Linnéuniversitetet
Institutionen för informatik

Examensarbete i Informatik

Magister med inriktning digital affärsutveckling

Digitala leveranskedjor och höga krav på informationssäkerhet
-*Implikationer för att stärka Sveriges digitala motståndskraft*

Författare: Christian Dohrendorf
Handledare: Niclas Eberhagen
Termin: VT2024
Kurskod: 4IK51E

Sammanfattning

Syftet med uppsatsen är att öka kunskapen kring organisationers och kringliggande aktörers förmåga att stärka den digitala motståndskraften i digitala leveranskedjor genom införande av ett omfattande regelverk.

Uppsatsen beskriver hur tillkommande regelverk med höga krav på informationssäkerhet inom de digitala leveranskedjorna påverkar en enskild organisation. Uppsatsen beskriver även implikationerna ur ett övergripande systemperspektiv. Utifrån införandet av Digital Operational Resilience Act (DORA) beskrivs både potentiella hinder som riskerar hämma Sveriges digitala motståndskraft och de möjliggörande åtgärder som leder till att Sveriges digitala motståndskraft stärks.

Uppsatsen identifierar genom en fallstudie ett antal hinder som enskilda organisationer bör beakta, men som även har stora beroenden till andra kringliggande aktörer och systemet i sin helhet. Uppsatsen beskriver att det kan uppstå följdeffekter som lätt leder till oönskade effekter. Komplexitetshöjningen genom tillkommande regelverk kräver medvetna handlingar av ett stort antal aktörer för att undvika att hinder blir alltför hämmande och därmed hindrande för Sveriges digitala motståndskraft. Speciellt mindre leverantörers situation lyfts som problematisk i sammanhanget.

Uppsatsen identifierar behovet av en holistisk inställning som nödvändig för att kunna skapa utrymme för medvetna handlingar. Komplexitetshöjningen som tillkommande regelverk innebär behöver hanteras både internt inom en enskild organisation och genom externa samarbeten. Uppsatsen beskriver att identifierade möjliggörande åtgärder inte enbart bör värderas utifrån direkta effekter, utan även utifrån mer långsiktiga indirekta effekter och resurspåverkan i systemet. Först då finns det förutsättningar att genom medvetna handlingar uppnå positiv effekt och därmed stärka Sveriges digitala motståndskraft.

Använda förkortningar

DORA	Digital Operational Resiliance Act
NIS	Network and Information Security Directive
IKT	Informations- och Kommunikationsteknik
CIA	Confidentiality, Integity, Availability
SLA	Service Level Agreement
CTI	Cyber Threat Intelligence
IS	Information Security

Förord

Jag vill tacka min handledare Niclas Eberhagen som under uppsatsskrivandet bidragit med värdefull återkoppling. Uppsatsen hade vidare inte varit möjlig utan det tillmötesgående deltagandet från samtliga respondenter i intervjuerna, stort tack även till er. Slutligen vill jag gärna tacka medstudenter som bidragit med värdefull konstruktiv kritik under seminarier och därmed varit till stor hjälp under uppsatsskrivandet.

_____

Christian Dohrendorf

Innehåll

1. Introduktion

I introduktionskapitlet presenteras bakgrund och problemformulering som kopplar an till relevanta händelser och tidigare forskning. Detta leder till att syfte och forskningsfrågor presenteras. Slutligen visas även de begränsningar som föreligger, samt målgrupp för arbetet.

1.1 Bakgrund

Med tanke på omvärldsläget med både kriget i Ukraina och Sveriges intåg i NATO är det en situation som kräver att Sveriges digitala motståndskraft tas på allvar. Riskerna för allvarliga samhällspåverkande händelser behöver minska. Allvarligheten potentieras av att det finns identifierade brister i Sveriges systematiska informations- och cybersäkerhets-arbete, vilket Myndigheten för samhällsskydd och beredskap (MSB, 2023) påpekar i en sammanfattande rapportering. En ökad trend mot digitalisering leder till mer omfattande potentiella händelser med allvarligare konsekvenser. Enligt rapporten framkallar det skärpta säkerhetspolitiska läget, samt de uppkomna sårbarheterna som återfinns bland flertalet samhällsviktiga aktörer, ett behov för att systematiskt införa omfattande åtgärder. Enligt MSB krävs det åtgärder såsom kompetensutveckling, cyberlägesbilder, stärkt beredskap och fokusering inom totalförsvaret, internationell samverkan, målgruppsanpassat stöd, och övningar som avser kontinuitetshantering. Ett intressant inslag i rapporten är incidentstatistiken. Systemfel anges som främsta orsak till störningar i de samhällsviktiga tjänsternas tillgänglighet, konfidentialitet eller riktighet. På en andra plats anges mänskliga misstag som orsak. Först på plats tre anges angrepp som orsak till störningar. I detta sammanhang är det dock viktigt att påpeka att ett angrepp innebär att det finns aktörer som aktivt verkar för att störa tjänsternas kvalitet. Det skulle kunna innebära att denna typ av incident får allvarligare konsekvenser. MSB visar i sin rapport även att monoberoenden, där det finns större beroenden till en enskild leverantör, kan få mycket omfattande konsekvenser för samhället vid en störning. MSB beskriver i rapporten att organisationer därför ska fokusera på att upprätthålla en rimlig nivå av informationssäkerhet genom införande och upprätthållande av ett systematiskt informationssäkerhetsarbete. MSB beskriver även att det är väldigt viktigt att förstå och upprätthålla kunskap om de digitala leveranskedjorna. Detta motverkar enligt MSB risken för bristande kommunikation vid störningar, då det annars kan leda till värre konsekvenser vid en incident, än vad som hade behövt vara fallet. MSB beskriver vidare vikten av att uppmuntra samverkan mellan offentlig och privat sektor, vilket även kommer att behöva innebära att lagstiftning ses över för att motverka eventuella målkonflikter. Slutligen konstaterar MSB att en hög grad av digital motståndskraft och resiliens är avgörande för att stärka Sveriges förmåga att hantera cyberattacker eller andra störningar.

Att det kan ske allvarliga störningar som involverar monoberoenden eller tätt sammanflätade digitala leveranskedjor har visat sig både i närtid och historiskt. Tietoevry (2024) publicerade information om en ransomware-relaterad händelse med påverkan på ett stort antal kunder. Att händelsen haft stor omfattning och omfång konstaterade Lindström

(2024) i en artikel som publicerats för Computer Sweden. I artikeln beskrivs det att 120 myndigheter, däribland flertalet universitet, påverkats av händelsen genom att HR-systemet Primula stängts ner i samband med attacken. Enligt artikeln kan händelsen härledas till den ryska hackergruppen Akira. En annan händelse som kan kopplas till monoberoenden eller digitala leveranskedjor är Kaseya-incidenten, som enligt Eriksson (2021) påverkat IT-leverantören Kaseyas 60 direkta och 1500 indirekta kunder. I Sverige fick speciellt Coop mycket massmedial uppmärksamhet riktat mot sig utifrån denna händelse. Händelsen ledde till omfattande påverkan på betallösning i butikerna, och det fick därmed även en direkt konsumentpåverkan. En intressant spaning är att det i Kaseya-fallet gick att återskapa viss information, då krypteringsnyckel kunde inhandlas för 70 miljoner dollar. I dagens läge, med statlig påverkan från främst Ryssland, finns det indikationer på att händelser och incidenter inte längre innebär att det efterkrävs en lösensumma. Vissa attacker handlar i stället om påbörjad hybridkrigföring. Det gör att konsekvenser av attacker kan bli betydligt mer omfattande ur ett samhällsperspektiv, än vid mer ekonomiskt sinnad brottslighet.

Det finns även händelser längre bakåt i tiden, som inte kopplas till rena cyberattacker, utan som i stället kopplas till mycket låg grad av kompetens i upphandlingsförfarandet. Ohlin (2019) beskrivet en kort sammanfattning över den olycksaliga upphandling som Transportstyrelsen genomfört avseende outsourcing av IT-driften till IBM. Händelsen orsakade stor potentiell skada med röjande av sekretessbelagda uppgifter. Näringsdepartementet (2018) har utfört en granskning för att dra slutsatser kring händelsen. Granskningen beskriver en alarmerande situation där grundläggande informationssäkerhets-relaterade krav och processer inte följts. Ett exempel som beskrivs är att Transportstyrelsen saknat kunskap om den information som myndigheten haft ansvar över, vilket nog bör anses vara grundläggande för att överhuvudtaget kunna dra slutsatser om hur informationen bör skyddas. Utredningen visar vidare på brister i intern och extern samordning och kommunikation, brister i dokumentation, brister i att bedöma relevanta regelverk att förhålla sig till, oförmåga att prioritera upphandlingar för att undvika tidsatta risker, samt oförmåga att utifrån uppmärksammade risker dra slutsatser och tillsätta resurser för hantering. I grunden har det enligt utredningen funnits en avsevärd oförmåga att hantera komplexa frågeställningar och beslut kopplade till upphandling i en datadriven organisation. Det har till stor del kunnat härledas till ledningens oförmåga. Sammantaget kan det beskrivas som ett praktexempel på en informationssäkerhetshärdsmälta och är därmed ett skolboks-exempel för kommande generationer att förfasas över.

Det har enligt MSB (den 3 april 2023) skett en större förflyttning de senaste åren inom lagstiftningen för att stärka EU:s motståndskraft inom informations- och cybersäkerhetsområdet. Ett exempel utgör EU-förordning Digital Operational Resilience Act (THE EUROPEAN PARLIAMENT AND THE COUNCIL, 2022a) – hädanefter i denna uppsats benämnt som DORA. Detta kommer att påverka den finansiella sektorn inom EU och innebär mycket omfattande krav på organisationernas förmåga att hantera informations- och kommunikationsteknikrelaterade risker (IKT-risker) i de sammanvävda digitala leveranskedjorna.

Ett annat viktigt EU-direktiv som beslutats och som kommer att påverka svensk rätt är Network and Information Systems 2 Directive (THE EUROPEAN PARLIAMENT AND THE COUNCIL, 2022b) – hädanefter i denna text benämnt NIS2. NIS2 förväntas börja tillämpas 18 oktober 2024. Det får då en påverkan på de samhällsfunktioner (offentliga eller privata) som genom nätverk- och informationssystem erhåller samhällsviktiga tjänster eller produkter. Målet är att öka den digitala motståndskraften genom att minska splittring, öka medvetenheten, säkra förmågor, samt möjliggöra effektivare samarbeten. Framför allt handlar det om att säkra att sårbarheter upptäcks, påtalas, och i förlängningen hanteras. Säkerheten i hela leveranskedjan förväntas därmed stärkas. En del i förmågorna som beskrivs är att säkra grundförmågor inom incident- och krishantering, användning av kryptering, samt riskhantering. NIS2 innebär även betydligt ökade tillsynsåtgärder, höga sanktionsavgifter, samt andra omfattande påföljder vid bristande efterlevnad.

Sammantaget utgör de olika förordningarna och direktiven som tillkommer en holistisk ansats, med regelverk som påverkar både offentlig och privat sektor. Initiativen förväntas sammantaget stärka den digitala motståndskraften. Det förutsätts vidare att nationella strategier sätts upp, vilka syftar till att säkrar handlingskraften att hantera större händelser. Det uppmuntras genomgående till samarbete mellan privat och offentlig sektor, samt mellan medlemsstater.

1.2 Problemformulering

Tillkommande reglering leder till att de företag och offentliga organisationer som omfattas behöver utföra insatser för att säkerställa en förflyttning, som leder till att respektive organisation efterlever regelverken. Det behöver samtidigt leda till förutsättningar som skapar en holistisk balans utifrån organisationens övriga målsättningar. Det har under lång tid funnits ett behov av att hantera informationssäkerhet som en mer självklar grundpelare, vilket beskrivs av Dlamini et al. (2009) i nedan citat:

> *[…] the scope of information security has widened and its focus is fast shifting towards a strategic governance one. Security issues now require a more coordinated and focused effort from the national and international society, governments and the private sector. It is no coincidence that the study shows a shift towards legal and regulatory compliance, risk management and digital forensic fields. […] most of today's security challenges are to a greater extent related to the human and organisational aspects […] of security. All indicators points to a multi-disciplinary approach in the future development of the information security discipline. However, as we move forward to address the new challenges it is also critical that we continue strengthening the technologies. New research efforts is required that minimise the gap between regulatory issues and technical implementations. (s. 197)*

Samtidigt uppstår det frågetecken om de enskilda organisationer som påverkas av tillkommande regelverk verkligen har upprättat en förmåga att integrera informationssäkerhet utifrån ett holistiskt perspektiv, med de förmågor som då krävs. Behovet blir än tydligare i fallet med DORA, där det innebär en avsevärt utökad kravställning mot de finansiella entiteterna att kunna hantera IKT-relaterade risker genom de digitala leveranskedjorna. Komplexiteten ökar därmed avsevärt. Schneider et al. (2017) visar att det finns olika vägval att hantera externt tillkommen komplexitet. I det ena fallet ökar organisationen den interna komplexiteten för att svara upp mot den externa komplexiteten. I det andra fallet samverkar organisationen med andra aktörer för att svara upp mot komplexiteten. Att identifiera möjliga vägar framåt som skapar en balans utifrån olika perspektiv blir väldigt viktigt. En rimlig balans minskar risken för att större negativa händelser inträffar. Det möjliggör samtidigt att organisationernas övriga mål ej hindras på ett ofördelaktigt sätt. Med ökad komplexitet och tillkommande krav kommer det att finnas potentiella målkonflikter. Potentiella målkonflikter kan yttra sig dels internt inom en större koncern med internt utlagd verksamhet, dels mellan koncernen och dess externa underleverantörer. Att verka för effektivitet och holistisk balans är nödvändigt. Silic och Back (2014) uttrycker behovet av att stötta organisationerna i att ta rätt beslut. Det medför då att organisationernas begränsade medel används på ett balanserat sätt:

> *How can scholars help organizations to invest in smarter, faster, more efficient and more impactful ways? Our research clearly shows that the protection of information has never been more important. Information security has to be seen from the management and technical aspects, and in that context, scholars can play an important role. While on the one hand, there is a good academic answer when it comes to understanding the threats related to information security, on the other hand, from the economic and business aspects of information security, there is still an ongoing research gap. We believe that it is the right time for scholars to help practitioners by studying some of these research questions: Can information security be implemented off-the-shelf? What is the importance of information security governance? Is there a "Silver Bullet" in IS? (s. 303)*

Begreppet digital motståndskraft förekommer i högre utsträckning som samlingsbegrepp för att beskriva medlemsstaters och därmed EU:s sammantagna förmåga. De krav som tillkommer i de förordningar och direktiv som är på väg att införas, rör till stor del redan kända förmågor, som ryms inom begreppet informationssäkerhet (IS). Det blir därmed intressant att förstå hur organisationerna uppfattar dessa tillkommande regelverk och hur de påverkar organisationernas informationssäkerhetsarbete. Även myndigheternas, leverantörernas och andra aktörers perspektiv är intressant att undersöka utifrån en holistisk ansats. Med tanke på informationssäkerhetsrelaterade händelser, både historiskt och i närtid, finns det ett stort behov av att identifiera hinder och möjliggörande åtgärder. Vad behöver organisationer och myndigheter tänka på för att skapa goda förutsättningar för en effektiv omställning mot stärkt digital motståndskraft?

1.3 Syfte och forskningsfrågor

Syftet med uppsatsen är att öka kunskapen kring organisationers och andra aktörers förmåga att stärka den digitala motståndskraften i digitala leveranskedjor genom införande av ett omfattande regelverk. Uppsatsen förväntas bidra med kunskap som faktiskt är användbar utifrån en given organisations förutsättningar. Det förväntas vägleda i en riktning som både stärker den enskilda organisationens, dess digitala leveranskedjors, samt systemets totala digitala motståndskraft. I förlängningen förväntas det bidra till att Sveriges digitala motståndskraft stärks. Nedan forskningsfrågor är aktuella att besvara i uppsatsen:

1. *Är begreppen digital motståndskraft och digital leveranskedja tillräckligt definierade?*
2. *Vilka hinder hämmar syftet om stärkt digital motståndskraft i de digitala leveranskedjorna utifrån ett DORA-införande?*
3. *Vilka möjliggörande åtgärder främjar syftet om stärkt digital motståndskraft i de digitala leveranskedjorna utifrån ett DORA-införande?*
4. *Vilka skillnader finns det i att hantera internt utlagd verksamhet i förhållande till helt extern leverans utifrån ett DORA-införande?*
5. *Leder DORA och utökade krav på riskhantering inom digital leveranskedjor till ökade förutsättningar att öka Sveriges digitala motståndskraft?*

1.4 Avgränsning

Det görs en av avgränsning mot att undersöka införandet av DORA inom finansiell sektor genom en fallstudie. Valet grundar sig på insikten att den finansiella sektorn är speciellt utpekad genom DORA-förordningen. Samtidigt omfattas den finansiella sektorn även av NIS2, som har en bredare ansats med betydligt fler utpekade sektorer. Det finns ett större överlapp mellan DORA och NIS2. DORA är dock lex specialis (har företräde) i förhållande till NIS2. Därmed är det naturligt att använda DORA som en initial utgångspunkt.

Informationssäkerhet är ett komplext begrepp med otaliga förgreningar, som dessutom förändras över tid. Åtgärder som införs förändrar dynamik och komplexitet i systemet i sin helhet. En enskild uppsats kommer därmed inte att kunna täcka in samtliga möjliga perspektiv. Det kommer däremot att vara möjligt att skapa ett kontextuellt och övergripande angreppssätt som organisationer eller andra aktörer har behållning av, helt oavsett de specifika hinder och möjliggörande åtgärder som identifieras inom ramen för uppsatsen.

1.5 Målgrupp

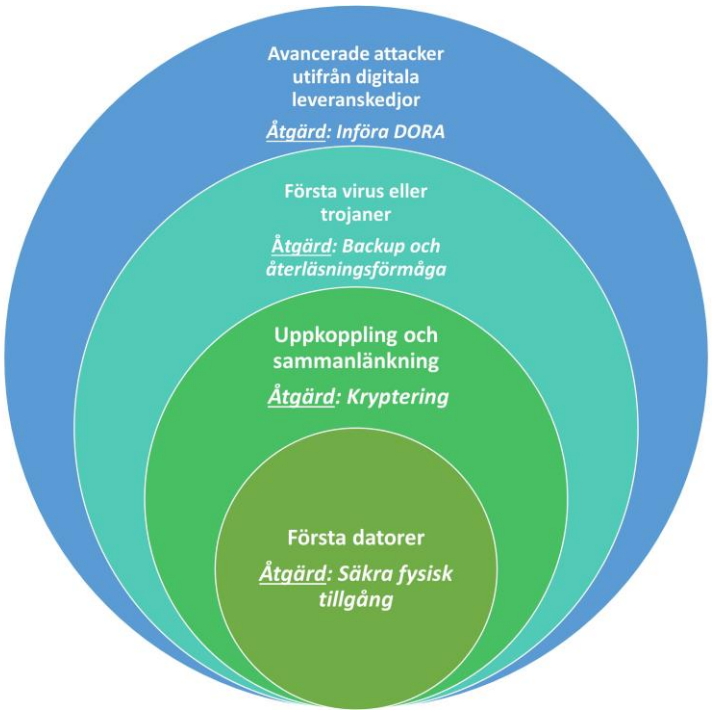
Studiens målgrupp är samtliga organisationer som önskar stärka den egna organisationens digitala motståndskraft genom hantering av risker inom digitala leveranskedjor. Ytterligare målgrupp är de företag som vill erbjuda tjänster och produkter som främjar den digitala motståndskraften i systemet som helhet. Även tillsynsmyndighet eller närliggande myndigheter, med ansvar över relaterade områden bedöms ha en behållning av arbetet. Slutligen finns det en behållning att läsa sammanställd uppsats för de individer som bidrar i att införa eller förändra standarder, ramverk, eller certifiering utifrån ett DORA-perspektiv.

2. Teoretisk bakgrund

I detta kapitel beskrivs relevanta begrepp och teorier som finns kopplade till dimensioner inom informationssäkerhetsområdet. Kapitlet berör de dimensioner som krävs för att kunna definiera den undersökningsmodell som presenteras i slutet av kapitlet.

2.1 Begreppet informationssäkerhet

Det går att argumentera för att begreppet informationssäkerhet varit aktuellt ända sedan dess att information tillkommit som en del i människans interaktioner, för att skydda skrift som lagrats, och de meddelanden som skickats. Dlamini et al. (2009) beskriver tillkomsten av olika lager av informationssäkerhetsåtgärder genom historiens gång. I samband med att de första datorerna på 1940-talet introducerades, bestod dessa säkerhetsåtgärder framför allt av rent fysiska aktiviteter för att hindra obehöriga att få åtkomst till informationen. Med tiden kunde informationen nås även på avstånd och genom delade resurser. Därmed krävdes det fler lager av informationssäkerhetsåtgärder för att kunna skapa en rimlig och riskanpassad informationshantering. Utvecklingen har fortsatt och det har lagts på fler lager utifrån de behov som uppstått. I nuläget med komplexa attacker mot digitala leveranskedjor, samt mål om att stärka Sveriges digitala motståndskraft, finns det ett behov av att definiera åtgärder kopplat till detta nya lager. En del i detta är då att införa DORA, som naturligtvis innehåller mer detaljerade åtgärder. Se figur 1 som exemplifierar förändringarna över tid:



Figur 1: Informationssäkerhet i ständig förändring (anpassad från Dlamini et al., 2009)

Begreppet informationssäkerhet har i mer modern tid enligt Dhillon (2006) ofta beskrivits utifrån att säkra skyddsvärd information inom dimensionerna confidentiality, integrity och availability (CIA). En bredare ansats är dock nödvändig enligt Vuorinen och Tetri (2012). Det beror på att informationssäkerhet inte kan ses som en rent statisk företeelse, utan i stället bör ses som en transformativ och bestående ”entitet”, som utifrån aktiviteter kopplat till CIA, även tillför komplexitet till det system inom vilket det implementeras. Vuorinen och Tetri (2012) argumenterar att denna betydligt mer omfattande definition leder till att informationssäkerhet även bör undersökas utifrån de mer indirekta effekterna som uppstår vid en förändring. Gränssnittet mellan användare av en informationsmängd, och själva informationsmängden i sig, påverkas således när informationssäkerhet tillförs som en ”aktör” mellan dessa delar i systemet. En bredare definition möjliggör en mer holistisk ansats. Morecroft (2020) beskriver en mer holistisk ansats, genom att visa möjligheterna med att använda systemperspektiv och systemtänkande för att fånga helheten. Med tanke på att informationssäkerhet är en komplexitetshöjande ”entitet” eller ”aktör”, så är det rimligt med en bred ansats. Dhillon och Torkzadeh (2006, s.306) exemplifierar komplexiteten genom att visa att det kan finnas väldigt olikartade fundamentala målsättningar kopplat till informationssäkerhetsarbetet på en övergripande nivå:

- Enhance management development practices
- Provide adequate human resource management practices
- Develop and sustain an ethical environment
- Maximize access control
- Promote individual work ethic
- Maximize data integrity
- Enhance integrity of business processes
- Maximizing privacy
- Maximize organizational integrity

Att komplexiteten i målsättningarna ökar ytterligare visas av Dhillon och Torkzadeh (2006, s.307) genom att hänvisa till underordnade möjliggörande målsättningar:

- Increase trust
- Provide open communication
- Maximize awareness
- Optimize work allocation practices
- Establish ownership of information
- Clarify centralization/decentralization issues
- Ensure legal and procedural compliance
- Improve authority structures
- Ensure availability of information
- Promote responsibility and accountability
- Understand work situation
- Maximize fulfillment of personal needs

- Understand individual characteristics
- Enhance understanding of personal financial situation
- Ensure censure
- Understand personal beliefs

Att informationssäkerhetsdesign samt metoder för att uppnå målsättningar förändrats med tiden observerades redan av Baskerville (1993). Den höga förändringstakten reflekteras även inom senare forskning. Shiau et al. (2023) beskriver att det saknas en övergripande helhetssyn över informationssäkerhet som forskningsområde, vilket beror på att det är en ständigt föränderlig materia. Detta beror på att angreppsytor och attackpotential kontinuerligt förändras. Med tiden tillkommer det därmed förändringar i övergripande tekniska-, beteendevetenskapliga-, ledningsbetingade-, filosofiska- eller organisatoriska perspektiv. Shiau et al. (2023, s.14) har genomfört en sammanställning för att försöka definiera aktuella kunskapsområden och trender inom forskningsområdet. Ett antal kunskapsgrupper presenteras:

- Intrusion detection
- Privacy protection
- Secure machine learning
- Cryptosystem
- Data service security
- Malware analysis
- Security decision-making
- Security management
- Incident management
- Physical security
- Third-party security

Ovanstående grupper är ett försök att definiera avskilda områden inom informationssäkerhet. Vid forskning kopplat till digitala leveranskedjor finns det naturligtvis behov av att förhålla sig till samtliga kunskapsområden. Mer direkt finns det en koppling till *third-party security* som kunskapsområde, som dock beskrivs som ett nytt tillkommande kunskapsområde, utifrån en mer allmän förflyttning mot molnbaserade lösningar. Det finns även en mer direkt koppling till kunskapsgruppen *data service security* som av Shiau et al. (2023) beskrivs som nära kopplad till molntjänster. Denna kunskapsgrupp avser hur den data som outsourcats bör hanteras utifrån både säkerhetsåtgärder och användbarhet. För övriga kunskapsområden så finns det en mer indirekt koppling då det rör förmågor som är oberoende av vald leveransform. När det gäller kunskapsgruppen *security management* till exempel, så har den en styrningsmässig koppling till digitala leveranskedjor. Det avser att organisationer behöver sätta upp en styrning som innehåller och tar hänsyn till krav på grundläggande informationssäkerhet, eller även andra regelefterlevnadsrelaterade dimensioner. Ett annat exempel är kunskapsområdet *security decision-making* som innebär att en organisation måste ha en

förmåga att utifrån riskbedömningar kunna ta beslut kring säkerhetsåtgärder eller andra mitigerade aktiviteter. Sammantaget finns det i litteraturen inte en fullständig, allmängiltig och detaljerad beskrivning av hur de digitala leveranskedjorna bör hanteras ur ett informationssäkerhetsperspektiv. Samtidigt finns det naturligtvis litteratur som beskriver enskilda dimensioner eller orsakssamband. En delmängd av dessa bedöms vara intressanta och relevanta att beskriva vidare utifrån syftet att besvara forskningsfrågorna i min uppsats.

2.2 Begreppet digital motståndskraft

Det finns en viss spridning i begreppen som omnämns för att beskriva digital motståndskraft. Sammantaget kan det dock härledas att det rör förmågan att holistiskt hantera informationssäkerhetsrelaterade dimensioner över tid. Beroende på om direktiv eller förordning avser enskild sektor, eller medlemsstatens sammantagna motståndskraft, kan begreppet avse olika förmågor. Dessa förmågor harmoniserar dock i hög grad. För den enskilda organisationen är det därmed i grunden samma typ av förmågor som avses. Här visas ett exempel utifrån DORA-förordningen (2022a):

> *[…] digital operational resilience' means the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions (artikel 3, första paragrafen)*

Enskilda medlemsstater förväntas införa ytterligare samordnande förmågor. Medlemsstaternas samverkan skapar i förlängningen ett extra lager av motståndskraft. Det finns således ingen större förändring kopplat till begreppet digital motståndskraft, annat än att det genom tillkommande reglering skapas ett tryck till att som organisation (privat som offentlig) arbeta holistiskt utifrån begreppet informationssäkerhet. Trycket består framför allt i att tillkommande regelverk medför allvarliga konsekvenser utifrån beskrivna påföljder, i det fallet organisationerna ej kan påvisa efterlevnad.

