UPTEC STS 25032
Examensarbete 30 hp
Juni 2025

UPPSALA
UNIVERSITET

NIS 2 och nya krav på cybersäkerhet i leverantörskedjor

En fallstudie av krav och kravuppfyllnad inom informationssäkerhet i ett infrastrukturprojekt

Anton Mämmi

Civilingenjörsprogrammet i system i teknik och samhälle

UPPSALA UNIVERSITET

NIS 2 and new supply chain cybersecurity requirements

Anton Mämmi

Abstract

In 2022, the NIS 2 directive was adopted by the European Parliament. The directive imposes new and stricter cybersecurity requirements, than those found in the previous NIS directive, for actors operating in several different sectors deemed to be of societal importance. One of these new requirements is that the actor must guarantee the security of its supply chain. In this study, one of the projects commissioned by Trafikverket was studied based on the actors' approach to maintain information security in their respective supply chains.

The study is based on data collected through interviews, a questionnaire and a documentation review. This data has then been analyzed using the STPA (System-Theoretic Process Analysis) method, which is based on the theoretical framework STAMP (System-Theoretic Accident Model and Processes). Within this framework, accidents and risks occur because of a lack of control. This control takes the form of control measures and feedback between different components of the studied system. The study also aimed to evaluate STAMP in the project organizational context, in which the study took place.

In accordance with the method, the data was analyzed through a hierarchical control structure. This analysis identified several deficient areas among the actors' approach to maintain information security in the project. Trafikverket relies heavily on documents to convey information security requirements. These documents' ability to act as control measures is unfortunately lacking due to several different reasons. Trafikverket also does not carry out sufficient supervision to ensure compliance with information security requirements within the project. The company in turn conveys requirements in an inadequate way to its foreign resources and is also lacking in supervision when it comes to information security.

Teknisk-naturvetenskapliga fakulteten

Uppsala universitet, Utgivningsort Uppsala/Visby

Handledare: Anonym Ämnesgranskare: Anders Arweström Jansson

Examinator: Elísabet Andrésdóttir

Populärvetenskaplig sammanfattning

Informationssäkerhetsarbete har blivit alltmer aktuellt i och med att världsläget blivit alltmer instabilt. I samband med denna utveckling beslutade EU om NIS 2-direktivet i december 2022. Detta direktiv ställer krav inom cybersäkerhet, och pekar ut ett antal samhällssektorer som kritiska. Bland annat kommer verksamheter som uppfyller vissa storlekskrav och är verksamma inom någon av de utpekade sektorerna även behöva uppfylla krav på säkerhet i leverantörskedjan, vilket medför nya utmaningar i jämförelse med de krav som ställdes av de äldre NIS-direktivet från 2016.

En aktör som påverkas av detta är Trafikverket, som ansvarar för det svenska transportsystemet som helhet samt den framtida planeringen av detta system. I kontexten av detta arbete driver Trafikverket ett stort antal olika projekt genom olika leverantörer. I denna fallstudie studeras både Trafikverket och det företag som driver ett projekt åt dem, i kontexten av deras förhållningsätt gentemot informationssäkerhet i respektive leverantörsrelation, detta för att undersöka om aktörernas förhållningsätt är tillräckligt för att uppfylla de nya krav som ställs av NIS 2. Därtill utvärderas även den systemteoretiska olycksteorin STAMP i denna typ av kontext, genom den analytiska metoden STPA. Inom denna teoretiska ansats uppstår risker och olyckor inte på grund av enskilda fel, utan på grund av en avsaknad av kontroll mellan olika komponenter i systemet.

För att få en bild över hur informationssäkerhetskrav förmedlas inom respektive leverantörsrelation, både mellan Trafikverket och företaget, och mellan företaget och dess utländska arbetskraft, genomfördes tre olika typer av datainsamling. Datainsamlingen genomfördes dels genom intervjuer med nyckelpersoner i projektet, dels med en enkät utskickad inom företagets projektorganisation och slutligen genom en genomgång av projektdokumentation. Den data som samlats in analyserades sedan genom den tidigare nämnda metoden STPA.

Resultatet av denna analys pekar på ett behov av granskningsprocedurer från Trafikverkets sida inom informationssäkerhetskrav, genom att nyttja den rätt till insyn i respektive leverantörs informationssäkerhetsarbete som kontraktdokumentationen medför. Detta kan komma att kräva tydligare åtgärder från en högre nivå inom Trafikverket. Därtill bör sättet som dessa krav förmedlas genom, i form av styrande dokument, ses över. Krav bör samlas och förtydligas för att säkerställa att relevant part får en möjlighet att ta till sig innehållet.

En liknande problematik återfann analysen hos företaget, som dock uppvisade en mer mogen ansats inom området av informationssäkerhet i och med ett aktivt arbete med att certifiera sig gentemot informationssäkerhetsstandarden ISO 27001. Analysen belyser att företaget också bör utöka de granskningar av förhållningsätt till informationssäkerhet

som görs ute i verksamheten. Utöver detta bör företaget tydligare belysa vad begreppet informationssäkerhet innebär och hur det är kopplat till det alldagliga arbetet inom projektorganisationen, samt se över de riktlinjer som existerar när de kommer till översatta kravdokument och styrmedel gentemot de utländska resurserna, för att säkerställa att dessa ges bättre förutsättningar att uppfylla de krav på informationssäkerhet som ställs. STAMP och den tillhörande STPA metoden visade sig vara relativt komplex att tillämpa, men det systemteoretiska perspektiv som denna ansats innebär gav fortfarande en god möjlighet att lyfta påträffade problem bortom individnivå, till något med som är behjälpligt för organisatoriska förändringar.

Förord

Detta arbete markerar slutet på min tid på Civilingenjörsprogrammet System i teknik och samhälle vid Uppsala universitet. Det har varit en resa fylld av både stora utmaningar och *magiska* upplevelser Jag vill tacka alla på företaget och min ämnesgranskare Anders Arweström Jansson, som stöttat mig under resans gång och svarat på den saliga blandning av frågor jag ställt under de senaste månaderna. Jag vill även tacka min kära partner och familj, som stått vid min sida under hela arbetes gång. Jag vill även rikta ett tack till mina kära kursare, speciellt Freja och Julie för alla år av grupparbeten och slit, utan er vet jag inte om de blivit någon examen. Men med denna tid bakom mig är det nu dags för nya upplevelser och nya utmaningar.

Anton Mämmi

Juni 2025

Innehållsförteckning

1. Inledning

Rysslands pågående invasion av Ukraina och annektering av Krimhalvön, de ökande spänningarna mellan Indien och Pakistan, konflikten i Gaza och en mångfald av andra kriser och konflikter runt om i världen, har inneburit att det globala säkerhetspolitiska läget har blivit alltmer instabilt. I samband med denna utveckling har cybersäkerhet blivit en allt större fråga. Bland annat rankades ”cyber insecurity” som den fjärde största upplevda riskfaktorn bland organisationer 2024 (World Economic Forum, 2024 s.11), och samma år inträffade även ett sextiotal allvarligare cyberattacker (CSIS, 2025). Sales (2013, s.1556f) framhäver att behovet av cybersäkerhet blir allt större i och med att samhällets förlitan på kritisk nätverksinfrastruktur blir alltmer omfattande.

För att säkerställa cybersäkerhetskapaciteten inom EU antog det europeiska parlamentet i december 2022 NIS 2-direktivet, eller direktivet för säkerhet inom nätverk och informationssystem. Målsättningen med direktivet var att stärka cybersäkerheten inom hela unionen genom att införa strängare krav än i det tidigare NIS-direktivet från 2016. NIS 2 omfattar en avsevärt bredare målgrupp än det tidigare direktivet, och ställer krav på en allriskansats inom målgruppen. Denna allriskansats innefattar bland annat högre krav på riskhanteringsåtgärder, incidentrapportering och krav på att aktörer arbetar med cybersäkerhet inom sina leverantörskedjor. Direktivet innefattar även möjligheten till avsevärda sanktionsavgifter för aktörer som ej uppfyller de krav som ställs på dem ((EU) 2022/2555).

Direktivet var ämnat att vara tillämpat i lag inom EU:s olika medlemsstater senaste i oktober 2024 (MSB, 2024a). Vid tiden för denna studies start i januari 2025, har dock den svenska lagstiftningen ännu inte antagits. Det är därmed fortfarande oklart vilka specifika krav som lagstiftningen kommer att ställa på påverkade svenska entiteter, hädanefter kallade verksamhetsutövare, för att efterfölja svensk terminologi (SOU 2024:18, s.123). Däremot vet vi att kraven på riskanalyser kommer att skärpas och att verksamhetsutövare bland annat kommer att behöva uppfylla krav på en ökad insyn i sina leverantörskedjor.

En sektor som pekas ut av direktivet är transportsektorn. Transportsektorn spelar en stor samhällsviktig roll (Johanson, 2024), och behovet av cybersäkerhet är därmed stort inom sektorn. Exempelvis drabbades det australienska hamnoperatörsföretaget DP World av en cyberattack 2023. Företaget hanterade då runt 40% av den totala import- och exporten till landet, och attacken medförde att företagets verksamhet tvingades stänga ner under flera dagar, innan drifter kunde återställas (BBC, 2023).

En viktig verksamhetsutövare inom den svenska transportsektorn är Trafikverket, som bland annat ansvarar för många av de största infrastrukturprojekten i Sverige. I denna

studie kommer ett större järnvägsinfrastrukturprojekt som Trafikverket beställt att analyseras utifrån de inblandade aktörernas förhållningsätt gentemot informationssäkerhet i respektive leverantörsrelation, för att undersöka om aktörernas förhållningsätt kommer att uppfylla de krav som NIS 2 ställer.

Det finns många metoder för att analysera organisatoriska strukturer ur ett riskanalytiskt perspektiv. Ett alternativ, som används i denna studie är STAMP. STAMP är ett systemteoretiskt ramverk som betonar samspelet mellan olika systemkomponenter, beslutsprocesser och reglersmekanismer för att undvika förlustscenarion. Även ett komplement till STAMP, i form av agentteori, kommer att prövas. Agentteori kan användas för att ytterligare belysa hur informationsasymmetrin inom en relation påverkar möjligheten till goda regleringar mellan komponenter.

1.1 Syfte och frågeställningar

Målsättningen med studien är att bidra till en förståelse för hur aktörer navigerar inom ett komplext nätverk av krav och processer. Studien ämnar bidra till detta genom en riskanalys av hur aktörerna inom en projektorganisation förhåller sig till informationssäkerhet inom respektive leverantörsrelation, detta genom att undersöka hur aktörerna arbetar med krav och kravuppfyllnad inom området. Vidare ämnar studien utvärdera tillämpbarheten av det teoretiska ramverket STAMP inom denna typ av kontext, genom att utvärdera ramverkets förmåga att belysa organisatoriska aspekter av den undersökta projektorganisationen, samt huruvida ett tillskott av agentteori är behjälpligt för att förbättra denna analys. Detta kommer att göras genom att följande forskningsfrågor behandlas:

- I vilken utsträckning uppfyller aktörernas nuvarande förhållningssätt de krav på informationssäkerhet i leverantörskedjan som ställs av NIS 2-direktivet?
- På vilka sätt kan ramverket STAMP utvecklas för att bättre belysa organisatoriska utmaningar?

Detta genom att följande frågeställningar besvaras:

1) Vilka krav ställer Trafikverket på företaget när de kommer till informationssäkerhet?
2) Hur förhåller sig företaget till kravställningar relaterade till informationssäkerhet?
3) Vilka informationssäkerhetskrav ställer företaget på sin utländska arbetskraft?
4) Vilken tillsyn av kravuppfyllnad genomförs inom området av informationssäkerhet inom projektorganisationen?
5) Vilka styrkor och svagheter besitter STAMP för att illustrera denna typ av projektorganisation, och kan ett tillskott av agentteori bidra till en ökad förståelse över de faktorer som STAMP identifierat?

1.2 Avgränsningar

Eftersom det krav på en allriskansats som ställs av NIS 2 är väldigt omfattande, fokuserar denna studie på de krav på informationssäkerhet i leverantörskedjan som direktivet ställer. Detta bland annat eftersom detta är ett nytt krav som ej återfinns i det gamla NIS-direktivet (Vandezande, 2024). Vidare, eftersom studien genomförts på beställning av företaget, kommer företagets förhållningsätt i frågan vara i fokus. Studien begränsar sig även att studera ett enskilt större projekt drivet av företaget, på grund av de begränsade tidsmässiga resurser som funnits tillgänglig för författaren. Företaget är verksam i ett flertal projekt gentemot Trafikverket, och en bredare kartläggning av parternas förhållningsätt till informationssäkerhet i relationen hade bidragit till studiens djup, men detta bedömdes som bortom den tidsmässiga ramen för arbetet. Vidare presenteras ett resonemang för den valda distinktionen mellan cybersäkerhet och informationssäkerhet i avsnitt 3.1 ”Vad är cybersäkerhet och informationssäkerhet?”.

1.3 Studiens disposition

Resterande av studien är strukturerade enligt följande. I avsnitt två presenteras relevant bakgrundsinformation som ligger till grund för studiens syfte, samt en belysning av annan relevant kontext till studien. I avsnitt tre presenteras de teoretiska begrepp och ramverk som använts i studien. I avsnitt fyra presenteras de metodval som gjorts, tillsammans med den genomförda datainsamlingen. I avsnitt fem presenteras resultatet av den genomförde dokumentationsgranskningen, enkätstudien samt intervjuerna. Detta resultat analyseras därefter i avsnitt sex, där det resulterande diagrammet av den valda analysmetoden redovisas. I avsnitt sju, diskuteras de analytiska slutsatserna i kontexten av studiens forskningsfrågor. I samma avsnitt presenteras även en metoddiskussion. I studiens slutgiltiga avsnitt presenteras de slutsatser som dragits, tillsammans med en rekommendation till fallprojektets intressenter och möjliga framtida forskningsmöjligheter.

2. Bakgrund

I följande avsnitt presenteras relevant bakgrundsinformation. Först redogörs en beskrivning av de krav som NIS 2-direktivet ställer. Efter detta presenteras en beskrivning av det studerade fallprojektet och dess involverade aktörer. Informationen gällande företaget, företagsorganisationen och fallprojektet, inhämtades från företagets intranät, företagets hemsida samt de genomförda intervjuerna.

2.1 NIS 2

Vid denna studies skrivande under den första halvan av 2025, har NIS 2-direktivet ej införts i svensk lagstiftning, men förslag på regelverk har gjorts. Förslaget innefattar en ny cybersäkerhetslag med tillhörande förordning, samt nya myndighetsföreskrifter (MSB, 2025). Eftersom NIS 2 är menad att agera som ett minimikrav, finns det inget som hindrar olika medlemsstater från att införa en striktare lagstiftning för att säkerställa en högre cybersäkerhetsnivå ((EU) 2022/2555, Artikel 5). Detta gör det svårt att avgöra hur den svenska lagstiftningen kommer att se ut. Dock ges förslag på detta i delbetänkandet om genomförandet av NIS 2, SOU 2014:18 Nya regler om cybersäkerhet.

2.1.1 Vem kommer NIS 2 tillämpas på?

Direktivet är ämnat att tillämpas på både offentliga verksamhetsutövare, såsom myndigheter, och privata aktörers som uppfyller vissa storlekskrav samt vars verksamhet är inom någon av de 11 högkritiska eller sju kritiska sektorer som definieras av direktivet. Exempel på högkritiska sektorer inbegriper transport, energi och bankverksamhet. Storlekskravet innebär att verksamhetsutövare som definieras som större än litet enligt EU kommissionens rekommendation (2003/361/EG), dvs som har en omsättning större än 10 miljoner euro eller har mer än 50 anställda, ska förhålla sig till direktivet. Undantag ges för verksamhetsutövare som innehar en viktig roll inom nationell säkerhet, och medlemsstaterna har även möjlighet att göra egna bedömningar om utbildningsinstitut och verksamhetsutövare inom offentlig förvaltning på lokal nivå ska omfattas av direktivet ((EU) 2022/2555, Artikel 2).

Det tidigare NIS-direktivet med tillhörande lagstiftning, ställde i huvudsak krav på de verksamheter som definierades som ”leverantörer av samhällsviktiga tjänster”, som bland annat innebar att de verksamheter som identifieras som samhällsviktiga innehade en anmälningsplikt vid cyberincidenter gentemot relevant tillsynsmyndighet (SFS 2018:1175). NIS-direktivet gav även medlemsstaterna själva möjlighet att avgöra vilka verksamheter som bör ses som leverantörer av samhällsviktiga tjänster, även om direktivet även uttrycker en vikt av enhetlighet i denna bedömning mellan medlemsstater ((EU) 2016/1148). Denna typ av frihet saknas i NIS 2.

2.1.2 Vilka krav ställer NIS 2 på verksamhetsutövare?

NIS 2 ställer i huvudsak tre krav på verksamhetsutövare. Den första är att verksamhetsutövare behöver identifiera om denne omfattas av direktivet och i så fall anmäla sig till relevant tillsynsmyndighet, där rollen som tillsynsmyndighet inom transportsektorn rekommenderas att tillfalla Transportstyrelsen (SOU 2024:18, s.214). Det andra kravet är att verksamhetsutövaren ska arbeta systematiskt med informationssäkerhet, och det tredje att verksamhetsutövaren ska rapportera in incidenter (MSB, 2024b).

Arbetet med informationssäkerhet ska utgå från en allriskansats och minimikrav ställs på att verksamhetsutövaren har strategier för riskanalys för informationssystems säkerhet. Direktivet ställer krav på att verksamhetsutövaren ska arbeta med incidenthantering, säkerställa driftkontinuitet, säkerställa säkerheten vid förvärv, utveckling och underhåll av olika nätverks- och informationssystem, och slutligen arbeta med säkerhet inom sin leveranskedja. Delkravet på säkerhet inom leveranskedjan beskrivs som följande ((EU) 2022/2555, Artikel 21.2):

"säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet [verksamhetsutövare] och dess direkta leverantörer eller tjänsteleverantörer"

I SOU 2024:18 (s.195) görs bedömningen att varje verksamhetsutövare " *endast behöver vidta riskhanteringsåtgärder i förhållande till sin [direkta] leverantör*", även om utredningen även menar på att kraven bör specificeras närmare av olika föreskrifter. I artikel 21.3 förtydligas att verksamhetsutövare ska ((EU) 2022/2555):

"*beaktar de sårbarheter som är specifika för varje direktleverantör och tjänsteleverantör och den övergripande kvaliteten på deras leverantörers och tjänsteleverantörers produkter och cybersäkerhetspraxis, inbegripet deras förfaranden för säker utveckling*"

Utöver dessa krav ska verksamhetsutövaren därtill inbegripa utbildning inom cybersäkerhet, säkerställa personalsäkerhet och använda sig av multifaktorautentisering eller liknande lösningar för exempelvis textkommunikation inom den egna verksamheten. Verksamhetsutövaren ska även bedöma effektiviteten i de genomförda riskhanteringsåtgärderna ((EU) 2022/2555, Artikel 1–3, 21).

Direktivet saknar tydliga avgränsningar gällande vilka delar av en verksamhetsutövares verksamhet som ska omfattas av direktivet, och slutsatsen som dras inom SOU 2024:18 är att hela verksamheten bör ses som omfattade. Denna slutsats grundas bland annat i att nätverk och andra informationssystem tenderar att vara sammankopplade inom en verksamhet, och att gränsdragningar därmed skulle kunna leda till problematik (SOU 2024:18, s.125).

2.2 Företagsbeskrivning

Fallföretaget som behandlas i denna studie kommer förbli anonymt och hädanefter refereras till som “företaget”. Företaget är ett stort svenskt konsultföretag och bedriver verksamhet inom ett antal olika områden, inklusive arkitektur, miljö- och hållbarhet samt transportinfrastruktur. Företaget har en bred expertis inom olika projekttyper, och antar olika roller beroende på kundens behov. Bland annat erbjuder företaget tjänster inom projektering, projektledning, olika säkerhetstjänster och expertrådgivning inom olika områden. Företaget är en del av en större internationell koncern, med verksamheter spridda runt om i Europa.

Företagets verksamhet består av ett antal olika verksamhetsområden som fokuserar inom olika inriktningar. Dessa verksamhetsområden är uppdelade i olika affärsenheter, som i sin tur är uppdelade i mindre grupper vars medlemmar arbetar inom olika projekt. Det verksamhetsområde som utför projektet är verksam inom transportsektorn, och inom verksamhetsområdet är det företagets järnvägs-affärsenhet som driver projektet.

Som en del av företagets expertstöd till olika funktioner och uppdrag, nyttjar företaget kompetens från utlandet i form av ”resursstödsenheter”. Dessa resursstödsenheter kan bidra med stöd inom områden så som uppdragsstyrning och olika teknikområden. Denna kompetens, lyfts in från utlandet i syfte att hålla företaget konkurrenskraftigt i en alltmer snabbföränderlig värld, samtidigt som nyttjandet av detta stöd medför en möjlighet att tillgå konsulter som både är väl kvalificerade för uppdraget, samt som kan tillgås till en konkurrenskraftig kostnad, något som är behjälpligt för verksamheten då tillgången till personal i Sverige är begränsad. Dessa resursstödsenheter står i dagsläget för en avsevärd del av det verksamhetsområde som driver fallprojektets ekonomiska resultat. Resursstödsenheter finns både inom och utanför EU och faller formellt under företagets verksamhet i Storbritannien. Inom fallprojektet verkar kompetens från dessa resursstödsenheter i huvudsak genom att bistå inom området av projektering.

Företaget besitter även ett ledningssystem, som tar grund i olika internationellt erkända standarder såsom ISO 9001:2015 och ISO 14001:2015, något som medför att processer för bland annat kvalité, säkerhet och miljö finns inbyggda som steg i företagets övergripande projektmodell.

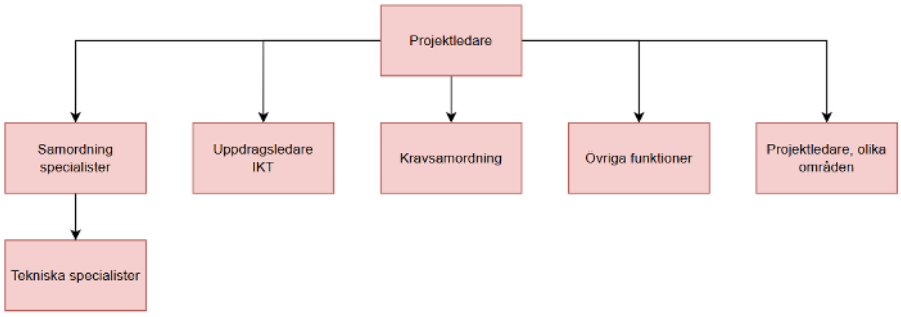
2.3 Projektbeskrivning

Fallprojektet, hädanefter ”projektet”, är ett omfattande infrastrukturprojekt inom järnvägssektorn, med ett kontraktsvärde på tiotals miljoner kronor för företaget. Företaget har vunnit projekteringen av projektet, vilket innefattar uppdraget att förse och upprätthålla förfrågningsunderlag samt bygghandlingar för utförandentreprenad. Förfrågningsunderlag innefattar de material som beskriver vad som ska upphandlas och vilka krav som kommer att ställas på anbudsgivaren. Projektet är multidisciplinärt, och kräver insatser från ett flertal av grupperna inom företagets järnvägs-affärsenhet.

