organiseras, prioriteras och genomförs. Jag hade tidigare en relativt begränsad bild av cybersäkerhet som något separat från projektledning, men genom arbetet har jag insett hur nära integrerat det behöver vara, särskilt i konsultdrivna IT-projekt med flera externa parter.

En annan viktig lärdom har varit kopplad till projektstyrningsmodellerna. Vi valde tidigt att fördela arbetet så att jag ansvarade för analysen av agila arbetssätt medan min medförfattare Linn tog huvudansvar för vattenfallsmodellen. Denna uppdelning gav oss båda möjlighet att fördjupa oss i ett område och bli "experter" på varsin modell, vilket gjorde våra diskussioner och analyser mer dynamiska. Jag upplevde att jag fick ett djupare grepp om de styrkor och svagheter som finns i agila metoder, särskilt när det gäller att hantera komplexa säkerhetskrav i en föränderlig miljö. Samtidigt krävde det också att jag höll mig väl insatt i den andra modellen, för att vi skulle kunna jämföra och sammanfatta gemensamma slutsatser.

Vi samarbetade nära i alla andra delar, från att formulera syfte och forskningsfrågor, till intervjuer, analys och skrivande. Intervjuerna var särskilt intressanta och utvecklande för mig. Genom att arbeta med intervjuerna fick jag en bättre förståelse för hur olika projektledare resonerar kring cybersäkerhet. Det var särskilt intressant att se hur uppfattningen om ambitionsnivån i cybersäkerhetsarbetet varierade mellan

projektledarna, vilket i sin tur påverkade deras syn på vad som är realistiskt att genomföra i praktiken.

Metodmässigt har jag lärt mig mycket om kvalitativ datainsamling och tematiskt analysarbete. Det var utmanande att gå från rå intervjutext till strukturerade teman och ännu mer utmanande att sedan diskutera dessa i relation till vårt syfte. Jag upplevde att jag växte mycket under just denna fas, då det krävde både analytiskt tänkande och förmåga att se samband.

Under arbetets gång har jag blivit mer medveten om hur jag uttrycker mig i skrift. I början tenderade jag att skriva för tekniskt, vilket ibland gjorde texten svår att följa för en läsare utan samma bakgrund. Genom återkoppling och omskrivningar har jag lärt mig att anpassa språket bättre, att behålla precision utan att tappa läsbarhet, och att skriva akademiskt utan att det blir onödigt komplicerat.

Slutligen har detta arbete stärkt min förståelse för vad det innebär att samarbeta professionellt. Vi har kompletterat varandra väl, haft ett öppet samtalsklimat och hela tiden haft fokus på målet. Att arbeta med ett komplext ämne som cybersäkerhet, där det inte finns tydliga svar, har krävt att vi kunnat tänka självständigt, men samtidigt vara lyhörda för varandras perspektiv. Jag tar med mig många insikter som jag vet kommer att vara värdefulla i mitt framtida yrkesliv inom IT-konsultbranschen.

Linn Jutéus

Inför det här examensarbetet hade jag förväntan att få lära mig mer om projektledning, både teoretiskt och praktiskt. Jag var också särskilt nyfiken på hur projektledning tillämpas inom IT-konsultbranschen, en bransch som jag upplever som både spännande och högaktuell. Jag såg det här arbetet som en möjlighet att få en djupare förståelse för en yrkesvärld jag tidigare bara haft en övergripande bild av. Mina förväntningar på kursen har överträffats och det har varit mycket roligare och intressantare än jag trodde att det skulle bli.

När vi påbörjade studien hade jag begränsade kunskaper om både projektledning och IT-konsultbranschen. Det gjorde att nästan varje moment i processen innebar ny kunskap och nya insikter, vilket bidrog till att arbetet blev både lärorikt och intressant. En av de saker jag snabbt insåg var hur omfattande projektledning faktiskt är. Under arbetets gång har jag fått en bredare förståelse för hur projektledarrollen ser ut i praktiken, särskilt inom en bransch där förändringstakten är hög och flexibilitet är avgörande.

De intervjuer vi genomfört har varit en av de mest givande delarna av arbetet. Att få möta personer som själva arbetar som projektledare inom IT-konsultbranschen, och höra dem berätta om sina erfarenheter, har gett mig konkreta exempel på hur teori omsätts i verkligheten. Varje intervju har bidragit med olika perspektiv, utmaningar och lösningar, något som har gjort materialet levande och hjälpt mig att förstå hur komplex och varierad projektledning kan vara beroende på sammanhanget.

En aspekt av arbetet som jag upplevt som särskilt utvecklande har varit att vi själva har fått ta fullt ansvar för hur vi lagt upp vårt arbete. Eftersom vi inte haft så mycket schemalagda lektioner under perioden, har det varit upp till oss att planera vår tid, fördela arbetsuppgifter och hålla oss till våra deadlines. Det har ställt krav på självdisciplin, kommunikation och samarbete, men det har också varit väldigt givande. Jag upplever att detta ansvar inte bara gjort mig mer strukturerad, utan också gett en inblick av hur det kan vara att arbeta självständigt i ett projekt, vilket jag tror kan vara relevant för arbetslivet.

Sammanfattningsvis har det här examensarbetet varit en väldigt givande upplevelse. Det har väckt ännu större intresse för projektledning än jag hade tidigare, och jag känner mig både inspirerad och motiverad att fördjupa mig ytterligare inom området. Jag tar med mig värdefulla erfarenheter och insikter som jag vet kommer vara till stor nytta.