2.3 Begreppet digitala leveranskedjor

Det finns i DORA-förordningen (2022a) inte inlagt en fullständig definition på digitala leveranskedjor. Men det går att utläsa tillhörande övergripande krav genom att mer i detalj genomlysa förordningen:

> *Where the contractual arrangements on the use of ICT services supporting critical or important functions include the possibility that an ICT third-party service provider further subcontracts ICT services supporting a critical or important function to other ICT third-party service providers, financial entities shall weigh benefits and risks that may arise in connection with such subcontracting, in particular in the case of an ICT subcontractor established in a third-country […]*

> *[…] Where the contractual arrangements on the use of ICT services supporting critical or important functions provide for subcontracting, financial entities shall assess whether and how potentially long or complex chains of subcontracting may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect (artikel 29, andra paragrafen)*

Ovanstående innebär att det läggs ett väldigt stort ansvar på organisationen att kunna hantera och förutse risker som kopplas till en kedja av direkta leverantörer och indirekta underleverantörer.

2.4 Outsourcing

Att organisationer väljer att anlita leverantörer för att lägga ut leverans som rör informations- och kommunikationsteknik (IKT) är en naturlig del i att uppnå olika målsättningar. Det kan röra allt från att utöka förmågor och kapabilitet till att skapa kostnadseffektivitet. Enligt Mani et al. (2010) så bör organisationer som lägger ut leverans definiera strategiska målsättningar och anpassa relaterade processer som säkrar olika dimensioner, till exempel kvalitet och transparens. Detta leder då till möjligheter att säkra värdet som den utlagda leveransen medför. Pang och Tanriverdi (2022) visar att det finns fördelar med att använda outsourcing som en del i att modernisera IT-landskapet och därigenom minska riskerna för informationssäkerhetsincidenter. Xiao et al. (2013) beskriver att uppsatt och delad styrning kan leda till förtroendefull samverkan, som består och utvecklas mellan organisation och leverantör, trots uppenbara obalanser i maktförhållandet. Det förutsätter dock enligt Xiao et al. (2013) att den svagare avtalsparten kan påvisa och försäkra den starkare avtalsparten om att dess nivå av informationssäkerhet är acceptabel och hållbar över tid. I det fall den starkare avtalsparten önskar säkra en mer långsiktig relation, kan det krävas att det starkare parten bidrar med åtgärder och investeringar för att skapa denna typ av kvalitetssäkring. Williams (2011) beskriver att kunskapsöverföringen främjas i outsourcingsituationer när det sker utbildande aktivitet som säkerställer den utläggande partens perspektiv på ett tillfredsställande sätt. Utbildande aktivitet krävs i högre utsträckning om den utläggande partens omvärld förändras i snabb takt.

När det gäller uppföljande aktivitet för mätning och utvärdering av IKT-leverantörens informationssäkerhetsförmåga finns det flertalet modeller att välja mellan. En tidig och generell ansats ges av von Solms et al. (1994). Utvärdering kan ske på olika sätt genom till exempel självskattning eller mer direkta bevisinhämtande aktiviteter. En viktig aspekt i uppföljning av leverantörer är enligt Larson (1998) uppsatta, definierade och avtalade service level agreements (SLA) för den tjänst eller leverans som har lagts ut mot leverantör. SLA bör definieras på sätt som gör dem mätbara, managerbara, utvärderingsbara, samt om möjligt bedömningsbara utifrån monetära termer. Begreppet availability, eller på svenska tillgänglighet, är tätt knutet till begreppet SLA. Det beror på att en tjänsts upptid (att säkra tjänstens tillgänglighet) enkelt går att beskriva utifrån en SLA-definition. När det kommer till andra delar av inom CIA (confidentiality eller integrity) så är dessa antagligen mer

svårdefinierade utifrån den av Larson (1998) presenterade modellen. Dessa delar har dock en indirekt koppling till modellen genom att de påverkar slutanvändarens nöjdhetsgrad. Att inte användarens personuppgifter läcker ut är dock ett mer binärt tillstånd, som inte är lika naturligt att följa som ett uppsatt SLA. Däremot skulle eventuellt tidsramen inom vilken leverantören hanterar uppkomna sårbarheter av en viss kritikalitet kunna definieras som ett SLA. Det skulle i sådana fall vara ett mer indirekt SLA. Det mitigerar inte en risk för läckta personuppgifter direkt, men det finns åtminstone ett indirekt samband.

Med tanke på att komplexiteten ökat, samt att angreppsytorna är betydligt fler, kan det finnas fog för att även se över de mjukare aspekterna av utvärdering. Det säkrar grundförutsättning till uppföljning i gränssnittet mellan organisation, dess direkta leverantörer, och eventuella underleverantörer. Dhillon och Torkzadeh (2006) visar att det finns en risk att uppföljande aktiviteter utförs rent pliktmedvetet som en ”check in the box” aktivitet. Det bidrar då inte till målsättningarna som är rimliga utifrån ett holistiskt informationssäkerhetsarbete. Det behöver enligt Mähring (2018) ske uppföljande aktivitet i outsourcingsituationer som inte enbart syftar till ren kontrolluppföljning, utan som tar hänsyn till möjligheterna att överföra kontrollperspektivet till leverantören. Det bör alltså inte enbart ske kontroller utifrån leverantörens efterlevnad, utan det krävs även en mjukare uppföljning utifrån gränssnittets effektivitet, vilket då säkrar kvaliteten genom hela kedjan.

En annan intressant aspekt är i vilken grad en leverantör delar med sig av information kring IKT-relaterade incidenter eller händelser som påverkat leverantören. Wang et al. (2019) beskriver hur informationsdelning uppstår mellan konkurrerande privata organisationer. Det visar sig att det finns en större benägenhet att dela information mellan organisationer som tillhandahåller liknande produkter eller tjänster. Intressant är även att sannolikheten för informationsdelning minskar i de fall det rör sig om incidenter eller händelser som beror på interna misstag, eller i fall då personuppgifter exponerats. Även om den av Wang et al. (2019) utförda undersökningen inte granskat förhållandet och informationsdelningen mellan leverantör och dess kund, kan det antas att det finns liknande risk för undanhållande av information mellan dessa parter, om det inte införs informationsfrämjande insatser. Gupta och Zhdanov (2012) visar även att det finns ekonomiska motiv till att ingå (eller inte ingå) i ett större nätverk med outsourcad nätverksövervakning, samordnad patchning, eller andra säkerhetsåtgärder. Beroende på nätverkseffekter kan det löna sig att samordna insatser genom att ingå i förening med andra aktörer, eller genom att köpa tjänst från vinstmaximerande part. Det går att anta att ett DORA-införande innebär en kraftig ökning i komplexiteten, samt att det då även kräver högre grad av samordning eller samarbete mellan aktörer. Förstärkta nätverkseffekter skulle då kunna leda till utökade samarbeten, eller även leda till att helt nya tjänster och produkter införs på marknaden. Samtidigt skulle det då potentiellt även kunna leda till högre koncentrationsrisker inom systemet i sin helhet.

En del i den kravställning som kommer att behöva hanteras i förhållandet mellan organisation och IKT-leverantör utgörs av informationssäkerhetsrelaterade krav. Ett exempel som kan exemplifiera informationssäkerhetsrelaterade krav är att leverantören förväntas hantera kända sårbarheter (givet ett visst riskvärde) inom ett förutbestämt

tidsintervall. Temizkan et al. (2012) beskriver detta som ett intressant exempel, då det även kan visas att det i det fallet finns en koppling i leverantörernas hantering givet tillkommande lagstiftning. Enligt Temizkan et al. (2012) kommer leverantörernas hantering av informationssäkerhetsrelaterade krav således även påverkas av gällande lagstiftning, oavsett vad som avtalat mellan organisation och leverantör. Ett annat sätt att säkra allt mer omfattande cybersäkerhetsrelaterade risker skulle enligt Kotsias et al. (2023) vara att tillföra ett ytterligare lager bestående av cyber threat intelligence (CTI-as-a-service). Det blir då viktigt att lösning sätts upp som inte enbart baseras på sannolikhet och konsekvens utifrån en viss händelse, utan att den även bygger på information om potentiellt hotande aktörer, samt deras förmåga och vilja till att utföra handling. Det skulle vidare krävas att det sätts upp en styrning emellan organisation och leverantör som möjliggör ytterligare lager av informationsinsamling och kvalitetssäkring. MSB (2024 s. 15) har beskrivit ett antal rekommendationer för fyra specifika aktiviteter för att säkra digitala leveranskedjor, nämligen att (1) införa tydliga upphandlingsklausuler som avser informationsplikt från leverantörerna vid incidenter, att (2) granska och dokumentera de beroenden som finns när det gäller externa leverantörer för organisationens informationssystem, att (3) anpassa arbetssätt för incident hos en leverantör, samt att (4) sätta upp redundanta arbetssätt som ger handlingsalternativ om en incident inträffar.

2.5 Riskbedömning, regelefterlevnad och revision

På en väldigt grundläggande nivå behöver en organisation ha en förmåga att kunna hantera informationssäkerhetsrelaterade risker. Förmågan består enligt Straub och Welke (1998) av att identifiera risker, analysera risker, välja relevanta åtgärder, att implementera åtgärderna i en rimlig prioriteringsordning, samt slutligen att återkoppla resultat och kvarstående avsteg. Förmågan bör även kopplas till insatser för att höja kunskapsnivån inom organisationen. Det behöver även säkerställas att förteckning över möjliga åtgärder hålls uppdaterad. I de olika faserna som riskhanteringen innebär, föreslås det olika styrningsmässiga åtgärder för att säkra helheten.

Williams (2011) beskriver att det är önskvärt för en utläggande part att införa kvalitetssäkring mot leverantörer genom att utföra gap-analyser, samt att utifrån resultatet införa åtgärder. Cavusoglu et al. (2015) beskriver att det finns ett normativt tryck på organisationer att investera och upprätthålla en validerbar nivå av informationssäkerhet. Detta leder då till utökade möjligheter att binda till sig andra organisationer genom samarbeten. Wall et al. (2016) beskriver att det går att sätta upp modeller för att kunna bedöma sannolikheten för att en organisation kommer bryta mot regelverk. Det ger då indikation för risken att organisationen drabbas av en större negativ finansiell händelse. En intressant aspekt i att upprätthålla förtroende är validerbarhet. Det visar sig enligt Nuijten et al. (2018) att oberoende revisorer fångar upp informationssäkerhetsrelaterade risker tidigt. En oberoende part kommer dessutom att identifiera högre riskvärden än om organisationens chefer på egen hand utför riskanalyserna. Wall et al. (2016) argumenterar för att oberoende revision av risker kopplat till regelefterlevnad även leder till ökad transparens och ökad riskmedvetenhet. Därav är det sannolikt att en validerbar och oberoende granskning leder till högre grad av förtroende mellan olika aktörer.

2.6 Övergripande informationssäkerhet

Utifrån lagstiftning och avtalade informationssäkerhetsrelaterad krav så kommer det att krävas att leverantörens sammantagna processer, teknologi och anställda samverkar för att upprätthålla en acceptabel nivå av informationssäkerhet. Tsohou et al. (2015) beskriver att säkerhetsmedvetenhet uppstår i samspelet mellan dessa beståndsdelar. Beståndsdelarna kan därmed inte ses som helt separata. Det finns även mer allmänna informationssäkerhets-relaterade betänkanden i att sätta upp strategiska målsättningar när det gäller utläggning av digital leverans. En informationssäkerhetsrelaterad incident kan enligt Goldstein et al. (2011) få konsekvenser som yttrar sig genom både direkta och indirekta finansiella kostnader. Hedström et al. (2011) visar att det finns grundläggande potentiella målkonflikter i nutidens mer komplexa organisationer, med dess olika processer och informations-mängder. Detta stöds även av Stahl et al. (2012) som visar att detta även kan förstärkas om policy för informationssäkerhet blir ett politiskt maktmedel för att cementera roller och positioner. Ett viktigt perspektiv enligt Ogbanufe et al. (2021) är att säkra ledningens engagemang (och i förlängningen investeringsvilja) i informationssäkerhetsfrågor. Detta underlättas framför allt genom att visa och exemplifiera att ledningen står personligt ansvariga när negativa händelser uppstår. Det är enklare att säkra prioritering och investering genom denna typ av budskap än att hänvisa till mer indirekta konsekvenser. Ogbanufe (2021) föreslår även att kommunikation mot ledningen bör ske utifrån att risker beskrivs i monetära termer, eller utifrån påverkan på organisationens övriga målsättningar. Detta är speciellt viktigt när övriga målsättningar ligger närmare ledningens mer direkta ansvar.

Ett annat viktigt perspektiv som enligt Kwon och Johnson (2014) bidrar till att minska riskerna för negativa händelser, är ett proaktivt angreppssätt. Med proaktivitet avsätts medel och investeringar tidigt för att minska både sannolikhet och konsekvensen av negativa händelser. Detta är enligt Kwon och Johnson (2014) speciellt viktigt i miljöer med snabbt föränderlig hotbild. Vidare är det intressant att en frivilligt uppsatt proaktivitet leder till bättre resultat än vid uppsatt proaktivitet kopplad till införda regelverk. Kwon och Johnson (2014) beskriver att organisationer vid införande av åtgärder kopplat till regelverk ofta blir passiva och då agerar enbart för att möta det som ses som externt pålagda krav. Det kan då leda till att organisationen missar att genomföra en egen analys för problematiken. Angst et al. (2017) beskriver att det är viktigt att även agera långsiktigt utifrån att integrera informationssäkerhet i organisationens väsentliga processer och rutiner. Det ska inte ses som en kortsiktig implementation som sedan upphör. Li et al. (2023) beskriver behovet av att öka nivån av proaktivitet, då det minskar både antal och konsekvensen av cybersäkerhetshändelser. Det förutsätter att det tidigt investeras och utvecklas förmågor utifrån en medveten hotbildsanalys. Det gäller även att inte satsa medel och resurser på reaktiva förmågor kopplat till IT-lösningar som är inaktuella och föråldrade. Li et al. (2023) visar att modernisering av IT är en förutsättning för att minska cybersäkerhetsriskerna. Att modernisering av IT är en väsentlig faktor beskrivs även av Pang och Tanriverdi (2022). En annan aspekt som behöver balanseras är prioriteringen av förebyggande säkerhetsåtgärder i förhållande till upptäckande eller skadehanterade säkerhetsåtgärder. Paul och Wang (2019) visar att det utifrån en given hotbild finns ett optimalt läge för hur investeringarna bör

balanseras. Det måste ske aktiv och medveten prioritering för att nå denna balans. Nazareth och Choi (2015) beskriver att det lönar sig att prioritera att investera i förmågor som tidigt detekterar attacker. Det främjar förmågan att hantera och avvärja attacker. Givet att organisationer prioriterar säkerhetsåtgärder utifrån en limiterad budget, så finns det enligt Sawik (2013) en tendens till att välja bort säkerhetsåtgärder som bedöms vara applicerbara för mer katastrofala och osannolika scenario. Samtidigt bygger prioritering av säkerhetsåtgärder ofta på subjektiva bedömningar.

Tillgängligheten är sårbar för externa angrepp när organisationer har öppningar mot Internet. Han et al. (2023) visar att det finns händelser där angrepp ligger oupptäckta under lång tid, där angriparen bereder sig än mer skadepotential, än vid en mer direkt attack. Ett angrepp kan således även få konsekvenser inom dimensionerna integritet och/eller konfidentialitet. Chen et al. (2011) beskriver exempel på proaktiv hantering för att minska konsekvensen utifrån en allvarlig cyberhändelse. Det beskrivs att det utifrån ett tillgänglighetsperspektiv behöver skapas strategier som minimerar risken för omfattande avbrott genom diversifiering och redundans. Detta innebär dock även potentiella negativa effekter utifrån skalbarhet och kostnadseffektivitet. Sammantaget innebär det enligt Chen et al. (2011) att det krävs en riskanalys utifrån respektive organisations förutsättningar och målsättningar för tjänsternas tillgänglighet. Slutligen beskrivs det att samhället i sin helhet skulle ha behållning av att diversifiering eller redundans introduceras som en åtgärd för riskminimering, alltså att det blir ett mer diskuterat och undersökt begrepp.

2.7 Enskilda anställdas efterlevnad

Li et al. (2023) beskriver att säkerhetsmedvetenheten bland organisationens anställda är väsentlig för att minska risken för cybersäkerhetshändelser. Bulgurcu et al. (2010) visar att det är speciellt viktigt att fokusera på de anställdas säkerhetsmedvetande för att uppnå styrningsrelaterade målsättningar inom regelefterlevnad. Yazdanmehr och Wang (2016) förstärker detta budskap genom att visa behovet av utbildningsinsatser för att stärka de anställdas insikt i behovet av en hög nivå av informationssäkerhet, samt för att påvisa hur de anställda påverkar och är en del i informationssäkerhetsarbetet. Samtidigt visar Stahl et al. (2012) att policy som sätts upp kring informationssäkerhet ofta är detaljerade i vad som måste efterlevas, men att det inte beskrivs varför så bör ske. Vidare beskrivs det att det finns en risk att policy är skriven på ett sätt som kan missförstås, då den ofta är svårtolkad och använder ett akademiskt språkval. Det föranleder behov av kompletterande mer beskrivande och enkla riktlinjer, samt vägledning som visar relevans och som är anpassad för de målgrupper som påverkas. Budskapet att det krävs balans i att sätta former och budskap samt kommunikation kring informationssäkerhetspolicy stöttas även av Lowry och Moody (2015). Puhakainen och Siponen (2010) visar att anställda som inte efterlever informations-säkerhetsrelaterade regelverk utgör en allvarlig risk för den organisation de verkar inom. Donalds och Barclay (2022) beskriver att insatser för att höja säkerhetsmedvetandet adresserar olika informationssäkerhetsrelaterade målsättningar. Det innebär att de informationssäkerhetsrelaterade krav som ställs från en organisation mot en leverantör behöver säkras inte enbart genom avtal. Det krävs således relaterade insatser som drivs direkt av leverantören för att adressera dess anställdas säkerhetsmedvetenhet och faktiska

handlingar. De anställda bör dessutom enligt Spears och Barki (2010) ses som en tillgång i att skapa en god nivå av informationssäkerhet. Detta förutsätter att användare och anställda aktivt involveras och deltar i allt från uppsättning till testning av säkerhetskontroller. Lin et al. (2022) visar på medarbetarna som en källa till kreativ och proaktiv informationssäkerhetshantering. De bör utifrån detta perspektiv ses som problemlösare och inte enbart ses som en källa till informationssäkerhetsrisker.

Att hantera informationssäkerhetsrelaterade krav mellan organisation och leverantör enbart utifrån ett avtalsperspektiv, med klausuler om avtalsbrott och negativa påföljder, kommer antagligen inte alltid få den effekt som eftersträvas från organisationen. Siponen och Vance (2010) beskriver att användare rationaliserar bort handlingar som ej är förenliga med kravställd informationssäkerhet utifrån jämförelse med andra dimensioner som upplevs som viktigare. En del i detta är även att rollkonflikter och arbetsbelastning leder till hög grad av vad Ayyagari et al. (2011) beskriver som ”technostress”. Det kan antas att informationssäkerhet lätt rationaliseras bort i sammanhang där speciellt arbetsbelastning och rollkonflikter förekommer i hög grad. Detta leder enligt Siponen och Vance (2010) även till att beskrivna negativa påföljder ej realiseras av användarna i den grad som kan förväntas. Vidare beskrivs Siponen och Vance (2010) att mer formellt beskrivna påföljder inte förutspår graden av regelefterlevnad. Att varken påföljder eller belöningar leder till regelefterlevnad stöttas även av Moody et al. (2018). Chen et al. (2018) balanserar detta perspektiv genom att beskriva att det finns indirekta effekter kopplat till negativa påföljder. Liang et al. (2012) beskriver att det kan finnas kulturella olikheter utifrån länder som organisationer verkar inom, vilket då påverkar i vilken grad påföljder och belöningar får en avsedd verkan eller inte.

Det går att anta att formellt beskrivna artefakter som avtal och informations-säkerhetsrelaterade krav i vissa fall skapar en ”falsk trygghet”. Son (2011) visar att det finns fog för att fokusera på de anställdas intrinsiska motivation till att upprätthålla en fullgod nivå av informationssäkerhet, i stället för att fokusera på extrinsiska variabler som belöning eller straff. Kraften av att ta hänsyn till de anställdas intrinsiska motivation i informationssäkerhetsarbetet beskrivs även av Guo och Yuan (2012). Vance at al. (2012) tar upp ett antal viktiga aspekter för att säkra informationssäkerheten, varav en är enkelhet. Det behöver finnas förutsättningar för de anställda att kunna följa rutiner och processer som relaterar till informationssäkerheten. Herath et al. (2014) visar att användare i högre utsträckning använder lösningar som främjar informationssäkerhet om de är enkla och om det finns en upplevd hög nivå av användbarhet. En annan del i om en lösning kommer att användas är upplevd risk och i vilken utsträckning som användaren upplever att lösningen motverkar risken. Det återfinns enligt Drummond (2011) ofta processer inom organisationer som satts upp för att övervaka och hantera risker, vilka inger en falsk trygghet. Det kan till och med motverka förmågan att förutspå risker. Nyttan ligger inte alltid i mängden information och antalet uppsatta processer. Nyttan återfinns nämligen även i förmågan att kunna tänka utanför uppsatta boxar, för att täcka in risker som ej identifierats ännu. Det krävs enligt Lyytinen (2011) en balans i perspektiven kontroll och illusionen av kontroll, det vill säga att mer dialektiskt förstå begreppet kontroll. Posey et al. (2024) beskriver att

en grundförutsättning är att de anställda ej har för mycket aktiviteter, eller är för hårt pressade och belastade. Detta leder annars lätt till situationer där informationssäkerheten inte längre beaktas. Bélanger et al. (2017) förstärker detta budskap genom att visa att det kan leda till ogynnsamma förhållanden. Därmed kan införandet av nya säkerhetskrav försvåras eller försenas. Ormond et al. (2019) visar att det krävs insatser som gör att organisationens processer och krav inte leder till onödig frustration. Negativa emotioner leder nämligen i högre utsträckning till betydligt lägre grader av regelefterlevnad. Lowry och Moody (2015) beskriver att det är en komplex avvägning i att skapa hög grad av kontroll genom väldigt rigida riskmitigerande åtgärder, i förhållande till de potentiella reaktiva och negativt emotionellt styrda svar detta kan framkalla bland de anställda. Cram et al. (2019) beskriver att en hög grad av regelefterlevnad uppstår när anställda upplever policy och riktlinjer som rimliga, användbara och lämpliga. En hög grad av regelefterlevnad främjas även av att de anställda upplever sig kunna agera vid händelser utifrån tillräcklig utbildningsnivå och kompetens. Yazdanmehr och Wang (2016) beskriver nödvändigheten av att utforma rollerna i en organisation på ett sätt som gör att ansvar för informationssäkerheten upplevs som uppenbar och som en naturlig del i vardagen. En annan väg att förstärka individens medvetenhet kring informationssäkerhet är enligt Vishwanath et al. (2020) att hänvisa till begrepp som ”cyber hygiene”, vilket enligt författarna är en naturlig del i både arbetsliv och privatliv, utifrån en allt mer uppkopplad vardag. Donalds och Barclay (2022) visar att det även går att involvera de anställdas förmåga mer direkt för att identifiera och rapportera uppenbara hot mot organisationen. Ett exempel kan vara att de anställda deltar i att märka och rapportera misstänkta mejl. De anställdas förmåga underskattas ofta när det gäller att improvisera och hitta lösningar inom situationer där ramverk eller ledningssystem inte ger tillräcklig vägledning eller stöd. Enligt Njenga och Brown (2012) kommer kompetenta anställda att kunna improvisera i mer dynamiska och krävande situationer. De kan därmed identifiera lämpliga resurser och verktyg för att adressera ett visst problem.

2.8 Grupperspektivet

Det finns även vissa indikationer på att ett grupperspektiv är viktigt att beakta för att avgöra sannolikheten av regelefterlevnad. Vedadi och Warkenti (2020) beskriver fall där medarbetare hanterar regelefterlevnad utifrån ett flockbeteende. Detta visar sig framförallt i tidiga faser med ny teknologi, eller där det finns oklarheter kring vad regelefterlevnaden innebär. Detta kan i dessa fall leda till ett flockbeteende, att individer vänder sig till vägledning inom grupper. Yoo et al. (2020) visar att individer utifrån förmåga till handling behöver koordinera sig inom grupper för att uppnå informationssäkerhetsrelaterade mål. Att lyfta perspektivet till en gruppnivå kan leda till bättre informationssäkerhetsrelaterade resultat. Ifinedo (2014) beskriver att om medarbetarna bedömer att informationssäkerhet har implikationer utifrån en social kontext, så kommer det vara mer sannolikt att de efterlever informationssäkerhetsrelaterade krav. Yoo et al. (2020) beskriver att detta kan leda till att vissa mer opportunistiska individuella handlingar minimeras. Guo och Yuan (2012) visar att det går att använda grupperspektivet. De effekter som uppstår utgör en värdefull tillgång i att skapa motivation för de anställda att efterleva uppsatta policy och riktlinjer för informationssäkerhet. Det leder även till en bredare förmåga att hantera komplexa

händelser. Yazdanmehr och Wang (2016) beskriver att det är viktigt att ledningen verkar för att påverka de sociala normer som byggts upp kring regelefterlevnad utifrån ett grupperspektiv. Utifrån detta blir även gränssnittet mellan en organisation och en leverantör viktigt. Det vill säga hur processer och samarbete sker över organisationsgränserna utifrån ett informationssäkerhetsperspektiv. Ett exempel rör förmågan till incidenthantering vid en incident som kräver kontinuitetsförmåga sett till helheten. Det innefattar då förmågor och resurser hos organisationen, hos direkt leverantör, samt indirekta underleverantörer.

2.9 Ledningssystem för informationssäkerhet

I fallet med en organisation som lagt ut delar av leveransen till en leverantör går det att anta att det blir än svårare att förutspå säkerhetsmedvetenheten. Avtal som upprättas är antagligen inte tillräckliga för att säkerställa en tillräcklig nivå av informationssäkerhet. Detta kan potentieras i fall där det ej utförs återkopplande aktivitet och rapportering, eller där avtal fokuserar på en begränsad världsbild som inte tar hänsyn till helheten. En del i att skapa en mer heltäckande holistisk informationssäkerhetsförmåga är att införa en variant av ett ledningssystem, som då tar hänsyn till informationssäkerhet, till exempel ISO 27001. Detta kan sedan kopplas till mer detaljerad standard som beskriver relevanta dimensioner i digitala leveranskedjor. En sådan tillhandahålls av Swedish Institute for Standards (SIS, 2023). I denna beskrivs ett stort antal processer som bör uppdateras för att säkerställa förhållandet mellan organisation och dess leverantörer, genom hela livscykeln, från upphandling till avveckling av leverantör. Standarden förutsätter en helhetsöversyn genom ett stort antal processer för att säkra de digitala leveranskedjorna. Behållningen blir därmed att uppnå en godtagbar, mätbar och avvägd risknivå kopplat till de digitala leveranskedjorna.