Projektet är vidare uppdelat i tre olika faser. Den första fasen är en “planerings-, orienterings- och utredningsfas”, den andra en detaljprojekteringsfas och den tredje fasen innefattar att företaget ska agera som stöd under ibruktagandet av det som projekterats, samt ta fram förvaltningsdata, vilket är den information som ska agera som stöd för förvaltningen av det som projekterats efter att byggandet färdigställts (Trafikverket, 2022).

2.3.1 Trafikverket

Ägaren till projektet är Trafikverket, som ansvarar både för drift och underhåll av vägar och järnvägar, men även för långsiktig planering av transportsystemet (Trafikverket, 2023). Trafikverket är även en beredskapsmyndighet med sektorsansvar inom transportsektorn, vilket innebär att myndigheten ansvarar för planering av totalförsvaret och krisberedskap inom sektorn (SFS 2022:524). Projektet drivs av Trafikverkets verksamhetsområde Stora projekt och består av ett antal olika roller. Nedan, i figur 1, presenteras en övergripande bild över Trafikverkets projektorganisation. Illustrerat är projektets kärngrupp samt vissa delar av den utökade projektgruppen. De existerar ytterligare ett antal andra involverade från Trafikverkets sida, såsom olika förvaltningsansvariga och individer som kontaktas vid behov under projektet, exempelvis i form av roller såsom Samverkansledare och Kalkylsamordnare.



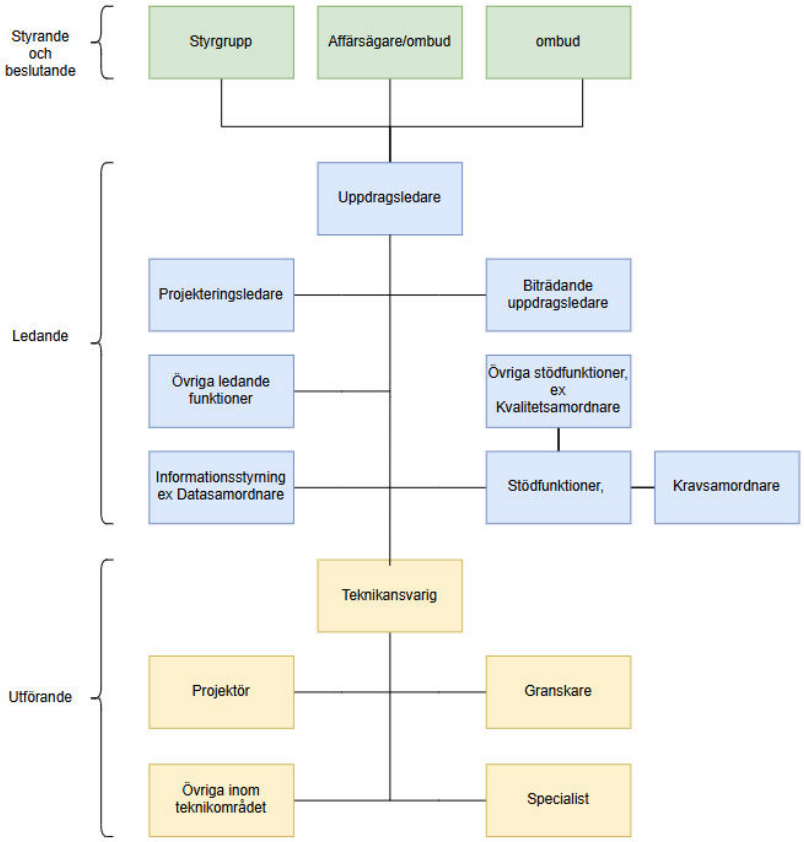
Figur 1: Trafikverkets projektorganisation

I denna studie har kontakt erhållits med Trafikverkets projektledare, som ansvarar för projektet som helhet. Detta ansvar inkluderar projektets ekonomi, men även att säkerställa att kontakt mellan olika parter upprätthålls inom projektet, exempelvis i form av att kommunikationsrutinen Fråga/Svar sker på ett tidsmässigt rimligt sätt och att de arbete som utförs dokumenteras korrekt.

2.3.2 Företagets projektorganisation och roller

Företagets projektorganisation i projektet kan i grova drag delas upp i tre generella funktioner, en styrande och beslutsfattande funktion, en ledande funktion, och en utförande funktion. En översiktlig representation presenteras i figur 2. Varje roll inom uppdragsorganisationen innefattar olika uppgifter och kommunicerar i olika omfattning

med Trafikverkets projektpersonal. Vissa roller fylls av samma person i projektet, exempelvis av är krav- och kvalitetssamordnaren samma person.



Figur 2: Översikt av projektorganisation

Inom den ledande funktionen verkställs kravuppfyllnad av flera olika roller inom projektorganisationen, såsom projekteringsledare, som bland annat har i uppdrag att säkerställa att tekniska lösningar uppfyller kundens krav. Kvalitetssamordnaren i sin tur har bland annat ansvaret att se till att krav kommuniceras på ett tydligt sätt inom uppdraget och ansvarar för att beakta kundens krav gällande kvalité, vilket bland annat kan innefatta att säkerställa att olika processer inom uppdraget genomförs på ett sätt som matchar kundens krav. Kravsamordaren i sin tur arbetar med att verifiera att både interna och externa krav uppfylls inom uppdraget. Datasamordnaren ansvarar för att se till att den digitala hanteringen inom projekt sköts utifrån de projektspecifika krav som finns, vilket bland annat inkluderar att ställa krav på resterande av projektorganisationen när de kommer till dokumenthanteringen samt kontrollera att dessa krav efterföljs. Inom vissa projekt, såsom detta, finns även en samordnande roll i form av Tekniksamordnare, som samordnare de olika teknikområdena genom respektive Teknikansvarig. Teknikansvarig samordnar sitt teknikområde, och innehar bland annat uppgiften att beakta resursplanering, teknikval och riskhantering inom teknikområdet. Teknikansvariga samverkar även med bland annat kravsamordnaren i kravhanteringsprocessen.

Den utförande delen av projektorganisationen består av enskilda enheter för respektive teknikområde. Inom varje teknikområde varierar antalet personal beroende på områdets omfattning i projektet, och i varje teknikområde finns i grova drag tre olika roller. En av dessa är specialisterna, som ansvarar för att säkerställa att föreslagna tekniska lösningar uppfyller de krav som ställs av kunden. En annan är granskaren, som ska säkerställa att den projekterade lösningen uppfyller kravställningar, genom att bland annat granska dokumentation och andra handlingar som tillkommit under uppdragets gång. Utöver dessa är projektörerna de som utför själva projekteringen i projektet. Projektörerna utför även egenkontroller för att säkerställa kravuppfyllnad i det egna producerade materialet, och tilldelas arbete av respektive teknikansvarig. De tidigare nämnda resursstödsenheterna som verkar i projektet, härstammar från Indien och bidrar i huvudsak med projektörer till projektet.

2.3.3 Krav och kravhantering i projektet

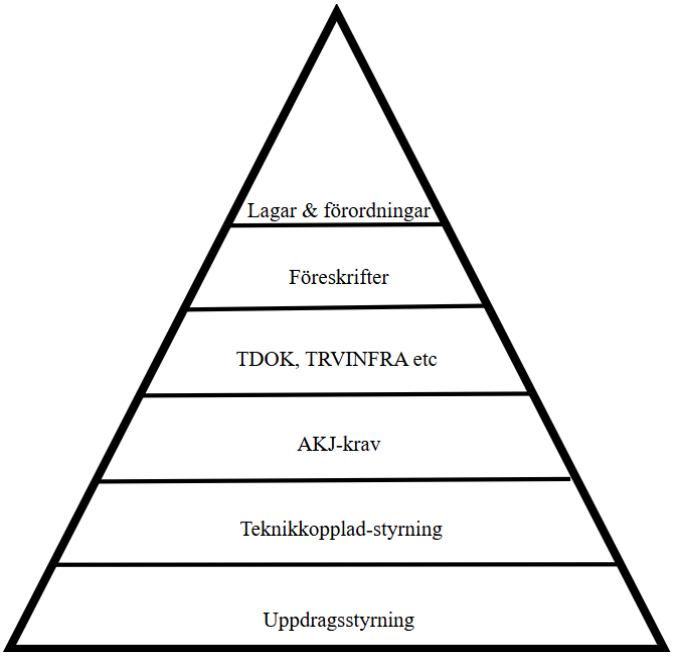
Dick et al., (2017, kapitel 1) beskriver att krav agerar som grundpelare till projekt och definierar vad varje involverad intressents behov är, samt vad SuC:en (system under consideration) behöver göra för att uppfylla dessa behov. Dick et al. menar vidare på att intressenters behov kan vara i direkt konflikt med varandra, samt att dessa behov inte nödvändigtvis är helt tydligt definierade vid ett projekts startskott. Dick et al. menar att det är av stor vikt att krav kommuniceras på ett sätt som alla intressenter förstår, utan onödig tvetydighet eller formuleringar av en så pass avancerad teknisk grad att endast experter inom området kan förstå dem. Dessutom beskriver Dick et al. vidare att ofullständiga kravställningar är den största faktorn till misslyckade projekt.

Tabell 1: Härkomst av olika krav

Ord/förkortning	Betydelse
ABK 09	Allmänna bestämmelser för konsultuppdrag inom arkitekt- och ingenjörsverksamhet
AKJ	Anläggningsspecifika krav järnväg, dokument som beskriver krav på bland annat teknisk funktion vid byggnation och drift, samt funktionskrav på färdigställd anläggning
TDOK	Trafikverkets styrande och stödjande dokument, finns både externa, som är tillgängliga via Trafikverkets webbplats och interna, som endast kan tillgås via olika projekt eller inom Trafikverket.
TRVINFRA	Dokument ur Trafikverkets infrastrukturregelverk
Teknikkopplad-styrning	Krav som härstammar från ett specifikt teknikområde

I projektet härstammar krav från flera olika källor, se tabell 1 för en översikt, och vid motsägelser mellan dessa använda en hierarki-pyramid för att avgöra vilka krav som ska

prioriteras, se figur 3. Detta medför att om ett uttryckt krav inom AKJ motsätts av ett krav formulerat inom någon relevant TDOK, så ska kravet från TDOK:en gälla. Utöver de kontraktskrav som återfinns i ABK 09, ställs ytterligare krav i andra kontraktsdokument och avtalshandlingar. Kontraktskrav tar som regel plats inom ”TDOK, TRVINFRA etc” i pyramiden, även om undantag finns. Denna hierarki är något som förmedlats av Trafikverket inom projektet.



Figur 3: Kravhiearki i projektet

Företagets kravsamordnare (K) i projektet beskriver att vid större projekt såsom det studerade i denna studie, kan kravmassan, dvs den totala mängd krav, bli väldigt stor. Till exempel kan ett enskilt TDOK-dokument innehålla ett stort antal krav och vid ett stort projekt blir många TDOK:ar relevanta. Inom projektet har dessa dokument, inklusive TRVINFRA och andra teknikkopplad-styrningsdokument sammanställts inom ett ”kravpaket”. Detta paket består av ca 350 TDOK- och TRVINFRA dokument, samt ett femtiotal andra dokument.

Olika krav hanteras på olika sätt inom projektet beroende på dignitet inom projektet. TDOK- och TRVINFRA krav kan bland annat hanteras genom Fråga/Svar, medan de mer tekniska AKJ-kraven kräver en mer formell hanteringsstruktur. Ur ett företagsperspektiv hanteras dessa krav inom företagets projekteringsprocess genom ett flertal steg. Den interna processen följer 5 faser. Dessa är:

- Systematisera: avser processen att definiera ansvarsfördelningen för uppfyllandet av ett krav.
- Acceptera: Den fas där samsynen gentemot kunden kring projektets krav arbetas fram.

- Ändringshantering: Den fas där förändring av krav sker. När de kommer till omformuleringar och avstyrkan av krav så ska detta ske enligt en överenskommen process.
- Identifiera och formulera: Denna fas innefattar de arbete som görs för att identifiera nya krav under projekteringen.
- Verifiera: Den fas där företaget demonstrerar att det uppfyller krav, genom att exempelvis hänvisa till olika handlingar.

Ett flertal av dessa faser har ett tidsöverlapp, vilket innebär att relevanta processer sker i samsyn. Denna process speglar ett förhållningssätt från företagets sida, men i projekt beställda av Trafikverket, vet Trafikverket i stora drag bara om att denna process sker och kanske mindre om vars i processen företaget och projektet faktiskt är.

Utöver de krav som kan direkt kopplas till projektet, existerar även en omfattande mängd krav inom informationssäkerhet från företaget själv. Dessa utgår från olika styrdokument, i form av exempelvis policys och riktlinjer. Dessutom bedrivs inom företagets teknikområden en kvalitetsäkringsprocess som inkluderar flera olika steg av granskning av skapade handlingar. Dessa steg inkluderar egenkontroll, en interngranskning av en oberoende person, säkerhetsgranskning för vissa tekniker samt samgranskning inom och mellan teknikområden för att identifiera gränssnittskrockar. Därtill granskas även handlingar innan leverans som regel av en datasamordnare. Denna process dokumentera utförligt för att säkerställa teknisk kravuppfyllnad.

2.3.4 ProjectWise

ProjectWise är en molnbaserad projektsamordningsplattform som används inom projektet. Plattformen medför bland annat möjligheten för användarna att samverka inom olika projekt, möjligheten att granska olika handlingar och agerar som ett versionshanteringssystem samt har inbyggda referenshanteringsfunktioner, vilket medför att en god spårbarhet kan upprätthållas inom projekt. Utöver detta kan användaren även arbeta med ett stort antal olika filformat på plattformen, såsom olika CAD-format och GIS-data.

Alla produkthandlingar och produktdokument som tas fram under projektets gång ska lagras och bearbetas på plattformen, även om företaget även använder andra interna arbetsytor såsom Uppdragsportalen, en Sharepoint-yta. Denna Sharepoint-yta är ämnad att endast användas som en samlingsyta för intern uppdrags-generell information, såsom tidskoder och processdokument. Även Trafikverket använder en Sharepoint-yta, som är ämnad för lagring av exempelvis kontraktsdokument. Alla handlingar som ska levereras till Trafikverket av företaget, ska lagras inom ProjectWise.

Plattformen medför även en möjlighet att, genom behörigheter för olika användare, låsa mappar. Detta möjliggör hanteringen av material av olika sekretessklassning, även om vissa klasser av material ej är tillåtna på plattformen.

3. Teori

I följande avsnitt presenteras de teoretiska utgångspunkter som studien utgår ifrån. Först presenteras det val av begreppsapparat som gjorts när de kommer informationssäkerhet, samt hur organisationer kan arbeta med informationssäkerhet. Därefter presenteras tre relevanta begrepp till området av informationssäkerhet, i form av MTO, risk och Safety. Slutligen presenteras det teoretiska ramverket STAMP, som står till grund för den använda analysmetoden STPA som beskrivs i metodavsnittet, tillsammans med en övervägning av hur detta val av ramverk gjordes samt tillskottet av agentteori.

3.1 Vad är cybersäkerhet och informationssäkerhet?

Det finns många definitioner av begreppet cybersäkerhet och hur begreppet är relaterat till informationssäkerhet (von Solms & von Solms, 2018). von Solms & von Solms argumenterar för att, ur ett perspektiv för att hjälpa styrande och verkställande ledning att få en förståelse över begreppet cybersäkerhet, är det behjälpligt att se cybersäkerhet som en delmängd av informationssäkerhet. Detta medför en möjlighet att presentera cybersäkerhet på ett mer konkret sätt, även om von Solms & von Solms även poängterar att denna definition är en förenkling som inte alla kommer vara nöjda med. En konkret förklaring av begreppet kan vara välbehövt, eftersom bland annat Oscarson (2019, s.48) belyser området av informationssäkerhet som omoget och att det kan uppfattas som abstrakt och utan verklig nytta.

Denna syn på cybersäkerhet som en delmängd av informationssäkerhet stärks av att internationellt erkända standarder inom området, såsom ISO 27000-serien, speglar samma synsätt. ISO 27000-serien av standarder för informationssäkerhet, cybersäkerhet och dataskydd, som beskrivs nedan i delavsnittet 3.1.2 ”*ISO 27000-serien för informationssäkerhet, cybersäkerhet och dataskydd*”, beskrivs som följande av Svenska institutet för standarder (SIS, u.åa): *”ISO 27000-serien baseras på att just skydda information, och eftersom den idag ofta finns digitaliserad så omfattar den givetvis även cybersäkerhet”*, vilket är en beskrivning som ligger i linje med von Solms & von Solms synsätt av cybersäkerhet som en delmängd av informationssäkerhet.

I kontexten av detta ter sig begreppsvalet av informationssäkerhet eller cybersäkerhet till stor del vara en semantisk fråga, och med bakgrund i detta kommer informationssäkerhet vara den fråga som behandlas inom denna studie, och begreppen kommer därtill behandlas som likvärdiga. Dock kommer begreppet cybersäkerhet att användas vid referat där begreppet används.

För att konkretisera vad som avses med begreppet informationssäkerhet inom denne definition, refereras återigen till ISO 27000. En av standarderna inom ISO 27000 är ISO 27002, som definierar informationssäkerhet utifrån tre attribut. Dessa är Confidentiality (konfidentialitet), Integrity (riktighet) och Availability (tillgänglighet). Dessa attribut utgör den så kallade CIA-triangeln. Konfidentialitet kan tolkas som egenskapen av att tillgången till information för obehöriga parter är begränsad, riktighet som egenskapen

att informationen inte är manipulerad på ett otillåtet sätt och därmed trovärdig och korrekt, och tillgänglighet egenskapen att informationen är tillgänglig när den är menad att vara tillgänglig (Niels et al., 2017).

3.1.1 Hur kan organisationer arbeta med informationssäkerhet?

Det finns ett stort antal olika ramverk för hur organisationer kan arbeta för att uppnå en högre cybersäkerhet (Djebbar & Nordström, 2023), och i kontexten av leverantörskedjan beskriver NIST (2018, s.16) ett antal effektiva åtgärder som en organisation kan genomföra för att stärka cybersäkerhet i hela leverantörskedjan. Dessa inkluderar att aktören i fråga identifierar vilka cybersäkerhetskrav som den bör ställa på sina underleverantörer, att dessa kravställningar speglas i de kontrakt som skrivs, att underleverantören informeras om hur dessa kravställningar kommer att verifieras och att organisationen genomför denna verifiering.

Arbete med informationssäkerhet inom leverantörskedjan är av relevans inom stora infrastrukturprojekt, som det som studeras i denna studie, då värdet av en välfungerande leverantörskedja är stort. En effektiv förvaltning av leverantörskedjor leder till ökad effektivitet, kostnadsreduceringar och övergripande mer framgångsrika projekt (Mehmood et al, 2024).

Nyttorna med en god informationssäkerhet inom en organisation är därtill ett flertal. Bland annat kan de leda till minskade informationssäkerhetsincidenter, möjliggöra efterlevnaden av rättsliga krav men även leda till ett ökat förtroende och konkurrensförmåga gentemot andra aktörer (Oscarson, 2019, s.49–52). Dock ses cybersäkerhet i många organisationer som en i huvudsak teknisk fråga (Ervural & Ervural, 2018, s.269), men bortom tekniska åtgärder innefattar begreppet cybersäkerhet även policys och procedurer syftade att upptäcka och mildra konsekvenserna av cyberattacker (Tzavara & Vassiliadis, 2024, s.1697). Exempelvis definieras begreppet inom NIS 2 utifrån EU förordningen ((EU) 2019/881) som:

"*cybersäkerhet: all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot*."

vidare definieras cyberhot inom förordningen som:

"*cyberhot: en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare dessa system och andra personer*."

Arbete med informationssäkerhet är en kontinuerlig process, vilket innebär att insatser inom området inte bör betraktas som en engångsföreteelse med ett slutgiltigt mål. I stället bör målsättningen vara ett fortsatt kontinuerligt arbete för ständig förbättring och anpassning. Detta speglas i det krav som ställs på ett systematiskt informationsskyddsarbete inom lagstiftningen, exempelvis SFS 2018:1174 och av

expertråd från exempelvis Nationellt cybersäkerhetscenter (2025) och MSB (2024d). Vidare så innebär de hot som existerar mot dagens system, att det krävs en holistisk systemsyn, där människan, organisationen och teknik samverkar för att skapa förutsättningarna för cybersäkerhet (Shrobe et al., 2018).

Organisationers cybersäkerhetstrategier har delvis tagit form som en konsekvens av framväxten av regelverk och standarder (Abrahams et al, 2024). Inom informationssäkerhet formulerar standarder grundläggande säkerhetsprinciper som agerar som kontrollmekanismer för att en aktör ska kunna påvisa efterlevnad av en god säkerhetspraxis. Standarder används bland annat som ett verktyg vid tillsyn, utveckling och dokumentation av processer (Dhillon, 2017, kapitel 7). Användning av standarder är därför en grundläggande del av en organisations säkerhetsarbete. Standarder spelar även en viktig roll inom upphandlingar då det medför att beställare och leverantör lättare kan tydliggöra kravställningar (SIS, u.åb). Inom informationssäkerhet kan en tillämpning av standard vidare ha en positiv effekt på omvärldens förtroende för en aktör (Oscarson, 2019, s.52). Dessa standarder kan variera i detaljeringsgrad. Exempelvis är ISO 9001:2015 en generell standard för kvalitetsledning, medan ISO 22163:24 är en tillämpning av standarden inom järnvägssektorn, med egna specificerade krav. Samtidigt finns det dock också potentiella svagheter med förhållandet till generella säkerhetsstandarder, då dessa inte alltid täcker specifika behov och risker som kan existera inom en given verksamhet (Siponen & Willison, 2009).

Inom NIS 2-direktivet refereras användandet av standarder som en möjlig metod för att säkerställa att de åtgärder som krävs i termer av riskhanteringsåtgärder inom cybersäkerhet genomförs ((EU) 2022/2555, Artikel 21.1) och Jan-Olof Andersson, en representant från SIS, lyfte under MSB Cybersäkerhetskonferens att vid arbete enligt standarden ISO 27001 (Informationssäkerhet- Cybersäkerhet och integritetsskydd - Ledningssystem för informationssäkerhet), så bör en organisation täcka in det krav som ställs utav NIS 2-direktivet (MSB, 2024c). Kecklund & Sandblad (2021, s.74) belyser dock att användningen av standarder kräver kunskap och kompetens för att kunna användas på ett effektivt sätt. Standarder agerar inte som “kokböcker”, utan tolkningar och val måste göras utifrån en god expertisgrund och används standarder felaktigt riskerar detta att bidra till att nya risker uppkommer.

3.1.2 ISO 27000-serien för informationssäkerhet, cybersäkerhet och dataskydd

ISO 27000 är en serie av standarder som i huvudsak behandlar två olika huvudområden (SIS, u.åb). Den första är ledningssystemstandarder. Ett ledningssystem är ett verktyg som hjälper organisationer att bedriva verksamhet enligt fastställda rutiner, processer och policys genom att agera som ett ramverk för hur dessa faktorer ska organiseras (SIS, u.åc). Seriens andra huvudområde är vägledningsstandarder, som innehåller vägledning för säkerhetsåtgärder. Serien är menad att vara tillämpningsbar inom alla organisationer, oavsett storlek eller vilken verksamhet som bedrivs.