Standarder kan inte alltid ge vägledning i vilka åtgärder som behöver prioriteras utifrån en begränsad budget. Shiau et al. (2023) beskriver att det i valet av en enskild standard kan finnas en risk för att det saknas väsentliga perspektiv som bör vara av vikt för att kunna skapa ett holistiskt informationssäkerhetsarbete. Det medför enligt Smith et al. (2010) behov för ett omfattande arbete och analys utifrån respektive organisations utgångsläge och behov, speciellt i fall då det rör införande i offentlig verksamhet. Det finns därmed enligt Smith et al. (2010) inte förutsättningar att enbart införa en standard utan att samtidigt ta hänsyn till organisationsspecifika variabler. Detta budskap förstärks även av Niemimaa och Niemimaa (2017) som visar att det krävs att standarden eller ledningssystemet kontextualiseras. Genom det tillförs en meningsfullhet eller översättning till organisationens specifika förutsättningar. Hedström et al. (2011) bidrar med att visa behovet av att förstå målkonflikter inom organisationer. Det räcker inte med införande av en standard, det krävs en mer kontextuell ansats. Cavusoglu et al. (2015) visar att organisationer som genomför en gap-analys (internal security needs assessment) i högre grad investerar och prioriterar informationssäkerhet, än organisationer som ej genomför gap-analys. Vidare är det fördelaktigt att kontextualisering sker genom brett deltagande av organisationens anställda, samt att det sker en involvering för att fånga upp de organisationsspecifika aspekterna tidigt. Andersson et al. (2022) visar även att det finns potentiella problem att helt förlita sig på det som beskrivs som ”best practice” utifrån en given standard kopplad till informationssäkerhet. Det beror på att det finns betänkanden kring i vilken mån standarder

som tas fram är tillräckligt inkluderande. Det är oklart om det leder till tillräckligt avvägda underlag för att uppnå en kontextualisering utifrån organisationen och dess omvärld. Lee et al (2016) visar att väldigt specifika och högt kravställande standarder kan leda till att resurser och åtgärder används på fel sätt, att det blir hämmande och minskar graden av informationssäkerhet. Ett införande av ett ledningssystem för informationssäkerhet kan vara ett första steg att lyfta upp informationssäkerhet på ett strategiskt plan. Det påvisar då ledningens engagemang, vilket Puhakainen och Siponen, (2010) beskriver som en framgångsfaktor och nödvändighet för att säkra de anställdas efterlevnad av de regelverk som kopplas till införandet. Armenia et al. (2021) visar att ett ledningssystem kan utgöra en grund för att utföra vidare analyser. Detta möjliggör sedan i sin tur mer anpassade investeringar i de förmågor som krävs för att hantera cyberhot på ett kostnadseffektivt sätt.

2.10 Sammanfattande teorimodell

Utifrån teorigenomgången har tabell 1 tagits fram. Denna sammanfattar de dimensioner som identifierats som speciellt framträdande och intressanta i den vidare undersökningen. Tabellen utgår ifrån en modell från Checkland och Puolter (2020) som kommer att beskrivas mer i detalj under metodkapitlet. Det kan redan nu konstateras att det finns ett stort antal olika handlingsalternativ (P – What) som på olika sätt (Q – How) kommer att kunna bidra till olika ändamål (R – Why). Det är naturligt att antalet handlingsalternativ är högt med tanke på att digital motståndskraft och digitala leveranskedjor är relativt vida begrepp.

Tabell 1: Sammanfattande teorimodell (anpassad från Checkland och Puolter, 2020)

Införande av DORA förväntas leda till ökad digital motståndskraft inom samhället			
DORA påverkar målsättningar inom IS (Dhillon och Torkzadeh, 2006) Develop and sustain an ethical environment (övergripande målsättning) Ensure legal and procedural compliance (möjliggörande målsättning)		Relevanta kunskapsområden (Shiau et al., 2023) Third-party security & Data service security (direkt) Security management & Security decision-making (mer indirekt)	
P (What)	**Q (How)**	**R (Why)**	**Källa**
Tydliga klausuler vid upphandling om informationsplikt	Inför tydliga klausuler vid upphandling om informationsplikt från leverantörer om incidenter eller annan information.	För att minska risken för att ansvar är otydligt eller faller mellan stolarna.	MSB (2024)
Genomföra analys över informationsflöden och leverantörskedjor	Granska och dokumentera beroenden i organisationens informationssystem, särskilt gällande externa leverantörer.	För att veta omfattning och beroenden	MSB (2024)
Säkra incidenthantering	Planera och inför arbetssätt för hantering av incidenter i de digitala leveranskedjorna.	För att minska risken (både sannolikhet och konsekvens) för att en incident får en större påverkan.	MSB (2024) Chen et al. (2011) Yazdanmehr och Wang (2016)

P (What)	Q (How)	R (Why)	Källa
Säkra kontinuitet- och återställningsförmåga	Inför alternativa arbetssätt om något skulle inträffa en tjänst hos en leverantör, som organisationen är beroende av, för att kunna fortsätta verksamheten.	För att kunna hantera kriser eller mer långvariga incidenter.	MSB (2024)
Säkra att definitionen för digital motståndskraft är tydlig	Genom att iterera i branschforum, att svara på remisser, eller annan aktivitet som leder till samsyn.	För att minska risken för begreppsförvirring	DORA-förordningen (2022a)
Säkra att definitionen för digital leveranskedja är tydlig	Genom att iterera i branschforum, att svara på remisser, eller annan aktivitet som leder till samsyn.	För att minska risken för begreppsförvirring	DORA-förordningen (2022a)
Uppdatera uppföljning mot leverantör	Säkra uppföljande uppföljning mot leverantör som tar hänsyn till digitala leveranskedjor.	För att minska risk för att leverantör eller underleverantör inte håller avtalad nivå av IS	Xiao et al. (2013)
Höjd säkerhetsmedvetenhet genom utbildning	Kravställa utbildande aktivitet hos leverantör eller utföra utbildning i den egna organisationen.	För att minska risker för negativa händelser som utgår ifrån personers för låga säkerhetsmedvetenhet.	Williams (2011) Li et al. (2023) Yazdanmehr och Wang (2016)
Säkra relevanta SLA per leverantör	Att tydligt definiera SLA utifrån respektive tjänst som lagts ut, för att övervaka att det efterlevs. Även SLA som avser hantering av sårbarheter tex.	För att kunna följa upp och säkra att leverantören prioriterar att upprätthålla rätt tjänster.	Larson (1998) Temizkan et al. (2012)
Uppdatera avtal med leverantörerna	Att gå igenom och uppdatera avtalen med respektive leverantör, beroende på leverantörens kritikalitet.	För att minska risken att krav missats i avtal ur ett IS-perspektiv.	Larson (1998)
Säkra relevant gränssnitt med leverantör	Att sätta upp relevanta forum med respektive leverantör	För att lyfta kvalitet och kontroll ur ett bredare IS-perspektiv	Mähring (2018)
Samarbeta med andra aktörer	Dela information med andra aktörer i branschforum eller liknande	Kunna reagera snabbt och minska kostnader.	Wang et al. (2019) Gupta och Zhdanov (2012)
Uppdatera Threat Intelligence tjänst	Upphandla tjänst för hantering av sårbarheter eller händelser inom hela leverantörskedjor.	För att kunna reagera snabbt och minska risken vid händelser.	Kotsias et al. (2023)
Säkra riskhanteringen	Uppdatera riskmodeller för att ta hänsyn till hela digitala leveranskedjor.	För att undvika att risker ej beaktas.	Straub och Welke (1998) Cavusoglu et al. (2015)

P (What)	Q (How)	R (Why)	Källa
Oberoende granskning och certifiering	Tillsätta externa IS-revisorer	För att öka proaktiv riskhantering	Nuijten et al. (2018) Wall et al. (2016)
Säkra finansiering av IS	Bedöma organisationens IS-förmåga och att regelbundet återkoppla till organisationens ledning kring finansiellt behov	För att skapa förutsättningar att proaktivt leda ett riskavvägt IS-arbete	Cavusoglu et al. (2015) Wall et al. (2016) Kwon och Johnson (2014) Angst et al. (2017)
Säkra holistisk styrning	Sätta upp IS-hantering som harmoniserar med övrig styrning för organisationen	För att minska målkonflikter i styrningen.	Tsohou et al. (2015)
Säkra ledningens engagemang i IS-relaterade frågor	Exemplifiera ledningens ansvar eller annan aktivitet.	För att främja prioriteringsförmåga ur ett IS-perspektiv.	Ogbanufe et al. (2021)
Moderniserad IT	Modernisera utifrån framtagen målarkitektur.	Minskar komplexitet och ökar effektivitet.	Li et al. (2023) Pang och Tanriverdi (2022
Säkra styrning för IT-upphandling och erbjuda stöd till upphandlarna	Sätta tydliga ramar samt tillsätta resurser inom upphandling.	Enklare att upphandla tjänster (lättare att göra rätt).	Siponen och Vance (2010) Moody et al. (2018) Vance at al. (2012) Herath et al. (2014) Posey et al. (2024) Bélanger et al. (2017) Ormond et al. (2019) Lowry och Moody (2015) Cram et al. (2019)
Säkra ett relevant IS-ledningssystem	Använda anpassad version av ett ledningssystem inom ISO-serien, NIST, eller annat som är relevant.	För att säkra att ledningssystem för IS är aktuellt och relevant.	Shiau et al. (2023) Smith et al. (2010) Niemimaa och Niemimaa (2017) Hedström et al. (2011) Andersson et al. (2022) Lee et al (2016) Puhakainen och Siponen (2010) Armenia et al. (2021)

3. Metod

I detta kapitel beskrivs den vetenskapliga ansatsen som använts i uppsatsen. Metodvalen beskrivs utifrån datainsamling och tematisk analys inom ramen för fallstudien. Slutligen presenteras ett sammanfattande stycke som avser etiska, estetiska och logiska avväganden och en bedömning över hur dessa påverkat uppsatsens holistiska nytta.

3.1 Inledning

Forskningen inom informationssystemsområdet är enligt Constantinides et al. (2012) karaktäriserat av att det kan beskrivas som tvärvetenskapligt. Det innebär att det finns utmaningar i att skapa en relevans som leder till en naturlig koppling mellan teori och de praktiska aspekterna. Det kommer enligt Constantinides et al. (2012) därav behövas en ansats som leder till att det utförs en bedömning över relevansen. De mångfacetterade aspekterna i målsättningarna och syftet med den forskning som bedrivs föranleder detta, se nedan citat:

> *Such a critical questioning of the ends of IS research brings into sharper focus the need to consider all possible relevant ends—and with it the greater good that researchers, as producers of knowledge, are striving to serve. By suggesting this, we acknowledge that IS researchers will always find themselves entangled in a landscape of conflicting ends that need to be navigated—and this is exactly what makes the question of ends a serious and urgent one. We are also suggesting that such complex individual and collective problems cannot be solved by uncritically accepting only one interpretation of relevance, at the exclusion and expense of others, which may be equally important and transformative, or by bracketing these questions to be handled later or by someone else. Rather we want to suggest that these questions of conflicting ends are intricately tied to all aspects of our research practice and need to be reflected upon, and explicitly dealt with by every researcher. In other words, we believe there is a need for a framework which might guide IS researchers to consider and address this intricate landscape of conflicting ends in an explicit and justifiable way. (s. 2)*

Givet ett omfattande syfte med uppsatsen, samt de uppsatta forskningsfrågorna, bedöms angreppssättet vara applicerbart och behövligt i mitt arbete. Det innebär att även mina avvägningar behöver formuleras och beskrivas. Den ansats som beskrivs av Constantinides et al. (2012) innebär att målsättningen för forskning bör bedömas utifrån ”maximal holistisk nytta” (översatt från The Highest Good) som uppstår i gränssnittet mellan etiska, estetiska och logiska avväganden. Det tillkommer även en dimension kring maktrelationer som uppstår genom den utförda forskningen. Jag kommer utifrån mina metodrelaterade avvägningar att beskriva implikationerna, vilken återfinns i slutet av detta kapitlet under stycke 3.5.

3.2 Vetenskaplig ansats

Det finns ett flertal olika vägval som kommer att påverka undersökningen och som därmed även påverkar arbetets möjligheter att skapa en holistisk nytta. Gregor (2006) sammanfattar ett antal steg och vägval för att identifiera en rimlig ansats givet det aktuella forskningssyftet och de uppsatta forskningsfrågorna. Gregor (2006) beskriver även vidare att själva ställningstagandet kring den väldigt abstrakta nivån med ontologi, exempelvis mellan positivism och hermeneutik, inte är det väsentliga i sig. Detta stöder även Jacobsen (2002) som beskriver att det finns fog att sammanbinda perspektiv genom att i stället för begreppet sanning hänvisa till begreppet intersubjektivitet, det vill säga en mer pragmatisk typ av ansats. Med begreppet intersubjektivitet avses enighet mellan individer, i stället för begreppet absolut sanning. Användandet möjliggör en undersökning av individernas delade upplevda verklighet, vilken även är skild från forskarens subjektiva upplevelse.

Som redan konstaterats i problembeskrivning och teoretiska bakgrund är att begreppet informationssäkerhet och tillhörande underbegrepp komplexa till sin natur. Ett område som innebär förändrade krav inom gränssnittet mellan organisation, dess direkta leverantörer, samt indirekta underleverantörer, kommer nödvändigtvis innebära att det finns flertaliga världsbilder och tolkningar. Detta potentieras sedan även av att det finns ytterligare intressenter som till exempel tillsynsmyndigheter och ämnesspecialister. Dessutom är införandet av kraven pågående under tiden då uppsatsen skrivs. Utifrån detta är det fördelaktigt med en vetenskaplig ansats utifrån ett systemperspektiv, vilket Jackson (2003) beskriver:

> *The only way we can get near to a view of the whole system is to look at it from as many perspectives as possible. Subjectivity should be embraced by the systems approach (s. 139)*

Samtidigt finns det ett värde i att återanvända de perspektiv och begrepp som redan finns beskrivna inom litteraturen. Att återanvända redan befintlig kunskap inom ett område som informationssäkerhet bedöms leda till att högre grader av holistisk nytta uppnås. Utifrån denna bedömning har en abduktiv ansats valts. En abduktiv ansats innebär enligt Bryman och Bell (2017) ett tredje alternativ för att övervinna begränsningar som uppstår inom strikta deduktiva eller induktiva ansatser. En abduktiv ansats erkänner forskarens begränsade förmåga till mekanistiskt rationellt handlande och fokuserar i stället på en mer kognitiv och iterativ process för teoriutveckling. Det är en process där olika förklaringsgrunder undersöks för att slutleda konkurrerande förklaringar eller tolkningar. Det innebär därmed en öppning som tillåter att oväntad kunskap växer fram.

3.3 Metodval

Gregor (2006, s.634) beskriver ett antal teoribildningsalternativ som valbara utifrån uppsatta forskningsfrågor och syfte med arbetet, (1) *theory for analyzing*, (2) *theory for explaining*, (3) *theory for predicting*, (4) *theory for explaining and predicting*, och slutligen (5) *theory for design and action*.

Vidare beskrivs det att det inte föreligger hinder att kombinera dessa för att uppnå bättre resultat. I mitt arbete föreligger det delvis forskningsfrågor som kopplas till de tema eller dimensioner som identifierats inom teorikapitlet. Vidare är syftet med forskningsfrågorna att ge övergripande inriktningsförslag eller vägledning för de olika aktörerna utifrån ett införande av DORA. Det innebär att en kombinerad ansats med alternativ 2 (theory for explaning) och alternativ 5 (theory for design and action) bedöms som relevanta i mitt vidare arbete.

Med tanke på beskriven komplexitet i problembeskrivningen och dess kontext, har en bedömning gjorts utifrån av Jackson (2003, s.18) beskriven modell som utgår ifrån graden av komplexitet och tillhörande divergens i intressenternas världsbilder. Jackson (2003) beskriver att en Soft Systems Methodology (SSM) är tillämpbar och lämplig i undersökningar som innebär en förväntad spridning utifrån flertalet intressenters världsbilder. Jag har utifrån detta bedömt att SSM även är lämpligt för att undersöka mina forskningsfrågor. Jackson (2003) beskriver behållningen med denna SSM i nedan citat:

> *SSM is a methodology, setting out principles for the use of methods, that enables intervention in ill-structured problem situations where relationship maintaining is at least as important as goal-seeking and answering questions about 'what' we should do as significant as determining 'how' to do it. (s.182)*

Jacobsen (2002) beskriver att en holistisk ansats kräver att fenomenen som undersöks behöver ses som ett komplext samspel mellan både individerna och deras sammanhang. I undersökningen kommer av Checkland och Poulter (2020) beskriven metod för SSM att användas. Det bedöms leda till att forskningsfrågorna kan hanteras och besvaras på ett tillfredsställande sätt. Metoden består av ett antal iterationer (eller steg) för att beskriva och hantera problembeskrivningarna. I början används verktyg som till exempel rik bild ”*rich picture*” för att ge ett sammanhang över den specifika problemställningen. Det sätts sedan upp ett antal möjliggörande åtgärder ”*purposeful activities*” som beskrivs utifrån olika aktörer givet problemställningen. Denna del kan dessutom med fördel använda kunskap utifrån redan befintlig teoribildning. Sedan testas det som tagits fram i förhållande till olika intressenters världsbilder. I denna fas kan det även tillkomma kunskap eller idéer kring hur problem bör ses eller hanteras. Här finns det utrymme att generera nya insikter utifrån identifierade åtgärder som är både rimliga och önskvärda. Det finns även förutsättningar att föreslå vidare åtgärder som intressenterna bedöms kunna leva med. Det skapar därmed en medling mellan intressenternas olika världsbilder. De möjliggörande åtgärderna kan även bedömas utifrån olika mått, såsom ”*efficacy*”, ”*effectiveness*” och ”*efficiency*”, vilka benämns som 3E. Samtliga steg som beskrivits utgör enligt Checkland och Puolter (2020) en iterativ cykel för lärdom, eller så kallad ”*learning cycle*”. Hela cykeln kan sedan återupprepas beroende på behov. Det beror i hög utsträckning på hur mycket ny kunskap som framkommer och dynamiken i den specifika situationen. Med tanke på omfattningen för denna undersökning kommer antalet iterationer att vara begränsat. Uppsatsen ger ett första lager av kunskap, som kan utökas genom flera iterationer. Dessa ytterligare iterationer inkluderas inte inom ramen för denna uppsats.

3.4 Datainsamling genom fallstudie

I denna studie har en kvalitativ metod genom fallstudie använts. Bakgrunden till metodvalet är de av Benbasat et al. (2002) beskrivna karaktärsdragen för fallstudier, vilka bedöms harmonisera väl med denna uppsats syfte och forskningsfrågor. Det ryms vidare inom det av Gregor (2006) beskrivna angreppssättet för *theory for explaining,* samt bedöms även relevant för att hantera *theory for design and action,* som en del i att utröna föreslagna vägar framåt utifrån handlingsalternativ. Enligt Jacobsen (2002) så finns det olika typer av fallstudier, där det gemensamma är att studieobjektet är avgränsat i tid och rum. Vidare konstateras det att fallstudier lämpar sig väl för att gå på djupet och att identifiera kunskap som inte varit känd redan i förväg. En potentiell nackdel är att en snävt definierad fallstudie kan innebära svårigheter i att generalisera kunskapen. Det innebär att det kan finnas utmaningar i att utifrån kunskapen generalisera samtliga insikter. Ett sätt att enligt Jacobsen (2002) hantera detta, är att skapa en kombinerad extensiv/intensiv utformning genom att använda designtriangulering. Det innebär att i ett antal steg utföra undersökning med mål om att uppnå både hög grad av generalisering och samtidigt behålla relevans. I fallet med DORA-införande och implikationer för förhållande mellan organisation, dess leverantörer och andra aktörer, är det naturligt att välja en anpassad ansats för att fånga flera världsbilder. Det ger då bättre förutsättningar att skapa relevans i den enskilda fallstudien. Designtriangulering bedöms därmed även vara ett rimligt i denna undersökning. Den kunskap som identifieras kommer att undersökas inte enbart genom fallföretaget, utan även utifrån ämnesexperter inom informationssäkerhetsområdet. Det utgör ett extra steg för att belysa, samt relativera kunskapen, som tillkommit i den initiala fasen. Genom att intervjua ämnesexperter skapas en ytterligare dimension, vilken bedöms underlätta analys och öka möjligheterna till generaliserbarhet.

3.4.1 Urval och metod

En enskild fallstudie har satts upp utifrån ett fallföretag (svensk bank) som påverkas av DORA-förordningen och som påbörjat implementationen. Fallföretaget ingår vidare i en koncern som består av ytterligare entiteter som omfattas av DORA. Företaget valdes ut medvetet. En större svensk bank bedöms vara ett väl avvägt fallföretag utifrån forskningssyftet och forskningsfrågorna. Vidare har en leverantörer som kopplas till fallföretaget valts ut att ingå i fallstudien. Ytterligare informationsinsamling genom intervjuer med ämnesexperter inom informationssäkerhetsområdet har utförts som en tillkommande del i uppsatsen. En myndighetsrepresentant har inkluderats som respondent för att ytterligare öka möjligheterna att få in väsentliga aktörers perspektiv. Urval av fallstudieobjekt och representanter för intervjuer har skett i enlighet med vad som Benbasat et al. (2002) beskriver som främjande faktorer för att skapa väl avvägda resultat utifrån det behov som forskningsfrågorna föranleder.

Med tanke på omfattningen i forskningsfrågorna går det att argumentera för att det hade varit önskvärt med ännu mer omfattande urval. Främst utifrån flera företag eller organisationer som håller på att införa DORA-förordningen. I detta arbete har det gjorts en rimlighetsbedömning över att skapa praktisk hanterbarhet. I samband med det har det

beslutats att fokusera undersökningen mot en holistisk helhet med både fallföretag, leverantörer, ämnesexperter, samt myndighet. Detta har bedömts resultera i avvägd undersökning med störst holistisk nytta. Vidare bedöms det vara svårt att genomföra intervjuer i konkurrerande verksamheter. DORA påverkar ett begränsat antal större finansiella aktörer. Även om de finansiella aktörerna kanske inte konkurrerar inom just informationssäkerhetsområdet, så kan det finnas en risk att man inte gärna delger information. De etiska övervägandena skulle då dessutom försvåras avsevärt. Att använda ämnesexperter som har relevant erfarenhet, bedöms vara en rimlig ansats för att öka möjligheterna till generaliserbarhet.

Valet att använda en kvalitativ undersökning genom semistrukturerade intervjuer grundar sig i att problemformuleringar och forskningsfrågor kräver en större grad av öppenhet. Jacobsen (2002) beskriver detta som en av styrkorna med denna metod. Det finns genom ett balanserat angreppsätt bättre möjligheter att skapa relevans. En rent kvantitativ ansats genom datainsamling genom till exempel enkäter innebär risker för låg svarsfrekvens. Enligt Bryman och Bell (2017) kan det dessutom leda till att viktiga perspektiv ej fångas upp. Införande av DORA-förordningen med tillhörande krav på uppföljning och riskhantering inom digitala leveranskedjor är ett komplext ämne, vilket bedöms kräva en hög grad av öppenhet för att kunna skapa ett holistiskt värde i undersökningen.

När det gäller urval av respondenter har det funnits goda möjligheter att styra omfattning och djup. Det har varit naturligt att intervjua de personer som varit föremål för urvalet till följd av deras roll eller kompetens. Därav har urvalet helt styrts utifrån mål om relevans sett till forskningsfrågorna. Intervjuerna genomfördes på ett semistrukturerat sätt. Det innebär enligt Bryman och Bell (2017) att det även finns möjlighet att balansera perspektiven struktur och öppenhet. Med denna ansats så styrs intervjuerna för att säkerställa att viktiga teman och begrepp belyses, samt att det säkerställs att det finns en täckning för de forskningsfrågor som satts upp. Samtidigt innebär det att det finns en öppenhet att låta oförutsedda frågor och begrepp integreras i intervjuerna genom följdfrågor eller infall. Själva genomförandet specificeras i vidare detalj under avsnitt 3.4.4.

3.4.2 Om fallföretag och koncern

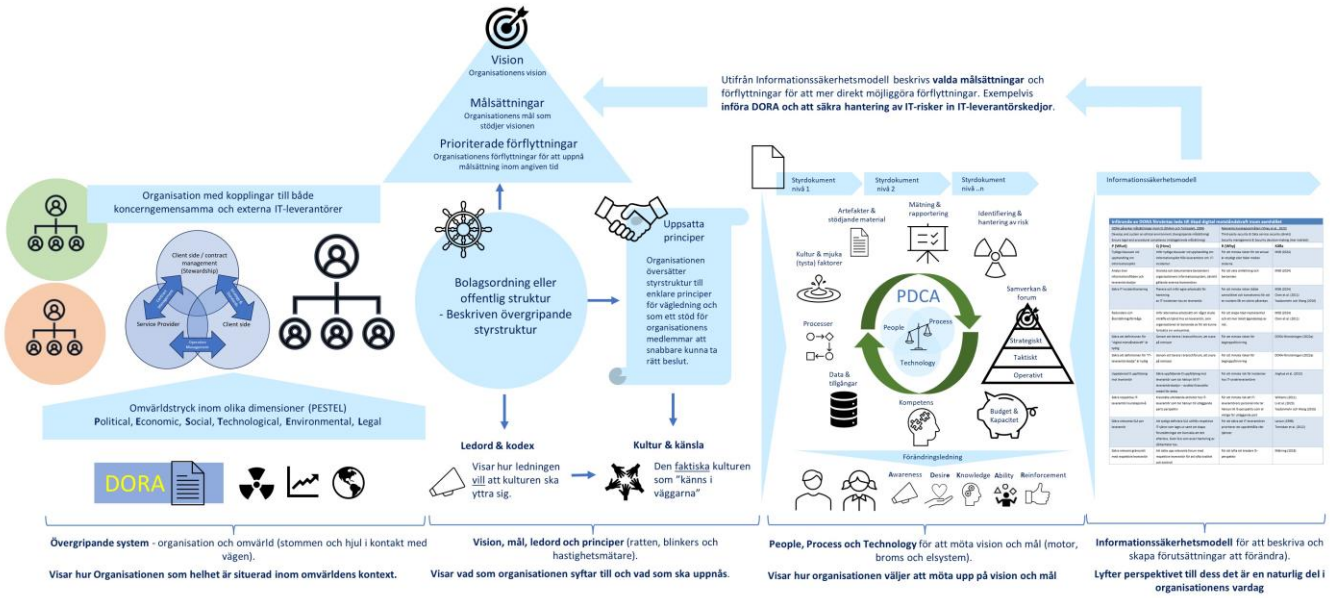
Fallföretaget är en större svensk bank som verkar inom en koncern. Koncernens främsta målsättning är att skapa digitala kundupplevelser i världsklass. Kundernas upplevelse, och framförallt begreppet enkelhet, står i centrum som målsättning för koncernens verksamhet och utveckling. Koncernen verkar för en kraftigt ökad grad av digitalisering. Det har satts upp en mer långtgående marknadsplan med tre övergripande prioriteringar:

- Konkurrenskraftig digital kundupplevelse
- Hållbara och värdeskapande erbjudanden och tjänster
- Effektiva kundmöten

För att uppnå målsättningarna inom de prioriterade områdena förtydligas förutsättningarna i uppsatt målarkitektur, genom strategiska planer och genom utvecklingsplaner. Styrningen utgår ytterst från ett konsortium som är sammansatt utav fristående konsumentägda bolag. Styrningen riktas vidare mot den övergripande koncernen och sedan vidare slutligen in till fallföretaget. Fallföretaget utgör själv en bankkoncern med ett antal dotterbolag, vilka samtliga verkar inom bank- och finanssektorn. Fallföretaget avropar och nyttjar tjänster som moderbolaget tillhandahåller. Framför allt IT-driften hanteras av moderbolaget, vilket även är en medveten strategisk förflyttning och målsättning. Moderbolaget har i sin tur upphandlat och lagt ut delar av IT-drift och annan leverans mot underleverantörer. Styrningsmässigt hanteras den internt utlagda verksamheten genom uppsatta forum, riskhanteringsprocesser och andra styrningsmekanismer. Dessa har funnits uppsatta och definierade innan det att DORA-förordningen tillkommit. Banken har även upphandlat leverans direkt från externa leverantörer.

Inom både fallföretaget och koncernen i sin helhet finns det uppsatta och befintliga processer inom informationssäkerhets- och säkerhetsområdet. Dessa innefattar även perspektiv som leverantörer och outsourcing. Det finns övergripande och omfattande riskhanteringsprocesser. Fallföretaget har sedan innan satt upp en omfattande formaliseringsgrad för att hantera externa regelverksdrivna krav, vilket även inkluderar styrdokument och kopplade utvärderande och rapporterande processer. För att skapa anpassning mot DORA-förordningen har det sedan en tid pågått insatser för att projektleda förändring och anpassning. Det har tagits in externt konsultstöd för anpassning och det finns beroenden till pågående projekt inom koncernen.

Som en del i att beskriva fallföretaget har det tagits fram en rik bild i enlighet med modell som beskrivs av Checkland och Poulter (2020). En rik bild ger stöd i att förstå och på ett mer visuellt sätt visa upp kopplingar och intressanta perspektiv. Det är även ett vidare stöd i både intervjufas och analysfas. Det ger möjligheter att bättre förstå förhållanden mellan olika dimensioner som undersöks. Samtidigt ska det inte ses som en absolut sanning som är bestående för all framtid. Se figur 2 nedan som visar sammanfattad rik bild över fallföretaget.



Figur2: Rik bild (anpassning utifrån Checkland och Poulter, 2020)

3.4.3 Om respondenterna

När det gäller respondenter för de semistrukturerade intervjuerna så valdes dessa ut enligt fördefinierad typmodell, utifrån rimlighet givet till roll som respondent innehar och utifrån uppsatsen ämne. Antalet respondenter var från början uppsatt till 10, vilket bedömdes rimligt givet komplexitet och bredd i forskningsfrågorna. Merparten av respondenterna (7) återfanns i fallföretaget eller moderbolaget. Övriga korrespondenter (3) valdes ut utifrån möjlighet till perspektiv utifrån olika intressenters världsbilder. Det kompletterades även med ytterligare respondenter allt eftersom intervjuerna påbörjats, utifrån förslag från respondenterna. Detta gjordes för att säkerställa en rimlig täckning av respondenter i förhållande till forskningsfrågorna. Ett liknande förhållningssätt beskrivs även av Bryman och Bell (2017) och ger en viss fördel då det leder till ”snöbollseffekt” som gör att insikter kan fångas, vilka inte förutsetts initialt. Samtidigt kan det leda till viss avvikelse eller färgat resultat. Då samtliga respondenter upplevs som väsentliga i att beskriva och undersöka forskningsfrågorna, är bedömningen att det varit ett rimligt angreppssätt. Se tabell 2 som beskriver respondenterna:

Tabell 2: Respondenter

Organisation	Roll, befattning eller beskrivning
Fallföretag	Ansvarig för Stabsfunktion IT
Fallföretag	Leverantörsansvarig
Fallföretag	Ansvarig Outsourcing
Fallföretag	Risk Manager
Fallföretag	Ansvarig IKT risker
Moderbolag	Ansvarig IT-säkerhet
Moderbolag	Säkerhetsstrategiskt ansvarig
Leverantör	CISO
Specialistföretag säkerhet	Ämnesexpert standardisering
Specialistföretag säkerhet	Service Provider - CISO
Specialistföretag säkerhet	Ämnesexpert bank
Myndighet	Strateg – sakkunnig DORA

Förutom de semistrukturerade intervjuerna har även en hel del intern dokumentation granskats utifrån införande för DORA-förordningen samt kringliggande styrdokument. Detta har resulterat i en högre grad av relevans utifrån intervjufrågor och påverkat genomförandet.

3.4.4 Genomförande

Intervjuerna genomfördes utifrån av Kvale och Brinkmann (2009) metod för tematisering och planering av intervjustudie. I metoden ingår det sju stadier. De första två stadierna som avser tematisering och planering har redan beskrivits i tidigare stycken. Initial förberedelse genomfördes utifrån en systematisk litteraturgenomgång. I denna identifierades relevanta dimensioner utifrån informationssäkerhetsbegreppet och dessa återfinns under stycke 2.10 som visar sammanfattande teorimodell. I planeringsstadiet informerades respondenterna med syftet för arbetet samt de aktuella forskningsfrågorna. Det återfinns i bilaga 1 en sammanfattning med text som använts i utskicket. Utifrån teorimodellen skapades det även ett utkast med frågor inför de semistrukturerade intervjuerna som återfinns i bilaga 2. I detta sammanhang kan frågorna ev. upplevas som något invecklade utifrån att det är en specifik förordning med detaljerat beskrivna krav. Samtidigt måste det påpekas att respondenterna utifrån roll har stor erfarenhet av att införa eller bedöma komplexitet givet regelverksinföranden. Syftet med intervjun presenterades även i intervjuerna. I samband med detta beskrevs det även för respondenterna att intervjuerna var frivilliga. Det beskrevs

vidare att intervjuerna skulle hållas anonyma, med undantag för de fåtal personer som granskar uppsatsen inom Linnéuniversitetet. Datum för intervjuer bokades upp för att säkerställa att nödvändig tid skulle finnas tillgänglig utifrån respondenternas perspektiv.

Intervju
Intervjuerna genomfördes på distans genom användande av teams. I alla intervjuer utom en hölls kameror igång för att kunna få en bättre dynamik i samtalen. Intervjuerna dokumenterades med hjälp av inspelningsfunktion som finns inbyggd i teams. En backupinspelning utfördes med hjälp av funktionen röstmemon som finns inlagd på Iphone 15. Innan inspelning av intervjuerna säkrade en inledande orientering att det ej uppkommit obesvarade följdfrågor på det som skickats ut, samt att formerna för intervju byggt på frivillighet. Intervjuerna iscensattes för att uppmuntra respondenterna till att öppet delge perspektiv och världsbild. I snitt tog intervjuerna 45 minuter vardera. Det upplevdes som att frågeställningarna och svaren inte stressades fram, utan att respondenterna uttömligt kunde svara på perspektiv och fördjupande följdfrågor. I slutet av intervjun hölls en uppföljning för att minska risken att respondenten upplevt att något varit oklart eller behövt förtydligas. Efter avslutad inspelning fanns det även tillfälle att yttra ytterligare information.

Utskrift
Utgångspunkten för utskrift av intervjuer var att använda i teams inbyggd funktion för transkribering. Genom detta automatiseras transkriberingen i ett väldigt grovt format. Utifrån detta gjordes sedan en noggrann genomgång för att renskriva och rätta till direkt felaktiga uttryck, ord, eller meningar, som skapats i den automatiska transkriptionen. Det tog uppskattningsvis 4 timmar per transkription att skapa denna mer noggranna utskrift. Då forskningsfrågorna inte rör samtalsanalys, gjordes valet att skapa en utskrift utifrån en skriftspråklig karaktär. Det innebar att utskrifterna justerades för att undvika upprepningar, eller mer talspråkliga ord. Vissa ord som skulle kunna röja personens identitet, eller som skulle kunna anses känsliga omvandlades för att minska riskerna för detta. Ändringarna gjordes utifrån perspektivet att öka kvalitet och läsbarhet, och syftade således inte till att förändra respondenternas uttryckta åsikter. I fasen för utskrift skapades det även ett kompletterande dokument med anteckningar som avsåg att underlätta analysfasen, utifrån speciellt intressanta teman och vidare kodning.

Analys
Analysfasen bestod av att utskrifterna tematiserades utifrån en meningstolkning, för att skapa möjliget att kategorisera eller koda informationen till mer koncentrerade begrepp. Då en abduktiv ansats valts i arbetet utfördes en grundläggande kodning utifrån teorimodellen som presenterades under stycke 2.10, vilket då kan anses vara en begreppsstyrd kodning. Detta kompletterades med en datastyrd kodning för att fånga upp perspektiv eller tema som inte ryms inom den framtagna begreppsmodellen. Kodningen användes även för att koppla begreppen till aktör. I de fall där begreppen var mer allmänna, eller där samtliga intressenter uttryckt likande åsikter, så kopplades dessa till en övergripande nivå. För forskningsfråga som avser internt utlagd verksamhet skapades det ej en ytterligare separat kategorisering eller kodning. Forskningsfrågan använder till stor del begrepp eller koder utifrån den

tidigare beskrivna kodningen som avser hinder och möjliggörande åtgärder. För forskningsfrågorna kring begreppen digital motståndskraft eller digitala leverankedjor så mynnar dessa till stor del ut i en kod för ett hinder (otydliga definitioner). Det finns även tydliga kopplingar till en stor mängd koder utifrån möjliggörande åtgärder.

Verifiering och rapportering

Verifieringen utgår ifrån att bedöma intervjuresultatens validitet, reliabilitet och generaliserbarhet. *Reliabilitet* beskriver i vilken mån resultaten kan anses vara tillförlitliga eller konsistenta. *Validitet* avser graden av giltigheten, eller sanningsenligheten samt styrkan i intervjuresultaten. Begreppet *generaliserbarhet* avser om intervjuresultaten enbart är av ett lokalt intresse, eller om de är relevanta även skulle kunna överföras på andra situationer eller i ett större sammanhang. Sammantagen diskussion utifrån dessa tre begrepp presenteras i slutet av uppsatsen under stycke 5.2, vilket visar forskningsbidrag och metodreflektion. Själva rapporteringen av intrevjuresultaten framgår i nästa kapitel som avser empiri och analys. Målet har varit att skapa en läsbar produkt som ger ett värde för läsaren, men som även motsvarar medveten vald metod och som motsvarar vetenskapliga kriterier.

3.5 Etiska, estetiska och logiska implikationer

I tabell 3 återfinns bedömning utifrån Constantinides et al. (2012) modell. Modellen har applicerats på de mer övergripande val som utförts i undersökningen. Mindre metodval finns även beskrivna och motiverade i den löpande texten genomgående i hela detta kapitel.

Tabell 3: Bedömd holistisk nytta (anpassad från Constantinides et al., 2012)

Val eller ansats	Logisk implikation	Etisk implikation	Estetisk implikation	Bedömd holistisk nytta
Intersubjektivitet, ej ren positivism eller hermeneutik	**Fördel:** Kan möjliggöra undersökning även om forskaren ej är specialist., att resonemang kan bedömas oavsett utförare. **Nackdel:** Kan leda till något mer begränsade slutsatser då det kräver att det finns någorlunda harmoniserande delade perspektiv eller begrepp.	**Fördel:** Möjliggör deltagande och att respektive respondent får presentera sitt perspektiv. Ökar relevansen i det som analyseras. **Nackdel:** Kan leda till att vissa perspektiv eller åsikter som enskild respondent har inte blir relevanta och belysta i analysen.	**Fördel:** Ger en mer hållfast beskrivning utifrån de begrepp som kvarstår genom analys och slutresultat. **Nackdel:** Kan leda till att arbetet upplevs som begränsat.	**Sammantaget är bedömningen att ansatsen med en intersubjektiv ansats ger en avvägd och rimlig väg att hantera arbetet och inte leder till för stora begränsningar i arbetets holistiska nytta.**
Användning av en abduktiv ansats	**Fördel:** Leder till att minskade begränsningar som rent deduktiva eller induktiva ansatser medför. **Nackdel:** Skulle kunna leda till att det är svårt att avgöra när tillräckligt med material har insamlats.	**Fördel**: Innebär att respondent och forskare itererar öppet i en dialektisk dialog för att minska missförstånd. **Nackdel:** Kan leda till att mycket kraft läggs på att identifiera/hantera missförstånd. Det kräver hög noggrannhet och objektivitet för att skapa goda förutsättningar.	**Fördel:** Ger större sannolikhet att identifiera nya och djupa insikter, vilka annars hade missats. **Nackdel:** Kan leda till resultat som justerats i för stor grad utifrån nya insikter.	**Sammantaget är bedömningen att en abduktiv ansats är rimlig med tanke på forskningsfrågorna samt IS som område. Det ger en rimlig ingång till att återanvända relevanta IS-perspektiv, men att samtidigt behålla öppenhet för nya insikter.**
Fallstudie genom designtriangulering	**Fördel:** Ger fördelen att i flera steg kunna utföra undersökningen och dra flera typer av slutsatser. **Nackdel:** Tar längre tid och det är inte säkert att det leder till ett bättre resultat.	**Fördel:** Kan innebära att det blir enklare att dela upp respondenter utifrån fas för arbetet, vilket då underlättar deras input i intervjuer eller liknande. **Nackdel:** Kan innebära att respondenter inte kan påverka hela studiens resultat genom medverkan.	**Fördel:** Bör leda till bättre förutsättningar att kunna både generalisera och skapa djupare relevans i det enskilda fallet. **Nackdel**: Kan leda till att tid avsätts till något som trots insats inte blir generaliserbart.	**Sammantaget är bedömningen att de potentiella fördelarna med angreppssättet överväger nackdelarna.**
Kvalitativa och semistrukturerade intervjuer	**Fördel:** Ger forskaren möjlighet till att besvara forskningsfrågor som kräver viss grad av öppenhet. **Nackdel:** Tar längre tid att sammanställa än en kvantitativ undersökning och ger därmed ett litet urval.	**Fördel:** Det finns möjlighet till att belysa följdfrågor eller att hantera oklarheter för att minska risken för missförstånd. **Nackdel:** Kan leda till förhastade slutsatser och att enskilda perspektiv väger för mycket i frågor som det är svårt att skapa generaliserbara insikter utifrån.	**Fördel:** Ger en fördel i att kunna styra innehåll i intervjuer och att samtidigt hålla öppenhet för att hantera nya insikter. **Nackdel:** Kan leda till låg grad av generaliserbarhet eller att det missats delar i att sätta upp den strukturerade delen av intervjuerna.	**Bedömningen är att de potentiella fördelarna med angreppssättet överväger riskerna som nackdelarna innebär. Det är rimligt givet forskningsfrågorna och komplexiteten i IS som område.**

Val eller ansats	Logisk implikation	Etisk implikation	Estetisk implikation	Bedömd holistisk nytta
Användning av SSM	**Fördel:** Ger möjligheter att skapa insikter som faktiskt är användbara och som leder till direkt förändring. **Nackdel**: Kan innebära nackdel då det tar hänsyn till att medla flera världsbilder och kräver aktivt deltagande.	**Fördel:** Erbjuder en ansats där flertalet världsbilder välkomnas, ju fler desto bättre. Beskrivs som en modell med väldigt brett användningsområde. **Nackdel:** Kan innebära att det tar lång tid att medla mellan världsbilderna.	**Fördel:** Har en möjlighet att fånga in väldigt mycket data och stor öppenhet. **Nackdel:** Kan innebära att det är omöjligt att medla mellan olika världsbilder, vilket då leder till att resultat inte ger ett högt värde.	**Sammantaget ger ansatsen en möjlighet att fånga in flera världsbilder. Det krävs viss medling och hög grad av aktivt deltagande för att skapa ett rimligt resultat. Då jag i mitt arbete är anställd av fallföretaget bedöms fördelarna väga upp nackdelarna.**
Urval i intervjuer (snöbollseffekt)	**Fördel:** Kan leda till att insikter fångas upp vilka inte var kända från början. **Nackdel:** Kan leda till ett förlopp som tar längre tid än vad som varit känt från början.	**Fördel:** Leder till att perspektiv fångas upp under arbetets gång på ett organiskt sätt. **Nackdel:** Kan leda till påverkan då respondenter med visst intresse föreslår fler respondenter med samma intresse.	**Fördel:** Kan leda till att insikter fångas upp vilka inte var kända från början. **Nackdel:** Skulle kunna leda till ett färgat resultat.	**Då samtliga respondenter upplevs som väsentliga i att beskriva och undersöka forskningsfrågorna är bedömningen att det varit ett rimligt angreppssätt.**
Intressekonflikter och annat som avser makt (Power relations)	Det uppstår ett antal frågeställningar då jag är anställd i fallföretaget och om det kan färga eller påverka resultatet. Utgångspunkten har varit att vara öppen med att arbetet sker utifrån ett högre samhällsvärde och att det trots allt är frågor som hade behövts hanterats oavsett detta faktum. Utifrån ett SSM-perspektiv är det tvärtom önskvärt eller nödvändigt med involvering. Det ger då möjlighet att verkligen driva förändring. Även intervjuer kan innebära risk för färgning. Forskningsfrågorna, syfte för uppsatsen, samt övergripande tema för intervjuerna delades innan respektive intervju. Det har beskrivits för respondenterna att undersökningen varit frivillig och att muntligt samtycke inhämtats i samband med intervjuerna. Det har även säkrats att undersökningen anonymiseras och att personuppgifter kopplat till undersökningen ej spridits utanför det som krävs för uppsatsen syfte. Detta för att undvika onödig påverkan på respondenterna. Det går aldrig att helt utesluta risk för färgning. Åtgärderna som införts för att minska risken för färgning är i min uppfattning tillräckliga. En annan fråga har rört det faktum att det rör sig om förhållanden mellan fallföretag och leverantör. Leverantörerna har intervjuats utifrån mer generell nivå och ej kopplade frågor till det valda fallföretaget. Det har ej ställts frågor som avser det specifika förhållandet mellan en enskild kund och specifik leverantör. Detta för att minska riskerna att svaren färgas av maktförhållandet mellan fallföretaget och leverantör. Vidare har jag själv i min roll för fallföretaget inte kontakt med de externa leverantörer vars representanter intervjuats. När det gäller intervjuer för ämnesexperter inom det oberoende konsultföretaget så har det ej observerats risker för att maktförhållande skulle påverka arbetet. Konsultföretaget hade vid tillfället för arbetet ej uppdrag med fallföretaget. I detta fall var frågorna dessutom på väldigt hög och abstraherad nivå.			

4. Empiri och analys

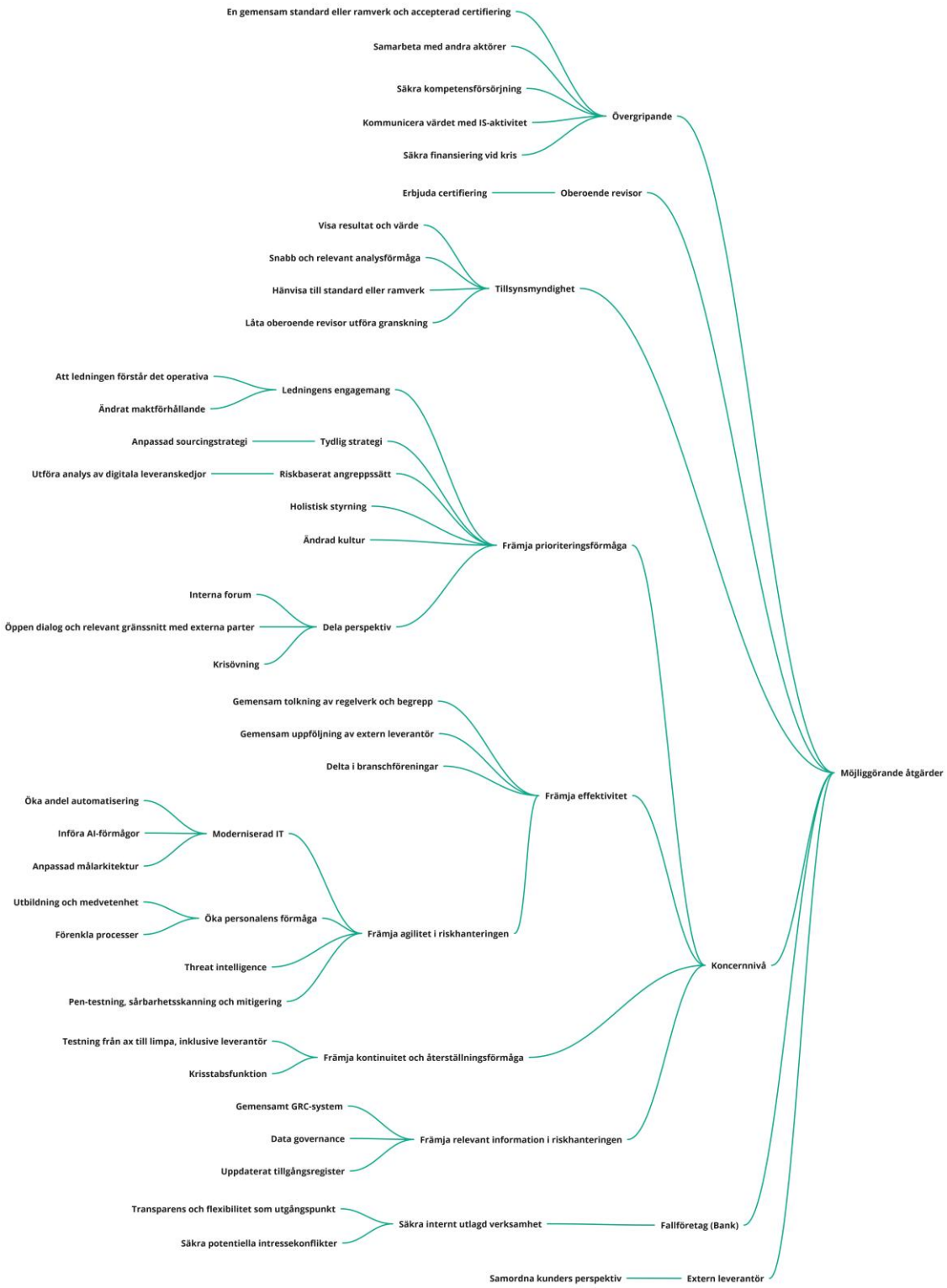
I detta kapitel presenteras intervjuresultatet. Kapitlet inleds med en visuell presentation av de tema som framkommit i undersökningen, kopplat till både hinder och möjliggörande åtgärder. Sedan följer en beskrivning av vad som framkommit kring begreppen digital motståndskraft och digitala leveranskedjor. Efter detta analyseras potentiella hinder som ett DORA-införande kan innebära utifrån de olika aktörernas perspektiv. Sedan analyseras de möjliggörande åtgärder som identifierats i samband med DORA-införande utifrån de olika aktörernas perspektiv. Det är även invävt ett separat stycke med implikationer utifrån internt utlagd verksamhet inom koncernen.

4.1 Inledning

Den tematiska analysen resulterade i ett stort antal dimensioner som bedöms vara relevanta för en vidare djupdykning. Det identifierades ett stort antal hinder. Figur 3 visar de teman som identifierats utifrån att de hindrar den digitala motståndskraften. Samtidigt visar tematisk analys att det även finns ett stort antal möjliggörande åtgärder. Figur 4 visar de teman som identiferats som möjliggörande åtgärder för att främja den digitala motståndskraften. Sammantaget är hinder och möjliggörande åtgärder vågskålens två ytterligheter, vilka utifrån fallföretagets och övriga respondenters perspektiv är väsentliga att beakta när digital motståndskraft i digitala leveranskedjor belyses. Vågskålen kan tippa över åt endera sida, beroende på aktörernas sammantagna handlingar. Det betyder att en djupdykning och samtidig beskrivning av helheten bedöms relevant för att ge aktörerna möjlighet att ta medvetna beslut. Detta är en av vägarna för att främja en digital motståndskraft i systemet som helhet. Samtliga respondenter i intervjuerna framförde att tillkommande regelverk innebär en komplexitetshöjning som kräver en medveten ansats och medvetna beslut. Sedan har respektive respondent framfört olika teman som de ser vara speciellt värdefulla att beakta. Vissa teman har återkommit övergripande och får då ett utökat utrymme i analysen.

I min rapportering har jag använt av Nylén (2005) beskriven framställningsmetod utifrån sammanhållen fallbeskrivning. Detta kombineras med att direkt analysera och framhäva argument utifrån insikter som uppstått under arbetet med intervjuresultatet. Målet är att skapa en kontextaulisering eller tolkning av de citat som väljs ut. Då det har varit ett omfattande arbete med flera 100-tals sidor utskrifter måste jag begränsa mig till de citat som förhoppningsvis ger läsaren en välstrukturerad och läsbar produkt. I citaten som avser fallföretaget och moderbolaget har jag bytt ut roll mot en mer generell personnumrering. Detta görs då rollerna kan kännas igen inom fallföretag och moderbolag. Citaten bedöms inte vara direkt kontroversiella, men det ger ett ytterligare lager av säkerhet. För övriga respondenter så bedöms det vara väldigt osannolikt att person ska kunna identifieras, därför kvarstår en generell beskrivning av roll i dessa citat.

Figur 3: Identifierade koder för hinder till att uppnå Digital Motståndskraft i samband med ett DORA-införande



Figur 4: Möjliggörande åtgärder för att höja Digital Motståndskraft i samband med ett DORA-införande

4.2 Begreppen digital motståndskraft och digitala leveranskedjor

Redan här kan det konstateras att det finns omfattande utmaningar eller hinder kopplat till att definitioner inte överensstämmer inom olika regelverk, eller i kommunikationen från olika myndigheter. Enskilda organisationer tolkar dessutom definitionerna på olika sätt. Problematiken kommer även att beskrivas mer generellt under senare stycke som avser hinder för ett DORA-införande.

När det gäller begreppet digital motståndskraft så finns det utifrån intervjuerna en relativ samsyn på att det ger förutsättningar att direkt förstå syftet med ett DORA-införande, vilket syns i följande citat:

> *Jag tycker att det är ett bra begrepp. Det synliggör syftet på ett mycket tydligare sätt. Att det verkligen handlar om motståndskraften. (Moderbolag – person 2)*

Om det bredare begreppet digital motståndskraft används, att det inte kopplas mot det operativa som ingår en del i DORA (där O står för Operational), då finns det en viss otydlighet, vilket syns i följande citat:

> *Digital operativ motståndskraft tänker då kanske också som definitionen är? Ja, det är egentligen alla mekanismer som behövs för att ha en motståndskraft, en digital och operativ motståndskraft. Policy och procedur, men det är inriktat på digitalt så det blir framför allt inom IT-verksamheten. Om man lägger till operativt så är det egentligen inte styrdokument och sådant i första hand. Det finns redan på plats. Utan nu är det mer den operativa förmågan att både kunna förbereda sig inför, samt att kunna agera vid, en IKT riskhändelse. (Fallföretag – person 2)*

Det finns samtidigt utifrån ett NIS-perspektiv en behållning med att använda det mer övergripande begreppet om det övergripande perspektivet ska kunna behållas. Det utgår då ifrån att den finansiella sektorn även omfattas utifrån ett helhetsperspektiv, vilket beskrivs i detta citat:

> *I NIS-direktivet så handlar det om att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet, i nätverk och informationssystem, som NIS står för. Så NIS-direktivet har en liknande definition, bara att den är lite mer övergripande. Det är precis så det ska vara, eftersom NIS avser alla sektorer, inklusive den finansiella sektorn. Jag tycker att NIS-direktivets definition med syftet av vad det ska uppnå, är en bättre och mer övergripande definition på digital motståndskraft (Myndighet – Strateg – sakkunnig DORA)*

Sammantaget finns det således ingen egentlig motsättning till begreppet digital motståndskraft, med den skillnaden att DORA trycker på den operativa förmågan utifrån en utökad detaljeringsgrad.

När det gäller begreppet digital leveranskedja så visade det sig att jag själv bidrog med begreppsförvirring. I mitt utskick till respondenterna så benämnde jag begreppet först som IT-leverantörskedjor, vilket då orsakade att det inte riktigt kändes igen utifrån en bredare definition som används, det visar sig i detta citat:

> *DORA fokuserar på IKT-tjänster och tredjepartsleverantörer och den är väldigt ambitiös kopplad till tredjepartsleverantörer. Men man skulle kunna ha digitala leveranskedjor som begrepp, och sen inrikta sig på i de delarna som digitala leveranskedjor fokuserar på. Alltså mjukvara och uppdatering av mjukvara. För det kan vara säkerhetsprogramvaror och halvledare och molntjänster. Vi fokuserar på digitala produkter, i allmänhet, och NIS2 är kanske mer omfattande än vad DORA är. Så det är kanske inte så konstigt att DORA fokuserar väldigt mycket på IKT-tjänster och så vidare. Medan NIS fokuserar på hela digitaliseringsarbetet. Digitala leveranskedjor är det begreppet vi använder. IT-leverantörskedjor har jag inte hört förut. (Myndighet – Strateg – sakkunnig DORA)*

Utifrån detta har jag i uppsatsen ändrat om mitt initiala begrepp, till det vidare begreppet digitala leveranskedjor. Det betyder inte att det finns en motsättning i perspektiven utifrån att DORA har en tydligare IKT-koppling. Däremot är det ett bra exempel på att det är enkelt att gå fel i tolkningen av olika begrepp. Oavsett om man ser till mitt initiala begrepp, eller till begreppet digitala leveranskedjor, så är det trots allt tydligt att det som avses är en mycket bred definition. Respondenterna trycker även här på ökad omfattning och detaljeringsgrad utifrån ett operativt perspektiv, vilket syns i följande citat:

> *Jag uppfattar att DORA gör det ganska mycket bredare än vad tidigare regelverk har gjort det. Då tänker jag både EBA och EIOPA regelverken, där man pratar väldigt mycket om väsentliga utläggningen, att det ställs krav utifrån den utlagda verksamheten. Jag tycker att DORA gör det mer utifrån hotbilden. Att man även ska kunna se mindre leveranser eller komponenter som kan utgöra en stor risk när man till exempel tittar på managerings-programvaror. Till exempel SolarWinds-attacken, eller hur Log4j kan påverka en tredjepartskomponent, långt ner i en lösning. Jag tycker att regelverket omfamnar de perspektiven. (Moderbolag – person 2)*

Det är ett annat perspektiv som tillkommer med DORA, nämligen att det krävs omfattande förhållningssätt till att hantera de risker som kan uppstå i de digitala leveranskedjorna. Det leder till att antalet leverantörer som omfattas även ökar i antal. Detaljeringsgraden som efterkrävs är även den höjd, utifrån att fokuseringen ligger på den operativa hanteringen. Det innebär vidare att det tillkommer krav på omfattande register utifrån relationerna i de digitala leveranskedjorna:

> *Det som jag ser som helt nytt är den här typen av register, eller egentligen stora databasen, med alla relationerna. Det är ju större än leverantörerna. Det handlar ju om vilka våra kritiska funktioner är, hur de ser ut, och att kartlägga hela verksamheten utifrån det. (Fallföretag – person 1)*

Sammantaget så innebär det att både begreppet digital motståndskraft och digitala leveranskedjor täcker in DORA-perspektivet. Begreppen är då så pass breda att de innefattar helheten. Däremot så finns det alltid en risk för begreppsförvirring, speciellt i den mån det finns överlapp mellan olika regelverk.