Inom ISO 27002, en vägledningsstandard, som agerar som en praktisk guide för hur en organisation kan arbeta för att uppfylla kraven som ställs av ISO 27001, en ledningssystemstandard, presenteras tydliga instruktioner upp om hur en organisation kan arbeta med informationssäkerhet inom leverantörsrelationer. Standarden innefattar bland annat instruktioner kring vilka processer som en organisation bör ha i åtanke, och instruerar bland annat att organisationen bör (SIS, 2022a):

- Identifiera sina leverantörer, vilken typ av tjänst eller produkt som denna tillför och vilken information från organisationen som leverantören har tillgång till samt möjliga risker förknippat med denna tillgång.
- Ställa och övervaka att säkerhetskrav uppfylls, och använda kompletterande åtgärder om krav inte kan ställas.
- Klassa information inom verksamheten och mappa den egna klassningsmodellen gentemot leverantörens informationsklassningsmodell.
- Inkludera i kontrakt rätten att granska leverantörens förhållningsätt till informationssäkerhet.
- Genomföra regelbunden övervakning, granskning och utvärdering av förändringar i leverantörens informationssäkerhetsarbete.

ISO 27001 belyser även hur organisationen bör arbeta för att säkerställa att den egna verksamheten uppfyller de krav som ställs av exempelvis policys, standarder och andra regeldokument. Bland annat lyfter standarden att organisationen bör överväga användningen av automatiska verktyg för att rapportera och mäta verksamhetens efterföljande av krav (SIS, 2022b).

Många organisationer använder ISO 27000-serien för att säkerställa sin informationssäkerhet, och även delar av företagets verksamhet är certifierade gentemot ISO 27001. Även Trafikverket beskriver sig bedriva sitt systematiska informationssäkerhetsarbete i enlighet med ISO 27001 (se exempelvis TDOK 2011:175 “Informationssäkerhet i Trafikverket”), även om Trafikverket inte är certifierade.

Under ett internt webbinarium beskriver en av företagets verksamhetsområde-chefer att även resten av verksamheten arbetar aktivt med att certifiera sig mot ISO 27001. Detta för att säkerställa att företaget förhåller sig proaktivt till förändrade marknadsförutsättningar. En av företagets utvecklingschefer (U), som varit med och drivit företagets certifieringsprocess, lyfter i sin tur tre drivkrafter till att hens del av verksamheten certifierat sig. För de första, att kunderna börjat ställa mer krav kring certifiering och inom vissa upphandlingar ställs krav på att anbudsgivaren är certifierad, för de andra att medarbetarna inom företaget själva önskat att ha något tydligt att förhålla sig till, dels för att ha något i ryggen vid dialog med kunder, dels för att kunna känna sig trygga i att de agerar rätt. Den tredje anledningen som (U) lyfte var att omvärldsläget och de reella hot som detta innebär medför, innebär att certifiering är en klok idé.

3.2 MTO – Människa, teknik och organisation

Ett socioteknisk system är ett system där teknik och människa samverkar. Dessa system är ofta komplexa och dynamiska (Kecklund & Sandblad, 2021, s.22). En ansats för att kunna analysera sådana system är MTO. Kecklund & Sandblad (2021, s.35) beskriver begreppet MTO som både ett synsätt och kunskapsområde, men även ett samlingsnamn för metoder där samspelet mellan människa, teknik och organisation samt utformningen mellan dessa betonas. Vid studier av komplexa verksamheter, krävs ett helhetsperspektiv (Kecklund & Sandblad, 2021, s.78). Eftersom informationssäkerhet innefattar allt från tekniska åtgärder, exempelvis i form av multifaktorautentisering, till säkerhetspolicys menade att påverka användarens beteende och den övergripande organisationens säkerhetskultur, krävs därmed en holistisk ansats i detta arbete. Ett MTO-perspektiv medför att dessa aspekter beaktas, vilket är centralt för att uppnå en långsiktig effektiv och hållbar säkerhetsstrategi (Kecklund & Sandblad, 2021, s.282f).

3.3 Risk och Safety

I kontexten av informationssäkerhet är begreppen risk och Safety framträdande och begreppens betydelse blir därför av vikt. Det finns många definitioner av risk inom litteraturen, men många av dessa följer en struktur av sannolikheten för en negativ konsekvens bedömt tillsammans med storleken av konsekvensen (Hollnagel, 2008). Inom NIS 2-direktivet ((EU) 2022/2555, Artikel 6) definieras risk som: "*risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att en sådan incident inträffar*.", något som är jämförbart med de vedertagna litteraturmässiga definitionerna.

Det saknas dock en tydlig definition av begreppet Safety inom det EU-material som rör cybersäkerhet, och utöver detta saknas det även en tydlig svensk översättning av ordet, bland annat som en konsekvens av att både Safety och Security översätts till säkerhet på svenska. Detta trots att begreppen har vedertagna skillnader i betydelse på engelska, speciellt inom informationssäkerhet (Bartnes, 2006). Det existerar vidare även olika existerande synpunkter på hur Safety bör definieras inom litteraturen. Hollnagel (2013) beskriver en process där begreppet utvecklats från att definieras som: "*avoiding that something goes wrong*", ett synsätt han kallar Safety-I, till att som alternativ i stället beskrivas som: "*ensuring that everything goes right*" ett synsätt som han kallar Safety-II. Ett tredje alternativt presenteras av Leveson (2020, s.27) genom Safety-III, som menar på att Safety i stället kan, och kanske börs definieras som:

"*Safety is defined as freedom from unacceptable losses as identified by the system stakeholders. The goal is to eliminate, mitigate, or control hazards, which are the states that can lead to these losses*."

Definitionen av Safety är av vikt då definitionen kommer ha en påverkan på det val av riskstrategi som är lämplig (Hollnagel, 2018, s.50). Inom det val av teoretiskt ramverk som gjorts i denna studie, i form av STAMP, beskriver Leveson (2004, s.249) Safety

som: ”*an emergent property of systems that arises from the interaction of system components*”.

Inom CSM-RA förordningen ((EU) 402/2013), vilket är den förordning som utgör den rättsliga grunden för den gemensamma säkerhetsmetod för riskutvärdering som används inom järnvägssektorn, definieras Safety som:”*frånvaron av oacceptabel risk för skada*”, vilket även är den definition som Trafikverket hänvisar till inom exempelvis TDOK 2020:0236 ” Metod för riskhantering vid ändringar gällande trafiksäkerhet järnväg (CSM RA)”. Ett antagande görs därmed att Trafikverkets syn på säkerhet speglar detta.

3.4 STAMP

Många traditionella olycks- och riskmodeller baseras på tankar om att det existerar ett linjärt samband mellan orsak och konsekvens, även kallat Event Chain Models (EAC). Dessa modeller fungerar väldigt bra när systemen de appliceras på är enkla och tydliga samband kan utläsas mellan felande komponenter och konsekvenser, men dessa modeller har flera tydliga svagheter i en värld där system blir alltmer komplexa. Leveson (2004, s.3–5) menar på att vid användningen av EAC:s blir bland annat valet av "initiating event” och “root cause” till stor grad arbiträr, eftersom hon menar på att valet av båda är beroende av en subjektiv bedömning. Detta kan bland annat leda till att det resultat som denna typ av analys resulterar i, blir av en allmän karaktär, med litet värde för att kunna användas för att undvika liknande situationer i framtiden.

Leveson (2004, s.9–11) menar även på att olycksmodeller som analyserar stora sociotekniska system behöver se systemet som en helhet. En analys av en komponent ur sitt sammanhang är menlös, då det är komponentens interaktioner med andra komponenter i systemet som leder till de hon kallar “emerging properties” eller framträdande egenskaper. “Safety” är en av dessa egenskaper, och kan därför endast förstås i kontexten av en komponents interaktion med resterande delar av systemet.

I kontexten av detta krävs det en annan teoretisk ansats för att vi ska kunna bättre analysera stora komplexa system. Ett alternativ som Leveson (2004, s.12–13) presenterar är Systems-Theoretic Accident Model and Processes (STAMP). STAMP har sina teoretiska rötter inom systemteori, och olyckor sker i denna kontext som en konsekvens av otillräcklig kontroll eller en bristande efterlevnad av säkerhetsrelaterade begränsningar. STAMP använder fyra huvudsakliga begrepp: begränsningar, kontroll-loopar, processmodeller och grader av kontroll som teoretiska byggstenar för att förklara system och interaktionen mellan olika hierarkiska nivåer.

Begränsningar är de regler eller säkerhetskrav som systemet måste följa för att fungera säkert och styr de interaktioner som sker inom systemet. En kontroller eller kontrollenhet i systemet, som kan vara både exempelvis en människa eller en dator, består av tre delar: en kontroll-loop, en processmodell, och en kontrollalgoritm. Kontroll-loppen består av de kontrollåtgärder eller de förmedlade begränsningar som

kontrollen kan utföra gentemot en annan styrd kontroller eller process, och av feedback, som används för att uppdatera kontrollerns processmodell. Processmodellen hos en kontroller kan beskrivs som kontrollerns uppfattning om vad som ”händer” i processen eller hos den styrda kontrollern. Kontrollalgoritmen kan ses som det regelverk med vilket kontrollern tolkar sin processmodell, och tillsammans skapar de förutsättningarna för de kontrollåtgärder som utförs. Med grader av kontroll syftar teorin på att olika kontrollenheter i systemet innehar olika nivåer av kontroll, vilket innebär att de kan påverka systemet på olika sätt och i olika utsträckning (Leveson, 2004, s. 12–17).

Leveson menar vidare på att det flesta olyckor sker i så kallade "boundary areas” och i “overlap areas”. Ett boundary area är ett område det existerar förvirring gällande vilken kontroller som bestämmer. Inom dessa områden är oftast de funktioner som sker dåligt definierade, och kommunikationen är som regel undermålig. Ett overlap area å andra sidan definierar Leveson som ett område där mer än en kontroller styr över samma process. Detta medför en potential till att konflikter uppstår, som negativt påverkar funktionens utfall (Leveson, 2004, s.24–25).

3.4.1 STAMP, relaterade metoder och utvecklingsområden

Det finns i huvudsak två metoder kopplade till STAMP, Causal Analysis Using System Theory (CAST) och Systems-Theoretic Process Analysis (STPA), vilket är den metod som används i denna studie. En omfattaningsgranskning av Patriarca et al. (2022) visar på att ansatsen av STAMP, STPA och CAST är vedertagna inom den publicerade akademiska världen. Samtidigt påpekar Patriarca et al. att många av publicerade verk föreslår förändringar och tillskott till ramverken, vilket tyder på att det finns en uppfattning om att ramverken bör användas som flexibla ramverk snarare än strikta metodguider eller “kokböcker”. I den granskning som Patriarca et al. genomförde var en stor del av de publicerade verken inriktade på flyg-, sjöfart- och bilsektorn, men ramverken har även tillämpats inom området av cybersäkerhet vid flera tillfällen, exempelvis av Kondo et al. (2018), som lyfter STAMP som ett alternativ för att skapa processdiagram som underlag för diskussioner kring de behov av separation som behövs inom ett nätverk. Ett annat exempel är av Wright & Jun (2019) som i sin tur använder STAMP för att illustrera värdet av ramverket vid analys av cybersäkerhetsfrågor genom att applicera ramverket på det dataintrång som drabbade den amerikanska detaljhandelskedjan Target under 2013/2014.

Ramverket har dock tydliga utvecklingsområden. Bland annat menar Salmon et al. (2012) att STAMP, på grund av sin kontroll- och systemteoretiska bakgrund, innefattar en begreppsapparat som inte alltid lämpar sig väl för att illustrera fel som ej är av en teknisk natur, exempelvis när det kommer till organisatoriska fel. Zhang et al. (2022) identifierar i sin tur två huvudsakliga områden där det kan finnas utrymme för vidare forskning: integreringen av kvantitativ analys samt en stärkt integreringen av mänskliga och organisatoriska faktorer i kontrollstrukturen. Zhang et al. menar att tillskottet av en kvantitativ dimension till ramverket skulle kunna bidra med ytterligare information som är värdefull för analysen och menar att mänskliga- och organisatoriska faktorer till viss

del är av begränsad omfattning i det ursprungliga ramverket. Zhang et al. föreslår utvärderingen av flera olika ramverk i detta syfte, såsom hybrid-ramverken STAMP-HFACS (human factors analysis and classification system) och STAMP-VSM (viable system model). Dessa bör enligt Zhang et al. valideras genom fler applikationer. Andra exempel på ramverks-utvidgningar inkluderar Souza et al. (2020), som utvidgade STPA med STRIDE, en hotmodell utvecklad specifikt för cybersäkerhet. Souza et al. fann att verktygen kompletterade varandra och medförde en djupare analys än vad som hade varit möjligt med hjälp av den ena eller den andra.

3.5 Val av teoretiskt ramverk

Ett flertal val av teoretiska ramverk övervägdes under studiens gång. Alternativ som övervägdes inkluderade nätverksteori och spelteori, som båda erbjuder olika perspektiv inom problemområdet, samt VSM eller viable systems model, som är ett ramverk för att förstå hur ett system "överlever" i sin omgivning.

Nätverksteori har sin grund inom grafteori och fokus läggs på att analysera relationen mellan olika aktörer inom nätverket. Ett nätverk är en uppsättning av noder, där varje nod kan bestå av exempelvis enskilda människor eller hela organisationer och där kopplingarna mellan noder representerar olika typer av sociala band. Nätverksteori kan användas på nästan alla sociala system, såsom projektgrupper och organisationer och medför en möjlighet att kombinera olika typer av data för att skapa en deskriptiv avbildning av interaktioner mellan olika parter (Borgatti & Ofem, 2010). Spelteori i sin tur innefattar, i grova drag, användandet av matematiska modeller för att modellera den strategiska interaktionen mellan olika beslutstagare. Spelteori kan därför användas för att analysera interaktioner för att ge insikter inom exempelvis konfliktscenarion (Myerson, 1997), och har använts flitigt inom ett stort antal områden, såsom inom ekonomi och vid analys av samarbete i system med många agenter (Kapliński & Tamošaitienė, 2010).

Efter noggrant övervägande valdes dock STAMP som ramverk till studien, detta då ramverket medför en möjlighet att genomföra en systemorienterad analys av komplexa processer och riskhanteringsåtgärder, vilket är centrala teman för denna studie. Vidare existerar ett tydligt gap i forskningen kring användandet av ramverket i denna typ av kontext, se avsnittet 3.4.1 "STAMP, relaterade metoder och utvecklingsområden" ovan, vilket medför en möjlighet för studien att bidra till detta område.

Även tillskottet av VSM övervägdes i enlighet med Zhang et al. (2022), som rekommenderade en utvärdering av hybridramverket STAMP-VSM. Efter en genomgång av modellen ansåg författaren att modellen krävde en djupare förståelse för den underliggande teorin för att kunna tillämpas än vad som ansågs tidsresursmässigt passande. I stället valdes agentteori, som beskrivs nedan i avsnitt 3.6 "Agentteori", som ytterligare ett teoretiskt verktyg, då det är ett välanpassat verktyg för att beskriva varför intressekonflikter kan uppstå i beställare-utförare relationer, vilket är ett betydande område i kontexten av informationssäkerhet.

3.6 Agentteori

Principal-agent theory (PAT) eller Agency-theory, hädanefter agentteori, kan användas för att beskriva de intressekonflikter som kan uppstå när en intressent eller utförare (agent) utför en uppgift åt en annan intressent (principal), bland annat som en konsekvens av den informationsasymmetri som existerar mellan principalen och agenten. Eftersom principalen saknar fullständig insyn i agentens beteenden kan detta leda till att agenten agerar på ett opportunistiskt sätt, där egna incitament har högre prioritet än principalens (Shapiro, 2005).

Shapiro (2005) menar på att eftersom en principal inte kan observera allt som sin agent gör, behöver principalen förlita sig på substitut, som Shapiro menar på kan leda till att agenten i sin tur matchar sitt beteende gentemot de observerbara substituten för att ge intrycket av att de presterar bättre än vad de faktiskt gör. Ett exempel som Shapiro använder är studenter (agenter) som lägger ansträngningen på att bli bättre på att prestera på prov i stället för att få en bättre förståelse för kursinnehållet, då det är genom prov som läraren (principalen) gör sin bedömning om elevens förståelse över området.

Denna informationsasymmetri kan existera åt båda håll i en leverantörsrelation. Exempelvis kan en beställare inneha en bättre insikt i sina verkliga behov, men välja att inte förmedla detta för att uppnå en förhandlingsfördel, eller i form av att en principal ljuger om arbetsförhållanden för att exploatera sina agenter. En intressent kan även uppfylla rollen av både agent och principal samtidigt inom olika kontext och olika roller (Shapiro, 2005).

Ramverket av agentteori har applicerats inom en mängd olika discipliner, såsom ekonomi och management (Shapiro, 2005), men även inom kontexten av riskallokering är ramverket ett möjligt verktyg, något som Shrestha et al. (2019) gör genom att använda ramverket som en ansats för att analysera risköverföring inom PPP:s (public private partnerships). Shrestha et al. belyser att på grund av den tidigare nämnda informationsasymmetrin mellan olika intressenter, så kan även bedömningar av olika projektrisker skilja sig åt.

Perspektivet av agentteori är även av vikt vid analys av cybersäkerhetsrisker. Moore (2010) beskriver att: "*Information systems are prone to fail when the person or firm responsible for protecting the system is not the one who suffers when it fails*." Olika intressenter har olika intressen och dessa intressen är inte alltid i linje med de ansträngningar som krävs för cybersäkerhet. Moore menar därför att cybersäkerhetsanalyser bör börja med en analys av vilka incitament som finns bland intressenterna.

4. Metod

I följande avsnitt beskrivs den valda analysmetoden STPA samt den genomförda datainsamlingen, i form av intervjuer, enkätstudie och dokumentgranskning. Även en diskussion gällande studiens validitet presenteras i slutet av avsnittet.

4.1 STPA

STPA är ett riskanalysverktyg för att på ett heuristiskt sätt illustrera sambandet mellan systemrisker och osäkra kontrollåtgärder, genom att uttrycka svagheter inom systemets komponenter och dessa komponenters interaktion med varandra. STPA bygger på den teoretiska grunden av STAMP och använder de teoretiska begrepp och den systemteoretiska ansats som teorin innehar. Detta illustreras genom en hierarkisk kontrollstruktur, där kontrollers utför kontrollåtgärder gentemot andra kontroller och processer. Dessa åtgärder baseras på enhetens processmodell, som uppdateras genom feedback från den kontrollerade kontrollern eller processen. Ett sätt att förklara kopplingen mellan STPA och STAMP är att STAMP beskriver hur risker uppstår, och STPA är en metod för att identifiera risker. STPA kan även ses som ett konkret verktyg för att tillämpa STAMP i praktiken.

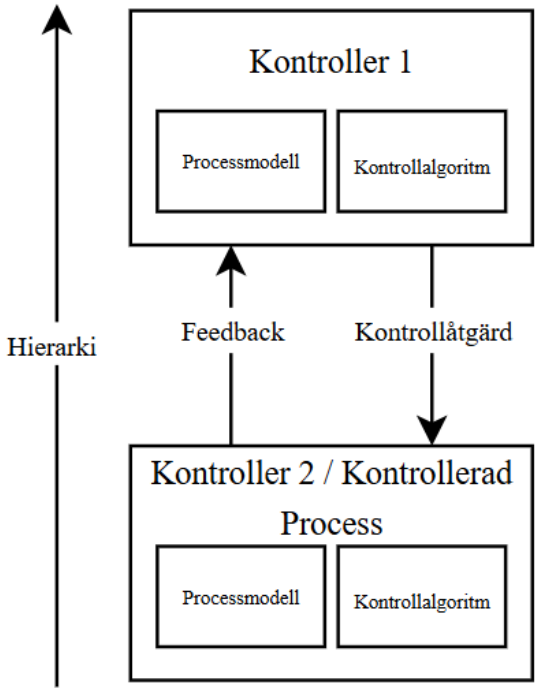
Följande beskrivning av STPA grundas i Leveson & Thomas STPA Handbook, och är endast en översiktlig beskrivning av metoden (Leveson & Thomas, 2018). De begrepp som används inom analysmetoden förklaras mer ingående inom tabell 2.

Tabell 2: Förklaring av STPA begrepp

Begrepp	Förklaring
Kontroller	En entitet i modellen som utför kontrollåtgärder för att styra en process eller annan kontroller.
Processmodell/Mental modell	En abstraktion av vad en kontroller tror om den process eller annan kontroller som denne styr
Kontrolalgoritm/Regler för beslutsfattande	Det ramverk som styr de kontrollåtgärder som en kontroller utför, baserat på sin processmodell.
Kontrollåtgärd	Den styrning som en kontroller utför gentemot en process eller annan kontroller. En osäker kontrollåtgärd är en åtgärd som i en viss kontext leder till ett negativt utfall.
Feedback	Feedback används för att uppdatera en kontrollers processmodell, och härstammar från den kontrollerade processen eller kontrollern.

Den övergripande processen för STPA kan sammanfattas i fyra steg:

1) Definiering av syftet med analysen, inklusive specifikation av systemgränser och vilken typ av negativa utfall som önskas undvikas.
2) Modellering av kontrollstrukturen. Ett exempel på en enkel kontrollstruktur ges i figur 4.
3) Identifiering av osäkra kontrollåtgärder. Exempel på en osäker kontrollåtgärd är att en kontrollåtgärd saknas eller att den ges vid fel tillfälle.
4) Identifiering av negativa utfall, eller förlustscenarion.



Figur 4: Enkelt exempel av kontrollstruktur

Leveson & Thomas beskriver en formell process för alla fyra steg, exempelvis genom att olika delar av analysen tilldelas olika nummer för att på ett enklare sätt möjliggöra en spårning av härkomst av exempelvis felaktiga kontrollåtgärder och potentiella negativa utfall. Detta kommer dock inte att göras i denna studie, eftersom Leveson och Thomas i STPA Handbook även beskriver en något annorlunda ansats när systemet som ska analyseras är av organisatorisk eller social natur. Leveson & Thomas beskriver att en av de största skillnaderna vid en sådan analys, kontra vid en STPA:s använd på en "engineered product", är hur man fastställer vad problemet som ämnas att lösas är, eftersom denna process kan vara mer komplex för denna typ av system. Denna ansats beskrivs i stället som följande (Leveson & Thomas, s86f):

1) Identifiering och förståelse över vilket problem som behöver lösas.

2) Identifiering av hur den organisatoriska miljön ser ut inom problemområdet och hur denna bör se ut för att lösa det identifierade problemet.
3) Skapandet/identifieringen av krav för att förbättra problemområdet.
4) STPA av systemet/organisationens kontrolstruktur för att identifiera var dessa krav implementeras.
5) Användningen av resultatet från föregående steg för att ge förslag på förändringar i den organisatoriska designen.

I denna studie speglas och presenteras metodens olika steg som följande: Steg 1) genom studiens fyra första frågeställningar, steg 2) genom presentationen av resultatet av den datainsamling som gjorts inom projektet, steg 3) och 4) genom den efterföljande analysen och steg 5) i de slutgiltiga rekommendationerna till företaget och Trafikverket.

I syfte att uppnå studiens andra syfte och svara på frågeställningen av vilka styrkor och svagheter som STAMP besitter för att illustrera en projektorganisation, kommer den hierarkiska kontrollstrukturen och dess användning för att identifiera kravimplementation att utvärderas.

4.2 Datainsamling

Datainsamlingen genomfördes i huvudsak genom tre metoder. För det första genom intervjuer, för det andra genom en dokumentationsgranskning, och för det tredje genom en enkät. Vidare hölls även mailkonversationer med ett flertal av respondenterna vid behov av förtydligande av frågeställningar som dykt upp under intervjuerna.

4.2.1 Intervjuer

För datainsamling nyttjades intervjuer, som genomfördes med en kvalitativ och semistrukturerad ansats, vilket medförde att övergripande frågeställningar formulerades i förhand och presenterades under intervjutillfällena, men att en viss frihet togs när de kommer till exempel till ordningen av frågorna och följdfrågor, i linje med Bryman (2012, s.471). Denna intervjumetod valdes då den ger respondenten en möjlighet att djupdyka inom de områden som denne finner vara av störst vikt och mest relevanta. Det var av särskild vikt att intervjupersonerna skulle få möjligheten att framställa sin förståelse över problemformuleringarna som låg till grund för frågeställningarna (Bryman, 2012, s.471). Semistrukturerade intervjuer är vidare en mycket flexibel metod för datainsamling, bland annat eftersom det medför möjligheten till att ställa följdfrågor. Frågorna formulerades utifrån en övergripande generell utgångspunkt för att undvika att möjligheten till följdfrågor begränsades (Bryman, 2012, s.471).

I tabell 3 presenteras en översikt över genomförda intervjuer. Intervjufrågorna återfinns i appendix C, och kolumnen ”Vilka frågor” illustrerar vilka frågor som ställdes till vilken respondent. Totalt genomfördes sex intervjuer, både med personal som varit involverade i företagets certifieringsprocess mot ISO 27001, som en del av företaget certifierat sig mot och med deltagare från projektet. Detta inkluderar deltagare både från

företaget och Trafikverket. För en förklaring över respektive deltagares ansvarsområde inom projektet, se avsnitt 2.3.1 ”Trafikverket” och 2.3.2 ”Företagets projektorganisation och roller”. Intervjuerna med deltagarna från företaget spelades in och transkriberades. Detta för att minska behovet av tillförlit till det egna minnet och för att det även medförde en bättre möjlighet att analysera deltagarnas svar (Bryman, 2012, s.482). Däremot fanns ej denna möjlighet till detta vid intervjun med Trafikverkets projektledare.

Urvalsprocessen för intervjupersoner gjordes utifrån den givna problemformuleringen, och intervjuerna genomfördes med fokus inom två huvudsakliga områden. För det första för att få en förståelse över hur kravställningarna arbetas med inom projektorganisationen, och för de andra för att få en förståelse för själva projektet. Utöver detta genomfördes även en intervju med den chef som drivit den certifierade delen av företagets certifieringsprocess gentemot ISO 27001, detta för att skapa en bättre förståelse över certifieringens betydelse och dess möjlighet att hjälpa företaget uppfylla de krav som ställs av NIS 2.

Inom samtliga roller som intervjuats inom projektet, innehas rollen av en enskild individ, förutom inom rollen som teknikansvarig, eftersom varje teknikområde inom projektet har en egen teknikansvarig. Eftersom studien ämnar illustrera förhållningsättet gentemot underleverantörer, valdes den teknikansvarige ut vars teknikområde innehade störst antal utländska medarbetare.

Tabell 3: Översikt över genomförda intervjuer

Deltagare och beteckning	Område	Vilka frågor	Datum
(K) Kravsamordnare	Projekt	Kravställningar företag	19/2
(U) Utvecklingschef	Certifieringsprocess	Certifieringsprocessen	25/2
(PLT) Projektledare Trafikverket	Projekt	Trafikverket PLP	31/3
(TA) Teknikansvarig	Projekt	TA Företag	9/4
(DSF) Datasamordnare	Projekt	Datasamordning	10/4
(PLF) Projektledare företag	Projekt	Projektledning företag	14/5

En intervju med Trafikverkets kravsamordnare i projektet eftersträvades, men hen ersattes innan någon intervju hann genomföras. Bedömningen gjordes då att den nya i tjänsten inte uppfyllde kravet på expertis inom projektet som efterfrågades. Vid vidare efterforskning visade det sig även att rollen fyllts av ett flertal olika personer under projektets gång.

Vidare genomfördes den första intervjun med (K), med en något mer öppen ansats jämfört med resten av intervjuerna, detta eftersom intervjun hade ett tvådelat syfte, dels att skapa en förståelse för kravsamordningsprocessen i projektet, dels för att få en insikt i vilka organisatoriska förutsättningar som projektet bedrivs under, något som författaren bedömde bäst kunde uppnås om (K) fick möjlighet att prata lite mer fritt.

För att säkerställa att ingen av deltagarna till intervjustudien försattes i en svår situation på grund av den information som de delades med sig av, har intervjudeltagarna anonymiserats. De refereras i stället till med hjälp av respektive yrkestitlar, som även i hög grad speglar deras kompetensområde. Eftersom dessa titlar är vanliga inom branschen som företaget är verksamt inom samt att det finns ett stort antal andra aktörer av liknande typ inom branschen, gjordes bedömningen att det är möjligt att förhålla sig till en övergripande anonymisering i studien.

Även en avvägning gällande studiens syfte och möjligheten att uppnå detta trots anonymisering gjordes. Då studien i sin helhet presenterades för företaget vid färdigställande och att författaren vid denna presentation hade möjlighet att ge förtydligande kontext vid behov, bedömde författaren att anonymiseringen inte påverkade studiens värde för företaget. Vidare ansågs studiens möjlighet att uppfylla sitt andra syfte, att utvärdera användningen av STAMP i denna typ av projektorganisatoriska kontext, att vara opåverkad av anonymiseringen.

4.2.2 Enkät

Under intervjuprocessen uppfattade författaren området av informationssäkerhet som väldigt oklart och abstrakt bland respondenterna. I syfte att få en djupare grund att stå på inför analysen valde författaren därför att även skicka ut en enkät till de som är verksamma inom projektet. Genom denna enkät möjliggjordes även informationsinsamling från parter som de ej fanns möjlighet att intervjua, på grund av de begränsningar av tid som fanns till författarens tillgång. Denna enkät skickades ut över mail baserat på projektets organisationsförteckning till de som var en del av företagets svenska verksamhet. Denna förteckning visade sig vara något föråldrad, och ett antal av de tillfrågade respondenterna meddelade att de inte längre var aktiva i projektet. Vissa av frågorna i enkäten ställdes både projektspecifikt och generellt, för att ge en bättre bild av hur informationssäkerhetsarbetet i projektorganisationen såg ut som helhet. Totalt sett fick enkäten 21 svar, se tabell 4. Med ett bortfall på ~ 10 personer som ej längre är verksamma i projektet ger detta en svarsfrekvens av ≈ 24%.

Tabell 4: Antal tillfrågade och svar enkät

Totalt antal tillfrågade	Antal svar
101	21

Design av enkäter kräver stor eftertanke, något som bland annat Lietz (2010) visar genom att presentera en översyn av enkätdesign och hur olika val påverkar kvaliteten på svaren. Lietz belyser bland annat att frågor bör vara så korta som möjligt för att öka läsarens förståelse, även om lite längre frågor även kan vara av värde då detta kan ge respondenten intrycket att frågan är viktig och därmed förtjänar extra ansträngning. Frågorna bör formuleras med en låg grad av grammatisk komplexitet, och mer komplexa frågor bör brytas ner till enklare frågor. Ett för avancerat vokabulär kan leda till att respondenten känner sig dum, vilket påverkar svarskvalitén negativt, och genom att undvika vaga eller generella ord såsom “kanske” och "antagligen" samt undvika

användningen av hypotetiska frågor ökar kvaliteten av svaren ytterligare. Man bör som designer av enkäter vidare undvika användningen av "double barreled questions", vilket är frågor som innehåller två olika koncept. Dessutom bör man undvika negativt formulerade frågor då dessa kräver längre tid för respondenten att begripa (Lietz, 2010, s.250–255).

Olika val av frekvensord, såsom "alltid" och "sällan", leder till stora skillnader i respondenternas tolkning. Detta kan mitigeras genom att precisera svarsalternativen, med exempelvis en formulering på formen "en gång i månaden". Ordningen av frågor spelar även de en roll, och som regel är det bättre att ställa generella frågor före specifika. Resonemanget bakom detta är att om en specifik fråga behandlas före en generell, så påverkar detta hur respondenten tänker kring den generella frågan, och den specifika aspekt som behandlats kanske inte tas i beaktning av respondenten vid besvarande av den generella frågan. Tillhörighetsfrågor eller demografifrågor, såsom om kön och ålder, bör även de komma efter resten av frågorna. Detta för att undvika att de negativa känslor som kan uppstå av tillhandahållandet av denna information, ej påverkar respondentens svar (Lietz, 2010, s.255–257).

När det kommer till formulering av svarsalternativ finns ett antal punkter att ha i åtanke. Vid användning av poängskalor finns exempelvis ett val av hur många svarsalternativ eller "poäng" som bör användas. Poängskalor mellan 5–7 är vanligast, men ett större spann av svarsalternativ kan leda till en större grad av särskiljning mellan svaren, vilket kan vara av värde. Ett alternativ är att använda en fempoängskala vid frågor där respondenten förväntas svara på en "absolute judgment"- fråga, dvs en fråga där respondenten måste välja ett svar utan möjlighet att jämföra med andra alternativ, och en poängskala på 7–9 i frågor som kräver en mer abstrakt ansats från respondenten. Dessutom bör negativa svarsalternativ tilldelas det numeriskt lägsta värdet, samt vid frågor där svarsalternativ i någon utsträckning kan tolkas som "social oacceptabelt", bör dessa placeras längst till vänster, eftersom det bidrar till att respondenterna läser alla svarsalternativ (Lietz, 2010, s.260–263).

Dessa rekommendationer har varit i åtanke under produktionen av enkäten. Lietz påpekar dock att en förhållning till dessa rekommendationer: "*...will only serve to go some way in the development of a questionnaire that is of high quality.*". Bland annat bör enkäten testas i mindre skala för att säkerställa att frågorna är förståeliga för respondenterna, och att svaren även är mätbara och kan användas för sitt syfte (Lietz, 2010, s.265–266). Detta genomfördes i denna studie genom att enkäten presenterades för ett antal verksamma inom andra projekt: två projektörer inom signalteknik, en projektör inom mark och biträdande uppdragsledare samt till handledaren för studien. Efter en revidering baserat på den insamlade feedbacken, skickades enkäten till projektets uppdragsingenjör. Eftersom uppdragsingenjören ansvarar för att samla in information från projektets medarbetare, exempelvis när det kommer till arbetsmiljö, bedömdes hen kunna bidra med ytterligare konstruktiv feedback. Baserat på denna feedback justerades enkäten ytterligare för att säkerställa dess kvalitet, innan den

slutligen skickades ut inom projektet. Den slutgiltiga enkäten finns tillgänglig i appendix A, tillsammans med ett kortare designdokument i appendix B.

4.2.3 Dokumentgranskning

Kecklund & Sandblad (2021, s.326) belyser dokumentgranskning som ett verktyg som kan användas för att få en bild av hur en verksamhet arbetar, och utöver intervjuer och enkäten genomfördes därför även en omfattande granskning av dokumentation relaterade till företagets förhållningsätt till informationssäkerhet. Resonemanget bakom detta är det systemperspektiv som ansats i denna studie, samt att företagets studerade underleverantör i projektet, dvs personalen från de tidigare nämnda resursstödsenheterna, ska förhålla sig till samma krav på informationssäkerhet som resterande av företagets personal.

Tillgång till projektets yta på ProjectWise erhölls, vilket möjliggjorde datainsamling direkt från projektdokumentationen. Detta inkluderade innehållet i ”kravpaketet”, avtalshandlingar, kvalité- och riskhanteringsinstruktioner samt övrig projektdokumentation. På grund av den omfattande mängd av dokumentationen som kravpaketet bestod av, nyttjades ett systematiskt angreppssätt för att hantera dokumentationen. Vid granskning av TDOK- och TRVINFRA dokument sorterades dokumentationens och dess titlar utifrån ett antal nyckelbegrepp eller nyckelområden. Dessa var: information-och datahantering, kravuppfyllnad och kvalitetsstyrning, projektering, risk-och säkerhet, sekretess samt behörighet. Vid granskning av TDOK- och TRVINFRA dokument ledde detta till ett resultat av 25 dokument som bedömdes ha möjlighet att innehålla relevanta krav till området. Inget TRVINFRA-dokument matchade sökkriterierna, vilket är rimligt då dessa dokument i huvudsak beskriver de krav som ställs på infrastrukturens egenskaper och skötsel (Trafikverket, 2025).

De dokument som matchade sökkriterierna var uppdelade i 18 öppet tillgängliga dokument, dvs med en sekretessklassning av ”Ej Känslig” och sju dokument av en högre klassning än ”Ej känslig”. Efter en granskning av de 18 externa dokumenten, bedömdes fem vara relevanta för studien eftersom de innehöll krav kopplade till informationssäkerhet. Av de interna dokumenten bedömdes att två vara relevanta, se tabell 5 nedan.

Tabell 5:

Externt tillgängliga dokument	Interna dokument
TDOK 2011:176 "Informationssäkerhet - krav riktade till medarbetare"	TDOK 2018:0623 “Hantering av information utifrån konfidentialitet
TDOK 2011:177 "Informationssäkerhet - krav riktade till IT-driftleverantör"	TDOK 2013:0261 “Informationsklassningsmodell avseende konfidentialitet, tillgänglighet, riktighet och spårbarhet

TDOK 2011:178 "Informationssäkerhet - krav riktade till verksamhetsansvariga"	
TDOK 2016:0032 “Kvalitetsstyrning i upphandlad verksamhet - entreprenad och projekteringstjänster”	
TDOK 2016:0411 “Hantering av data och dokumentation till/från förvaltade system - Järnväg”	

Samma ansats som för TDOK- och TRVINFRA dokumenten användes även för att sortera ut relevant dokumentation ur resterande av kravpaketet. Bland dessa dokument fanns ej några relevanta dokument i enlighet med de sökkriterier som specificeras ovan.

4.3 Studiens validitet

Eftersom studien utfördes åt företaget men ändå ämnar ge en bild över kommunikationen inom projektorganisationen har intervjuer genomförts även med beställaren, Trafikverket. Däremot existerar en tydlig diskrepans mellan mängden information som samlats in från de två parterna av Trafikverket och företaget. Antalet intervjuer samt mängden information som insamlats från företagets sida är avsevärt högre än från Trafikverkets sida. Denna obalans var tänkt att delvis mildras genom ytterligare en intervju med Trafikverkets kravsamordnare, men på grund av att personen i rollen av byts ut fler gånger under projektets gång bedömdes detta som inte möjligt eller passande. Därmed speglas företagets relation till dessa andra aktörer i huvudsak av den syn som olika människor inom företaget återgivet. Detta har tagits i beaktning vid bearbetning av materialet och all information insamlat från företaget har granskats utifrån ett kritiskt förhållningssätt.

Man bör även betona att den genomförda informationsinsamlingen endast kan spegla en del av verkligheten. Andra människor än de som intervjuats i denna studie kan inneha en annan bild av hur dessa processer ser ut. Däremot medför studiens ansats fortfarande möjligheten till värdefulla insikter i hur informationssäkerhetskrav arbetas med i praktiken av olika aktörer, vilket är i linje med studiens syfte.

5. Resultat

I följande avsnitt presenteras resultatet av den genomförda dokumentationsgranskningen, enkätstudien och slutligen intervjuerna med respondenterna verksamma inom projektorganisationen.

5.1 Resultat av dokumentationsgranskningen

I följande delavsnitt presenteras resultatet av dokumentationsgranskningen. Delavsnittet har delats upp i två huvudsakliga tematiska delar. Den första, en redogörelse över företagets interna informationsssäkerhetsåtgärder, exempelvis i form av olika policys. Den andra delen, en redogörelse över projektets styrande dokumentation i form av en redogörelse för innehållet i avtalsdokumentationen och kravpaketet.

5.1.1 Företagets interna informationssäkerhetsåtgärder

Företaget besitter omfattande informationssäkerhetspolicys som reglerar hur information ska hanteras och skyddas inom verksamheten. Dessa policys reglar även hur konsulter, underleverantörer och andra som verkar inom företagets verksamhet ska hantera information. Dessa policys omfattar både tekniska och organisatoriska åtgärder menade att bidra till ett starkt informationsskydd. Exempel på åtgärder inkluderar riktlinjer för hur social manipulation ska motverkas inom verksamheten, krav på användningen av multifaktorautentisering, regler för lösenordshantering, när användningen av säkra filöverföringssystem är ett krav och vilka molntjänster som får användas. Policyerna innefattar även beskrivningar av hur cyberincidenter ska hanteras och rapporteras, och en tydlig rapporteringsstruktur finns klargjord.

Policyerna innehåller även instruktioner gällande hur information ska klassificeras inom företaget, vilket innefattar både intern företagsinformation och kundinformation. Policyerna beskriver att all information som behandlas eller lagras inom företagets verksamhet ska hanteras utifrån tre kriterier. Dessa är: konfidentialitet, som innebär att endast de som har rätt till informationen, ska ha tillgång. Riktighet, som innebär att informationen ska vara korrekt och inte manipulerad, samt tillgänglighet, som betyder att informationen ska vara tillgänglig när den är menad att vara tillgänglig, dvs den tidigare nämnda CIA-triangeln.

Företaget innehar även en policy som reglerar användningen av AI inom verksamheten. Inom denna policy belyses bland annat att användningen av AI kan medföra att det material som skapas är vinklat, samt att företaget inte heller kan göra upphovsanspråk på de material som skapas genom AI. Policyn belyser vidare att vid användning av AI ska etiska, sociala och säkerhetsmässiga faktorer vara i åtanke. Policyn uppmanar dock till användningen av AI för bearbetning av kunddata, eftersom detta medför en möjlighet att förbättra analysen av denna data. Detta dock under förutsättningen att detta ej är explicit förbjudet av antingen lag eller i kontraktet mot kunden. Vid dokumentgranskningen av projektdokumentationen, återfanns inga tydliga direktiv från

Trafikverkets sida som explicit reglerar användningen av AI, vilket innebär att denna policy är det enda styrande dokument som reglerar AI inom projektet.

Informationssäkerhetspolicyerna beskriver vidare att informationssäkerhetssåtgärder är integrerade i verksamheten på tre olika skyddsnivåer. Den första nivån av skydd består av en efterlevnad av policys och processer för att informationssäkerhetsarbetet ska bli en naturlig del av verksamheten. Den andra skyddsnivå utgörs av IT-säkerhetsavdelningen, som bland annat har ett aktivt ansvar i att säkerställa att styrdokument är uppdaterade samt innehar ansvaret att bistå med stöd till resten av verksamheten inom informationssäkerhetsfrågor. Den tredje skyddsnivån består av både interna och externa granskningar av verksamheten, för att säkerställa att de åtgärder som gjorts har haft önskad effekt.

Utöver dessa policys använder sig företaget av kontinuerliga mailutskick och kortare utbildningar som påminner om olika aspekter av informationssäkerhet, såsom hur medarbetaren kan arbeta för att motverka social manipulation och vikten av att ej följa okända länkar i mail. Företaget har även ett antal ytterligare verktyg och rutiner för att hjälpa medarbetaren att arbeta i linje med informationssäkerhetspolicyerna. Detta inkluderar verktyg för att hjälpa medarbetaren ha koll på lösenord, hur kryptering av innehåll på USB:er ska genomföras, hur företagets VPN kan användas samt rapporteringsvägar för saker som upplevd phising och skadlig programvara.

5.1.2 Projektets styrande dokument

Det finns en mängd dokument som behandlar hur företaget ska arbeta med informationssäkerhetsfrågor inom själva projektet. Inom kontraktsdokumentationen, som består av uppdragsbeskrivningen (UB), uppdragskontraktet (UK) och administrativa föreskrifter (AF) formuleras ett antal krav när de kommer till informationssäkerhet.

Inom UB:n finner vi krav på att information ska hanteras ur ett informationssäkerhetsperspektiv och detta krav tar grund i både relevant lagstiftning inom området och TDOK 2018:0623 “Hantering av information utifrån konfidentialitet". UB:n beskriver även att företaget är skyldig att säkerställa att obehöriga inte får tillgång till information, i form av skyddsvärda uppgifter, verksamheter och tillgångar samt att denna information inte heller får manipuleras. Detta gäller både under projektet, och efter projektets slut. I samma avsnitt beskrivs även att all information som är en del av Trafikverkets interna hantering, där intern hantering även inkluderar arbetsuppgifter som utförs för Trafikverkets räkning, ska vara informationsklassat i enlighet med TDOK 2013:0261 “Informationsklassningsmodell avseende konfidentialitet, tillgänglighet, riktighet och spårbarhet”. Vad som inkluderas inom “arbetsuppgifter för Trafikverket” specificeras dock ej.

Inom UK:n finns en längre beskrivning av de krav på sekretess som företaget är skyldiga att förhålla sig till inom projektet. Bland annat beskrivs att företaget kommer

få ta del av sekretessbelagda uppgifter inom projektet, och att företaget därmed är skyldig att se till att alla inom företagets projektorganisation som tar del av uppgifterna, eller som kan antas få del av uppgifterna, är bundna av en sekretessförbindelse. Detta krav inkluderar exempelvis underkonsulter och Trafikverket kan även kräva att personer inom projektorganisationen ingår i individuella sekretessförbindelser gentemot Trafikverket. Slutligen beskriver de administrativa föreskrifterna att: "*Beställaren [Trafikverket] kan komma att genomföra revisioner av hur konsulten jobbar med informationssäkerhet genom självskattning eller revision på plats*".

Vid granskning av resterande av kravdokumentationen i enlighet med den process som beskrivs i metodavsnittet, uppmärksammades ett antal TDOK:ar med krav gällande informationssäkerhet, exempelvis TDOK 2011:176–178. Dessa var med i förteckningen över projektets styrande dokument, men har statusen "slopat" inom Trafikverkets dokumentdatabas. Detta lyftes av författaren till företagets kravsamordnare (K), som efter dialog med Trafikverket kom fram till att TDOK 2011:176–178 skulle fortsätta gälla inom projektet. Under intervjun med företagets projektledare (PLF) förtydligades detta, som beskrev att kontraktsdokumentationen uttryckligen beskriver att det är de dokument som återfinns inom kravpaketet som är den gällande, även om detta ej är den senaste versionen av dokumentet. Avsteg från detta kan göras, men endast efter diskussion med Trafikverket.

TDOK 2011:176–178 är riktade mot olika intressenter och ställer olika krav beroende på roll, och ställer omfattande krav när det kommer till informationssäkerhet. Däremot är det otydligt i kontexten av projektet vilka av dessa krav som förväntas uppfyllas av företagets projektpersonal, och vilka krav som är internt riktade inom Trafikverket. Dokumenten saknar även en tydliga beskrivningar av ansvarsfördelning, vilket kan bero på att dokumenten är bilagor till ett mer omfattande dokument.

Ett urval av krav som kan antas riktas mot extern personal på grund av sin formulering, beskrivs inom TDOK 2011:178. Dessa krav innefattar att extern personal ska informeras av chef eller uppdragsgivare gällande de villkor som gäller för tillgång och hantering av Trafikverkets informationstillgångar samt informationsbehandlingsresurser, att alla leverantörer och andra utomstående användare ska kontrolleras, med betoning på kontroller vid arbete med känsliga arbetsuppgifter eller annan konfidentiell information. Vidare ska även säkerhetsansvar klargöras för respektive uppdragstagare eller tredjepartsanvändare innan ett uppdrags start.