4.3 Hinder som hämmar digital motståndskraft

Jag kommer att ta upp de övergripande hinder som framkommit i intervjuerna. Då det rör sig om en stor mängd hinder, så kommer det inte finnas utrymme att lyfta upp samtliga teman med hjälp av citat. Jag begränsar detta utifrån de teman som flest respondenter belyst, eller som bedöms vara speciellt värdefulla då de upplevts som starkt begränsande eller hindrande. Jag börjar min analys utifrån de mer övergripande teman som framkommit.

Övergripande hinder

Ett hinder som framkommit från majoriteten av respondenterna är *otydliga begrepp*. Det är värt att notera att detta inte är begränsat till begreppen digital motståndskraft och digitala leveranskedjor. Här har det funnits problem redan tidigare, vilka nu verkar förstärkas genom ytterligare regelverk som träffar den finansiella sektorn:

> *Jag tror att det är 8 olika regelverk nu som är inne. Vi bönfaller så att de synkar sig lite mer. (Fallföretag – person 2)*

> *Det råder ingen brist på begrepp, och definitioner av begreppen finns det flera av. Inte ens samma tillsynsmyndighet använder samma definitioner för samma begrepp. Det gör det jättesvårt och tidskrävande för företagen. (Moderbolag – person 2)*

Att det är ett mer generellt hinder bekräftas även utifrån ett myndighetsperspektiv. Det finns flera olika intressenter, och det försvåras även av att det finns olika lagstiftningsområden. Detta gör att *delvis överlappande regelverk* försvårar samordning och att det kan leda till begreppsförvirring. Samtidigt visar nedan citat även att det finns en förståelse för problematiken och att man lyfter det i remissvar:

> *Om man ser på MSBs remissvar på olika lagstiftning, så är det någonting vi påpekar. Att det måste synkas. Speciellt då för CER, att det kommer förslag om cybersäkerhetslag, att man när det införs måste synka det. Det är ännu mer komplicerat, eftersom det är olika direktorat, som tar fram de olika lagstiftningsområdena på EU-nivå. Så det kan vara en helt annan direktorat på EU-nivå som tar fram en lagstiftning. Som då kanske vill bestämma inom sitt lagstiftningsområde. Det är det vi ser med DORA. Då kanske de möjligtvis vill använda andra begrepp där, än vad ett annat direktorat som tar fram en annan lagstiftning på området gör. Det är viss förvirring, så är det. Men det är någonting som vi tar upp. Jag tror det är flera myndigheter och remissinstanser som lyfter det i sina remissvar. (Myndighet – Strateg – sakkunnig DORA)*

Att delvis överlappande regelverk kan skapa oreda blir tydligt utifrån att det kan innebära att det då finns otydligheter i hur överlappen faktiskt ser ut. Det kan då riskera att vissa typer av åtgärder missas, eller att tillsyn kan ske utifrån olika tillsynsmyndigheter. Det finns även en större farhåga att det tillkommer fler regelverk utifrån sektorperspektiv, vilket då skulle leda till en ohållbar situation:

> *Det är en utmaning att det är en sektorspecifik unionsrätt, och att den inte är tillräckligt synkad med NIS2 som är horisontell. Det kommer bli en väldigt stor utmaning om vi får fler sektorspecifika unionsrätter. Reglering krävs, men det får inte dämpa innovationen och digitaliseringen. Det får inte bli en överreglering. Någon gång måste det ta stopp. (Myndighet – Strateg – sakkunnig DORA)*

Det kan därmed även leda till otydligheter genom kraftigt höjd komplexitet, vilket då även ställer höga krav på förmåga att hantera rätt åtgärder utifrån ett helhetsperspektiv:

> *DORA är lex specialis i förhållande till NIS2. Det innebär att de som omfattas av DORA inom riskhanteringsåtgärder och incidentrapportering då förväntas följa DORA, det trumfar alltså NIS2. Nu är den finansiella sektorn lite speciell. Men att få sektorspecifika unionsrätter som DORA, det är problematiskt. För att om det blir liknande i annan sektor som energi eller telecom, då blir det helt plötsligt sektorspecifika unionsrätter på cybersäkerhet. NIS2 är horisontell, det gäller alla sektorer. Ska vi göra som DORA för andra sektorer, då kommer vi ha en mängd olika regleringar inom olika sektorer. De kommer inte nödvändigtvis att synka jättebra med varandra. Telecom kan ha andra krav än vad DORA har. Så att generellt är det väl problematiskt att det har blivit en DORA, för att regleringen med NIS2 är till för den finansiella sektorn med. Sen kanske DORA är mycket mer ambitiös kopplat till IKT-tredjepartsleverantörer, att man har ställt mycket mer krav där. En sektorspecifik unionsrätt kan man kanske klara. Det är det man vill inom finansiella sektorn. Men i sig är det problematiskt. Det som är viktigt här, som jag tror den finansiella sektorn kanske inte har riktigt bra koll på, eller man undviker att tala om, det är att om man inte omfattas av DORA, då måste man göra bedömningen om man omfattas av NIS2. Det tror inte jag riktigt att den finansiella sektorn tänker på, utan man tänker utifrån om man omfattas av DORA eller inte. Sen kan det vara vissa delar som NIS2 tar upp, som DORA inte lyfter upp. Då är det så att man behöver följa delarna i DORA och även omfattas av övriga delar i NIS2. Man kan då även få tillsyn för detta från båda tillsynsmyndigheterna. Att det eventuellt blir olika tillsynsmyndigheter, och att tillsynen sker utifrån olika regleringar är någonting som den finansiella sektorn kanske inte riktigt tänker på än. Det är verkligen överlappningar här. (Myndighet – Strateg – sakkunnig DORA)*

Något som blir väldigt tydligt är att *kompetensförsörjningen* som krävs för att införa DORA är en större utmaning, vilket en majoritet av respondenterna anger. Kompetensförsörjning är ett potentiellt hinder som träffar samtliga aktörer. Ett stort antal komplexa regelverk som införs närliggande i tid, leder till att det blir utmanande att säkra specialiserad kompetens inom informationssäkerhetsområdet:

Jag tror också att man inte heller ska förringa det här med kompetens. Att man pratar ju oftast kring kompetensen för dem som ska implementera DORA i organisationerna, men man behöver även ha andra kompetenser ute för att stödja organisationerna att göra det arbetet. Då kan man fråga sig, vad har samhället för ansvar i det? Eller är det bara upp till var och en att skapa kompetensen? (Specialistföretag säkerhet – ämnesexpert standardisering)

Det är speciellt utmanande utifrån offentliga sektor, där det finns specifika problem med att löneläget inte upplevs tillräckligt attraktivt i förhållande till privat sektor. I samband med detta finns det inte tillräckligt med erfarna resurser som stöttar med att utbilda mer juniora resurser. Just de erfarna resurserna har fullt upp och har väldigt hög lönenivå, vilket då gör det svårt att få in kompetensen till den offentliga sektorn. Det potentieras även av att långa ledtider med säkerhetsprövning leder till att sökande hellre söker sig till den privata sektorn:

Det är klart att det finns resursbrist och problem med kompetensförsörjningen. Det har alla medlemsstater och det har även USA. Det är något som finns globalt. Vi har det här nya initiativet med Cybercampus Sverige som ska göra en kartläggning på området, för att jobba med kompetensförsörjningsområdet. Sen har vi lite mer utmaningar än näringslivet skulle jag säga, på grund av att myndigheter ställer höga krav på säkerhetsprövning. Det gör att inte alla kan få jobb, men också att det kan ta ganska lång tid. Nu är MSB ett av de bättre exemplen, alltså att det kanske inte behöver ta så lång tid. Men ser vi på FRA, så har de ganska långa ledtider på de här säkerhetsprövningarna. Kommer du direkt från KTH, eller någon annan skola runt om i Sverige, och vill ha ett jobb direkt efter ditt din utbildning? Ja, då kanske du påbörjar en rekrytering som tar 8-9 månader, medan i näringslivet så har du kanske 3 månader. Då väljer många näringslivet för att det tar alldeles för lång tid, vilket gör det svårt att rekrytera direkt från universitetet. Sen så har vi tryckt på detta ganska mycket. Inom den här branschen så eftersöker man väldigt mycket senior personal, att du ska ha jobbat i 5 år, och så vidare. Man lägger inte tiden på att ta in någon mer junior och lära upp dem. Det är ett problem också. Även om en myndighet tar in en junior, och den junioren slutar när den blir senior, att den börjar i näringslivet, så bidrar det till hela samhället och hela systemet. Så man måste verkligen se det positiva med att ta in en junior. KnowIT gjorde en rapport kring kompetensförsörjningen. Det finns inte jättemycket traineeprogram inom området, det finns inte tillräckligt många kurser och utbildningar. När man ska starta upp en kurs så är det inte nödvändigtvis en utmaning att hitta folk som ska söka kursen. Det är att hitta lärare. (Myndighet – Strateg – sakkunnig DORA)

Ett annat hinder som beskrivits i förhållande till DORA är att det är *kort tid för implementering*, vilket då även förvärras av just att kompetensförsörjningen är svår att hantera. Dessutom upplevs det att det sker *stora förändringar efter konsultation*. Det vill säga att kravställning och den praktiska omsättningen försvåras av att det kan komma att ske större förändringar allt eftersom införandet av DORA fortskrider:

Om man tittade på konsultationspapprena och gjorde implementeringar efter det, så ligger man lite dåligt till. För det har faktiskt skett en hel del förändringar, framför allt på incidentsidan och på risk-managementsidan. Sen tredje part en viss del också faktiskt. Men sen har du då de andra fem som är kvar, som är i konsultation fortfarande, där det förmodligen någon gång efter en sommarsemestrarna kommer komma en final draft. Det är ganska kort implementeringstid. (Specialistföretag säkerhet – Service Provider – CISO)

En annan effekt som har framkommit i flera intervjuer är att införande av DORA kan leda till att *koncentrationsrisker ökar* i det finansiella systemet som helhet. Det beror på att omfattande regelverk kan utgöra inträdesbarriärer för nya företag inom den finansiella sektorn. Det kan dessutom leda till att redan befintliga mindre aktörer, eller även befintliga banker, inte längre förblir konkurrenskraftiga:

Det kan absolut finnas en risk att techbolag eller start-up, inte väljer att gå in mot den finansiella sektorn. Att det kan hämma. Jag hade kontakt med någon tidigare som höll på med ett techbolag. De sade att, nej, vi kör inte mot finansbranschen. Det är för hårt reglerat. Så det är ju såklart att det är ett hinder. Ja, det finns nog en ganska stor risk för att man slår ut de mindre. (Fallföretag – person 4)

Vad har vi i Sverige, 35 banker tror jag, någonting sådant? Hur ska de mindre mäkta med och upprätthålla personal eller lokaler? Det är lite samma tema. Man säger att regleringen ska vara konkurrensneutral. På något sätt är det svårt att verkligen vara det. (Fallföretag – person 2)

Hinder på tillsynsmyndighetsnivå

En risk som förstärks i samband med att DORA, eller genom att annan mer detaljerad reglering tillkommer som avser hantera stora mängder insamlad information, är att den *aggregerade informationen inte skyddas tillräckligt*. Det är stora mängder av detaljerad information som aggregeras ihop på dels nationell nivå, dels utifrån hela EU-perspektivet. Det gör att den informationen blir betydligt mer värdefull för en illasinnad aktör. Det skapas stora incitament att komma över informationen och att sedan använda den i mer riktade och anpassade attacker. Det gavs ett par exempel i intervjuerna på situationer som upplevts osäkra med tanke på informationens känslighet och undermåliga skyddsåtgärder utifrån tillsynsmyndigheters håll:

Tillsynsmyndigheten ville att man skulle transportera via vanligt webbinterface som var vad jag minns 128-bitars kryptering. Vi sa att det där får ni nog tänka till om. Vi tänker inte skicka någon information med 128-bitars kryptering som rör våra kunder. Då finns det stor risk att vi bryter mot GDPR. Det är inte en situation vi vill ha. Då blev det bollande fram och tillbaka och så enades man om en helt annan standard till slut. (Specialistföretag säkerhet – Ämnesexpert bank)

Utifrån att det kommer att ske mer omfattande registerinsamling och uppföljning från tillsynsmyndighetens sida, i detta fall Finansinspektionen, samtidigt som informationen inte alltid uppdateras med omedelbar verkan, finns det en risk för att det bir *inaktuell information*. Det kan potentieras av att det finns långa ledtider i informationsinsamlingen. Tills dess att informationen når en aggregering på EU-nivå är frågan om den egentligen blir användbar utifrån syftet med informationsinsamlingen. En annan dimension som identifierats i intervjuerna är att det rör sig om *ökad omfattning av detaljerad information* som efterfrågas. Tillsynsmyndigheterna behöver naturligtvis ha en förmåga att hantera detta. Samtidigt behöver tillsynsmyndigheten även hantera de mer övergripande krav som DORA innehåller. Det innebär att det krävs ett förhållningssätt att kunna bedöma mer vagt formulerade krav, att därigenom kunna uttala sig vid en tillsyn eller för att ge rekommendationer. I det fallet kan det finnas hinder utifrån *oklara bedömningsgrunder:*

> *En konsultkollega som är jurist brukar alltid använda exemplet att du kommer ut på motorvägen och det står lämplig hastighet på hastighetsskylten. Sen så efter 1 km blir du stoppad. Polisen säger att du körde för fort. Du säger att, nej, det tycker jag inte att jag gjorde. Den här diskussionen kan fortsätta i all oändlighet. Väglag, fyrhjulsdrift, nya däck, motorväg med räcken, och så vidare. Hur ska de då kunna argumentera för att du har kört för fort? De kommer att bli svårt. Man kan se så också på säkerhetsskyddet. När man har tittat på granskningar av säkerhetsskyddet så är det ju oftast på sådana punkter som är binära och innebär val, ett eller noll. Att har man gjort det eller har man inte gjort det. Det är det man går på i första hand. Det är mycket enklare. Det är mycket enklare att ta en sådan fråga mot dig. Har du gjort granskningen? Utav den här enskilda delen? Ja, eller nej? Om svaret är nej, då åker du på sanktion. Men har jag gjort granskning och att de anser att den inte har varit tillräckligt kvalitativt bra, då har de svårt att argumentera i bedömningen. (Specialistföretag säkerhet – ämnesexpert standardisering)*

Ett hinder som framkommit är att den ökade detaljeringsgraden och de oklara bedömningsgrunderna resultera i önskan om mer information, feedback och stöd tillbaka från tillsynsmyndigheten. Det verkar enligt vissa respondenter finnas en *avsaknad av stöd*. Samtidigt finns det en viss behållning med att hitta en balans i perspektiven kontroll och stöd, alltså att tillsynsmyndighetens roll inte enbart kan bestå av stöd. Det som dock blir tydligt genom intervjuerna är behov av mer praktisk och teknisk vägledning utifrån den ökade kravställningen ur ett informations-, teknik- och standardiseringsperspektiv:

> *Hur ska vi ta det från teori till praktik? (Leverantör – CISO)*

> *Det är en sådan där fråga som kommer upp med vartenda regelverk egentligen, det här med kommunikation. Jag tycker ju å ena sidan så behöver det kommuniceras. Det ska finnas möjlighet för diskussion och öppna samtal. Men jag är ändå av den åsikten att en myndighet även ska kontrollera en aktörs mognad, och inte lägga för många saker i munnen på dem. Men däremot så borde det kunna vara lite mer att myndigheten står för standarder. Låt säga systemstöd och sådant. Det skulle kunna komma lite mer från centralt håll. För tar man fram olika format borde man kanske också hjälpa till med det tekniska kring det? (Fallföretag – person 3)*

Sammantaget leder detta till att *tillsynsmyndighetens förmåga behöver stärkas.* Detta då både omfång och djup tillkommer som en del i införandet av DORA. Det leder till att en omfattande transformation behövs även utifrån tillsynsmyndighetens perspektiv. Det kan dras paralleller till införande av GDPR, där det tog avsevärd tid för ansvarig myndighet att öka förmågan:

> *Det är egentligen bara att titta på en liknande förordning som kommer för några år sedan - GDPR. Dåvarande Dataskyddsinspektionen [IMY] hade inte personal som överhuvudtaget förstod sig på personuppgiftshantering, eller skydd av personuppgifter. Vi kommer se att det är likadant här. (Specialistföretag säkerhet – Service Provider – CISO)*

Hinder inom koncernen som helhet

Ett övergripande hinder som uppmärksammats både utifrån fallföretag och moderbolag är för låg grad av *prioriteringsförmåga*. Detta hinder har observerats i samtliga respondenters intervjuer utifrån fallföretaget och dess moderbolag. Det är samtidigt ett mer universellt grundproblem som uppstår när krav tillkommer utifrån reglering, som inte mer direkt upplevs utgå ifrån företags vinstmaximerande perspektiv:

> *När du har begränsat med resurser, men samtidigt väldigt mycket krav, då måste du prioritera ner vissa saker för att kunna prioritera upp annat. Väldigt ofta så blir affären lidande…Sen så kan det alltid finns motstånd. För varje gång som du inför ett regelverk måste du ta resurser för någonting som skulle kunna ha lagts på någonting annat. Kanske hade banken egentligen hellre velat lägga pengar på att utveckla en ny produkt, eller utveckla mobilappen lite bättre med mer funktioner, än att tillfredsställa myndigheter. De resurserna kommer då inte att finnas. Du får du stångas med produktägaren eller systemägaren (Specialistföretag säkerhet – Ämnesexpert bank)*

Om den för låga graden av prioriteringsförmåga bryts ner i mindre delar finns det ett antal övergripande teman som dyker upp i intervjuerna. En del är att det i samband med DORA-införande och andra tillkommande regleringar upplevs vara en så pass stor ökning av komplexitet, att det nu resulterar i en problematisk dynamik. Det ska samtidigt påpekas att koncernen i sin helhet innan införandet av DORA har kunnat anses som väldigt komplex. Varje tillkommande lager av regelverk, och tillhörande samordning som krävs för att uppfylla regelverken, leder till att komplexiteten höjs. Det kan ibland kännas som en exponentiell kurva. Det vill säga att varje tillkommande krav även får en potentiell påverkan på redan befintlig struktur, processer och informationsmängder. Då DORA *ökar detaljering i uppföljningen* bidrar detta naturligtvis till denna upplevelse. Vidare leder DORA till ett *utökat omfång i antal leverantörer att följa upp*, vilket förstärker effekten. Då det dessutom sker förändringar och införande av andra regelverk, samt att *många regelverk införts på kort tid*, potentieras effekten ytterligare. Se nedan citat som kärnfullt visar att prioriterings-förmågan är väsentlig:

Har man inte mognaden att komma ner i avväganden och prioriteringar, då kan det bli ett helvete helt enkelt. (Fallföretag – person 3)

Samtidigt är det så att prioriteringsförmågan naturligtvis även blir mycket viktig i ett läge där det finns begränsningar i *kompetensförsörjningen*. Det togs redan upp i tidigare stycken, utifrån att det är ett större hinder om man ser tillgänglig kompetens på marknaden. Det är därför inte förvånande att samma problematik uppstår i fallföretaget och inom koncernen som helhet:

Vi är en bank som är väldigt medveten och tycker att regelverk är viktiga. Vi har en hög grad av riskaversion. Vi har inte särskilt hög riskaptit, utan vi har en låg riskaptit. Det gör att sådana här saker ska finnas på plats, det minskar både kundernas och bolagets risker. Det är självklart i vårt bolag. Men problemet är när det kommer med kort tidsvarsel så måste du orka. Sedan är det många regelverk samtidigt. Det gör givetvis att det kan vara svårt att hitta resurser. Vad ska du välja mellan? Så att jag skulle vilja säga att tid och resurser hänger på något sätt ihop…Det är svårt att rekrytera, alla konsulter är upptagna på hela marknaden. Så jag tror att resursfrågan är ett hinder vid sidan av tid. (Fallföretag - person 2)

I samband med intervjuerna i fallföretag och i moderbolag så identifierades även ett annat tema som är tätt knutet till kompetensförsörjningsproblematiken. Regelverksinförandet kan leda till att *kompetens försvinner*. Kanske inte då nödvändigtvis de personer som jobbar mer direkt med regelverksinförandet, utan att det sker förflyttning av annan kompetens som påverkas mer indirekt av införandet. De ser det då som en för stor utmaning och väljer att lämna fallföretaget:

Vi kan även tappa kompetens som vi köper in för att de inte mäktar med regelverket (Fallföretag – person 3)

En annan dimension inom kompetensförsörjningen är att det inom koncernen finns *personberoenden* som gör det svårt att prioritera om aktiviteter utifrån enskilda detaljerade kravformuleringar:

Om alla kunde samma saker skulle det vara lättare. Nu är det sällan så, utan det är nyckelpersoner som är på olika områden. Bara för att man drar ner på ett område, betyder det inte att den personen direkt kan hoppa över och gasa i nästa område. (Moderbolag – person 2)

Sammantaget leder prioriteringsfrågan till att det behöver göras ställningstaganden, avväganden och prioriteringar utifrån flera perspektiv. Andelen informationssäkerhet och regelverksefterlevnad måste uppnå en balans som är rimlig, som inte leder till rent onödiga konflikter och friktion i efterföljande mer operativa och utförande led. För att uppnå balans krävs ett engagemang i ledningsgrupp och styrelse. Engagemanget kan inte enbart sträcka

sig till att ange affärsmål och mål om att samtidigt efterleva regelverk. Det ger då inte tillräckligt stöd för prioritering längre ner i organisationen. Det krävs således en förmåga inom *ledning och styrelse att förstå de mer operativa konsekvenserna.* Det är en del i att nå en hög grad av mognad. Samtidigt visar det sig genom intervjuerna att just denna del av förmågan antagligen inte riktigt har införlivats ännu:

> *Jag tycker att hos oss är ledningens engagemang jättehögt. Man är väldigt mån om att skydda kundinformationen. Problemet blir snarare i vardagen för mellancheferna eller middle manangement…Problemet blir vardagen, när det är mycket som ska göras samtidigt. Utmaningen hamnar ofta på middle management. (Fallföretag – person 2)*

Ett annat mer övergripande hinder som identifierats är en *för låg grad av effektivitet*. Denna dimension är naturligtvis tätt knuten till den ökade komplexiteten. Med ökad komplexitet så ökar även antalet interaktioner samt graden av samordning. Den mer administrativa andelen för att kunna hantera den ökade komplexiteten växer lätt exponentiellt. Det medför då även att det snabbt nås en punkt där effektiviteten blir lidande och där vardagen kan kännas som ohanterbar:

> *Nu när vi gör DORA så investerar vi en hel del. Tid i aktiviteter. Jag kan inte påstå att vi investerar så mycket i system direkt. Men vi lägger otroligt mycket tid på det här nu med kostnader för externa konsulter som är inne och hjälper oss. Men samtidigt så har vi ju svångremmen som ska dras åt lite mer och vi behöver balansera detta. Så att jag tror att vi måste i varje sammanhang bara tänka på; hur kan vi göra det här effektivare? Vi måste verkligen tänka effektivitet och vi måste få hjälp att tänka effektivt tror jag. För alla kan inte bara uppfinna hjulet på egen hand. (Moderbolag – person 1)*

Ett exempel på en sådan friktion som observerats är risken för *oklara tolkningsföreträden*. Alltså vem inom koncernen som ska gå först i att definiera begrepp, eller avgöra hur samordnande aktivitet ska genomföras mer praktiskt och operativt. Ett tydligt exempel på detta ges i följande citat:

> *Bara att vi i införandeprojektet behövde ta upp att vi ska ha en princip om att vi lägger tiden på att jobba fram ett gemensamt förslag, i stället för att lägga tiden på att vara passiva och lägga krutet på att svara på en massa kommentarer i en remiss, det tycker jag vittnar om att vi har ett kulturarbete att göra. Kring var vi är effektiva tillsammans, och hur vi samarbetar. (Moderbolag – person 2)*

Frågan kring tolkningsföreträde behöver inte nödvändigtvis uppstå mellan bolag inom en koncern, utan de kan likväl uppstå även internt inom ett enskilt bolag:

Second- and third-line kommer förmodligen vilja ha tolkningsföreträdet i väldigt stor del. Då kanske det inte blir så väldigt praktiskt heller, så att det inte går att använda i first-line. Så det kommer bli en diskussion om de bitarna. Det har det redan varit i samband med andra typer av regelverk. Vem har tolkningsföreträde? (Specialistföretag säkerhet – Service Provider – CISO)

Graden av effektivitet behandlar även i vilken mån som tillgänglig personal och uppsatta processer används till värdefulla aktiviteter. Det finns en risk att ett DORA-införande, eller den sammantagna massan av tillkommande regelverk, leder till en för stor det uppföljande och kontrollerande aktivitet. Alltså det som vanligtvis benämns som compliance:

Om man tittar utifrån de olika styrsystemen, den kompetens som jobbar i de olika styrsystemen. Om man då går enligt det där klassiska plan-do-check-act, så blir det ju väldigt stort fokus på check nu, att kontrollera. Så frågan är om alla resurser styrs nu mot check. Hur mycket resurser finns det till att agera, planera och genomföra? Troligtvis kommer vi se en ganska kraftig förskjutning mot kontroll. Sen är då frågan var finns kapaciteten för att åtgärda? Var finns den proaktiva styrning kring planeringen och genomförande? Det finns ju en risk att det där blir obalanserat. (Fallföretag – person 4)

En vidare dimension som blir viktig att hantera är att effektiviteten upplevs som lägre till följd av avsaknad av systemstöd i de processer som rör informationssäkerhet eller riskhanteringen. Personer som sitter med mer manuella processer upplever detta som en hindrande faktor:

Avsaknaden av effektiva system är hindrande. (Fallföretag – person 5)

Ett potentierande hinder som kan påverka graden av effektivitet negativt är att ett DORA-införande till styvende och sist leder till *ökade kostnader*. Antalet leverantörer att följa upp ökar. I fasen med att införa DORA ökar kostnaderna för att anpassa redan befintliga förmågor. I en långsiktig förvaltningsfas behöver de aktiviteter som införs utifrån DORA förvaltas. Med tanke på detta kan effektiviteten bli lidande, speciellt om inte aktiviteterna anpassas för att ta bort överlappande processer. Detta gäller speciellt i de fall som DORA ses som en separat del och inte som en naturlig del i en helhet:

Det blir väldigt kostsamt om man ska rapportera på olika sätt (Fallföretag – person 2)