De checklistor med krav och åtgärder som nämns inom samtliga av TDOK 2011:176–178 är strukturerade i enlighet med ISO 27002:2005, dvs en äldre upplaga av standarden ISO 27002. Av ytterligare intresse är att dessa dokument är bilagor till TDOK 2011:175 "Informationssäkerhet i Trafikverket", men att detta dokument inte återfinns i kravpaketet.

Inom TDOK 2016:0032 "Kvalitetsstyrning i upphandlad verksamhet - entreprenad och projekteringstjänster", som även refereras till inom AF:n, uttrycks att Trafikverket även

har rätt att i kontexten av kvalitetsförsäkran inom projekt, genomföra både anmälda och oanmälda revisioner, uppföljningar, kontroller och granskningar av leverantören samt av alla möjliga underleverantörer inom leverantörskedjan. Leverantören har en skyldighet att se till att dessa revisioner och granskningar kan genomföras hos sina underleverantörer och att tillhandahålla all nödvändig dokumentation. Inom denna TDOK ställs även kravet på att: "*informationssäkerhet [ska] säkras genom konfidentialitet, spårbarhet, riktighet och tillgänglighet*".

Det finns även styrande dokument från Trafikverkets sida som reglerar olika delar av informationsflödet mellan olika system och olika aktörer. Ett exempel är TDOK 2016:0411 "Hantering av data och dokumentation till/från förvaltade system - Järnväg", som bland annat innehåller rutiner för behörighet till ett 20-tal olika system, inklusive exempelvis ProjectWise. TDOK:en innehåller även beskrivningar av vilken typ av data som får lagras i respektive system och när denna information ska levereras till systemet.

Under genomgången av de externt tillgängliga dokumenten som bedömdes ha möjlighet att innehålla krav relaterade till informationssäkerhet, noterades att visa dokument från Trafikverket som återfanns i kravpaketet, exempelvis TDOK 2015:0279 "Telesystem. Behörighet för arbete med telefonisystem", refererar till gamla dokument från Banverket, en svensk myndighet som ombildades till Trafikverket 2010, i form av BVH 372 "Enhetligt tillträdesskydd för Banverkets byggnader och anläggningar". Detta trots att nyare dokumentation som behandlar området existerar. Referenser till Banverkets dokument upptäcktes även inom ett antal andra TDOK:ar, såsom TDOK 2012:1046 och TDOK 2015:0280.

Av de interna dokument som återfanns i kravpaketet och som bedömdes vara av relevans för området av informationssäkerhet, innehade TDOK 2013:0261 konfidentialitetsstatusen "Ej Känslig", och kunde därför delges till författaren. TDOK 2013:0261 beskriver att all information, oavsett om den hanteras inom Trafikverket eller av någon extern part, ska klassas utifrån faktorerna av konfidentialitet, riktighet, tillgänglighet och spårbarhet, dvs CIA-triangeln med ett tillskott av ett krav på spårbarhet. Kravet på spårbarhet medför att förändringar av information ska ha en entydig spårning till en identifierad användare. Följandet av den metod för informationsklassning som dokumentet beskriver är ämnad att agera som stöd för hantering av behörighet för klassad information, och beroende på klassningsnivå ställs stora skillnader i krav på hur informationen ska hanteras och vem som kan anses vara tillåten att komma åt den.

TDOK:en beskriver vidare att ansvaret för informationsklassning, beror på kontext och vilken typ av information som ska klassas. (PLT) tillfrågades om vem som utför klassningen av de material som laddas upp på ProjectWise i projektet, och beskrev då att det är Trafikverket som utför själva klassningen, men att företaget ska föreslå en klassning i enlighet med TDOK:en.

Den andre interna TDOK:en, TDOK 2018:0623 ”Hantering av information utifrån konfidentialitet” innehade stämplingen Intern, och kunde därför inte delges till författaren. Däremot återfanns detta dokument trots denna klassning uppladdat på företagets Sharepoint. Författaren har valt att inte beskriva innehållet i dokumentet för att säkerställa att inga brott mot sekretess begås.

5.1.3 Sammanfattning av dokumentationsgranskning

Företaget ställer omfattande interna krav på informationssäkerhet, i huvudsak genom olika informationssäkerhetspolicys. Inom dessa policys formuleras både tekniska och organisatoriska informationssäkerhetsåtgärder. Därtill innehåller policyerna även beskrivningar kring hur AI får användas, vilket saknas inom projektdokumentationen.

Inom själva projektet ställer Trafikverket flera olika krav på informationssäkerhet samt sekretess. Dessa krav är utspridda mellan flera olika dokument, inklusive kontraktsdokumentation och olika TDOK:ar. Dessa krav är som regel formulerade i termer av vad som ska uppfyllas, och inte hur dessa krav ska uppfyllas. Trafikverket innehar även rätten att granska både företagets och företagets underleverantörers förhållningsätt till informationssäkerhet.

Vidare har vissa TDOK:ar som innehåller informationssäkerhetskrav slopad status inom Trafikverkets egna databas, och det saknas viktig kontext till flera av dessa dokument, då de endast är bilagor till mer omfattande dokument, som saknas i kravpaketet. Vissa av de TDOK:ar som innehåller informationssäkerhetskrav är även av en konfidentialitetsklassning som medför att de ej får spriddas helt öppet. Andra dokument, även om det inte är relaterade till informationssäkerhet, innehar referenser till mycket gamla dokument.

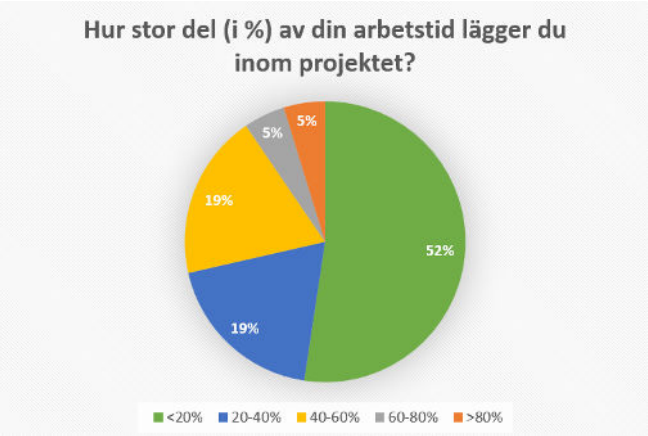
5.2 Resultat av enkätundersökning

I följande delavsnitt presenteras resultatet av enkätundersökningen. Först presenteras en kvantitativ sammanställning av enkätsvaren och därefter de kvalitativa fritextsvaren.

5.2.1 Kvantitativ sammanställning

Ett par av frågorna i enkäten var flervalsfrågor, vilket innebär att procentandelarna för dessa frågor inte nödvändigtvis kommer att motsvara andelen av respondenterna som valde ett visst alternativ. I stället illustrerar dessa procentandelar hur stor andel av de totala svaren som ett visst alternativ utgjorde. Dessa frågor markeras med *.

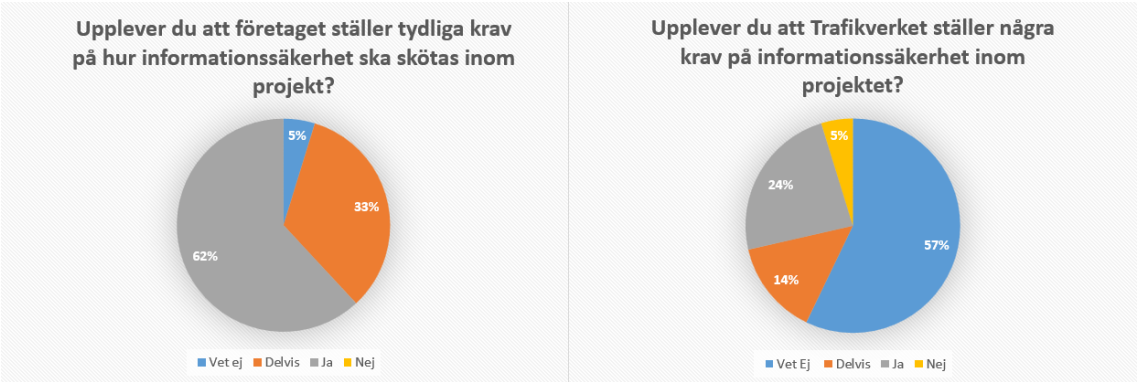
Demografimässigt återficks svar från en majoritet av de verksamma teknikområdena i projektet. På frågan om arbetstid i projektet, se figur 5, svarade runt 50% av respondenterna att de lägger mindre än 20% av sin arbetstid inom projektet. Endast mindre antal av respondenterna svarade att de lägger mer än 40%.



Figur 5: Fördelning av arbetstid i projektet

På frågan av hur viktigt respondenten anser att informationssäkerhet är inom sitt respektive teknikområde var det genomsnittliga svaret 6 av maximalt 7. Svarspridningen var dock rätt stor, med ett flertal av respondenter som svarade 3,4 eller 5. Även på frågan av hur ofta respondenterna hade informationssäkerhetsfrågor i åtanke varierade svaren avsevärt. Bland annat svarade fyra av respondenterna att de aldrig hade informationssäkerhet i åtanke, och nio att de alltid eller nästan alltid hade informationssäkerhet i åtanke.

På frågan om respondenten upplever att företaget ställer tydliga krav på informationssäkerhet, varierade svaren, se figur 6. En tydlig majoritet (62%), uppfattade de krav på informationssäkerhet som ställs från företaget som tydliga. 33% svarade däremot ”Delvis” på samma fråga och 5% ”Vet ej”. På frågan om respondenten upplevde att Trafikverket ställer några krav på informationssäkerhet inom projektet, var spridningen ytterligare större bland svaren, se figur 6. 57% svarade ”Vet ej”, 14% ”delvis”, 5% ”Nej” och 24% ”Ja”.



Figur 6: Respondenternas upplevda informationssäkerhetskrav

På frågan om respondenten någonsin upplevt någon typ av granskning när det kommer till informationssäkerhetsfrågor*, se figur 7, bestod 16% av svaren av ”Vet ej” och 44% av ”Nej”. Av de resterande svaren, uttrycker 20 % att de granskats av kund, och 20% att de granskats internt på företaget.

Figur 7: Upplevd granskning när det kommer till informationssäkerhet

På frågan om upplevelsen av granskning inom projektet*, se figur 7, svarade endast 1 respondent till att de upplevt detta, både av Trafikverket och av företaget. Resterande av svaren var en blandning mellan ”Vet ej” och ”Nej”, med en högre svarsfrekvens av ”Nej”.

5.2.2 Beskrivning av uppfattade krav och granskningar

Enkäten innehöll även ett antal möjligheter till fritextsvar. Dessa frågor behandlade vilka uppfattade krav på informationssäkerhet som ställs av Trafikverket och företaget. Därtill fanns även en fråga som efterfrågade om respondenten upplevt att dennes arbete granskats, antingen av företaget eller av en kund, både inom och utanför projektet.

Inom projektet beskriver en respondent att ett av de krav som Trafikverket ställer är att varje enskild resurs behöver behörigheter för att få tillgång till Trafikverkets olika system. Respondenten beskriver vidare att Trafikverket inte heller tillåter utländska resurser i projekt att få tillgång till vissa av dessa system, på grund av de säkerhetsrisker som detta kan innebära. En annan respondent beskriver att de krav på informationssäkerhet som Trafikverket ställer, främst gäller de sträckor av projektet som är säkerhetsklassade. De underlag som beskriver dessa sträckor får endast ett fåtal inom projektet ta del av. Detta är en punkt som respondenten menar att Trafikverket varit mycket tydliga med under möten. En tredje respondent beskriver att hen uppfattar att Trafikverket generellt ställer krav på vilka medier som är tillåtna för att dela information genom och i vilka fysiska miljöer man har rätt att arbeta med Trafikverkets projekt i. Exempelvis är de inte tillåtet att arbeta på Trafikverkets projekt på offentliga platser eller att arbeta genom offentliga nätverk. En annan respondent beskriver att de finner sig tydligt informerade om vad som gäller och att de som är verksamma inom Trafikverkets projekt ska ha koll på informationssäkerhetsfrågor och inte avvika från detta. Slutligen beskriver en respondent att hens roll i projektet är mycket liten, och att hen därför inte har koll på projektets kravpaket.

När det kommer till granskning av informationssäkerhet inom projektet inkom inga fritextsvar. Däremot beskriver en respondent att hen i andra kontext fått besvara frågor gällande sin användning av molntjänster samt om vilken information som hen bedömt

som öppen eller inte. En annan beskriver att hens arbetssätt när de kommer till informationssäkerhet granskats som en del av den säkerhetsintervju som hen genomfört vid arbete vid en sekretessbelagd anläggning. Slutligen beskriver en respondent att hen som en del av sin SOS-planering behövt besvara motfrågor gällande informationssäkerhet.

5.3 Resultat av intervjuer

I följande delavsnitt presenteras resultatet av intervjuerna. Avsnittet har delats upp i tre huvudsakliga tematiska delar. Den första behandlar vilka krav som Trafikverket ställer inom projektet, den andra hur krav kommuniceras inom projektorganisationen, och den tredje hur kvalitetsprocessen ser ut när det kommer till uppfyllandet av krav.

5.3.1 Krav från Trafikverket

Kravsamordnaren i projektet (K) beskriver att mängden av krav inom olika TDOK- och TRVINFRA dokument medför att få inom projektet har en fullständig bild över alla krav som ställs av Trafikverket, och att det även har tillkommit krav som ej var del av den ursprungliga kravmassan under projektets gång. Även den teknikansvarige (TA) som intervjuats lyfter liknande tankar, som beskriver att hen även finner att många av de krav som ställs inom projektets kravpaket är väldigt luddigt formulerade, och menar på att de händer att hen väljer att acceptera krav från Trafikverket trots att de inte är glasklart vad kravet faktiskt innebär. Hen lyfter även att förhållningen till kravpaketet prioriteras ner under perioder då det är mycket att göra, men menar också på att detta brukar leda till att kravsamordnaren (K) i projektet lyfter detta och ser till att de verksamma inom projektet gör som de ska, något som (TA) lyfter som mycket positivt.

Projektets datasamordnare (DSF) beskriver att enligt hens erfarenhet varierar kraven på digital hantering från Trafikverket rätt mycket mellan olika projekt. I mindre projekt saknas ibland datasamordnare, medan större projekt, såsom detta, tenderar att ha omfattande krav på digital hantering och därmed även ett behov av datasamordning. I sådana projekt finns ofta en ekvivalent roll hos Trafikverket. Tillsammans med denne brukar (DSF) bearbeta formella krav för att ta fram exempel och mallar som resten av projektorganisationen kan förhålla sig till, något som även gjorts i detta projekt.

Inför intervjun med Trafikverkets projektledare (PLT), förmedlades en önskan om att få fråga om hur informationssäkerhetsfrågor behandlas i deras leverantörsrelation gentemot företaget. Under själva intervjun lyftes dock i stället begreppet av sekretess av (PLT). Vid frågan om vad hen syftade på med begreppet, förklarade hen sin tolkning av begreppet utifrån termen av Security, och pratade mycket om att sekretess i hens värld handlar om att se till att information skyddas från otillåten användning eller tillgång, vilket sammanfaller med den tolkning av informationssäkerhet som gjorts i denna studie. (PLT) beskriver att de övergripande kraven på sekretess i projektet i huvudsak regleras av UK:n, även om det också finns mer specificerade krav för exempelvis olika teknikområden inom olika TDOK:ar, något som (PLT) dock erkände att hen inte hade

stenkoll på. Oklarheten i vad som innefattas i begreppet av informationssäkerhet uppmärksammades även i intervjun med (K), eftersom hen uttryckta att hen inte hade kännedom om några uttryckta krav på informationssäkerhet från Trafikverkets sida i projektet. Detta trots att (K) gav intrycket av en övergripande god förståelse av de krav som Trafikverket ställer.

Vikten av en god förståelse för sekretess belyses vidare av de möjliga konsekvenserna för ett kontraktsbrott inom området. (PLT) beskriver att konsekvenserna för denna typ av kontraktsbrott kan variera, där ett alternativ är en hävning av kontraktet. Detta är dock ovanligt och skulle kräva att omfattningen av incidenten är mycket stor. (PLT) beskriver också att hen inte kände till några viten kopplade direkt till denna typ av kontraktsbrott. Hen spekulerar att olika mindre omfattande planer finns, exempelvis i form av en ökning av antalet revisioner och krav på handlingsplaner hos företaget.

Vidare, beskriver (PLT) även att det är Trafikverkets direkta underleverantör som ansvarar för fortplantningen av krav till möjliga underleverantörer inom projekt. Som regel ställs samma krav på företagets underleverantörer som på själva företaget i projektet.

5.3.2 Kommunikationen av krav inom projektorganisationen

Trafikverkets projektledare (PLT) beskriver att vid kommunikation av krav finns en problematik i hur dessa krav presenteras. I projekt där beställaren (Trafikverket) använder sig av olika styrande dokument för att formulera den lista med krav som leverantören ska förhålla sig till, behöver Trafikverket förhålla sig till att ett antal av dessa kravdokument endast är internt tillgängliga på Trafikverket på grund av sin sekretessklassning. Detta innebär att beroende på vilken klassning dokumentationen har, så får de inte ges ut i sin helhet till leverantörer. Detta innebär att (PLT) själv behövt göra sekretessbedömningar av vissa dokument och på egen hand maskera innehåll ur dessa dokument som hen bedömt att leverantören inte är av behov av. Denna process var något som hen gav intryck av att hen inte var helt bekväm med. (PLT) lyfte dock även att det finns tillgång till säkerhetsspecialister inom Trafikverket när frågor som är bortom projektledningens kompetens dyker upp. Denna expertis tillfrågade (PLT) innan intervjun för att säkerställa att (PLT) kunde prata om projektet. Denna kompetens spelar även roll innan anbuds skeendet, och hjälper till att göra bedömningen över vilken nivå av sekretess som är nödvändig inom ett projekt.

De maskerade dokument som (PLT) nämnde, laddar hen sen upp på en låst yta på ProjectWise, där endast ett begränsat urval från leverantören har tillgång till materialet. (PLT) lyfte också under intervjun problematiken med att Trafikverket vet att många av dessa sekretessbelagda dokument finns sparade lokalt hos många av Trafikverkets leverantörer, något som skapar en potentiell säkerhetsrisk ifall dessa dokument skulle hamna i fel händer. Detta är något som (PLT) belyser att Trafikverket behöver förhålla sig till när de lämnar ut informationsdokument.

Denna farhåga bekräftades vid intervjun med (TA), som beskriver att hen i vissa fall behövt förmedla TRVINFRA-dokument till sina indiska projektörer, dokument vars konfidentalitetsklass medför att hen var osäker om detta var förenligt med projektörernas behörighetsnivå. Hen lyfter att trots att dokumenten inte innehåller något projektspecifikt innehåll eller innehåll som hen bedömer hade kunnat missbrukas, så är hen tveksam till vad korrekt procedur är i frågan. (PLT):s anmärkning om att dokument sparas av Trafikverkets leverantörer bevisades ytterligare i och med att TDOK 2018:0623 ”Hantering av information utifrån konfidentialitet” återfanns sparat på företagets Sharepoint under dokumentgranskningen.

När de kommer till dem mer övergripande kommunikationen inom projektet, beskriver kravsamordnaren (K), att hens kommunikation med Trafikverket skett genom löpande diskussioner mellan hen, företagets teknikstöd och med motsvarande ansvarsområden på Trafikverket. Ur ett företagets perspektiv har dessa diskussioner tjänat syftet att nå en samsyn kring kraven i AKJ, “acceptera” i företagets kravhanteringsprocess, och har bland annat innefattat att avsteg och ändringar gjorts gentemot vissa krav, “ändringshantering” i kravhanteringsprocessen. (K) beskriver att processen från början innefattade att en bulk av krav slängdes in från början, för att sedan över tid bearbetas och kokas ner till de krav som är relevanta för företaget och projektet.

(TA) i sin tur beskriver att hen hittills i huvudsak kommunicerat med uppdragsledningen i projektet, men att mer av hens fokus kommer att hamna på den egna tekniken i och med att projektet börjat röra sig djupare in i projekteringsfasen av projektet. I och med att projektet innebär mycket arbete gentemot indiska resurser belyser (TA) vikten av uppföljningar och samtal. Bland annat eftersom det finns en språklig barriär. (TA) menar att trots att båda parter talar engelska på en liknande nivå så kan missförstånd fortfarande uppstå. (TA) lyfter även att de existerar kulturella skillnader, och belyser att de indiska resurserna tenderar att förhålla sig till en starkare hierarki samt att de även tenderar att ha de svårare att säga till när de är något som de inte förstår. Hen beskriver att dessa resurser är rätt nya, och att de därför får arbeta med saker som nyare projektörer får arbeta med. Hen lyfter dock att de tenderar att ta längre tid för dessa resurser att “ta sig vidare till nästa steg” på grund av de tidigare nämnda kulturella och språkliga barriärerna. (TA) säger sig trots barriärerna ha bra insyn i dessa resurser arbete och vad de håller på med. Även (DSF) belyser att språkbarriären gentemot de indiska resurserna medför vissa risker när de kommer till översättningar, men säger även att hen i det stora hela inte uppfattar några större skillnader inom sitt teknikområde vid arbete gentemot dessa resurser kontra de svenska.

(DSF) lyfter dock en annan möjlig kommunikationsproblematik, och beskriver att det finns en problematik med att det är Trafikverket som bestämmer och är kravställare, men att det är företaget som besitter den egentliga expertisen över vad som behövs i projektet. Bland annat beskriver (DSF) en problematik med att Trafikverket har en dålig insyn i vilken tidsinvestering som vissa förändringar som de ber om kommer att kräva. Hen lyfter att en så enkel sak som att byta namn på filer kan innebära många timmars

arbete, då ett byte av ett filnamn även kommer att kräva att alla andra filer som refererar till originalfilen uppdateras. Ett annat exempel är att Trafikverket inte heller har en förståelse över vilka handlingar som behövs som underlag till andra handlingar. Eftersom projektet följer en något annorlunda leveransstruktur än den som återfinns i andra projekt, görs mindre leveranser vid satta skeden. Trafikverket kan då begära material i en leverans som är beroende av underlag som inte ska levereras förrän mycket senare. Trafikverket kan även be om material, som exempelvis underlag till bygghandlingen, i ett tidigt skede, även om materialet då kommer att behöva förändras ett stort antal gånger i framtida leveranser, något som skapar en massa extrajobb och arbete med att säkerställa dokumentversioner.

(DSF) lyfter även att projektet har en rätt utmanande tidsplan, och att samspelet gentemot Trafikverket därav blir av ytterligare vikt. (DSF) lyfter dock även att hen finner att samarbetet med Trafikverket ändå fungerar väl i detta projekt. Även (PLF) belyser den snäva tidsplan som den största utmaningen inom projektet. Vid frågan om (PLF):s upplevelse av hur projektet går, beskriver hen att företaget levererat allt det ska inom projektet, men att även företaget och Trafikverket inte alltid är överens kring dessa leveranser. (PLF) belyste området som komplext, och ville inte gräva djupare i frågan.

(K) beskriver även en annan kommunikationsväg inom projektet som nyttjas av ett flertal olika roller inom projektorganisationen är Fråga/Svar, som är en rutin för att möjliggöra att olika frågeställare från företaget på ett enkelt sätt ska kunna formulera frågor till Trafikverket, exempelvis i syfte att klargöra någon teknikområdesrelaterad fråga. Rutinen används även för avsteg och omformuleringar kring krav funna i TDOK- och TRVINFRA dokument. Fråga/Svar innebär att frågor formuleras på en form som Trafikverket kan svara på med antingen Ja eller Nej. Aspekter såsom svaret, vem som tillfrågats och vem som ställde frågan dokumenteras. Kommunikation sker även genom underrättelser (UR), ett samlingsbegrepp för uppgifter och dialoger förda över exempelvis mail.