Som företag så vill man naturligtvis vara compliant. Men man tjänar inte pengarna på att genomföra en stor kampanj för snygg myndighetsrapportering. Utan det vill man ska vara så enkelt och så effektivt som möjlig (Moderbolag – person 2)

Hinder utifrån ett externt leverantörsperspektiv

Naturligtvis är det inte enbart koncernen som träffas av de utökade DORA-kraven. Även externa leverantörer och underleverantörer behöver förhålla sig till en hel del krav. Framför allt finns det ett övergripande hinder som avser att en *ökad belastning* leder till *ökade kostnader som måste föras vidare till kunden*. Mycket av problematiken kan kopplas till att *kunderna agerar själva i sin uppföljning mot leverantör*, i stället för att hantera det hela genom ett mer standardiserat angreppssätt, till exempel genom att kräva in oberoende certifiering. Det leder till att olika format för information efterkrävs, och att det blir väldigt utmanande att ta fram informationen. Det blir en stor ökning i andelen administration och det leder till högre kostnader för leverantören:

> *Just nu upplever jag att alla, eller många kunder, har tagit fram sina egna third-party-assessment-modeller. Så kommer det ett batteri av frågeställningar från kund x, och så kommer det ett annat batteri av frågeställningar från kund y, och så vidare. Vi jobbar mot att vi skall bli ISO27001-certifierade. Min dröm när vi inledde arbetet var att, ja, men då kommer vi ha ett certifikat att dela med oss. Då kommer alla vara glada och nöjda. Tyvärr tror jag inte riktigt på det längre. Det har varit en insikt i det här. Att, jo, vi jobbar då med att ta fram våra direktiv och procedurer. Vi mappar det mot ISO27001-krav, vi mappar det mot DORA-krav. Vi mappar det mot PCI-krav. Vi mappar det mot SWIFT-krav. Vi gör det på ett systematiskt sätt. Att vi skriver våra direktiv och procedurer utifrån det. Att vi beaktar alla de här kraven, från olika håll. Men jag märker ändå att kunderna har sina egna varianter. De har sina egna konsulter inblandade, alla vill sätta sin egen prägel. Sedan är det vi stackare som ska hålla svara på de där frågorna, ur alla möjliga och omöjliga synvinklar. Det känns inte hållbart. Jag ser framför mig att genomför vi hotbaserade tester, så ska vi kunna få ett certifikat, som vi sedan delar med våra kunder. Det visar att vi har genomfört den här typen av till exempel hotbaserad testning. För annars finns också risken att kunderna kommer från sina respektive håll. Att de säger, ja, nu måste vi göra hotbaserade tester, nu måste vi involvera den här leverantören i det hela också, så vi ser hela kedjan. Jag ser en risk och jag har lite ont i magen för det. Att vi kommer att ha massor med kunder, som kommer att vilja genomföra sina egna hotbaserade tester, och så ska vi vara en del av det. Det finns en risk att vi bara kommer att sitta och administrera. Det är nog medaljens baksida. Det måste snurra några varv runt det här, innan vi hittar modellen för att gå vidare. Men under en övergångsperiod, då alla är på tårna och alla vill visa framfötterna med DORA compliance, så finns det en risk att det blir alldeles för mycket administration. (Leverantör – CISO)*

Att uppföljningen är mycket mer omfattande bekräftas även utifrån respondenter i fallföretaget. Det medför krav på att kunna följa och bedöma den initiala leverantörens förmåga att hantera vidare underleverantörer:

Sen har det ju kommit en RTS också om sub contracting, där det egentligen innebär att den uppföljningen som görs idag mot direkt part, den behöver bli otroligt detaljerad mot underleverantörer också. Vid förändringar så ska du göra due diligence, så du ska också bedöma om din egen leverantör har förmåga att kunna följa upp och styra den andra leverantören. Du måste gå in mycket mer bakom gardinen än vad du gör idag. I praktiken så blir det ju ganska utmanande och omfattande. (Fallföretag – person 1)

Samtidigt har respondenter i fallföretaget även realiserat problematiken. Det blir viktigt att hitta en balans för att inte helt sänka leverantörens förmåga att kortsiktigt svara upp mot olika typer av förfrågningar:

Jag vill inte att vi tynger ner våra leverantörer. Även om man har jättemycket i det här att göra och framför allt när vi är en koncern. Att vi då inte kommer med olika frågor om samma sak, eller olika sätt att redovisa, och så vidare. Så att vi upprätthåller affärsmässighet i det här också. (Fallföretag - person 3)

Det visar sig således att leverantörerna skulle ha en behållning av att erhålla vägledning som beskriver vägen från teori till praktik. Ett hinder är att *det saknas vägledning*, vilket även försvåras av att befintliga *informationssäkerhetsstandarder som ISO27000-serien upplevs vara för bred*. Det finns därmed inte överenskommelse eller praxis inom den finansiella sektorn och utifrån tillsynsmyndigheterna att använda en *standard i uppföljningen av DORA.* De tekniska standarder som krävs ur ett informationsinhämtande perspektiv är inte satta ännu. Det som kunderna efterkräver genom uppföljande och kontrollerande aktivitet täcks inte in i *en oberoende certifiering*.

Ett vidare hinder som intervjuerna identifierat är att det kan finnas *motstånd för initial leverantör att kräva in information i efterföljande led av underleverantörer*. Det är en omfattande informationsinsamling, där det kan finnas informationsmängder som kan upplevas som ytterst känsliga att lämna ut uppåt i en kedja. Det kan i vissa fall även bero på *att avtal inte finns för att följa upp underleverantörer* längre än genom direkt underleverantör:

Om jag är banken, eller den finansiella entiteten, så har jag direkt avtal med den direkta underleverantören. Men jag har inga avtal med rank två och rank tre. För det finns i de föregående rankorna, så hur ska jag kunna gå ut och fråga dem om den här informationen? För de kommer inte svara. Det finns en hel del information där som också är känslig. Till exempel vad betalar jag som första rankens third-party för den andra ranken? Den informationen ska kunna flöda uppåt. Vill du verkligen det? Vi är en third-party, en service provider. Så vi behöver samla in den från våra underleverantörer. Då har vi fått ihop information på rank ett och två. När vi sen kommer till rank tre, blir det lite svårare. (Specialistföretag säkerhet – Service Provider – CISO)

Motståndet kan även uppstå i de fall en mindre leverantör försöker sig på att följa upp en riktigt stor underleverantör. I de fallen är det ofta så att den stora underleverantören själv hänvisar till certifikat eller annan information som tillhandahålls till samtliga kunder. Där har den stora underleverantören genom sin marknadsposition säkrat och prioriterat effektivitet för sig själv:

> *Skulle vi från vår lilla firma komma och utmana. Att nu ska vi göra en audit här, hur ni sköter DORA-compliance, så skulle de bara skratta oss rakt i ansiktet. De skulle då säga, hör ni surfa in på den där sidan, där har vi samlat våra certifikat och bevis som tillkommit genom att de har haft olika externa företag som har auditerat dem. Då är det bara det man får. Då är det väl det man får lita på då och falla tillbaka på. Där kommer vi då till att varför skulle man inte kunna komma fram till tydliga mekanismer, där Finansinspektion säger hur DORA-verifieringen ska gå till? (Leverantör – CISO)*

En annan effekt som ett DORA-införande kan innebära är *längre ledtider*. Anpassningsbarheten skulle därmed kunna begränsas. Det kan leda till konsekvenser utifrån att förändringar som är nödvändiga ur ett informationssäkerhetsperspektiv försenas, eller att åtgärder för att affärsutveckla eller effektivisera begränsas för leverantörerna. I förlängningen leder det även till effekter på kundens förmåga. I fallet där en leverantör har flertalet kunder inom den finansiella sektorn försvåras det ytterligare:

> *Det finns två olika fall kan man säga då. Ett är då om vi själva anlitar en tredje partare. Två är då att det kan också vara så att vi anlitar en tredje partner på uppdrag av en finansiell entitet. Men i bägge fallen så ska det då göras en riskanalys. Du ska göra due diligence. Är det så att det är en ”normal” förändring? Ja, då har finansiella entiteterna 30 dagar på sig att säga bu eller bä om de tycker att det här är bra. Är det en major change, om man byter ISP för att ta ett exempel, då är det 60 dagar. Det gör att hela den här uppköpsprocessen förlängs med 30 eller 60 dagar. För inom den tidsperioden ska du ha fått informationen från den finansen entiteten. Om det då är som i vårt fall, med flera finansiella entiteter som är våra kunder, då ska alla säga ja till det här. Vad händer om någon säger nej? Det är inte prövat, det är det ingen som vet. (Specialistföretag – Service Provider – CISO)*

Det sista hinder som jag tänker belysa rör att det finns *en oklar hantering i den månen en leverantör agerar på flera EU-medlemsstaters marknader*:

> *Om du ska rapportera det här, då gör du det till den competent authority, som oftast är nationell. Men om du då har en business som är över flera EU-länder, ska du då rapportera till varje competent? Eller är det så att du rapporterar alltihopa till en, och att den sedan ska dela informationen med andra? (Specialistföretag – Service Provider – CISO)*

4.4 Möjliggörande åtgärder som stärker digital motståndskraft

Med tanke på de mer eller mindre omfattande hinder som beskrivits, är det naturligt att samtidigt beskriva möjliggörande åtgärder som främjar stärkt digital motståndskraft. Jag har här samma presentationslogik, där åtgärderna presenteras utifrån ett övergripande perspektiv först och sedan utifrån tillsynsmyndigheten. Efter detta kommer denna presentation dock att skilja sig åt utifrån de tidigare beskrivna hindren. Det har tillkommit en aktör, den oberoende revisorn. Det beror på att identifierade hinder föranleder ett behov av att få med denna aktör som en ytterst vital beståndsdel i att främja den digitala motståndskraften. När det gäller koncernen så har de flesta åtgärder inordnats precis på samma sätt som för avsnittet kring hinder. Det finns dock vissa perspektiv som avser själva fallföretagets, det vill säga bankens, direkta förmåga. För att säkra internt utlagd verksamhet, där moderbolaget även agerar leverantör, måste det finnas mer oberoende åtgärder kopplat till beställarorganisationen. Banken måste här kunna agera oberoende av koncernperspektivet för att undvika intressekonflikter. Det tillkommer således ett avsnitt för att belysa dynamiken med internt utlagd verksamhet.

Övergripande möjliggörande åtgärder

Något som verkligen framträder i majoriteten av intervjuerna är behovet av sammanhållen *gemensam standard eller ramverk samt accepterad certifiering* utifrån framförallt uppföljningsperspektivet mot leverantörer. Här är det främst leverantörerna själva som yttrat önskan. Det är hos dem som den ökade belastningen medför en väldigt problematisk situation. Framförallt mindre leverantörer verkar här se fördelarna, de riktigt stora leverantörerna använder hittills en marknadsposition för att erbjuda kunderna fördefinierad uppföljning.

> *I PCI och SWIFT-världen, där vi har de här certifieringarna från extern part, klarar vi oss väldigt långt med att dela med oss av attestation-of-compliance som ett bevis. Skillnaden kan man säga nu då mellan ISO27000 och PCI-världen är att PCI-världen har mycket mera detaljerade krav. Är man då compliant, så kan man bedöma företaget som kommer med sitt certifikat. Att mer på detalj ser att de följer ett specifikt krav. ISO27000 är lite mera mambo-yambo, om jag nu får uttrycka mig på det sättet. Att där är det mera att man certifieras på att du gör som du har sagt att du ska göra. Sen rent säkerhetsmässigt kan du ligga på helt olika nivåer på en skala med ganska brett omfång. Med ISO2700 har du bestämt lite mer själv, att det här är vår säkerhetsnivå, så här har vi tolkat de där uttalanden, och så vidare. Då kommer kunderna kanske ha lite svårt att acceptera det. Då kommer de hålla kvar sina egna assessments och auditeringar. DORA, ja, det kanske till viss del är lite mera konkret. Men jag ser väldigt mycket mappningar mot ISO2700 även i DORA. Där det är lite samma, med att du ska tolka. Du behöver själv avgöra, vilken nivå man lägger sig på för att anses compliant. Men för att slippa bort ifrån all överloppsbyråkrati så är det väl sannolikt så, att det behöver gå mot en sådan här oberoende, auditering skulle jag misstänka. (Leverantör – CISO)*

I detta sammanhang är det viktigt att det blir till en standard eller ramverk som har en tillräckligt hög grad av detaljeringsnivå för att kunna accepteras. Det kommer således också att bero på i vilken mån man kan komma överens om de mer tekniska standarder som krävs ur ett uppföljningssyfte. Sedan måste det påpekas att det finns många viljor i det här. Det finns olika typer av standard och aktörer som antagligen skulle trycka på för att få till just sin standard. Ska en standard ligga på EU-nivå, på nationell nivå, eller på branschnivå? Hur kan den drivas fram och vem kommer att hålla i taktpinnen? Det finns mycket oklarheter och osäkerhet:

> *Vi har ISO-standarderna och i USA har de NIST. I arbetet med framtagandet av NIS2 så har vi försökt synka det med ISO-standarderna så mycket som möjligt. Även koppla det till NIST, för att kunna samverka med bland annat USA. Men vi ser också med ett försök från kommissionen att sätta sina egna standarder. Om jag ska ge en personlig åsikt så tror jag att det kommer bli mer och mer så. Alltså att kommissionen försöker sätta sina egna standarder och sina egna krav. Att det kommer bli mer och mer så inom EU. Det tror jag. Om man ser till digitaliseringen med techföretag, de tillkommande kraven, och lagstiftning som skapas, så ser vi ändå liknande utveckling på cybersäkerhet. Det finns väl en vilja att sätta sig i den ena standarden. Vi får se vad som händer. (Myndighet – Strateg – sakkunnig DORA)*

Det skulle även kunna finnas en privat lösning utifrån att branschspecifika standarder tas fram. Behovet verkar finnas specifikt utifrån uppföljning mot leverantör. Men sedan kan det även finas ett motstånd till att driva fram standarder. Det visas i nedan citat:

> *Vi försökte ju för massor med år sedan utifrån standardisering att ta fram en standard för den finansiella marknaden, alltså för bank och försäkringsbolag. Men de har varit väldigt njugga. Vi pratar kanske om tiden för 10-15 år sedan. Hade de infört det då, så kanske man ändå kunnat haft ett internationellt perspektiv på hur man ska bedriva verksamheten utifrån ett informationssäkerhetsperspektiv. Då hade de själva kunde påverkat och utvecklat standarderna i stället. Det hade varit bra för den branschen. Men där är man ju inte nu. Nu kommer det här från sidan i stället för direkt från den finansiella sektorn. (Specialistföretag säkerhet – Ämnesexpert standardisering)*

Oavsett möjligheterna till standardisering, som antagligen kan ta en längre tid att samordna sig kring, så är en möjliggörande åtgärd att *samarbeta med andra aktörer*. Detta blir väldigt viktigt för att öka effektiviteten i hela systemet. Här finns det en bred samsyn i samband med intervjuresultaten. Ett exempel skulle kunna vara att mindre leverantörer söker partnerskap med större aktörer:

> *Det kanske blir att de mindre aktörerna behöver ha andra typer av partnerskap, för att kunna säkra leveranserna. Mindre techbolag kanske blir mer beroende av de större IT-jättarna. Att de behöver ha mer molnbaserade lösningar, för att täcka upp och leva upp på den tekniska delen av operativ motståndskraft. Så det finns säkert vägar att hitta. (Fallföretag – person 4)*

Samarbeten kan även mynna ut i innovativa lösningar och tjänster. Det positiva är att just digital motståndskraft egentligen inte är konkurrenssärskiljande. Det finns möjligheter till förändring som gynnar både den enskilda entiteten och systemet i sin helhet:

> *Jag tänker att det kan på ett sätt vara ungefär som kundkännedom, där det finns aktörer som ser en affärsmöjlighet. Antingen så är dom då uppbackade utav den finansiella sektorns huvudaktörer, eller att det är mer som ett startupbolag som ser att det finns en affär att göra. Här finns det ett business case om vi samlar in det här. Gör vi det och säljer det här som en prenumerationstjänst, kommer det att vara ett bra business case för våra kunder, för de kan då minska sin del som de lägger på det. Så jag tänker att det är marknadsekonomin som styr här. Jag tror kanske inte på EU-nivå eller på regleringsnivå, hur ska man ta ansvar för det här där? Man riskerar att då få någonting som inte möter marknadsbehovet. Utan det är bättre att det drivs fram utifrån marknadskrafter. För att känna att, ja, men den här tjänsten motsvarar det vi behöver. Att man har ett kundfokus på hur det här ska funka mot oss som försäkringsbolag eller bank. Så att antingen ett startup-bolag, eller ett startup-bolag som är backad av andra. Ett annat alternativ är att man går samman i en bransch i ett land. Att säga, ja, men för oss så är det här inte konkurrenssärskiljande på något sätt. Det här är ett gemensamt behov. Låt oss skapa ett gemensamt ägt bolag för den här typen utav frågor. (Moderbolag – person 2)*

Samarbeten kan även uppstå något mer lokalt för att samordna olika problemområden. Begreppsförvirring kan lätt uppstå, då finns det fördelar att utöka samarbetet i branschföreningar som ett exempel:

> *Bankföreningen jobbar ju aktivt. Jag tror den här pushen behövs. Det kanske är naturligare att det ligger i samarbete med Bankföreningen, åtminstone i vårt fall då. (Fallföretag – person 2)*

> *Det finns ju forum idag via Svensk Försäkring och Bankföreningen som jag tror skulle kunna samverka inom sig för att ha möte med Finansinspektionen. Just för att komma överens om den här nivån av rapportering och det data som ska in. Där tror jag vi kan hitta en styrka i branschen helt enkelt. (Moderbolag – person 1)*

Oavsett hur samarbetsformerna ser ut kommer *kompetensförsörjningen* utifrån Sverige och Europa i sin helhet att vara en möjliggörande åtgärd, eller snarare nödvändighet, för att kunna hantera samtliga regelverksinföranden som sker. Det ger även förutsättningar att hantera förvaltningsfasen:

> *Man får ju inte heller bara förlita sig på Universitet och högskolor. Vi har ju YH-utbildningar, men det är väldigt kortsiktiga program. Det kan vara ett år. Man behöver kanske flera år framåt driva kullarna och även driva utbildningarna framåt, så att de blir bättre och bättre. Kompetensförsörjningen ser jag som är väsentlig i det här. Även att man ska få upp nivån på dem som jobbar med informationssäkerhet i organisationer. (Specialistföretag säkerhet – Ämnesexpert standardisering)*

Det blir med andra ord även väldigt viktigt att även hitta samverkansformer i kompetensförsörjningen. Även här kan det finnas olika typer av samarbeten, lösningar och samgåenden, som behöver ske för att snabbt kunna tillföra kompetens. Inte minst blir det viktigt att respektive organisation även tar upp informationssäkerhet till att bli en mer naturlig del i vardagen. En del som då blir viktig för att främja perspektivet och få med samtliga resurser på ett grundläggande säkerhetstänk, är att även visa upp eller *kommunicera värdet som informationssäkerhet tillför.* En intressant spaning är att IT i sig bör ses som en helhet. Det ger förutsättningar att kommunicera utifrån ett helhetsperspektiv:

> *Jag tror att det här måste verkligen kunna påvisa ett business value eller som en growth accelerator på något vis. De delarna behöver hänga ihop så att det inte blir det här regelverksfokuset som jag tror man lätt hamnar i. Där tror jag att det krävs mycket, att förstå värdet. Att hålla sig till lagar och regler, det är inga konstigheter. Det vet de om i ledning och styrelse, de står som ansvariga, att man ska vara compliant. Men just det här med hur man gör det compliant, och samtidigt får ett värdeskapande. (Fallföretag – person 4)*

> *Att inte bara prata IT, det är det som är utmaningen tror jag. Därför att om man ser exempelvis på organisationen bakom, så pratar ju de också mycket om IT. Man måste förstå att ledningssystem, det är inte enbart IT, det är ju informationshantering i en bredare kontext. Det måste utgå ifrån ett allriskperspektiv. (Specialistföretag säkerhet – Ämnesexpert standardisering)*

En sista intressant möjliggörande åtgärd avser att *säkra finansiering vid kris* utifrån ett samhällsperspektiv. Det är trots allt troligt att det kommer ske attacker som får en påverkan. Mindre aktörer kan då ha utmaningar att övervinna något mer långsiktiga kriser. Finansieringen bör ses som en möjliggörare då det ger en trygghet, ungefär på samma sätt som en bankgaranti ger konsumenter för insättningar av finansiella medel:

> *Sen kan jag också tycka är att man har lite kvar på från myndigheter. Det fanns från 1936 en lagstiftning som handlade om att man kunde få hjälp med investeringar i samband med kriget. Så den lagen håller man på att titta över och ser hur det ska moderniseras. Om vi som bank ska kunna hålla öppet 24/7 över hela landet, oavsett situation, i 3 månader, ja, vem betalar för det? Någon motsvarande kanske man skulle fundera på utifrån IT-sidan för de mindre leverantörerna. (Fallföretag - person 2)*

Möjliggörande åtgärder för revisorer

Det finns redan i dagsläget flera större aktörer som erbjuder oberoende granskning och certifiering inom en rad områden. Ett typexempel är den omfattande granskning som sker utifrån ISAE3402 för att certifiera internkontrollsperspektiv. Det finns även i samband med DORA-införande stora möjligheter att fånga upp affärsmöjligheter och samtidigt tillföra värde till systemet i sin helhet:

Du har lite andra typer av audit som finns idag. Men jag kan tänka mig att service providers kan behöver få det. För annars så finns det risken givetvis att kunder vill komma och göra en audit. Har man många kunder så kan det bli ganska jobbigt. Det finns ett sätt idag som heter i ISAE3402. Det är ett sätt att ha en revisionsfirma som gör en revision och sen delar man den med alla kunder. Det kommer säkert komma. (Specialistföretag säkerhet – Service Provider – CISO)

Möjliggörande åtgärder för tillsynsmyndighet

Med tanke på den omfattande informationsinhämtningen, så blir en möjliggörande åtgärd att verkligen *visa det resultat och värde* som DORA tillför. I det blir det då naturligtvis även viktigt att kunna säkra en *snabb och relevant analysförmåga*. I mångt och mycket behöver det tillföras en förhöjd förmåga för att stärka de beståndsdelar som möjliggör detta. Till exempel handlar det om att säkra kompetensförsörjningen, som ju även identifierats som en mer övergripande möjliggörande åtgärd. Det krävs naturligtvis investeringar i det mer tekniska med:

Det behövs mer och mer resurser till både teknisk plattformen och verktyg. Så är det verkligen. (Myndighet – Strateg – sakkunnig DORA)

En på sikt möjliggörande åtgärd är att *hänvisa till standard eller ramverk*. Det bör ge bättre förutsättningar att få in standardiserad information till tillsynsmyndigheten. Det förstärker förmågan att bedöma och jämföra olika tillsynspliktiga entiteters regelefterlevnad. Det ger även möjligheter till att skapa samarbeten med andra aktörer. Det leder även till möjligheter att *låta oberoende revisor utföra granskning*. Sedan är detta som jag redan beskrivit kantat med utmaningar. Tekniska standarder som måste ligga till grund för delar av granskningen är inte fattade ännu. Det finns många intressenter på både bransch-, nationell och internationell nivå, som alla är intresserade av att få med de egna perspektiven. Samtidigt finns det en stor potential i form av att det framför allt minskar de mindre leverantörernas börda.

Implikationer utifrån internt utlagd verksamhet

Med tanke på att fallföretaget (banken) ingår i en större koncern, där det utifrån DORA ingår ett flertal tillsynspliktiga entiteter, finns det naturligtvis fördelar med att kunna hantera en stor del av åtgärder på en högre koncernnivå. En större förändring med DORA för koncernen i sin helhet, är att det nu ställs samma krav utifrån flera entiteter inom koncernen:

DORA ställer samma krav på försäkring och bank, om ett koncerngemensamt företag både har försäkring och bank, så har de ju samma spelregler. (Fallföretag – person 5)

Omfattningen för kraven utifrån DORA kan dock se lite annorlunda ut, vilket beror på antalet kritiska funktioner. En bank har antagligen fler kritiska funktioner än ett försäkringsbolag. Oavsett detta kan det nu krävas en viss grad av anpassning ur ett styrningsperspektiv:

> *Det beror på hur man har koncernens spelregler uppsatta och hur man har tolkat koncernens styrning. På det här företaget så tror jag att vi befinner oss i en förändring som inte alla kanske riktigt helt är medvetna om. Jag tror att det kan finnas olika tolkningar av vad den förändringen kan komma att innebära. Jag tror att det här företaget kommer att gå mot en mycket tydligare koncernstyrning, där dotterbolagens roll blir att vara en del utav koncernen. Att inte koncernen ska stödja dotterbolagen enbart. (Moderbolag – person 2)*

Det blir då väldigt viktigt att den koncernstyrning som sätts upp skapar en hanterbarhet som balanserar olika perspektiv eller världsbilder. De olika världsbilderna utkristalliseras ju närmare den mer operativa nivån som man kommer:

> *Ja, det är klart att vi behöver väl ha en gemensam inriktning. Men jag tror att den svåra biten är att världsbilden kan man ha gemensamt på en hög nivå. Men när man ska sätta det i relation till olika verksamhetsdelar, så kan världsbilden se väldigt olika ut. Allting handlar ju egentligen om information och vad det finns för informationstillgångar. Det skiljer sig väldigt mycket utifrån om du är en bankverksamhet, en sakförsäkringsverksamhet, eller om du har annan typ av investeringsrådgivning. De här olika verksamhetsdelarna gör att du inte riktigt har samma världsbild, även om du kan ha det på en väldigt hög nivå. Men när du ska börja operationalisera och bygga motståndskraften, då kommer du ha olika världsbilder ur det perspektivet. (Fallföretag – person 4)*

Det finns utifrån det vissa betänkanden att helt samordna både styrning och samtliga aktiviteter inom koncernen:

> *Jag tror att det antagligen skulle vara enklare för banken om vi varit ett autonomt eget företag och inte hade något annat att förhålla sig till, både utifrån hur vi jobbar med kraven, och hur vi följer upp. Vi ska ju såklart signa av hur banken ska göra det här. Men vi behöver säkert anpassa oss till andras arbetssätt, och synka med andra affärsenheter. Ner i hur:et. (Fallföretag – person 3)*

Framförallt uppstår det frågor kring hur den internt utlagda verksamheten ska hanteras och följas upp. I det fallet finns det potentiella intressekonflikter då moderbolaget även agerar leverantör:

Men det är ju fortsatt så att man inte får hamna i ett läge att där ett moderbolag styr de delarna i de fallen där de levererar tjänster, då finns det potentiella intressekonflikter. De kan inte styra och granska sig själva. Det blir väldigt viktigt att bevaka de här frågorna. Det är ändå de tillståndspliktiga separata bolagen som bär ansvaret för den styrning som sätts. Det kommer inte att fungera att peka på någon annan. (Fallföretag – person 4)

En del i det hela är att det sedan innan finns uppföljande aktiviteter på plats ur ett internt utlagt perspektiv. DORA ställer mer detaljerade krav på informationen och det gör att det behöver struktureras och standardiseras på ett annat sätt:

Att formalisera det som ibland känns självklart. Jag upplever att banken när jag anställdes hade bra koll. Det har man säkert gentemot moderbolaget med, men det måste ner i bevis och struktureras upp framför allt. (Fallföretag – person 3)

Så det behöver inte nödvändigtvis finnas motsättningar utifrån ett uppföljningsperspektiv. DORA ställer höga krav, helt oavsett om det rör sig om en intern leverantör inom en koncern, eller utifrån ett helt externt perspektiv.

Om man ser till uppdraget i sig, att vi har lagt ut någonting till vårt moderbolag, så bör det inte vara någon skillnad. När det gäller regelverk ska det inte vara det. Sen kan det ju vara så att det vid själva hanteringen runt hur vi följer upp kommer att se annorlunda ut. Jag ser DORA som en skänk från ovan när det gäller just relationen till vår egen koncern, vi kommer få bättre kontroll på våra interna leverantörer och även kunna följa upp saker som vi har velat följa upp redan tidigare. (Fallföretag – person 3)

Sammanfattningsvis är det alltså så att DORA inte innebär olika regelverkskrav beroende på det avser internt utlagd verksamhet, eller om det avser externa leverantörer. Det som däremot får en påverkan är att DORA föranleder större krav på detaljering och uppföljning. I samband med det kan det då även vara ett förändringstryck mot att standardisera uppföljningen för internt utlagd verksamhet. En förutsättning som då krävs är naturligtvis även att beroenden kartläggs och dokumenteras.

Med tanke på ovanstående beskrivning, där syftet är att samordna koncernstyrning och aktiviteter utifrån ett koncernperspektiv i den mån det går, har jag valt att beskriva möjligheterna på koncern- och fallföretagsnivå i enlighet med det. Det innebär att de flesta åtgärder återfinns på koncernnivå. De delar som utifrån ett internt utlagt perspektiv behöver kvarstå inordnas under fallföretaget.

Möjliggörande åtgärder på koncernnivå

Det som framgick av tidigare avsnitt kring hinder på koncernnivå är att det krävs åtgärder för att *främja prioriteringsförmågan*. I en komplex och mångfacetterad organisation är det många aspekter att ta hänsyn till. Det första som behöver säkras är *ledningens engagemang*. I detta sammanhang är det viktigt att påpeka att ledningens förståelse för informationssäkerhet och regelverksefterlevnad redan idag är på en hög nivå. I stället handlar det om *att ledningen förstår de operativa konsekvenserna* utav olika beslut:

> *De har engagemang. När det händer saker, då har vi deras engagemang. Men vi måste ha det hela tiden. (Moderbolag – person 1)*

För att säkra att perspektiven informationssäkerhet och regelverksefterlevnad verkligen kommer med och fångas upp i beslutsfattandet krävs det ett *ändrat maktförhållande*. Det innebär naturligtvis inte att alla beslut ska fattas enbart ur ett informationssäkerhets- eller regelefterlevnadsperspektiv, utan det ska ses som en väg att skapa prioriteringsförmåga utifrån en helhet:

> *Man kan nog se det som att den som är CISO borde få en ökad makt i organisationen, till följd av de här regleringarna som kommer. Den rollen bär såklart ett ansvar för att lyfta upp dom här frågorna. Men jag tror också att man kommer behöva se de här typerna av rollerna alltmer på högsta ledningsnivå, rent maktpositionsmässigt, framöver. (Fallföretag – person 4)*

En annan möjliggörande åtgärd som följer utav detta är att det ger förutsättningar att sätta en *tydlig strategi*. En del i det hela är även att skapa en tydlig sourcingstrategi. Sammantaget ger det då förutsättningar till att skapa prioritering av resurser mot olika områden. Det kan då även tydligare specificeras i vilken grad koncernen ska utföra rent kontrollerande aktivitet, i förhållande till annan aktivitet. Det ger därmed även tydlighet i hur anpassning ska ske utifrån regelverksimplementeringar framöver:

> *Det kanske behövs en strategi för hur man får in och efterlever regelverk inom IT-området. Den tror jag kommer vara väldigt, väldigt, viktig. För att säkerställa att det blir en snabb implementation, men också för att få till en snabb riskhantering. Men också då i de fallen där det mer är en ”pappersövning” för att vara compliant, att den tiden går så snabbt som möjligt, så att tid frigörs tid till de mer affärsutvecklande delarna. (Fallföretag – person 4)*

En möjliggörande åtgärd, som är väldigt naturlig, är ett *riskbaserat angreppssätt*. Det är ju ett annat begrepp för att beskriva prioriteringsförmåga. För att få denna förmåga krävs det naturligtvis även att man använder liknande riskmodeller inom koncernen och någorlunda liknande processer som harmoniserar. Det finns även förutsättningar att *samordna analysen av de digitala leveranskedjorna.*

En annan viktig möjliggörande åtgärd är en *holistisk styrning*. Samtidigt kan det, utifrån att utgångsläget är relativt spretig inom koncernen, även krävas en *ändrad kultur*. Det är en förutsättning för att kunna få effekt i genomförandet:

> *Men jag tror också att det handlar om kultur. Jag tror även att det handlar om arv. Hur har man tänkt tidigare? Hur har man alltid agerat? Vart är vi på väg? Att väga samman det, det är en övning som jag inte är säker på att alla är helt med på. (Moderbolag – person 2)*

En väg till ändrad kultur är att *dela perspektiv* genom att hitta olika aktiviteter som är okontroversiella, och där respektive deltagare snabbt ser ett faktiskt värde. Det leder då även till en utökad förståelse för helheten. Att dela perspektiv behöver ske inom organisationen genom *interna forum*, eller andra former som upplevs värdefulla. Det finns även en behållning med att hitta *relevanta gränssnitt med externa leverantörer och myndigheter*. Se nedan två citat som visar möjligheterna, dels ur ett internt perspektiv, dels ur ett externt perspektiv:

> *Vi jobbar inom säkerhetssidan, om vi säger banken då, och koncernen, så har det ju bildats informella grupperingar som träffas varje månad. Vi jobbar väldigt bra tillsammans, vi har samsyn. Men vi behöver få med oss andra viktiga intressenter. Jag gjorde precis en dragning för domänarkitekterna för en månad sedan och för dem var det ju en ögonöppnare. Men samtidigt så spelar jag lite in på deras bana och säger det här är en möjliggörare för det vi kallar zero trust. De är ju väldigt mycket inne på att vi måste bygga zero trust i olika delar nu, och jag visar att DORA är en möjliggörare, för nu går vi åt det här hållet. Då får man med sig den gruppen av människor. Så det gäller ju att förstå DORA, så att man kan förklara det på deras sätt. Så att de förstår möjligheterna, så att de också kan prioritera på rätt sätt. (Moderbolag – person 1)*

> *Jag sitter i förhandlingar nu med stora jättar. Vi har då från vardera sidan, leverantör och koncernen, gjort varsin DORA presentation för varandra. För att titta på, OK, den här leverantören jobbar med DORA på det här viset. Så visar sen koncernen motsvarande presentation. Det är jätteroligt att se vad de fokuserar på. De berättar ju inte alla brister de har såklart. De berättar vad de fokuserar mest på. Framför allt mycket, precis som vi, på dokumentation. Till exempel hur man dokumenterar hur man ska följa upp saker och ting. Det jag tror skapar en ömsesidig förståelse till att börja med, som grund för en bättre relation. (Moderbolag – person 1)*

En väg att sammanbinda perspektiv är att skapa relevanta och interaktiva *krisövningar*. Det ger förutsättningar för att verkligen uppleva konsekvenserna. Alltså inte enbart att rationellt ställa krav och sätta planer. Utan att vara ”hands on” och känna pulsen höjas:

Jag jobbade på en annan bank innan det att jag kom hit. Där gjorde vi så att för varje ledningsgrupp, både i koncernledningen och alla ledningsgrupper körde vi en kombinerad hotbildsstyrd övning. Där hade vi med oss ett externt bolag som gick in och utmanade. Så att det externa bolaget var då de attackerade kriminella, och vi var företaget som skulle skydda oss. Jag var med då, jag var säkerhetschef för försäkringssidan. Från början när övningen började så hade vi inga roller, utan rollerna sattes under övningen. Det var jättekul att byta roller med varandra. Helt plötsligt så sattes VD som säkerhetschef. Han sade, ”men jag vet inte hur jag ska…”, och samtidigt krävdes det snabba beslut. Vi måste utsätta ledningen för olika typer av lite mer avancerade övningar. Vi kör övningar redan, men man måste utmana och köra en mer avancerade övning. Så att de snabbt ska kunna ta beslut och ställas inför oväntade utmaningar. Se vilka roller de behöver ha omkring sig. Då kan vi börja prata. Då får man engagemang och förståelse. (moderbolag – person 1)

En annan sammanhållen dimension som visade sig vara problematisk är effektiviteten. Ett DORA-införande innebär att tillkommande komplexitet snabbt leder till tillstånd som upplevs ineffektiva. Därför krävs det att koncernen *främjar effektiviteten*. En annan stor del i effektivitet, speciellt i samband med att hotbild och attacker förändras i hög förändringstakt, är att koncernens *agilitetet i riskhanteringen behöver främjas*. Det räcker således inte att enbart effektivisera processerna, så att de upplevs mindre betungande, utan det kräver även att den grundläggande effektivisering resulterar i processer som blir snabbare och som kan ställas om utifrån uppkomna behov.

En tydlig del i effektivitet är att skapa *gemensam tolkning av regelverk och begrepp*. Alltså att det på koncernnivå aggregeras förmåga kring detta. Det kan finnas en risk för begreppsförvirring mellan intressenter i en komplex koncern, speciellt om förmågorna som tolkar regelverk är utspridda:

Ska man samla ihop kompetensen på ett ställe, eller ska man sprida ut dem på massa ställen och sen så ska de försöka jaga varandra, i stället för att försöka gemensamt skapa någonting bra? (Moderbolag – person 2)

Att aktivt *delta i de branschföreningar som koncernen ingår i* är en annan möjliggörande åtgärd som leder till minskad risk för begreppsförvirring. Sammantaget leder detta då även till andra potentiella möjligheter, till exempel att *samordna leverantörsuppföljning* ur både ett internt och externt perspektiv.

Att en *moderniserad IT* måste anses utgöra en möjliggörande åtgärd står klart. En *målarkitektur* som tar hänsyn till strategisk inriktning utifrån utförda vägval blir viktig för att kunna säkra både agilitet och tillhörande effektivitet. *Automatisering* och utökning av *AI-förmågor* är teman som bekräftats i intervjuerna.

Det som även blir viktig är att *öka personalens IS-förmåga* i stort. Det ger tydliga fördelar, då man kommer att kunna agera mer direkt. *Förenklade processer* betyder även att det blir en avlastning för hårt ansatta specialister inom informationssäkerhetsområdet.

> *Jag tror att det gäller inte alltid se säkerhet som någonting separerat. Oavsett om det är gentemot leverantörer eller någonting annat. Då kommer det kräva att vi utbildar vår personal. Det är lätt att sätta något på papper och säga att nu ska du göra det här. Men för mig, så handlar DORA om att man faktiskt höjer kompetensen inom cybersäkerhetsområdet. Inte för att den är dålig, men för att man ska förstå hur allting hänger ihop inom IT-verksamhet. Det tror jag är en förutsättning, att man är villig att utbilda och personalen får ta sig tiden till det. (Fallföretag – person 2)*

Vidare möjligheter som ökar agiliteten är *threat intelligence*, som ger förutsättningar att snabbt se inkommande attacker. *Testning som inkluderar sårbarhetsscanning och pen-tester* är ett annat tema som bekräftats i intervjuerna. *Att främja kontinuitet och återställningsförmåga* blir även det än viktigare i samband med ett DORA-införande. *Testningen behöver även säkras mer holistiskt från ax till limpa med leverantörer*. Att *krisstabsfunktion finns uppsatt och har en tillräcklig förmåg*a är aven det viktigt.

Ett annat område som är en grundförutsättning är att *främja relevant information* som en del i riskhanteringen. Ett *uppdaterat tillgångsregister* och *data governance* ger förutsättningar att använda ett *gemensamt GRC-system*:

> *Om man ska ha ett gemensamt GRC-system, så måste man vara överens om gemensamma tolkningar också. För att inte bara ska skapa flera öar i ett gemensamt hav, så att säga. (Moderbolag – person 2)*

Möjliggörande åtgärder fallföretag

Fallföretaget behöver *säkra internt utlagd verksamhet*. Det gäller att *förhindra potentiella intressekonflikter*. Samtidigt lyfter en respondent fram önskan om att flexibiliteten inte får hindras i för stor grad, att det måste finnas en grundläggande *flexibilitet som en utgångspunkt i det sammantagna arbetet*:

> *Jag tror att flexibilitet är jätteviktigt. Inte att man ska vara flexibel med regelverket. Men jag tror att man måste vara flexibel att känna så att ja, men OK, det kanske inte är 100% för den här verksamheten utifrån den här tolkningen, men den är good enough. Vi är 90% överens. Då kanske jag ska släppa det där, för vi har 10 andra frågor där vi också behöver bli 90% överens. Tänker man att man ska nå 100% i alla frågor, att alla ska vara överens om allt, så tror jag man aldrig blir klar. Det är det jag menar. Så jag tror att flexibiliteten är väldigt viktig. (Moderbolag – person 2)*

Därmed blir det viktigt att hitta vägar tillsammans som är transparanta och som balanserar perspektiven. Samtidigt kommer flertalet redan beskrivna möjliggörande åtgärder leda i denna riktning. En ledning som innehåller representant som förstår de operativa konsekvenserna har bättre möjligheter att besluta åtgärder som inte leder till intressekonflikter. En tydlig strategi och en holistisk styrning skapar mindre friktioner längre ner i organisationen. En kulturförflyttning där man hittar samverkansformer leder även det till att perspektiv delas:

> *Det kanske blir lättare och mer transparent i det interna tänker jag, för man samarbetar väl lite mer. Det är ju typiskt att en intern leverantör har mer transparens än vad en extern leverantör har. Så det tycker jag är en fördel. Men om man har en stor leverantör, som koncernen, som levererar till många olika bolag, då blir det ju naturligtvis en komplexitet att det är så många olika bolag som får leveranser. Man måste skapa den kartläggningen och där kan det ju vara en skillnad. Men det finns ju då på den positiva sidan att man har en transparens, som man inte har med externa leverantörer. Man har inte heller förmågan att trycka på eller förstå helheten då. När det kommer till uppföljning mot underleverantörer, så kommer det ju vara enklare i det interna sammanhanget, när man nu med DORA behöver vara mer aktiv. I den uppföljningen kommer man kunna ha ett närmare samarbete med koncernen som är den stora leverantören av IT-koncerngemensamma tjänster. (Fallföretag – person 1)*

Utifrån detta finns goda förutsättningar att skapa något som leder till en situation där perspektiven transparens, flexibilitet och säkerställda intressekonflikter kan harmonisera. Det hänger på att grundläggande åtgärder införs för att skapa en ännu stadigare grund att stå på. Det hänger även på att samtliga anställda ser DORA-införandet som en värdefull förflyttning.

Möjliggörande åtgärder extern leverantör

Leverantörer som ingår i de digitala leveranskedjorna påverkas i väldigt hög grad genom DORA-införandet. Speciellt mindre leverantörer med flera kunder kommer att uppleva en kraftigt ökad belastning. I väntan på att kunna hantera det genom oberoende revision och certifiering finns möjligheten för leverantörerna att själva *samordna olika kunders perspektiv.* Samtidigt tar det mycket tid och kraft, men det ger åtminstone förhoppning om att bördan minskar något:

> *Vi har ett forum med nyckelpersoner, säkerhetspersoner, från olika större kunder. Jag håller i det här forumet. Målsättningen är att vi ska prata samma språk, att göra det här arbetet en gång för att kunna nyttja resultatet flera gånger. Att få kunderna att synkronisera sig kräver ett enormt engagemang, från i det här fallet leverantörshåll. För att få kunden att prata ihop sig, måste man vara lite bestämd och sätta ner foten. Att, ja, men då gör vi så här. Är ni med på det? Och så ska man få dem att signa av på det. Kunderna kommer inte per default att ta kontakt med andra kunder för att*

synkronisera sig. Det kommer de inte. Jag är ganska säker på det. Men har man en central leverantör, som orkar hålla i dem, som kommer med konkreta förslag, då kan vi få till det fenomenet. Det är dit som jag vill gå. Men man ska ha tid för det och det kräver mycket engagemang. (Leverantör – CISO)

I övrigt finns det naturligtvis mer övergripande möjliggörande åtgärder som redan presenterats i tidigare stycken. Det kan till exempel handla om att samarbeta med andra aktörer som vill verka i samma riktning. Däremot är läget i nuläget något fragmenterat, vilket då skulle kunna leda till att för många aktörer försöker skapa en standard eller ramverk, som sedan omkullkastas när det väl utkristalliseras mer standardiserade lösningar.

5. Diskussion

I detta kapitel sammanvävs empirisk analys och den tidigare presenterade teorimodellen i en diskussion. Kapitlet inleds med en övergripande resultatdiskussion. Sedan följer en metodreflektion som sammanbinder insikter och reflektioner som kan dras utifrån den använda metoden.

5.1 Resultatdiskussion

Inledning

Utifrån insamling av empiri och analysen står det förhoppningsvis klart även för läsaren att det är en avsevärd komplexitet som skapas i samband med ett DORA-införande. För att koppla det mot Checkland och Puolter (2020) så innebär en *transformation* mot högre nivåer av digital motståndskraft ett stort antal *aktörer* som både påverkar och som påverkas. Om man ser till *slutlig förmånstagare* utifrån ett DORA-införande, så är det naturligtvis samhället i stort, med slutkonsumenterna som yttersta förmånstagare. Samtidigt innebär det att väldigt många *världsbilder* behöver harmonisera för att skapa en effektivitet. Ett holistiskt systemperspektiv kan leda till medvetna beslut som leder till både högre digital motståndskraft och som samtidigt minskar riskerna för att andra viktiga dimensioner påverkas negativt. Vem är det då som äger och styr denna transformation mot högre digital motståndskraft? Här går det att argumentera för att en enskild *ägare* inte går att hitta. Visserligen skulle beslutande organ inom EU kunna anses vara ägare. Samtidigt är komplexiteten så pass hög, med olika perspektiv som behöver beaktas för att verkligen komma ner till en mer operativ nivå. Det betyder att vi alla som vill verka mot högre digital motståndskraft, även äger transformationen i sig. Det finns många *omvärldsberoende begränsningar* som behöver beaktas för att transformera systemet mot en högre grad av digital motståndskraft.

Flera omfattande hinder

Det finns en rad potentiella hinder som kunde identifieras i denna fallstudie utifrån de olika aktörernas världsbilder. En avsevärd höjning av komplexitet slår olika hårt, beroende på vilken aktör som avses. Framför allt mindre leverantörers och underleverantörers förmåga att hantera DORA kan anses vara väldigt problematisk. Se tabell 4 som visar de mer övergripande hinder som identifierats. Fullständigt bild med underkategorier visas i figur 3 i empiri och analyskapitel.

Tabell 4: Identifierade hinder per aktör

Aktör	Identifierat hinder
Övergripande	Otydliga begrepp
Övergripande	Delvis överlappande regelverk
Övergripande	Kompetensförsörjning
Övergripande	Kort tid för implementation
Övergripande	Stora förändringar efter konsultation
Övergripande	Koncentrationsrisker ökar
Tillsynsmyndighet	Aggregerad information skyddas inte tillräckligt
Tillsynsmyndighet	Inaktuell information
Tillsynsmyndighet	Ökad omfattning med detaljerad uppföljning
Tillsynsmyndighet	Oklara bedömningsgrunder
Tillsynsmyndighet	Upplevd avsaknad av stöd
Tillsynsmyndighet	Förmågan behöver stärkas
Koncernnivå	Prioriteringsförmåga
Koncernnivå	För låg grad av effektivitet
Extern leverantör	Ökade belastning - kostnader som måste föras vidare
Extern leverantör	Det saknas vägledning
Extern leverantör	Motstånd hos underleverantör
Extern leverantör	Ej möjligt att följa upp senare led, inga avtal i led 2 eller 3
Extern leverantör	Längre ledtider
Extern leverantör	Oklar hantering med flera EU-kompetenter

Sammantaget kan det konstateras att det finns en stor risk för *begreppsförvirring* i samband med definitioner utifrån *överlappande regelverk* och olika tillsynsmyndigheter. När det gäller begreppen digital motståndskraft och digitala leveranskedjor så ligger dessa på en hög nivå och det framkom ingen egentlig motsättning till begreppen. Däremot visar mitt initiala utskick till respondenterna att det är lätt att gå fel. Begreppsförvirring kan även uppstå inom

sektorer eller inom större koncerner. *Kompetensförsörjningen* identifierades som ett större hinder för samtliga respondenter. Det är ett stort tryck i hela systemet på att få in kompetens. Det slår i högre grad på offentliga aktörer. Offentlig sektor har längre ledtider med väldigt tidskrävande säkerhetsprövning. Offentlig sektor har det svårare med att attrahera kompetens då löneläget är lägre än i privat sektor. Det hela försvåras ytterligare av att det är *kort tid för implementation* för DORA och andra regelverk. Dessutom sker det *stora förändringar efter konsultation*. Det gör att vissa vägval som tas för tidigt blir kostsamma. På ett mer övergripande plan kan själva införandet av DORA även leda till att *koncentrationsriskerna ökar* i systemet i sin helhet. Mindre aktörer kan få utmaningar att förhålla sig till regelverken och därmed slås ut från den finansiella marknaden. Innovativa uppstartsföretag kan komma att välja att inte ta sig in mot den finansiella sektorn.

När det gäller tillsynsmyndigheten så uppstår det en tillkommande risk med all den detaljerade information som nu krävs in och som ska sammanställas inom EU. Det kan leda till att *aggregerad information inte skyddas tillräckligt*. Utifrån exempel som framkommit i intervjuer (även utifrån min egen erfarenhet) är detta en reell risk. Ett annat potentiellt hinder är att *informationen som samlas in är inaktuell*. Alltså att det finns för långa ledtider inneboende i systemet och uppföljningen, vilket gör att informationen är inaktuell och inte kan användas. Naturligtvis *ökar även omfattningen för tillsynsmyndigheten*. Därmed behöver tillsynsmyndigheten tillsätta resurser och höja kompetensen. Det finns vidare risk för *oklara bedömningsgrunder*, speciellt när det gäller krav som är skrivna på en övergripande nivå och som kräver tolkning. Tillsynsmyndigheten behöver även bemöta övriga aktörers *upplevda saknad av stöd*. Sammantaget behöver tillsynsmyndighetens *förmåga stärkas*.

När det gäller fallföretaget och koncernen i sin helhet så innebär ett DORA-införande att komplexiteten höjs kraftigt. I samband med detta kan Schneider et al. (2017) ge indikationer på vad det innebär för en organisation. Det ena svaret på ökad extern komplexitet är att organisationen höjer den interna komplexiteten, vilket då möter det tryck som uppstår. Det innebär att det vid en extern komplexitetshöjning sker omfattande samordning för att öka både antal och omfång av befintliga interna aktiviteter och processer. I fallföretaget och koncernen är detta väldigt tydligt. Det leder till att befintliga processer och gränssnitt används för att påbörja implementation. Samtidigt kan en befintlig struktur då även riskera att nå en bristningsgräns där gammal doktrin inte längre gäller. Det kan då innebära att det skapas friktion, eller att det upplevs som att samordningen inte längre är tillräcklig för att hantera komplexitetshöjningen. Detta kan då yttra sig genom följdsymptom. I förlängningen kan det då upplevas som att *prioriteringsförmågan är för låg*, eller att det är en *för låg grad av effektivitet*. Detta visade sig väldigt tydligt i denna fallstudie. Det kan då även yttra sig som att organisationen inte upplevs som tillräckligt mogen. I intervjuerna var ett ord som ofta användes just mognad. Se ett citat nedan som sammanfattar det hela:

> *Det handlar ju också om bankens mognad, att kunna hantera kantbollar. Så att vi inte fastnar i för mycket detaljer. För många gånger så behöver man ju tänka affärsrisk kontra annan risk också. (Fallföretag – person 3)*

Det betyder inte att man inte haft väl fungerande processer innan införandet av DORA. Respondenterna uttryckte att det funnits en fungerande riskhantering, ett ledningssystem på plats, och så vidare. Så det handlar inte om att förmågan varit för låg initialt. Utan det handlar om att ökad komplexitet snabbt skapar synlighet i de delar som behöver förändras när komplexiteten når en bristningsgräns. Därmed ska ett DORA-införande mer ses som en indikation på vart flaskhalsar uppstår, vilka nu behöver adresseras. Alltså med andra ord att det leder till ett behov av att identifiera områden som behöver hanteras ur ett strukturellt perspektiv. Se nedan citat som visar detta:

> *I det stora hela så ser ju att det ändå är en positiv förflyttning som vi kommer behöva göra. Alltså att det kommer stärka vår styrning av tredjepartsleverantörer. (Fallföretag – person 4)*

När det gäller extern leverantör så finns det stora hinder som behöver överbryggas. Framför allt är det en *ökad belastning som leder till ökade kostnader*. Leverantörerna måste hitta vägar att överföra kostnadsökningen till kunderna, annars finns det risk för marginalförsämring. Små eller medelstora leverantörer med många kunder är särskilt utsatta. Dels utifrån att det blir en så pass stor höjning i administrationsandelen, dels att det samtidigt finns sämre förutsättningar att hantera detta rent finansiellt. Leverantörerna upplever att *det saknas vägledning* till att skapa genomförbarhet, att gå från teori till praktik. Det kan vidare finnas *motstånd hos underleverantörerna*, i vissa fall är det *ej möjligt att följa upp senare led utifrån att det saknas avtal med underleverantörer i led 2 eller 3.* Det finns en risk att DORA-införande innebär avsevärt *längre ledtider*. Detta då kunderna ska kunna ge input utifrån förändringar. Har leverantören då flera kunder kan det uppstå oklarheter om förändring ens kan genomföras. Slutligen kan det finnas en *oklar hantering när det finns flera EU-kompetenter*.

Sammanfattningsvis uppstår många hinder inom helt andra dimensioner än vad en ren IS-ansats medför. En låg grad av prioriteringsförmåga är inte enbart kopplat till IS-området. Utan det kan yttra sig i en annan del av organisationen eller systemet. Jag delar därför det perspektiv som Dlamini et al. (2009) ger i det citat som användes i problemformuleringen. Här följer en förkortad version av citatet (s. 197) :

> *[…] most of today's security challenges are to a greater extent related to the human and organisational aspects […] of security.*

En respondent uttryckte detta även på ett sätt som tål att förstärkas:

> *Att inte bara prata IT, det är det som är utmaningen tror jag. (Specialistföretag säkerhet – ämnesexpert standardisering)*

Många möjliggörande åtgärder

I den systematisk litteraturgenomgången kunde ett stort antal potentiella möjliggörande åtgärder identifieras, se avsnitt 2.10 som visar sammantagen teorimodell. Samtidigt måste det påpekas att mycket av litteraturen fokuserar på enskilda orsakssamband. En teorimodell som visar helheten över samtliga möjliga åtgärder är svår att fånga i en modell. Dhillon och Torkzadeh (2006) beskriver ett stort antal målsättningar med IS och det finns en uppsjö av möjliggörande åtgärder som potentiellt kan komma på fråga. I problemformuleringen använde jag mig av ett citat från Silic och Back (2014) där ett antal frågor ställs:

> *We believe that it is the right time for scholars to help practitioners by studying some of these research questions: Can information security be implemented off-the-shelf? What is the importance of information security governance? Is there a "Silver Bullet" in IS? (s. 303)*

Utifrån litteraturgenomgång och denna fallstudie står det klart att IS inte kan implementeras som något ”off-the-shelf”. Frågorna som ställs av Silic och Back (2014) tyder mycket på att författarna ser ett behov av att hitta lösningar som slutgiltigt hanterar IS-problematiken. Utifrån Vuorinen och Tetri (2012) måste man i stället se IS som en ständigt föränderlig ”entitet” eller ”aktör”, som då även påverkar andra beståndsdelar inom systemet. Det kräver en helt annan ansats. Jag ansluter mig till Morecrofts (2020) argumentation för ett systemperspektiv som värdefullt i detta sammanhang. Dlamini et al. (2009) visar att varje införd åtgärd inom IS får följdverkningar. Det blir tydligt i denna uppsats med exemplet på att koncentrationsrisker kan öka när DORA införs. Vidare innebär aggregerad information helt nya risker, som ibland uppstår på annan plats än där de initiala kraven riktas. Det finns därmed ingen ”silver bullet” inom IS. Det som däremot är fruktbart är att identifiera möjliggörande åtgärder som leder både organisation och systemet i en riktning mot högre grad av digital motståndskraft, och som inte får för omfattande negativa konsekvenser inom andra dimensioner. Den metodik som Checkland och Poulter (2020) beskriver med SSM ger förutsättningar att både återanvända befintliga och identifiera helt nya möjliggörande aktiviteter. I tabell 5 återfinns de möjliggörande åtgärder som undersökts utifrån teorimodellen inom ramen för denna fallstudie. I tabellen går det att utläsa om denna fallstudie ger stöd (direkt eller indirekt) för respektive möjliggörande åtgärd. Källor till respektive möjliggörande åtgärd återfinns i stycke 2.10 som beskriver teorimodellen.