(PLF) i sin tur beskriver att majoritetens av hens kommunikation skett inom uppdragsledningen, gentemot uppdragsingenjören, de olika tekniksamordrarna samt sin biträdande uppdragsledare. (PLF) beskriver att projekts specifika utmaningar, lägesrapporter, projektets ekonomi och tidsplan samt andra detaljfrågor diskuteras vid behov tillsammans med Trafikverket under regelbundna veckomässiga möten. Under dessa möten lyfts även de tidigare nämnda relevanta underrättelser och Fråga/Svar.

5.3.3 Insyn och kravuppföljning

När det kommer till kravuppföljning från Trafikverkets sida beskriver (K) att företaget endast följs upp eller granskas på ett mindre urval av alla krav som ställs inom projektet på något sätt, något som (K) delvis tilldelar till att Trafikverket har en stor mängd tilltro till företaget. Bland annat följs företaget i viss utsträckning upp på att de använder sig av korrekta versioner av olika styrande dokument, samt AKJ-krav, då dessa krav ”ägs” internt av olika avdelningar inom Trafikverket och den del av Trafikverket som är

beställare av projektet då behöver söka dispens gentemot kravägaren vid avsteg från dessa.

TDOK 2011:175 ”Informationssäkerhet i Trafikverket”, som är en del av Trafikverkets ledningssystem och som bland annat beskriver hur informationssäkerhetsarbete ska bedrivas inom myndigheten, uttrycker att det är den del av Trafikverket som har den verksamhetsmässiga relationen till respektive extern part som har det yttersta ansvaret för att avtalsmässiga förbindelser, i kontexten av informationssäkerhet uppföljs. (PLT) beskriver dock att Trafikverkets arbete med att säkerställa att deras leverantörer uppfyller de krav på informationssäkerhet som ställs, som svårt. (PLT) beskriver att Trafikverket kan göra kvalitetsrevisioner med olika inriktning, exempelvis för att undersöka hur leverantören arbetar med frågor inom kvalitet, fysisk säkerhet eller sekretess. När det kommer till informationssäkerhetsfrågan beskriver (PLT) området som omoget hos Trafikverket. Det saknas tydliga direktiv från ovan i hur insyn och arbete i informationssäkerhetsfrågor ska genomföras av Trafikverket inom sina leverantörsrelationer. I andra frågor, såsom på hur Trafikverket ska genomföra bedömningar kring leverantörers arbete inom jämställdhetsfrågor, finns rutiner och planer för hur revisioner ska utföras och hur förbättringsarbeten kan struktureras, och (PLT) spekulerar att en liknande process hade kunnat användas inom området av informationssäkerhet.

Ett tydligt krav från Trafikverkets sida är att material bearbetas på rätt arbetsyta. (DSF) beskriver att det är svårt att se till att folk arbetar exempelvis i korrekta arbetsytor, att kopior förvaras på ett korrekt sätt, och att det är en aspekt som “ryker” när hen har mycket att göra. Hen beskriver i stället strategin som hen tillämpar är att det ska vara enkelt att göra rätt. Exempelvis förväntar sig Trafikverket att de handlingar som levereras till dem är standardiserade utifrån de krav som ställs. I stället för att låta projektörerna och andra verksamma inom projektet följa någon instruktion och hämta en tom mall, så har hen valt att skapa mallar där alla de standardiserade attributer redan är fixade, och att de som är verksamma inom projektet i stället bara behöver fokusera på innehållet i olika dokument som de skapar.

När det kommer till den indiska kompetensen inom företagets verksamhet, beskriver (TA) att den kvalitetssäkrande processen gentemot dessa resurser ser likadan ut som för andra projektörer. En skillnad är att hen genomför fler uppföljningar för att säkerställa att arbetet fortgår på korrekt sätt, samt att hen ibland behövt genomföra en del av den kvalitetssäkringsprocess som krävs inom teknikområdet som kallas egenkontroll, åt dessa resurser, delvis för att det saknats underlag på engelska för dessa projektörer att använda. (TA) beskriver också att hen i andra projekt behövt ta fram mallar för att ge dessa projektörer underlag att kunna utföra arbetet på korrekt sätt. (TA) lyfter att hen är kritisk till att företaget inte har mallar och protokoll på engelska, bland annat för att det kräver en massa tid ute i projekten och att det lägger ytterligare ansvar på de ute i projekten, inom ett område som företaget borde sköta på högre nivå.

Denna avsaknad av underlag lyftes även under intervjun med (PLF). På frågan om hur det faktum att mycket av projektdokumentationen endast finns på svenska påverkar kommunikationsmöjligheterna gentemot den indiska kompetensen, beskriver hen att vissa delar av projektets dokumentation finns översatta på projektets Sharepoint-yta, men att det också finns en förväntning om att dessa resurser ska kunna använda Google Translate vid behov. Någon tydlig avgränsning på vilken del av projektdokumentationen som är översatt finns inte, och (PLF) beskriver inte heller att det finns några tydliga direktiv från företagets sida i frågan gällande vilket material som ska finnas översatt.

Även (DSF) lyfter en viss problematik med att handlingar, såsom bygghandlingar, är skrivna på svenska, eftersom detta är problematiskt för de indiska resurserna i projektet. Hen lyfter att som en del av lösningen så väljer många teknikområden att använda de svenska orden för att beskriva olika begrepp, även i kontakt med ej svensktalande. Detta då hen menar på att om det finns en risk med att man syftar på olika saker om man försöker hitta en egen översättning av olika tekniska begrepp, och att de fungerar bättre att projektörerna får lära sig de svenska orden. (DSF) beskriver att lösningar får hittas från fall till fall, och att desto mer man jobbar ihop med dessa resurser, desto lättare blir det.

5.3.4 Sammanfattning av intervjuer

Trafikverket ställer ett stort antal krav inom projektet, vilket medför svårigheter för medlemmarna i företagets projektorganisation att få en tydlig överblick. Under perioder av stress och hög arbetsbelastning tenderar även förhållningen till kravpaketet att prioriteras ner. Från Trafikverkets sida följs få av dessa krav upp på, och då främst de tekniska kraven. Dessa krav hanteras genom en granskningsprocess, som medför stora möjligheter till att påvisa kravuppfyllnad. Mjukare processkrav, hanteras som regel genom mindre formella processer.

Hos Trafikverket upplevs området av informationssäkerhet som omoget. Bland annat saknas tydliga instruktioner för hur granskningar av leverantörers informationssäkerhetsarbete ska gå till, vilket medför att inga granskningar genomförs inom projektet.

Inom projektet finns en avsaknad av underlag för den indiska kompetensen. Endast et litet urval av kravdokumentationen finns översatt, och de finns inga tydliga instruktioner från företaget kring vilket material som ska finnas översatt.

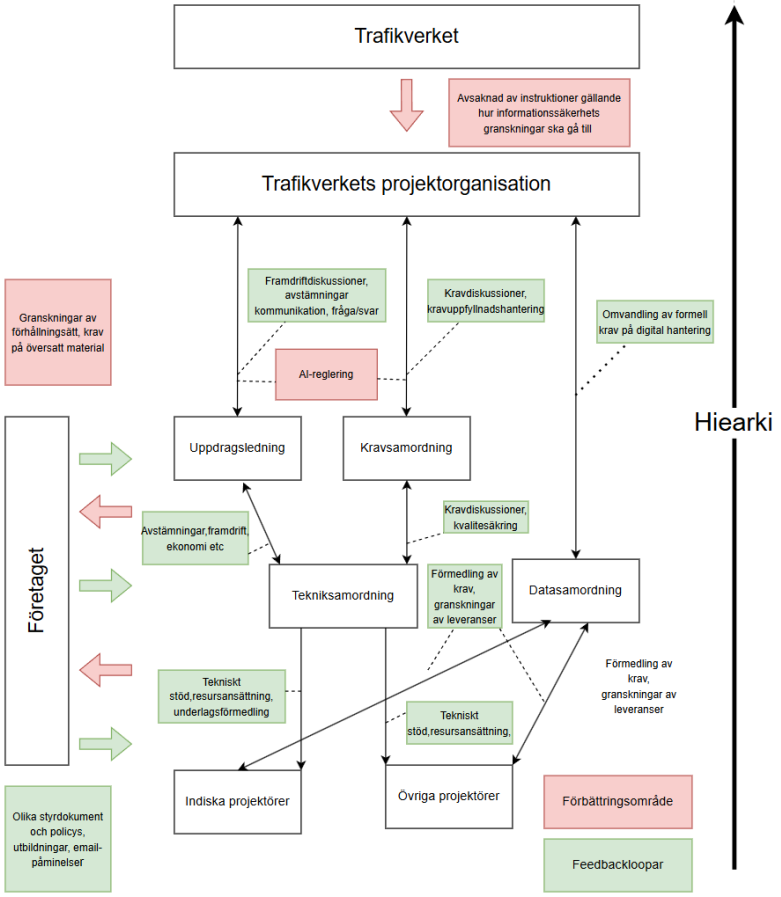
Relationen mellan Trafikverket och företaget upplevs överlag som bra, men viss friktion finns. Bland annat upplevs Trafikverket som oförstående när det kommer till vad deras krav och förändringar kommer att medföra för arbete inom projektet.

6. Analys

Inom följande avsnitt kommer studiens resultat att analyseras. Avsnittet är disponerats som följande. Först presenteras modelleringen av kontrollstrukturen tillsammans med gjorda antaganden. Därefter analyseras kontrollooparna inom kontrollstrukturen.

6.1 STPA - Modellering av kontrollstruktur

På grund av komplexiteten av kommunikation inom projektorganisationen, görs i denna analys en simplifierad ansats för att på ett tydligare sätt illustrera hur banden mellan olika intressenter formar förutsättningarna för informationssäkerhet, genom att illustrera mellan vilka komponenter som osäkra kontrollåtgärder genomförs. Vidare modelleras olika funktioner i stället för ”personer”, för att lyfta frågan om ansvar bortom personnivå för att ytterligare lyfta de systemperspektiv som STAMP belyser som av vikt. Dessutom, eftersom graden av insyn i hur samverkan mellan Trafikverkets styrande funktioner och Trafikverkets projektorganisation är begränsad och ingen insyn i graden av feedback mellan entiterna uppmärksammats, har detta utelämnats ur analysen.



Figur 8: Översiktlig modell av kontrollstruktur

Inom projektorganisationen, som illustreras genom kontrollstrukturen i figur 8, finns ett antal intressenter vars arbete påverkar projektets informationssäkerhet på grund av sin roll, antingen genom förmedlandet av krav till andra inom projektorganisationen och/eller genom sitt förhållningsätt till dessa krav. Baserat på insamlade data, har åtta olika huvudsakliga funktioner identifierats i denna kontext. Dessa är: Trafikverket, Trafikverkets projektorganisation, företaget, uppdragsledning, kravsamordning, tekniksamordning, datasamordning, den svenska projekteringen och slutligen den indiska projekteringen.

Ur ett hierarkiperspektiv existerar en styrande funktion från Trafikverkets sida bortom själva projektorganisationen. Även om en direkt inblick i detta saknas belystes dennes existens under intervjun med (PLT). Bland annat tilldelas denna funktion framtagandet av olika styrande dokument, i form av exempelvis TDOK:ar och annat underlag som Trafikverkets projektorganisation har att förhålla sig till.

Trafikverkets projektorganisation verkar i sin tur direkt i projektet och utför styrande kontrollåtgärder gentemot olika aktörer inom projektet. Utbyten gällande olika projektspecifika områden sköts genom olika möten med olika funktioner inom företagets projektorganisation. Teoretisk feedback inkommer till entiten genom granskning av kravuppfyllnadsdokumentation och handlingar från företagets projektorganisations sida.

Uppdragsledningen insamlar feedback från projektorganisationen genom olika avstämningar gällande projektets framgång, ekonomi och liknande frågor och framför och diskuterar dessa områden kontinuerligt med Trafikverkets motsvarigheter. Kravsamordning insamlar feedback från olika tekniker genom avstämmande med olika teknikområden, och diskuterar krav gentemot Trafikverket. Funktionen utför kontrollåtgärder gentemot de olika verksamma inom projektet för att säkerställa att de förhåller sig till de formella krav som återfinns inom exempelvis kravpaketet. Funktionen av datasamordning i sin tur utför kontrollåtgärder gentemot resten av projektorganisationen genom att omvandla krav på digital hantering tillsammans med sin respektive part hos Trafikverket, och framför dessa krav till resten av projektorganisationen. Förhållningen till dessa krav säkerställs genom granskningar av olika handlingar innan leverans. De teknikansvariga funktionerna ansvarar för resursanssättning i projektet inom respektive teknikområde, bestämmer uppgifter samt framtar underlag i vissa frågor. Funktionen intar feedback genom att granska tekniska lösningar och projektets framfart genom bland annat olika samtal med sina projektörer. De slutgiltiga stegen i hierarkin består av projektörerna, både svenska och kompetensen från de utländska resursstödsenheterna, som utför arbetsuppgifter baserat på de kontrollåtgärder som förmedlats till dem.

Utöver de som är direkt verksamma i företagets del av projektorganisationen, verkar även företaget som mer övergripande kontrollerande entitet på företagets verksamhet i kontexten av informationssäkerhet. Detta genom att utföra kontrollåtgärder i form av olika policyer, styrdokument, utbildningar och påminnelser via mail. Företaget

beskriver sig även besitta en granskningsprocess för att säkerställa att åtgärder är verksamma i verksamheten. Därtill kan även de åtgärder och krav som företagets ledningssystem innebära sammanställas i dessa kontrollåtgärder.

6.1.1 Identifierade osäkra kontrollåtgärder och avsaknad av feedback

En central insikt som identifieras under informationsinsamlingen är att den omfattande och komplexa kravmassan i projektet skapar utmaningar för kontroll och att möjligheten till en överblick av kravuppfyllnad. Detta är ett mer markant märkbart problem i kontexten av uppfyllanden av mjukare processkrav kontra mer konkreta produktkrav, eftersom den tekniska kravhanteringsprocessen inom företagets verksamhet upplevs som mer mogen än hanteringen av de mjukare processkraven. Detta märks särskilt tydligt då den tekniska kravhanteringsprocessen är präglad av en strukturerad granskningsprocess för handlingar, samt att AKJ-kraven har en tydlig systematisk process kopplad till sig. Detta kontra att de mjukare processkraven som återfinns inom exempelvis TDOK:ar sköts via kommunikationsmedier så som av Fråga/Svar, vilket kan medföra att den kontext som kraven hanteras inom innebär att större individuellt ansvar för att säkerställa kraven uppfylls, något som kan medföra en ökning i variation och implementering.

Trafikverkets projektstyrning använder i huvudsak olika styrande dokument som kontrollåtgärd gentemot de som är verksamma inom projektet. Ett flertal av de intervjuade belyste dock olika möjliga problem med användandet av Trafikverkets styrande dokument som ett sätt att förmedla krav. Den problematik som (TA) beskriver i att hen ibland väljer att acceptera krav, även om det inte är självklart vad det faktiska kravet innebär, är ett exempel. Ett annat är de faktum att volymen av dokumentation medför att denne blir svårhanterlig, något som uppmärksammas i form av att (K) lyfter att antagligen ingen har fullständig koll på alla krav som ställs.

Vidare, förefaller användningen av styrande dokument som styrmedel inom informationssäkerhetsfrågor besitta ytterligare brister, eftersom de framstår som att delar av den dokumentation som regler informationssäkerhet i projektet kan ses som bristfällig, något som lyfter farhågan om att de existerar vissa brister i Trafikverkets överblick och kontroll över innehåll i dessa styrande dokument. Detta ger upphov till en osäkerhet om dessa dokuments förmåga att agera som kontrollåtgärd inom området. Ett tydligt exempel är att TDOK 2011:175 ”Informationssäkerhet i Trafikverket” inte återfinns i kravpaketet, medan äldre ”slopade” bilagor till detta dokument gör det. Utöver detta kvarstår även hänvisningar till föråldrade dokument inom ett antal av de TDOK:ar som granskats, vilket indikerar en bristande dokumentuppdatering hos Trafikverket.

Enligt enkätundersökningen finner många av respondenterna att de krav som ställs av företaget på de som är verksamma inom projekt som tydliga, eller åtminstone delvis, detta till skillnad från upplevelsen av vilka krav på informationssäkerhet som Trafikverket ställer. En möjlig anledning till detta är att det krav som företaget ställer är

tydlig formulerad och samlad inom de olika policys som medarbetarna inom företaget förväntas förhålla sig till, medan de krav som Trafikverket ställer inom området är utspritt och återfinns i stor omfattning endast som mindre delar av större, mer omfattande dokument. Kraven inom dessa dokument är vidare oftast ställda på formen av ”ska”, vilket medför att det är upp till individen att göra bedömningen om hur detta ska genomföras i det egna arbetet. I kontexten av en förståelse av Trafikverkets informationssäkerhetskrav, är de beskrivningar som återfinns inom företagets olika informationssäkerhetspolicys behjälpligt.

Den höga frekvensen av svaret ”Vet ej” på frågan om Trafikverket ställer krav på informationssäkerhet inom projektet antyder att de krav som ställs inte är tydligt kommunicerade, inte ens till de som är svensktalande inom projektet. Detta kan dock även ha med att många inom projektet endast spenderar en mindre del av sin arbetstid inom projektet, vilket kan medföra en svårighet för medarbetarna att hinna med att ta till sig innehåll. Detta resonemang stärks av en av de kommentarerna som återfanns inom enkäten, i form av att en respondent rapportera att hen spenderar lite tid i projektet, och därför inte har koll på kravpaketet. Även om detta inte undersökts, är det sannolikhet att andra av Trafikverkets projekt innehar en likande omfattande mängd krav. Att krav på informationssäkerhet då arbetas in i generella kravdokument blir problematiskt, eftersom de ställer stora krav på att de som är verksamma inom Trafikverkets projekt att läsa sig in i och förstå diffust formulerade kravdokument. I linje med Dick et al. (2017) belysning av vikten av tydligt kommunicerade kravställningar, bör detta tillvägagångsätt övervägas.

Ytterligare en aspekt som upptäcktes under dokumentationsgranskningen var en avsaknad av explicita krav kring användningen av AI inom kontrakts-och kravdokumentationen. Även om generella informationssäkerhetskrav kan antas täcka in användningen av AI, kan avsaknaden av specifika riktlinjer medföra en användning av AI som ej uppfyller dessa krav. Här återfinns ett behov av kontrollåtgärd från Trafikverkets sida, bland annat eftersom företagets styrdokumentation uttryckligen överlämnar ansvaret för att reglera detta till respektive kund.

En annan insikt som uppmärksammats under datainsamlingen är att det finns en övergripande avsaknad av feedback inom olika nivåer av projektorganisationen. Inom kontraktsdokumentation beskriver Trafikverket att de har rätt att genomföra granskningar av både företaget och dess underleverantörer när det kommer till informationssäkerhet. Trots denna möjlighet, beskriver (PLT) att detta inte genomförs, och hänvisar till att området av informationssäkerhet är omoget hos Trafikverket, och att detta medför att det saknas tydliga direktiv i hur denna typ av granskning kan genomföras. En avsaknad av rutiner verkar dock inte vara hela sanningen, eftersom (K) även belyser att Trafikverket som regel genomför väldigt begränsad tillsyn av kravuppfyllnad inom projektet. Det är tydligt att området av informationsskydd är viktigt för Trafikverket i och med det omfattande konsekvenser som (PLT) beskriver att

ett kontraktsbrott inom området hade kunnat innebära. Avsaknaden av denna feedback lämnar dock fråga om hur Trafikverket skulle få reda på ett sådant kontraktsbrott.

Inom företaget finns en liknande problematik, något som bland annat enkätsvaren visar på i och med att ytterst få, om någon, upplevt att deras förhållningsätt till informationssäkerhet granskats inom projektet. Detta speglas även i respondenternas övergripande upplevelse av granskning inom området av informationssäkerhet, då endast 40% av de insamlade svaren beskriver att de upplevt någon typ av granskning inom området, vilket implicerar en övergripande avsaknad av strukturerad informationssäkerhets granskning inom företagets verksamhet.

Denna avsaknad av feedback inom olika delar projektorganisationen medför att möjligheterna till uppdatering av respektive processmodell försämras, vilket medför att det skapas utrymme för osäkra kontrollåtgärder. Utöver denna avsaknad av feedback inom projektorganisationen, medför även den problematik som (DSF) lyfter i form av att det är Trafikverket som är kravställare inom projektet, men att det är företaget som besitter expertisen, vissa svårigheter. Detta visas bland annat i att Trafikverket inte verkar helt medvetna om vad de krav som de ställer kommer att ha för konsekvenser för som arbetar ute i projektet. Detta är av vikt, eftersom både (DSF) och (TA) lyfter att förhållningen till de krav som finns prioriteras ner under perioder av stress. Denna beskrivning är i linje med agentteorins resonemang om hur informationsasymmetrin mellan en beställare och utförare kan medföra en obalans i kunskap. Denna obalans riskerar att leda till oavsiktliga konsekvenser, inklusive att viktiga krav förbises till följd av otillräckligt förankrade beslut.

Vidare, beskriver (PLT) att ansvaret för att krav förmedlas vidare till underleverantörer finns hos företaget, vilket även kontraktsdokumentationen styrker. Det blir därmed av vikt att relevanta delar av företagets kontrollers i projektet ges goda förutsättningar för att ge resten av de som är verksamma inom projektorganisationen korrekt kontrollåtgärder. I kontexten av detta är företagets förhållningsätt gentemot de indiska resurserna under kritik. Dessa resurser förväntas att förhålla sig till samma krav som resterande av de som är verksamma inom projektet, men ges sämre förutsättningar för detta, som en konsekvens av att kravdokumentationen i viss utsträckning ej finns tillgänglig för dem. Här saknas tydliga en förmedling från företagets sida kring vilken dokumentation som bör finnas översatt. Att exempelvis (TA) behövt översätta och förmedla dokument till dessa resurser är problematiskt. (TA):s påpekande att dessa resurser utöver detta tenderar att ha det svårare att förmedla när de inte förstår någonting är även de problematiskt, eftersom det riskerar att medföra att misstag förminskas. Vikten av korrekt underlag blir i denna kontext av ytterligare vikt.

Ur ett STAMP perspektiv går det även att argumentera för att arbetet med informationssäkerhet inom företagets projektorganisation exemplifierar begreppet av boundrary area. Bortom kortare uttryck i rollbeskrivningar, saknas de inom de dokumentationsmaterial som genomgåtts i denna studie, en explicit beskrivning över vem som ansvara för att säkerställa arbetet med informationssäkerhet ute i projektet.

7. Diskussion

I följande avsnitt kommer de analytiska slutsatser som dragits att diskuteras. Därefter presenteras en metoddiskussion, som inkluderar en diskussion av STAMP som val av teoretiskt ramverk, den genomförda informationsinsamlingen samt den begreppsdefinition som gjorts av ”informationssäkerhet”.

7.1 Är åtgärderna tillräckliga?

Huruvida om de krav på förhållningsätt som NIS 2 kommer att ställa uppfylls av Trafikverket och företaget inom området av informationssäkerhet inom respektive leverantörsrelation går att diskutera, delvis på grund av det råder en stor oklarhet i vilka krav som verksamhetsutövare faktiskt förväntas att behöva uppfylla. Därtill är det inte heller en självklarhet om de tjänster som företaget förmedlar inom transportsektorn medför en skyldighet att förhålla sig till de krav som ställs av NIS 2. Trafikverket kan däremot uttryckligen antas inneha denna skyldighet, delvis på grund av sin uttryckta samhällsviktiga roll och den målsättning med en övergripande god cybersäkerhet inom hela EU, som direktivet innehar.

Utifrån de nuvarande kända kraven, så kommer Trafikverket att behöva aktivt arbeta med sin säkerhet i leverantörskedjan. Detta resonemang härstammar från att Trafikverket i dagsläget inte genomför tillräcklig tillsyn inom sina leverantörsrelationer, samt att sättet som krav förmedlas på är bristfälligt. Även om Trafikverket både ställer krav och inkluderar rätten att granska företagets förhållningsätt till informationssäkerhet, vilket är i linje med exempelvis ISO 27001, medför en avsaknad av feedback mellan Trafikverket och företagets projektorganisation att Trafikverket har en begränsad förmåga att garantera att dessa krav uppfylls inom företagets projektverksamhet. Denna avsaknad belyses orsakas av otillräckliga förutsättningar för att inom projektet att inhämta tillräcklig feedback, vilket framstår härstamma från en grad av omogenhet inom frågan hos Trafikverket.

Ur ett företagsperspektiv går det även att diskutera huruvida om användandet av resursstödsenheter kan räknas som en leverantör enligt NIS 2, eller om dessa kan argumenteras för att vara en direkt del av företagets verksamhet. Det är dock fördelaktigt ur ett framtidsäkrande perspektiv att anta detta. Företaget ger i denna kontext intrycket av att inneha en liknande problematik som denne funnen hos Trafikverket, i form av att en avsaknad av feedback när de kommer till kravuppfyllnad inom informationssäkerhetsrelaterade krav. En stor skillnad mellan företaget och Trafikverket är dock företagets pågående certifiering mot standarden ISO 27001. I linje med expertutlåtandet av Jan-Olof Andersson under MSB Cybersäkerhetskonferens, så bör denna certifieringsprocess medföra att detta utvecklingsområde hanteras som en naturlig del av företagets fortsatta arbete med att utveckla sitt ledningssystem.

7.2 Metoddiskussion

I följande delavsnitt kommer STAMP, den metod som använts för informationsinsamling som använts i studien samt den övergripande valda studie-ansatsen att diskuteras.

7.2.1 Är STAMP ett bra val för denna typ av analys?

En av STAMP:s stora styrkor är den systemsyn som ansatsen innebär, eftersom detta medför att ansvar för felaktigt beteende ej placeras på de enskilda komponenterna, dvs individerna i denna studie, utan i stället ses som en konsekvens av en komponents interaktion med resterande av systemet. Detta medför en möjlighet att analysera den studerade projektorganisationen ur ett holistiskt perspektiv, där insatser kan riktas mot organisatoriska egenskaper i syfte att stärka säkerheten i organisationen som helhet. Som Salmon et al. (2012) belyser, medför dock STAMPS kontroll- och systemteoretiska bakgrund att begreppsapparaten inte är helt självklar för att illustrera den typ av ”fel” som analysen i denna studie påpekar. Därtill kräver även ansatsen omfattande underlag för att kunna spegla den typ av organisation som studerats i denna studie, och ställer då stora krav på en omfångsrik datainsamling.

Även systemperspektivet och den abstraktion av verkligheten som detta innebär, kan medför en viss problematik. Den övergripande illustration som gjorts av projektorganisationen implicerar, till viss del, att det enskilda människorna agerar på ett liknande sätt. En mer nyanserad blick hade medfört en mer explicit belysning av att varje enskild komponents har en egen kontrollalgoritm, som formas av aspekter bortom det system som studerats. En person med en IT-bakgrund kan komma att ha ett annat förhållningsätt till de krav på informationssäkerhet som ges i projektet, även om den i projekt-kontexten innehar samma förutsättningar som en annan person utan denna bakgrund. Ett förbiseende av de informella strukturer som formar de förutsättningar som individer tar beslut inom riskerar att medföra att felaktigt riskhanteringsåtgärder, vilket påvisar värdet i ett MTO-perspektiv vid analys av områden där människa, teknik och organisation samspelar.

STAMP fångar därtill inte på ett explicit sätt hur stort värdet av säkerhet som det olika komponenterna innehar, eftersom kontrollalgoritmen hos vardera entitet förblir abstrakt. Det går att argumentera att under olika tidpunkter i projektet har säkerhet olika mycket betydelse eller värde för de två intressenterna av Trafikverket och företaget, någonting som även om det inte undersökts närmare i denna studie, kan påverka förhållningsättet hos de olika verksamma komponenterna. Detta kan dock till viss del ses i företagets förhållningsätt i användandet av indiska resurser. Dessa lyfts till stor del in på grund av det marknadsmässiga fördelar som användandet av dessa innebär, samtidigt som Trafikverket inte tillåter dessa resurser, på grund av säkerhetsrisker, att få tillgång till alla av Trafikverkets system.

STAMP belyser inte heller att olika komponenter i ett system kan ha skillnader i mål, kompetens och den asymmetri i information som existera inom projektet. Detta är något som bland annat kan exemplifieras genom (PLT):s belysning av att frågan av informationssäkerhet är omogen hos Trafikverket, samtidigt som företagets pågående certifieringsprocess gentemot ISO 27001, och det arbete som gjorts för att inkorporera detta i företagets olika policy-dokument, implicerar en högre grad av förståelse av vikten av informationssäkerhet hos företaget i jämförelse med Trafikverket. Detta, samt att Trafikverket ger intrycket av att ha en viss oförståelse över vilket arbete som deras krav kan medför för företaget, belyser att en agentteoretisk utgångspunkt kan vara behjälplig för att förklara de omständigheter som olika kontrollåtgärder görs inom i kontrollhierarkin. Däremot bör man ha i åtanke att agentteori kan implicera en reducering av det mänskliga beteende till en typ av rationell egenintresse-optimering (Shapiro, 2005) och man bör ha i åtanke att det existerar ett samspel mellan företaget och Trafikverket som sträcker sig bortom detta enskilda projekt.

När de kommer till det analytiska verktyget av STPA, uppfattade författaren även en oklarhet i den roll som processmodell och kontroll algoritm har i termer av analytiska steg. Den tolkning som gjorts är att dessa begrepp i huvudsak presenteras inom STPA Handbook som ett sätt att tydligare förmedla analysmetodens koppling till STAMP, och därför saknas dessa explicit i den analys som gjorts.

7.2.2 Begreppsapparat, vad betyder egentligen informationssäkerhet?

En sak som uppenbarat sig vid design av enkäten samt vid intervjuerna är att begreppet av informationssäkerhet och andra liknande begrepp är abstrakt. Ett exempel är den beskrivning av begreppet sekretess som (PLT) lyfte under intervjun. Även om den ”regelrätta” betydelsen av begreppet beskrivs av exempelvis (Svenska Akademin, 2021) som: ” *på-bjudet hemlig-hållande av något; för att skydda person el. organisation*”, så innefattar begreppet ur (PLT):s perspektiv att de även ska utföras arbete för att säkerställa att information inte kommer till fel person, vilket kan liknas med den definition av informationssäkerhet som gjorts i denna studie.

Vidare, även om CIA-triangeln agerar som en återkommande beskrivning av de attribut som upprätthåller informationssäkerhet, saknar denna till viss del fortfarande en tydlig verksamhetsmässig koppling. Exempelvis saknas en tydlig avvägning av hur de tre aspekterna ska vägas mot varandra, något som beror på kontexten kring behovet av informationssäkerhet. Detta kan vara en förklaring till den något bristande förståelsen för begreppet inom projektorganisationen. I kontexten av en förbättrad informationssäkerhet inom projektorganisationen, är en förbättring av förståelsen för begreppet ett område värt att investera inom, eftersom exempelvis Siponen (2000) beskriver att en bristande förståelse för informationssäkerhet medför att informationssäkerhetsriktlinjer riskerar att bli ineffektiva. Siponen föreslår att en ansats för att minska användarfel när de kommer tillförhållningsätt är genom att organisationen systematiskt utvecklar medvetenhetsprogram för informationssäkerhet.

7.2.3 Informationsinsamling

Även om intervjuer genomförts med ett flertal olika individer i projektorganisationen är det dock av värde att ha i åtanke att alla inte alla deltagande i projektets åsikter har fått utrymme i denna studie. Bland annat genomfördes inga intervjuer med deltagare från någon resursstödsenhet och endast ett urval av teknikområden fick komma till tals, vilket innebär att de tolkningar som gjorts i denna studie kommer att ha färgats av vilka som intervjuats. Det finns även en risk att intervjudeltagarna valde att spegla en mer positiv bild av det egna förhållningssättet mot olika rutiner och processer i syfte att framstå som mer kompetenta eller på annat sätt vill påverka bilden av sig själva, något som kallas impression management (Bolino et al., 2016).

Ett annan antagande som gjorts är att de upplevelser rollen som teknikansvarig ser ut på ett liknande sätt för resterande av teknikområdena. Den TA som intervjuat har mycket erfarenhet, både inom rollen som TA, men även inom kontexten av samarbete med utländsk kompetens. En mindre erfaren TA inom en liknande sitts hade kanske betet sig på ett annat sätt i sitt förhållningsätt gentemot dessa resurser. Utöver detta, dök det ibland upp under intervjuerna svar som i efterhand varit svåra att tolka om dessa är projektspecifika eller om de är generella, även om frågan som besvarats ställts ur en projektspecifik utgångspunkt.

Ett annat möjligt förbättringsområde rör den ansats för datainsamling som gjorts inom intervjuerna. Som tidigare diskuterats, gav respondenterna intrycket att begreppet av informationssäkerhet upplevdes som abstrakt, både inom Trafikverket och företagets verksamhet. Under intervjuerna användes delvis därför en mer generell kravuppfyllnad ansats för att samla in information gällande hur ställda krav uppfylls inom projektet. Den tekniska kontext som begreppet tenderar att användas inom i företaget kan ha medfört förvirring för respondenterna, och det finns en möjlighet att respondenterna i huvudsak associerade kravuppfyllnad främst med hur väl tekniska krav uppfylls inom projektet, snarare än inom krav på förhållningsätt.

När de kommer till enkätstudien finns ett flertal möjliga förbättringsområden. På grund av den feedback piloten och uppdragsingenjören i projektet förmedlade, valdes begreppet av informationssäkerhet att förtydligas genom en koppling till företagets informationssäkerhetspolicy. Detta kan ha färgat respondenternas svar på exempelvis frågan: “Upplever du att företaget ställer tydliga krav på hur informationssäkerhet ska skötas inom projekt?”. Detta var en avvägning som gjordes under enkät-designen. Den bedömningen som gjordes var att det var av större vikt att få in information i de projektspecifika frågorna om informationssäkerhet, och att det i detta syfte var viktigt att respondenterna förstod vad som innefattas i begreppet. Trots detta förtydligande inkom enskilda svar där intrycket som gavs var att personen missuppfattat begreppet och blandat ihop de med begrepp som används inom säkerhetsgranskning.

Det går även att diskutera om enkätens svarsfrekvens är tillräcklig för att kunna användas som underlag för några slutsatser. Projektets uppdragsingenjör lyfte att hen

tidigare haft det svårt att få in en svarsfrekvens på mer än 20% i olika enkäter som hen skickat ut, och därför görs bedömningen att svarsfrekvensen är så bra som den kommer att bli. Baruch & Holtom (2008) belyser ”over-surveying” som en anledning till att tillfrågade ej svarar på enkäter, något som delvis kan förklara den någorlunda låga svarsfrekvensen i denna studie eftersom medlemmarna i företagets projektorganisation blir tillfrågade om en mängd enkätsvar.

8. Slutsatser, rekommendationer och framtida möjligheter

I denna studie har ett av Trafikverkets projekt inom järnvägsinfrastruktur analyserats utifrån de två huvudsakliga intressenterna i projektets förhållningsätt till informationssäkerhet inom sina leverantörsrelationer, med hjälp av det teoretiska ramverket STAMP. Detta har gjorts genom att de två forskningsfrågorna:

- I vilken utsträckning uppfyller aktörernas nuvarande förhållningssätt de krav på informationssäkerhet i leverantörskedjan som ställs av NIS 2-direktivet?
- På vilka sätt kan ramverket STAMP utvecklas för att bättre belysa organisatoriska utmaningar?

har behandlats genom att besvara frågeställningar kopplat till krav och kravhantering inom området av informationssäkerhet. Slutsatsen av studien är att området kommer kräva en del arbete av båda intressenter. Trafikverket bör se över sin användning av styrande dokument för att förmedla krav inom området av informationssäkerhet för att säkerställa att innehållet når de delar av projektorganisationen som kraven är riktade mot, samt se över sina rutiner när det kommer till insyn och granskning av sina leverantörers förhållningsätt inom informationssäkerhetsfrågor. Även företaget bör arbeta aktivt med att genomföra granskningar av förhållningsättet till informationssäkerhet inom den egna verksamheten, men även se till att de utländska resurser som lyfts in i projekt får tillgång till de material och underlag som behövs för att kunna agera rätt inom dessa frågor. Användningen av STAMP har belyst att ramverkets begreppsapparat inte är helt bekväm för denna typ av organisatorisk analys, men att systemsynen är ett kraftfullt verktyg för att lyfta olika möjliga problem bortom individnivå, vilket är värdefullt för meningsfull organisatorisk förändring.

8.1 Rekommendationer

Trafikverket

- Bör se över sin användning av styrande dokument för att förmedla krav.
- Krav på hur de som är verksamma inom projektet ska arbeta med informationssäkerhet bör förtydligas.
- Se över rutiner och utveckla en metodik för att genomföra granskningar när de kommer till informationssäkerhet. Ett alternativ är att ta stöd av det verktyg som ISO 27001 belyser inom detta område.
-

Företaget

- Den utbildning och uppmärksamhet som läggs på informationssäkerhet inom verksamheten är bra, men tydligare arbete bör drivas inom granskningsprocessen. Ytterligare arbete inom förståelsen för området av

informationssäkerhet bör också genomföras för att tydligare koppla samman begreppet med det arbete som görs uti inom projekt.

- Förbättra förutsättningarna för de som är verksamma inom projekt att hantera informationssäkerhet på korrekt sätt, genom att säkerställa att det underlag och dokumentation som behövs finns tillgänglig på ett språk som mottagaren förstår.

8.2 Framtida forskningsmöjligheter

Studien har trots sina begränsningar visat på vilka svårigheter som kan finnas när de kommer till förmedlandet och säkerställandet av uppfyllnad av informationssäkerhetskrav inom en aktörs leverantörskedja. Detta trots det begränsade omfång av underleverantörer som existerade i studiens studerade projekt. En möjlig framtida forskningsmöjlighet är därmed att undersöka hur företag förhåller sig till säkerhet i sina leveranskedjor när de agerar inom en landsöverskridande projektallians. Denna typ av relation kan medföra att ytterligare svårigheter med att leva upp till de krav som ställs av NIS 2 dyker upp, på grund av den omfattande ökning av leverantörer som verkar inom dessa projekt, samt det faktum att landsöverskridande projekt kan innebära att olika länders lagstiftningar inom området av informationssäkerhet skapar friktion.

Vidare, lyfte (U) under intervjun behovet av en tydligare kartläggning kring vilka av de stora antal olika tjänster och mjukvaror som företaget nyttjar inom olika uppdrag, som bör anses okej att använda, beroende på det specifika uppdraget i åtankes sekretessnivå. Baserat på formuleringen i NIS 2 bör även leverantörer av dessa inkluderas inom en verksamhetsutövares allriskansats.

Referenser

Abrahams, T., Ewuga, S., Dawodu, S., Adegbite, A., & Hassan, A. (2024). A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION. Computer Science & IT Research Journal. 5. 1-25. 10.51594/csitrj.v5i1.699.

Bartnes, M. (2006). Safety vs. security?. 10.1115/1.802442.paper151.

Baruch, Y., Holtom, B. C. (2008). Survey response rate levels and trends in organizational research. Human Relations (New York), 61(8), 1139–1160. https://doi.org/10.1177/0018726708094863

BBC. (2023). DP World: Australia sites back online after cyber-attack. *BBC*. 13 november. https://www.bbc.com/news/business-67400164 [hämtad 2025-02-03]

Borgatti, S. P., Ofem, B. (2010). Social network theory and analysis. Social network theory and educational change, 17, 29.

Bryman, A. (2012). Social research methods (4:e uppl.). New York: Oxford University

Bolino, M., Long, D., & Turnley, W. (2016). Impression Management in Organizations: Critical Questions, Answers, and Areas for Future Research. Annual Review of Organizational Psychology and Organizational Behavior, 3(1), 377–406. https://doi.org/10.1146/annurev-orgpsych-041015-062337

Center for Strategic and International Studies (CSIS). (2025). Significant Cyber Incidents. Tillgänglig online: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [hämtad 2025-02-03]

Europeiska kommissionen (2003). KOMMISSIONENS REKOMMENDATION av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (2003/361/EG) https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32003H0361 [hämtad 2025-05-20]

Europeiska kommissionen (2013). KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) nr 402/2013 av den 30 april 2013 om den gemensamma säkerhetsmetoden för riskvärdering och riskbedömning och om upphävande av förordning (EG) nr 352/2009. https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32013R0402&from=PL [hämtad 2025-06-18]

Dick, J., Hull, E., & Jackson, K. (2017). Requirements Engineering (4th ed. 2017.). Springer International Publishing. https://doi.org/10.1007/978-3-319-61073-3

Direktiv 2016/1148. Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016L1148

Direktiv 2022/2555. Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet). https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32022L2555

Djebbar, F., Nordström, K. (2023). "A Comparative Analysis of Industrial Cybersecurity Standards," in IEEE Access, vol. 11, pp. 85315-85332, 2023, doi: 10.1109/ACCESS.2023.3303205.

Dhillon, G. (2017). Information Security: Text and Cases 2nd Edition. Prospect Press.

Ervural, B, & Ervural, B. (2018). Overview of Cyber Security in the Industry 4.0 Era. 10.1007/978-3-319-57870-5_16.

Förordning 2019/881. Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten). https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32019R0881

Hollnagel, E. (2008). The Changing Nature of Risks. Ergonomics Australia Journal. 22.

Hollnagel, E. (2013). A Tale of Two Safeties. Nuclear Safety and Simulation. 4. 1–9.

Hollnagel, E. (2018). Safety-I and safety-II: the past and future of safety management. CRC press.

Johanson, Jens. (2024). TRV 2024/25605 Öppen antagonistisk hotbild mot transportsektorn. Trafikverket. https://trafikverket.diva-portal.org/smash/get/diva2:1902716/FULLTEXT02.pdf

Kapliński, O., Tamosaitiene, J. (2010). Game theory applications in construction engineering and management. Technological and Economic Development of Economy - TECHNOL ECON DEV ECON. 16. 348-363. 10.3846/tede.2010.22.

Kecklund, L., Sandblad, B. (2021). Den (o)mänskliga faktorn: MTO : digitalisering och automatisering för säkerhet och hållbarhet (Upplaga 1). Studentlitteratur.

Kondo, S., Sakashita, H., Sato, S., Hamaguchi, T., & Hashimoto, Y. (2018). An application of STAMP to safety and cyber security for ICS, Editor(s): Mario R. Eden, Marianthi G. Ierapetritou, Gavin P. Towler, Computer Aided Chemical Engineering, Elsevier, Volume 44, 2018, Pages 2335-2340, ISSN 1570-7946, ISBN 9780444642417, https://doi.org/10.1016/B978-0-444-64241-7.50384-0.

Leveson, N. (2004). A new accident model for engineering safer systems. Safety Science, Volume 42, Issue 4, 2004, Pages 237-270, ISSN 0925-7535, https://doi.org/10.1016/S0925-7535(03)00047-X.

Leveson, N. (2020). Safety III: A systems approach to safety and resilience. MIT Eng. Syst. Lab, 16.

Leveson, N., Thomas, J. (2018). STPA Handbook. MIT Partnership for Systems Approaches to Safety and Security (PSASS), Cambridge, Massachusetts, U.S. Tillgänglig online: https://www.flighttestsafety.org/images/STPA_Handbook.pdf [hämtad 2025-01-30]

Lietz, P. (2010). Research into Questionnaire Design: A Summary of the Literature. International Journal of Market Research, 52(2), 249–272. https://doi.org/10.2501/S147078530920120X

Mehmood, S., Fan, J., Dokota, I., Nazir, S., & Nazir, Z. (2024). How to Manage Supply Chains Successfully in Transport Infrastructure Projects. Sustainability. 16. 730. 10.3390/su16020730.

Myerson, R. B. (1997). Game theory. Harvard University press.

Myndigheten för samhällsskydd och beredskap (MSB). (2024a), Tidsplan för NIS2-införandet i Sverige. Tillgänglig online: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/krav-och-regler-inom-informationssakerhet-och-cybersakerhet/nis-direktivet/tidsplan-for-nis2-inforandet-i-sverige/ [hämtad 2025-02-3]

Myndigheten för samhällsskydd och beredskap (MSB). (2024b). Det här är NIS2-direktivet. Tillgänglig online: 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/ [hämtad 2025-02-03]

Myndigheten för samhällsskydd och beredskap (MSB). (2024c). Cybersäkerhetskonferensen 2024, 23 Standarder i informationssäkerhetsarbetet - ett verktyg för förmågeutveckling. Tillgänglig online: https://www.msb.se/sv/aktuellt/kalender/2024/oktober/cybersakerhetskonferensen-2024/ [sett 2025-01-31]

Myndigheten för samhällsskydd och beredskap (MSB). (2024d). Om informationssäkerhet. Tillgänglig online: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-informationssakerhet-och-cybersakerhet/om-informationssakerhet/ [hämtad 2025-03-25]

Myndigheten för samhällsskydd och beredskap (MSB). (2025). Så väntas NIS2-regleringen se ut. Tillgänglig online: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/krav-och-regler-inom-informationssakerhet-och-cybersakerhet/nis-direktivet/sa-vantas-nis2-regleringen-se-ut/ [hämtad 2025-02-03]

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, Volume 3, Issues 3–4, s103-117, ISSN 1874-5482, https://doi.org/10.1016/j.ijcip.2010.10.002.

Nationellt cybersäkerhetscenter. (2025). Cybersäkerhet i Sverige 2024. https://www.ncsc.se/siteassets/publikationer/cybersakerhet-i-sverige-2024.pdf

National Institute of Standards and Technology (NIST). (2018). Cybersecurity Framework Version 1.1. Tillgänglig online: https://doi.org/10.6028/NIST.CSWP.04162018

Niels, M., Dempsey, K., & Pillitteri, V. Y. (2017). An Introduction to Information Security, NIST Special Publication 800-12 Revision 1. Tillgänglig online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Oscarson, P. (2019). Informationssäkerhet (Upplaga 1). Studentlitteratur.

Patriarca, R., Chatzimichailidou, M., Karanikas, N., & Gravio, G. (2022). The past and present of System-Theoretic Accident Model And Processes (STAMP) and its associated techniques: A scoping review, Safety Science, Volume 146, 2022, 105566, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2021.105566.

Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174). Försvarsdepartementet. https://svenskforfattningssamling.se/sites/default/files/sfs/2018-06/SFS2018-1174.pdf

Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1175). Försvarsdepartementet. https://svenskforfattningssamling.se/sites/default/files/sfs/2018-06/SFS2018-1175.pdf

Förordning om statliga myndigheters beredskap (SFS 2022:524). Försvarsdepartementet. https://svenskforfattningssamling.se/sites/default/files/sfs/2022-05/SFS2022-524.pdf

Sales, N. A. (2013). Regulating Cyber-security, 107 Nw. U. L. Rev. 1503, 1503-1568. https://scholarlycommons.law.northwestern.edu/nulr/vol107/iss4/1

Salmon, P.M., Cornelissen, M., & Trotter, M. (2012). Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. Safety Science, Volume 50, Issue 4, Pages 1158-1170, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2011.11.009.

Shapiro, S. P. (2005). Agency Theory. Annual Review of Sociology, 31(1), 263–284. https://doi.org/10.1146/annurev.soc.31.041304.122159

Shrestha, A., Tamošaitienė, J., Martek, I., Hosseini, M. R., & Edwards, D. J. (2019). A Principal-Agent Theory Perspective on PPP Risk Allocation. Sustainability, 11(22), 6455. https://doi.org/10.3390/su11226455

Shrobe, H., Shrier, D., & Pentland, A. (2018). "CHAPTER 2 Cybersafety: A Systems Theory Approach to Managing Cybersecurity Risks—Applied to TJX Cyberattack," in New Solutions for Cybersecurity, MIT Press, 2018, pp.81-110.

Siponen, M.T. (2000). "A conceptual foundation for organizational information security awareness", Information Management & Computer Security, Vol. 8 No. 1, pp. 31-41. https://doi.org/10.1108/09685220010371394

Siponen, M., Willison, R. (2009). Information security management standards: Problems and solutions, Information & Management, Volume 46, Issue 5, 2009, Pages 267-270, ISSN 0378-7206, https://doi.org/10.1016/j.im.2008.12.007.

von Solms, B., von Solms, R. (2018). "Cybersecurity and information security – what goes where?", Information and Computer Security, Vol. 26 No. 1, pp. 2-9. https://doi.org/10.1108/ICS-04-2017-0025

Souza, N., Cesar, C., Bezerra, J., & Hirata, C. (2020). Extending STPA with STRIDE to identify cybersecurity loss scenarios. Journal of Information Security and Applications. 55. 102620. 10.1016/j.jisa.2020.102620.

Svenska institutet för standarder. (2022a). Informationssäkerhet, cybersäkerhet och integritetsskydd – Informationssäkerhetsåtgärder (ISO/IEC 27002:2022, IDT) https://www.sis.se/produkter/informationsteknik-kontorsutrustning/allmant/ss-en-isoiec-270022022/

Svenska institutet för standarder. (2022b). Informationssäkerhet - Cybersäkerhet och integritetsskydd - Ledningssystem för informationssäkerhet (ISO/IEC 27001:2022). https://www.sis.se/produkter/informationsteknik-kontorsutrustning/itsakerhet/isoiec-270012022/

Svenska institutet för standarder (SIS). (u.åa). Detta är ISO 27001, https://www.sis.se/iso27001/dettariso27001/ [hämtad 2025-02-07]

Svenska institutet för standarder (SIS). (u.åb). Standarder vid upphandling, https://www.sis.se/standarder/vad-ar-en-standard/Standarder-vid-upphandling/ [hämtad 2025-02-06]

Svenska institutet för standarder (SIS). (u.åc). Ledningssystem, https://www.sis.se/standarder/verksamhetsutveckling/ledningssystem/ [hämtad 2025-02-07]

Svenska Akademin. (2021). Sekretess. I *Svensk Ordbok*. Hämtad från https://svenska.se/

Nya regler om cybersäkerhet (SOU 2024:18). Försvarsdepartementet. https://www.regeringen.se/contentassets/1e56bf5cad214fc78eb80d91c11cccb6/nya-regler-om-cybersakerhet-sou-202418.pdf

Tzavara, V., Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. International Journal of Information Security. 23. 1-25. 10.1007/s10207-023-00811-x.

Trafikverket. (2022). Allmänt om överlämning. Tillgänglig online: https://bransch.trafikverket.se/for-dig-i-branschen/miljo---for-dig-i-branschen/arbetssatt-och-metoder-for-miljo-i-vag--och-jarnvagsprojekt/overlamning-av-miljorelaterad--dokumentation/allmant-om-overlamning/ [hämtad 2025-03-13]

Trafikverket. (2023). Vår verksamhet, vision och uppdrag. Tillgänglig online: https://www.trafikverket.se/om-oss/var-verksamhet-vision-och-uppdrag/#uppdrag [hämtad 2025-02-19]

Trafikverket. (2025). Trafikverkets styrande dokument. Tillgänglig online: https://bransch.trafikverket.se/tjanster/publikationer-och-styrande-dokument/trafikverkets-styrande-dokument/ [hämtad 2025-03-20]

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review, Volume 52, 2024, 105890, ISSN 0267-3649. https://doi.org/10.1016/j.clsr.2023.105890

World Economic Forum. (2024). The Global Risk Report 2024 19th Edition. Tillgänglig online: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf [hämtad 2025-06-17]

Wright, A., Jun, G.T. (2019). Human and organisational factors in cybersecurity: applying STAMP to explore vulnerabilities. Loughborough University. Conference contribution. https://hdl.handle.net/2134/36539

Zhang, Y., Dong, C., Guo, W., Dai, J., & Zhao, Z. (2022). Systems theoretic accident model and process (STAMP): A literature review. Safety Science, Volume 152, 105596, ISSN 0925-7535. https://doi.org/10.1016/j.ssci.2021.105596.

Appendix A

Förklarande text i mail:

Hej! Mitt namn är Anton och jag håller på med ett exjobb åt Företaget där jag undersöker informationssäkerhetsfrågor inom uppdraget PROJEKT. Jag skulle uppskatta det väldigt mycket om du kunde ta dig tid att svara på den enkät som du finner i slutet av detta mail. Enkäten tar mellan 2–5 minuter att genomföra. Detta mail har skickats till dig som är verksam inom uppdraget, och dina svar kommer vara anonyma och kommer endast att användas som underlag i mitt exjobb. Sista dagen att svara på enkäten är den 9 Maj.

Vad syftar jag på med informationssäkerhet?

Företagets informationssäkerhetspolicy beskriver informationssäkerhet som de åtgärder som görs för att skydda information från obehörig åtkomst, förändring eller förstörelse. Exempel på ett bra förhållningsätt till informationssäkerhet inkluderar att inte dela med sig av lösenord, att endast jobba på godkända arbetsytor och att inte dela med sig av information till obehöriga. Här är länken till enkäten: Länk

Mvh Anton

Förklarande text i enkäten:

Hej! Tack för att du tar dig tid att fylla i denna enkät. Syftet är att kartlägga förhållningssättet till informationssäkerhet inom PROJEKT och svaren kommer endast att användas som underlag i ett examensarbete. Enkäten tar mellan 2-5 minuter att fylla i, och sista dagen för att fylla i enkäten är den 9 Maj. Har du några frågor är du välkommen att skicka dem till: anton.mammi@företag.se

Hur ofta har du informationssäkerhetsfrågor i åtanke i ditt dagliga arbete?

Svarsalternativ: Aldrig/Nästan aldrig. En eller två gånger i månaden. En eller två gånger i veckan. Alltid/Nästan alltid

Upplever du att företaget ställer tydliga krav på hur informationssäkerhet ska skötas inom projekt?

Svarsalternativ: Ja, Delvis, Nej, Vet ej

Har du någonsin upplevt att ditt arbetssätt granskats när det kommer till informationssäkerhet, antingen av kund eller internt på företaget? Flera val möjliga.

Svarsalternativ: Ja, av kund. Ja, internt. Nej. Vet ej.

Om du svarade Ja på föregående fråga, hur gick detta till?

Svarsalternativ: Kort svarstext

Upplever du att Trafikverket ställer några krav på informationssäkerhet inom projektet?

Svarsalternativ: Ja. Delvis. Nej. Vet ej.

Om du svarade Ja eller Delvis på föregående fråga, vad innebär dessa krav?

Svarsalternativ: Kort svarstext

Har du upplevt att ditt arbetssätt granskats när det kommer till informationssäkerhet, antingen av Trafikverket eller internt av företaget, inom projektet? Flera val möjliga.

Svarsalternativ: Ja, av Kund. Ja, internt. Nej. Vet ej.

Om du svarade Ja på föregående fråga, hur gick detta till?

Svarsalternativ: Kort svarstext

Hur viktigt anser du att arbete med informationssäkerhet är inom ditt teknikområde? 1 = Inte speciellt viktigt, 7 = Mycket viktigt.

Svarsalternativ: 1 till 7

Hur stor del (i %) av din arbetstid lägger du inom projektet?

Svarsalternativ: Mindre än 20%. 20-40%. 40-60%. 60-80%. Över 80%.

Inom vilket teknikområde är du verksam inom projektet?

Svarsalternativ: Kort svarstext

Har du några övriga synpunkter? Skriv dem gärna nedan.

Svarsalternativ: Kort svarstext

Appendix B

Design metodik

Förändringar

- Arbetat bort frekvensadverb
- Funderat över "double barreled" formuleringar. Exempelvis kan fråga 1 kunnat argumenteras för att den är "double barreled". Gör bedömningen att formuleringarna är tydliga nog att detta inte är ett problem
- Valde att ha kvar "vet ej" som ett alternativ på flera frågor, då jag gör bedömningen att ett svar av "vet ej" även de kan användas eftersom det kan tänkas tyda på en genuin okunskap.
- Valde även formuleringen "Upplever du" för att ge intrycket till respondenten att det ej finns ett helt korrekt svar på frågan
- Ursprungligen tänkte jag skicka endast till TA inom projektet, eftersom rollen som teknikansvarig innebär mycket kontakt med kund och arbete med kravuppfyllnad, och människor inom rollens inställning, medvetenhet och arbetssätt i frågan bör därför vara värdefulla för syftet. Jag valde dock att skicka ut den till alla verksamma inom projektet, eftersom informationssäkerhet egentligen är organisations-omvälvande.

Feedback efter pilot:

- Vad är informationssäkerhet? Förtydligar genom att en mer tydlig koppling till företagets informationssäkerhetspolicy både i mail och i enkäten.
- Vad syftar informationssäkerhetsfrågor på egentligen? Är det områdesspecifikt eller för arbetsprocessen som syftas på? Valde att lämna detta öppet för att låta respondenterna göra sin egen tolkning.
- Blandningen av generella och specifika frågor bör övervägas, om de är förvirrande, försökt skapa en struktur av generella → specifika → demografi
- En del förändringar av språkbruk och omformuleringar av frågor.
- Någon ytterligare fråga om intern styrning och externa projektspecifika krav hade bra för syftet. Denna feedback gjorde att jag ändrade och lade till specifika frågor om detta.
- Korrigerat spann på fråga 10, saknades.

Feedback efter kontakt med projektets uppdragsingenjör:

- Belyste att ordet informationssäkerhet kan av de som arbetar med intern och säkerhetsgranskning i projektet misstolkas, och gav rådet att i det medföljande mailet förtydliga kopplingen till företagets policy.
- Även att enkäten är anonym kan leda till fler svar.

Syfte med frågor:

1–2. Få en bild över medvetenhet i projektet kring informationssäkerhet

3–4. Ge en bild över faktiskt arbete med informationssäkerhet i verksamheten

5–6 Få en bild över medvetenhet + om Trafikverket ställer några krav.

7–8 Ge en bild över faktiskt arbete med informationssäkerhet i verksamheten

9–11 Demografifrågor, placerade sist i enlighet med teori.

12. För att ge respondenterna möjlighet att lyfta mer egna tankar.

Appendix C

Vilka frågor - Deltagare

Kravställningar företag - Kravsamordnare (K)

Hej! Mitt namn är Anton och jag håller på med ett exjobb här inom företaget och ska titta på hur företaget förhåller sig till cybersäkerhet i sina leverantörsrelationer. Jag hörde av Handledare att du har bra koll på kring kravsamordningen i projektet, och undrar om du hade kunnat tänka dig att ställa upp på en intervju kring hur ni arbetar med kravställningar, exempelvis hur ni förmedlar dessa till olika intressenter och hur kravställningarna tar form?

6) Kan du berätta vad du heter och vilken roll du har inom företaget?
7) Kan du berätta lite kort om projektet och vilken roll du har inom det?
8) Vilka är de huvudsakliga intressenterna i projektet, och mellan vilka behöver krav samordnas? Är de i främst Trafikverket, eller behöver ni också förhålla er till krav från någon av de andra firmorna som arbetar inom projektorganisationen?
9) Vilka personer eller funktioner arbetar med kravframställningen i projektet?
10) Hur arbetar ni med att säkerställa att krav är tydliga, mätbara och genomförbara?
11) Hur arbetar ni med att säkerställa att krav uppfylls?
12) Hur hanteras motstridiga krav?
13) Ställs det några krav gällande informationssäkerhet på er av kunden?
14) Har ni några underleverantörer inom projektet?
15) Hur ställer ni krav neråt i projektet? Förlitar ni er på ramavtal, eller skapas krav specifikt för varje underleverantör?
16) Ställer ni några krav gällande informationssäkerhet?
17) Om ja, vad tar dessa grund i?
18) Om nej, varför inte?
19) Hur säkerställer ni att krav uppfylls?
20) Jag har hört att ni inom vissa projekt använder er av Designcentrum i utlandet, gör ni det i det här projektet?
21) Om ja, skiljer sig ert förhållningssätt på något vis i dessa relationer?
22) Finns det någon fråga som du önskar att jag ställt eller något område som du vill prata om lite extra?
23) Finns det någon du skulle rekommendera att jag pratar med?
24) Är det okej om jag skickar något mail ifall det dyker upp några oklarheter?

Certifieringsprocessen - Utvecklingschef (U)

Hej! Mitt namn är Anton och jag arbetar just nu med ett exjobb här på företaget och ska titta närmare på hur företaget förhåller sig till cybersäkerhet i sina leverantörsrelationer. Certifiering är ett verktyg som används inom området och därför är jag intresserad av den certifieringsprocess mot ISO 27001 som (del av

verksamheten) gjort rätt nyligen, och jag letar därför efter någon inom företaget som har koll inom den frågan. Har du möjligtvis det, och i så fall hade du kunnat tänka dig ställa upp på en kortare intervju kring ämnet? Alternativt om du kunnat skicka mig vidare till någon som kanske kan?

25) Kan du berätta vad du heter och vilken roll du har inom företaget?
26) Vilken roll och ansvar hade du inom verksamhetsområdets certifieringsprocess?
27) Kan du kort sammanfatta vad ISO 27001 innebär och varför detta är relevant för er verksamhet?
28) Vilka var de främsta drivkrafterna bakom beslutet att certifiera er?
29) Kan du sammanfatta hur certifieringsprocessen såg ut för er, steg för steg? Vad var det viktigaste milstolparna? Tog ni exempelvis stöd av ISO-27002?
30) Vilka delar av organisationen var mest involverade i denna process?
31) Fanns det några specifika utmaningar som ni stötte på under processen och hur hanterade ni dessa?
32) Fanns det något i processen som gick enklare än förväntat för er?
33) Om ni fick genomföra certifieringsprocessen igen, finns det något ni skulle göra annorlunda?
34) Jag hörde att det pågår ett arbete med att resten av företagets verksamhet ska certifiera sig, vet du om det finns några planer på att använda den kunskap som förvärvats under verksamhetsområdets process i detta arbete?
35) När 27001 inkorporerats även i andra verksamhetsområdens verksamhet, tror du att ledningssystemet kommer att se annorlunda ut hos dem?
36) Hur har certifieringen påverkat ert verksamhetsarbete mer konkret?
37) Har ni märkt några fördelar av att vara certifierade och finns det några prestandamått eller liknande som uttrycker värdet av certifieringen för företaget?
38) Hur fungerar det när en del av verksamheten är certifierad men inte en annan, exempelvis vid verksamhetsområdes-överskridande arbete?
39) Finns det någon aspekt av certifieringsarbetet som du tycker vi inte har berört men som du tycker är viktig att lyfta fram?
40) Är det okej om jag skickar något mail ifall det dyker upp några oklarheter?

Trafikverket PLP - Trafikverket projektledare (PLT)

Hej namn!

Mitt namn är Anton och jag utför just nu ett exjobb åt företaget där jag håller på att titta på hur informationssäkerhetsfrågor behandlas i deras leverantörsrelationer och har därigenom blivit indragen på ett litet hörn i projektet. Jag försöker få en bild av vilka krav på informationssäkerhet som ställs inom projektet av Trafikverket på företaget, samt hur dessa kommuniceras och om det sker någon typ av granskning av hur företaget förhåller sig till dessa krav. Jag undrar därför om du hade kunnat tänka dig ställa upp på en kortare intervju inom området, alternativt om du hade kunnat skicka mig vidare till någon som kanske kan?

1) Kan du berätta lite om din roll inom Trafikverket och vad du har för roll
2) inom projektet?
3) När du säger sekretess, vad är det du faktiskt syftar på?
4) Vilka delar av dokumentationen är de som reglerar denna sekretess?
5) Vilka delar av projektets dokumentation gäller sekretess och finns det olika grader av sekretess inom olika delar av dokumentationen? Om ja, vad tar bedömningen av klassningen grund i?
6) Ställer ni högre krav på sekretess på grund av att detta är ett ????-projekt eller av några andra skäl i jämförelse med andra järnvägsprojekt? Om ja, vad tar dessa grund i?
7) Kan du berätta lite om hur ni på Trafikverket arbetar med att se till att era leverantörer uppfyller de krav på sekretess som ni ställer? Hur vet ni att företaget agerar rätt i dessa frågor?
8) Hur ser er process ut ifall ett brott mot dessa krav på sekretess sker?
9) Vad är Trafikverkets övergripande inställning till användandet av underkonsulter i projektet? Behöver ni "vetta" eller verifiera dessa på något sätt?
10) Görs något arbete för att säkerställa att företaget förmedlar information gällande sekretess hos sina underleverantörer eller ligger detta ansvar hos leverantören?
11) Finns det några särskilda krav på sekretess på att information hanteras korrekt vid arbete utanför EU?

TA Företag - Teknikansvarig företag (TA)

Hej namn!

Mitt namn är Anton och jag håller på med ett exjobb där jag tittar på hur företaget arbetar med informationssäkerhet inom sina leverantörsrelationer och har därigenom hängt med lite på en kant inom projektet. Din roll som TA inom projektet är väldigt intressant för mitt exjobb, och jag undrar om du hade kunnat tänka dig att ställa upp på en kortare intervju? Mina frågor handlar i huvudsak om kommunikation, ansvar och kravuppfyllnad i projektet.

1) Kan du berätta lite om din roll inom företaget och vad du har för roll inom projektet?
2) Kan du beskriva vilka uppgifter i projektets som är kopplade till rollen som teknikansvarig?
3) Vilka kommunicerar du med inom projektet? Finns det något "rollberoende" i detta?
4) Jag har hört att det finns en rätt så stor variation mellan olika projekt i hur tydliga gränsdragningar som finns mellan den utförande sidan (projektörer osv) och den ledande sidan i olika projekt, hur skulle du säga att det ser i detta projekt?
5) Jag vill få en bild över hur kravhantering ser ut i verkligheten, hur stor roll skulle du säga att du har inom den frågan?
6) Hur mycket insyn har du i projektörernas arbete?

7) Finns det några delar där detta är svårare än andra?
8) Sen såg jag att det fanns ett gäng utländska projektörer inom teknikområdet. Är du även TA för dessa? Om inte, sker denna samordning av någon annan?
9) Har de någon specifik roll inom projektet eller agerar de som vanliga projektörer?
10) Hur arbetar ni med kvalitetsförsäkran gällande dessa resurser, skiljer sig de på något sätt från andra resurser, säkerställa ett enhetligt arbetssätt osv?
11) Vem ansvarar för att säkerställa att de förhåller sig till de krav som ställs av Trafikverket och företaget i frågor såsom sekretess?
12) Och sen min näst sista fråga, vad innefattas av i ditt teknikområde i detta projekt?
13) En sista avslutande fråga, finns det något som du finner extra utmanande för dig inom projektet?

Datasamordning - Datasamordnare (DSF)

Hej namn!

Mitt namn är Anton och jag håller på med ett exjobb där jag tittar på hur företaget arbetar med informationssäkerhet inom sina leverantörsrelationer och har därigenom hängt med lite på en kant inom projektet. Din roll som datasamordnare i projektet och arbete med exempelvis dokumenthantering är väldigt intressant för mitt exjobb, och jag undrar om du hade kunnat tänka dig att ställa upp på en kortare intervju inom området?

1) Kan du berätta lite om din roll som Datasamordnare och vad din roll innebär inom projektet?
2) Vad innefattar begreppet dokumentationshantering, vad är i praktiken inblandat? Är exempelvis frågor kring sekretess eller tillgångsförvaltning en del av området?
3) Varifrån kommer de krav som bestämmer hur dokumenthanteringen ska gå till? Trafikverket?
4) Förändras de krav som ställs inom dokumenthantering mellan projekt?
5) Vilka inom projektet kommunicerar du med och vilka skulle du säga att du har närmast samarbete med?
6) Har du någon direkt kommunikation med projektörerna?
7) Har du någon roll när det kommer till kravuppfyllnad inom datasamordning?
8) Behöver du ha koll på "all" dokumentation eller ligger fokus exempelvis på att det som levererats lever upp till kraven? Hur arbetar du med den frågan?
9) Ansvarar du även för datasamordningsfrågor när det kommer till den indiska/utländska kompetensen i projektet? Exempelvis i form av dokumenthanterings manualer?
10) Om ja, finns det några speciella utmaningar med detta?
11) Om inte, vem gör det?

12) Varierar dina uppgifter beroende på var i projektet som ni befinner er? När har du som mest att göra?
13) En sista avslutande fråga, Vilka är dina största utmaningar inom ditt ansvarsområde?

Projektledning företag - Projektledare företag (PLF)

Hej namn!

Mitt namn är Anton och jag håller på med ett exjobb där jag tittar på hur företaget arbetar med informationssäkerhet inom sina leverantörsrelationer och har därigenom hängt med lite på en kant inom projektet. Din roll som uppdragsledare är projektet är väldigt intressant för mitt exjobb, och jag undrar om du hade kunnat tänka dig att ställa upp på en kortare intervju?

1) Kan du berätta lite om din roll som Uppdragsledare(projektledare) och vad din roll innebär inom projektet?
2) Kan du berätta lite om vilka du kommunicerar mest med inom projektet? Hur mycket är Trafikverket med och pratar inom själva projektet?
3) Vilken roll spelar du inom arbetet med att säkerställa god kommunikation inom projektet?
4) Hur arbetar ni för att alla inom projektet ska veta vad som faktiskt förväntas av dem?
5) Vilken roll spelar ni i uppdragsledningen inom krav och kravuppfyllnadsarbetet när det kommer till det “mjukare” kraven på förhållningssätt i informationssäkerhet eller sekretess?
6) Hur framförs användningen av utländsk arbetskraft gentemot Trafikverket?
7) Hur förhåller ni er på uppdragsledningssidan till att styrande dokument osv är på svenska gentemot dessa resurser?
8) Finns det några tydliga direktiv från företagets sida hur ni ska förhålla er i frågan?
9) Skiljer sig sättet som ni i uppdragsledningen arbetar gentemot dessa resurser på något vis?
10) Vad är de största utmaningarna i projektet? Vad kommer du ta med dig från detta uppdrag till nästa?