Tabell 5: Återkoppling för teorimodell utifrån möjliggörande åtgärder

Möjliggörande åtgärder för att främja digital motståndskraft		
Möjliggörande åtgärd	**Applicerbarhet**	**Stöd utifrån fallstudien**
Tydliga klausuler vid upphandling om informationsplikt	Leverantör	**Indirekt** genom koppling mot hinder ”Ej möjligt att följa upp senare led, inga avtal i led 2 eller 3”
Genomföra analys över informations-flöden och leverantörskedjor	Koncernnivå	**Direkt** genom åtgärd ”Utföra analys av digitala leveranskedjor”
Säkra incidenthantering	Koncernnivå	**Direkt** genom flertal närliggande/underordnade möjliggörande åtgärder
Säkra kontinuitet- och återställningsförmåga	Koncernnivå	**Direkt**
Säkra att definitionen för digital motståndskraft är tydlig	Övergripande	**Indirekt** genom möjliggörande åtgärd ”En gemensam standard eller ramverk och accepterad certifiering”
Säkra att definitionen för digital leveranskedja är tydlig	Övergripande	**Indirekt** genom möjliggörande åtgärd ”En gemensam standard eller ramverk och accepterad certifiering”
Uppdatera uppföljning mot leverantör	Koncernnivå	**Direkt**
Höjd säkerhetsmedvetenhet genom utbildning	Koncernnivå	**Direkt**
Säkra relevanta SLA per leverantör	Koncernnivå	**Inget stöd**
Uppdatera avtal med leverantörerna	Koncernnivå	**Indirekt** genom hinder ”Ej möjligt att följa upp senare led, inga avtal i led 2 eller 3”
Säkra relevant gränssnitt med leverantör	Koncernivå	**Direkt** genom möjliggörande åtgärd ”Öppen dialog och relevant gränssnitt med externa parter”
Samarbeta med andra aktörer	Övergripande	**Direkt**
Uppdatera Threat Intelligence tjänst	Övergripande	**Direkt**
Säkra riskhanteringen	Koncernnivå	**Direkt** genom flertal närliggande/underordnade möjliggörande åtgärder
Säkra finansiering av IS	Övergripande	**Indirekt** genom möjliggörande åtgärd ”Säkra finansiering vid kris”
Oberoende granskning och certifiering	Oberoende revisor	**Direkt**
Säkra holistisk styrning	Koncernnivå	**Direkt**
Säkra ledningens engagemang i IS-relaterade frågor	Koncernnivå	**Direkt**
Moderniserad IT	Koncernnivå	**Direkt**
Säkra styrning för IT-upphandling och erbjuda stöd till upphandlarna	Koncernnivå	**Inget stöd**
Säkra ett relevant IS-ledningssystem	Övergripande	**Direkt**

I den fullständiga intervjuanalysen framkommer det flera teman som inte fångas upp av teorimodellen, eller som visserligen fångas upp, men som bör förstärkas. *Att samarbeta med andra aktörer* blir ytterst väsentligt. Schneider et al. (2017) ser detta som den andra vägen för organisationer att svara på en ökad extern komplexitet. Min fallstudie ger starkt stöd till detta. Att identifiera strategiska partnerskap eller andra samverkansformer kommer att vara en nödvändighet för att skapa effektivitet i systemet. DORA möjliggör detta. Nu gäller det att aktörerna snabbt inför nya, eller förstärker befintliga samarbeten. Det finns naturligtvis redan samarbeten genom branschföreningar och dylikt. Men det behöver verkligen stärkas i det stora hela. När det gäller *kompetensförsörjningen* så beskrivs den inte inom litteraturen för IS i tillräckligt stor grad. Det kan eventuellt bero på att omvärlden skiftat i så pass snabb takt, att detta inte varit en sådan stor utmaning tidigare. Med tanke på omfattning och kraftfullt höjd hotbild för västvärldens samhällen, blir detta en ytterst väsentlig dimension att ta hänsyn till. Här behöver samhälle och organisationer hitta vägar att skapa bättre förutsättningar. *Att kommunicera värdet med IS-aktivitet* finns indirekt beskriven i litteraturen utifrån Dlamini et al. (2009). Om IS verkligen ska bli ett mer vardagligt perspektiv är det viktigt att vi alla som arbetar med detta blir bättre på att kommunicera mot alla dem vi interagerar med. *Oberoende granskning och erkänd certifieringsstandard* beskrivs av Nuijten et al. (2018) samt Wall et al. (2016) som en möjliggörande aktivitet. Det stöds även i denna fallstudie. Det kommer öka effektiviteten i systemet som helhet. Det gynnar speciellt de mindre aktörerna som då får ett mer ”level-playing-field” med de större aktörerna. Tillsynsmyndigheten måste bli bättre på att *visa resultat och värde*. Det är stora insatser som nu görs utifrån de tillkommande kraven. I samband med det måste även tillsynsmyndigheten agera och leverera ett värde som leder till en ökad digital motståndskraft. Det handlar inte om ”pinnjakt”, det handlar om att kommunicera och att interagera. Tillsynsmyndigheten måste även säkra en *snabb och relevant analysförmåga*. I den mån det är möjligt behöver även tillsynsmyndigheten *hänvisa till standard eller ramverk* som leder till att *oberoende revisorer kan utföra granskning och utfärda certifiering.*

När det gäller fallföretaget och koncernen i sin helhet blir det tydligt att de hinder som upplevts med *låg prioriteringsförmåga* och *låg grad av effektivitet* är tydliga tecken på att komplexiteten har nått en nivå som kommer kräva omfattande förändring. Som konstaterades har tidigare uppsättning fungerat väl. Men en punkt har nåtts där det krävs omtag. Det börjar i toppen. *Ledningens engagemang måste höjas utifrån förståelse för operativa konsekvenser* inom IS-relaterade vägval. Det kräver ett *ändrat maktförhållande*. Som konstaterades i analysen är det inte så att ledningens engagemang är lågt. Det är i stället så att förmågan att förstå holistiska konsekvenser behöver stärkas. IS måste bli en fullt ut integrerad beståndsdel. Utifrån detta kan en *tydlig strategi* formuleras. Det *riskbaserade angreppssättet* blir än viktigare för att stödja förmågan till rätt prioritering. En *holistisk styrning* ger förutsättningar att kunna hantera tillkommande regelverkskrav som en mer naturlig del i vardagen. För att uppnå detta krävs det en viss *ändrad kultur*. Kulturen uppstår i samspelet mellan individerna som ingår inom koncernen. Att *dela perspektiv* blir en väg framåt. Det kan därmed krävas att interna forum som upplevs värdefulla tillåts växa fram. Dialogen behöver även säkras mot externa aktörer. Gemensam krisövning kan vara ett sätt

att förstå IS-relaterade perspektiv. För att säkra effektivitet skulle det vara fördelaktig med *gemensam tolkning av regelverk och begrepp*. *En gemensam uppföljning av extern leverantör* ger stora fördelar då det skapar effektivitet även hos leverantören. I förlängningen bör det även miska kostnadsbördan i systemet i sin helhet. *Moderniserad IT* blir viktigare än någonsin. Att *öka personalens förmåga* ger fördelen att rena IS-specialister på sikt kan avlastas. Det gäller då att förenkla processerna i tillräcklig grad. Att främja relevant information i riskhanteringen, till exempel genom ett gemensamt GRC-system, leder till än bättre förutsättningar. Det kräver naturligtvis även ett uppdaterat tillgångsregister.

För fallföretaget (banken) bör det säkerställas en *grundläggande transparens och flexibilitet som utgångspunkt.* Det minskar friktioner och onödig administration. Samtidigt måste fallföretaget behålla förmåga att *säkra potentiella intressekonflikter*. Det har beroenden till andra möjliggörande aktiviteter som redan beskrivits. Först och främst att ledningen förstår de operativa konsekvenserna. Sedan även att det skapas förutsättning till gemensam tolkning av regelverk och begrepp. Den holistiska styrningen är därmed också ett beroende i det hela.

För externa leverantörer kan det finnas en större behållning av att på kort sikt *samordna olika kunders perspektiv.* Det minskar börda och kostnader på sikt. Samtidigt bör andra aktörer verka för att arbeta fram standarder för uppföljning. Det ger då förutsättningar för oberoende granskning och tillhörande certifiering.

Vilka möjliggörande aktiviteter bör prioriteras?

Med tanke på ett stort antal möjliggörande åtgärder är då frågan vad som bör prioriteras? Här är det naturligvis så att det inte finns ett svar som är allmängiltigt för all tid. Som redan konstaterats innebär varje förändringar att det skapas följdverkningar i systemet som helhet. Det är därmed bättre att fokusera på att använda en metod som åtminstone innebär att prioriteringen bygger på en holistisk ansats, och där argumentation kan ledas tillsammans med andra intressenter. Jag har i min uppsats använt en anpassad version av SSM utifrån Checkland och Puolter (2020). Här finns det turligt nog även stöd för att beskriva hur en grundläggande utvärdering av de möjliggörande aktiviteterna bör se ut. Givet en transformation med syfte att stärka den digitala motståndskraften, bör utvärdering ske mot det som Checkland och Poulter (2020) beskriver som 3E. 3E består av begreppen *efficacy*, *effciency* och *effectiveness*. På svenska används ofta uttrycket *effektivitet*, vilket dock inte fullt ut visar nyanserna i 3E-begreppet. *Efficacy* kan beskrivas som graden av hur pass väl möjliggörande åtgärder mer direkt leder till att uppfylla syftet, mot i det här fallet stärkt digital motståndskraft. *Efficiency* kan beskrivas som ett mått på hur pass resurssnålt en möjliggörande åtgärd kan införas. *Effectiveness* kan beskrivas som ett mått för positiva effekter på lång sikt, eller även övergripande positiva effekter inom systemet som helhet. Tanken med den sammantagna 3E-modellen är att det ger förutsättningar att prioritera möjliggörande åtgärder som leder rätt, både på kort- och lång sikt, och som dessutom innebär en genomförbarhet med så låg grad av resurssättning som möjligt.

Jag har inte möjlighet att i detalj gå in och beskriva fullständig 3E-analys för samtliga möjliggörande åtgärder som identifierats. Jag väljer att i stället lyfta fram ett fåtal som exemplifierar det hela. Jag utgår ifrån leverantörens perspektiv, då det identifierats som problematiskt för systemet i sin helhet.

Som beskrivits genomgående i uppsatsen är mindre leverantörer utsatta och ett införande av DORA medför kraftigt ökad belastning och ökade kostnader. I förlängningen kan det leda till utslagningseffekter, eller att mindre aktörer väljer bort att erbjuda digitala tjänster och produkter inom den finansiella sektorn. Det kan leda till att koncentrationsrisker uppstår till följd av ett DORA-införande. Därav blir den möjliggörande åtgärden att *oberoende revisor erbjuder granskning och certifiering*. De är något som verkligen skulle skapa bättre förutsättningar på lång sikt. Effectiveness bör därmed ses som väldigt hög. När det avser efficiency så är även denna att anses som hög på sikt, då det blir en mindre grad av överadministration i systemet. Efficacy är däremot lägre, vilket beror på att det behöver skapas överenskommelser mellan ett flertal aktörer på kort sikt. Om man då i stället ser på den möjliggörande åtgärden att *samarbeta med andra aktörer* så går det att argumentera för att det leder rätt på kort tid, alltså har en hög grad av efficacy. När det gäller efficiency så är denna på sikt hög, då det ger en grundförutsättning att skapa lösningar som till exempel gemensamma standarder eller ramverk, vilka ligger till grund för en accepterad oberoende granskning och certifiering. Effectiveness är lägre, åtminstone initialt. Detta då det är svårt att skapa samverkansformer på kort sikt som snabbt leder till rätt följdeffekter. När det gäller den möjliggörande åtgärden att *säkra kompetensförsörjningen*, så har den en hög grad av både efficacy och effectiveness. Däremot så är effeciency naturligtvis låg, då det leder till att fler resurser används inom systemet.

Sammantaget finns det inget enkelt linjärt eller binärt svar på att just möjliggörande åtgärd x ska prioriteras. Däremot så finns det ett antal möjliggörande åtgärder som tillsammans förbättrar situationen för en enskilt aktör, och som samtidigt leder till positiva effekter för systemet i sin helhet. Ovan beskrivna tre möjliggörande åtgärder utgör ett exempel på detta utifrån ett leverantörsperspektiv.

5.2 Forskningsbidrag och metodreflektion

Forskningsbidraget består av att i litteraturen beskrivna möjliggörande åtgärder inom IS kunnat undersökas genom en fallstudie. Ett stort antal möjliggörande åtgärder fär stöd i fallstudien. Speciellt *oberoende granskning och certifiering* har genom fallstudien visat sig vara viktig utifrån mindre leverantörers perspektiv. Det går även att uläsa en rad andra viktiga möjliggörande åtgärder som stöds av fallstudien. Samtidigt visar uppsatsen att befintlig forskning ofta beskriver enskilda orsaksamband och att det då omöjligt går att fånga upp dynamiken i en komplex förändring. En abduktiv ansats valdes i metoden, vilket då även gav möjlighet att identifiera tillkommande möjliggörande åtgärder. Utifrån resultatet i fallstudien är min uppfattning att detta ökade det holistiska värdet med tillfört forskningsbidrag.

Fallstudien ger värdefull kunskap kring hur en ökad grad av komplexitet påverkar en större koncern. Det visar sig att en större koncern når en grad av komplexitet där möjliggörande åtgärder inte längre begränsas till IS-dimensionen i sig, där det då föranleder en strukturell omdaning. Uppsatsen exemplifierar därmed att det inte finns en ”silver-bullet” inom IS när en mer komplex förändring som ett DORA-införande undersöks. Det medför att det krävs en holistisk ansats för att kunna kommunicera kring både hinder och möjliggörande åtgärder. Min uppsats exemplifierar en sådan ansats genom användandet av Checkland och Poulter (2020) beskriven SSM. Fördelen med metoden är att helheten kan målas upp och att de olika aktörernas perspektiv eller världsbilder verkligen framhävs.

Undersökning har skett genom kvalitativ fallstudie och semistrukturerade intervjuer, där urval styrts med en initial ansats som sedan utökats utifrån ”snöbollseffekt”. Med tanke på omfattande dynamik och potentiella begreppsförvirringar bedöms detta ha varit en rimlig ansats. En mer kvantitativ ansats hade antagligen resulterat att i att begrepp tolkats olika och att mätvärden inte reflekterat det som avsetts utifrån mätningen. De semistrukturerade intervjuerna gav en inriktning som sedan anpassades utifrån respektive samtal. Naturligtvis kommer det i en kvalitativ ansats, som i sig innebär en tolkningsbarhet, även att finnas utrymme för att resultat kan påverkas av olika tolkningar. Detta är något som bör tas upp utifrån uppsatsens *reliabilitet*. I denna uppsats kan även det faktum att jag är anställd inom fallföretaget innebära risk för en färgad tolkning. Samtidigt har utgångspunkten varit att själva ämnet med digital motståndskraft inte är kontroversiellt i sig. Alla respondenter har sett att det finns ett behov av att öka motståndskraften i samhället i stort. Det upplevdes även som att det fanns ett intresse av att verkligen bidra till kunskapen inom forskningsområdet. En annan åtgärd har varit att intervjua respondenter utanför fallföretaget. Sammantaget gör jag bedömningen att det finns utrymme att följa själva tillkomsten av min undersökning genom utförlig beskrivning i metodkapitlet. Om inte annat möjliggör det för läsaren att vidare bedöma graden av reliabilitet.

När det gäller *validiteten* har det gjorts ständiga medvetna avvägningar i metoden. Dessa presenterdes under avsnitt 3.5 kring sammanfattande etiska, estetiska och logiska implikationer. Varje vägval har potentiella fördelar och nackdelar. Valen har gjorts för att skapa en så hög holistisk nytta som möjligt, vilket då även innefatttar validiteten i forskningsresultatet. Genom att välja respondenter som är specialister, vilka mer eller mindre direkt, hanterat eller påverkats av komplexa regelverksinföranden, bör det finnas utrymme att bedöma validiteten som relativt hög. När det gäller analysen med kodning av begrepp och teman, så grundar den sig på en systematisk litteraturstudie och framtagen teorimodell som återfinns i stycke 2.10. Sammanställningen i figur 3 och 4 visar helheten för utfallet, vilket åtminstone av författaren upplevs vara kongruent och rimligt.

När det gäller dimensionen *generaliserbarhet*, så är utgångspunkten en analytisk ansats genom välöverlagd analys, vilken framgår direkt i kapitel för empiri och analys. Fallstudien behandlar ett holistiskt perspektiv utifrån större potentiella hinder och de möjliggörande åtgärder som bör beaktas vid ett DORA-införande. Triangulering har använts för att öka möjligheterna till generalisering genom att fånga upp fler intressenters världsbilder, än

enbart dem som återfinns i det egentliga fallföretaget. Det ger bättre förutsättningar att se helheten. Läsaren av uppsatsen har möjlighet att se och följa argumentationen genom att läsa kapitel för empiri och analys. Det finns då även möjligheten för läsaren att själv bilda sig en uppfattning över generaliserbarheten. Jag ser således inte verkligheten som något absolut allmängiltigt, utan att det är något som växer fram i det komplexa samspelet av dialoger och interaktioner mellan människor. Den egna förståelsen utvecklas och anpassas ständigt, utifrån den just då upplevda sociala verkligheten. Läsaren uppmanas till att själv vara en del i den resan.

6. Avslutning

I detta kapitel presenteras först de slutsatser som de undersökta forskningsfrågorna föranleder. Efter detta följer teoretiska implikationer och tillhörande förslag till vidare forskning. Kapitlet avslutas genom att praktiska implikationer framförs.

6.1 Slutsatser

Syftet med uppsatsen har varit att öka kunskapen kring organisationers och andra aktörers förmåga att stärka den digitala motståndskraften i digitala leveranskedjor genom införande av ett omfattande regelverk. Uppsatsen förväntades bidra med kunskap som är användbar utifrån en given organisations förutsättningar, genom att vägleda i en riktning som både stärker den enskilda organisationens, dess digitala leveranskedjors och systemets totala digitala motståndskraft. I förlängningen förväntades det bidra i att Sveriges digitala motståndskraft stärks. Slutsatserna för forskningsfrågorna följer i nedan avsnitt.

Är begreppen digital motståndskraft och digital leveranskedja tillräckligt definierade?

Uppsatsen visar att begreppen är kopplade till en övergripande nivå som även täcker in perspektiven utifrån ett DORA-införande. Det finns ingen egentlig motsättning till begreppet digital motståndskraft, med den skillnaden att DORA trycker på den operativa förmågan, som då innebär en utökad detaljeringsgrad. Det finns en behållning med att använda mer övergripande begrepp för att behålla det övergripande perspektivet. Det utgår ifrån att den finansiella sektorn även omfattas utifrån ett helhetsperspektiv. Däremot så visar uppsatsen att det alltid finns en risk för begreppsförvirring, speciellt i den mån det finns överlapp mellan olika regelverk, eller utifrån olika delvis överlappande begrepp.

Vilka hinder hämmar syftet om stärkt digital motståndskraft i de digitala leveranskedjorna utifrån ett DORA-införande?

Uppsatsen identifierar ett stort antal hinder som utgår eller påverkar systemet på en övergripande nivå, eller utifrån specifik aktör. På en *övergripande nivå* identifierades hinder såsom kort tid för implementation, stora förändringar efter konsultation och att koncentrationsrisker ökar. För aktören *tillsynsmyndighet* identifierades hinder såsom aggregerad information som inte skyddas tillräckligt, inaktuell information, ökad omfattning med detaljerad uppföljning, oklara bedömningsgrunder, avsaknad av stöd, samt att förmågan behöver stärkas. På *koncernnivå*, vilket innefattar både fallföretaget och dess moderbolag, identifierades prioriteringsförmåga och för låg grad av effektivitet som hinder. När det gäller *extern leverantör* identifierades hinder utifrån ökad belastning, kostnader som måste föras vidare, att det saknas vägledning, motstånd hos underleverantör, att det ej är möjligt att följa upp senare led, inga avtal i led 2 eller 3, längre ledtider, samt oklar hantering med flera EU-kompetenter. Speciellt mindre leverantör upplever väldigt omfattande hinder.

Vilka möjliggörande åtgärder främjar syftet om stärkt digital motståndskraft i de digitala leveranskedjorna utifrån ett DORA-införande?

Uppsatsen identifierar ett stort antal möjliggörande åtgärder på en övergripande nivå, eller utifrån specifik aktör. På en *övergripande nivå* identifierades möjliggörande åtgärder såsom gemensam standard eller ramverk och accepterad certifiering, att samarbeta med andra aktörer, säkra kompetensförsörjningen, att kommunicera värdet med IS-aktivitet, samt att säkra finansiering vid kris. Utifrån *oberoende revisor* identifierades det att erbjuda certifiering är en möjliggörande åtgärd. För aktören *tillsynsmyndighet* identifierades möjliggörande åtgärder såsom visa resultat och värde, snabb och relevant analysförmåga, hänvisa till standard eller ramverk, samt att låta oberoende revisorer utföra granskning och utfärda certifiering. På *koncernnivå* identifierades möjliggörande åtgärder såsom att främja prioriteringsförmågan, främja effektivitet, främja agilitet i riskhanteringen, främja kontinuitet och återställningsförmåga, samt främja relevant information i riskhanteringen. För *fallföretaget* har den möjliggörande åtgärden med att säkra internt utlagd veksamhet avskiljts, för att säkra att intressekonflikter inte uppstår. När det gäller *extern leverantör* har det identifierats en möjliggörande åtgärd med att samordna kunders perspektiv.

Vilka skillnader finns det i att hantera internt utlagd verksamhet i förhållande till helt extern leverans utifrån ett DORA-införande?

Uppsatsen beskriver att DORA inte innebär olika regelverkskrav beroende på om det avser internt utlagd verksamhet, eller om det avser externt utlagd verksamhet. DORA föranleder större krav på detaljering och uppföljning. Det skapas ett förändringstryck mot att standardisera uppföljningen för internt utlagd verksamhet. Samtidigt finner uppsatsen att intressekonflikter måste säkras, oavsett vilka andra möjliggörande åtgärder som införs.

Leder DORA och utökade krav på riskhantering inom digital leveranskedjor till ökade förutsättningar att öka Sveriges digitala motståndskraft?

Uppsatsen kommer fram till att det övergripande skapas ett stort förändringstryck i samband med ett DORA-införande, vilket då leder till förutsättningar för olika aktörer att införa möjliggörande åtgärder. Samtidigt kommer de möjliggörande åtgärderna att medföra olika följdverkningar inom systemet som helhet. Aktörerna uppmanas att utifrån uppsatsen bedöma de möjliggörande åtgärderna utifrån 3E-modell av Checkland och Puolter (2020). I definitionen 3E ingår begreppen *efficacy* (avser direkta effekter som åtgärden innebär), *effectiveness* (avser hur pass resurssnål åtgärden är) och *effeciency* (avser indirekta, eller mer långsiktiga effekter i systemet som helhet). Detta ger bättre förutsättning än att enbart använda det svenska uttrycket *effektivitet*. Vidare innebär ett DORA-införande att det i mycket högre grad krävs samarbete med andra aktörer för att komplexitetshöjningen ska kunna hanteras på ett optimalt sätt. Speciellt de mindre leverantörernas situation behöver beaktas för att minska följdverkningar inom systemet som helhet.

6.2 Teoretiska implikationer och förslag till vidare forskning

Denna uppsats ger en insikt i att det inte finns en ”silver bullet” inom IS. Precis som Vuorinen och Tetri (2012) visar, uppstår det ständiga följdverkningar genom indirekt effekter. Detta uppenbarar sig speciellt om det rör en problemformulering som påverkar flera dimensioner inom IS. Ett DORA-införande är ett sådant exempel. Med tanke på att informationssäkerhet därmed bör ses som en komplexitetshöjande ”entitet” eller ”aktör” i sig, så är det rimligt med en holistisk ansats. Den litteratur som beskriver införande av ledningssystem av informationssäkerhet visade sig vid litteraturgenomgången vara mer inriktad på det holistiska, då detta precis som ett DORA-införande får breda effekter och flertalet följdverkningar. Det behöver inte nödvändigtvis betyda att annan litteratur som undersöker enstaka orsakssamband inte har ett värde. Genom fallstudien kunde flertalet orsakssamband bekräftas. Uppsatsen utgör ett exempel på en deduktiv ansats som ger möjligheter att använda befintlig forskning, men som även ger möjlighet att utifrån empiri komplettera med andra begrepp och tema. Detta är speciellt värdefullt med tanke på risken för begreppsförvirring, som kan uppstå om en rent deduktiv ansats används. Det finns flertalet begrepp som delvis överlappar. En deduktiv metod kan komma att innehålla felaktiga slutsatser om det inte sker kompletterande induktiva steg som ger utrymme för tolkning. Uppsatsen visar att en utgångspunkt med av Checkland och Poulter (2020) beskriven SSM lämpar sig för att skapa en mer holistisk översikt för komplexa systemmässiga effekter.

Genom uppsatsen har det identifierats att mindre aktörer kan påverkas negativt i hög grad utifrån större förändringar i systemet som tillkommer utifrån regelverksimplementation. Det skulle därav kunna finnas ett intresse av att bekräfta eller förkasta detta genom uppföljande forskning. Här skulle en kvantitativ ansats kunna vara lämplig, att genom omfattande urval säkra generaliserbarhet. Då uppsatsen avser ett fallföretag i Sverige skulle det kunna finnas behållning av att replikera undersökningen i andra EU-länder, med syfte att identifiera skillnader. Det har identifierats att samarbeten mellan aktörer bedöms vara en avgörande möjliggörande åtgärd. Därmed skulle det finnas behållning av att utifrån Schneider et al. (2017) jämföra kostnadsperspektiven för de två vägval som bemöter extern komplexitet, det vill säga (1) intern komplexitetshöjning, eller (2) komplexitetshöjning genom samarbete.

6.3 Praktiska implikationer

Den övergripande implikationen är att tillkommande komplexitet kan nå en punkt där det uppstår behov av att förändra inte enbart direkta IS-förmågor, utan att det även leder till att den sammantagna strukturen och styrningen i organisationen behöver ses över. Det leder även till behov av anpassning av organisationens externa samarbeten. Ett sätt att organiskt hantera detta, är att säkra att ledningen förstår de operativa konsekvenserna och därmed proaktivt agerar för att säkra en kontinuerlig anpassning. Det leder i förlängningen även till att IS-perspektivet mer naturligt integreras inom andra möjliggörande åtgärder som identifierats inom ramen för denna uppsats. Aktörerna bör även beakta indirekta effekter i systemet som helhet och utifrån andra aktörers perspektiv. Slutligen är det viktigt att värdet med IS och digital motståndskraft beskrivs och diskuteras. Det leder till bättre förutsättningar att öka den digitala motståndskraften som en naturlig del i vardagen.

Referenser

Andersson, A., Hedström, K., & Karlsson, F. (2022). Standardizing information security – a structurational analysis. *Information & Management, 59*(3), 1-13. https://doi.org/10.1016/j.im.2022.103623

Angst, C., Block, E., D'Arcy, J., & Kelley, K. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quaterly, 41*(3), 893-916. https://doi.org/10.25300/MISQ/2017/41.3.10

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems, 147*, 1-14. https://doi.org/10.1016/j.dss.2021.113580

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological Antecedents and Implications. *MIS Quaterly, 35*(4), 831-858. https://doi.org/10.2307/41409963

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys, 25*(4), 375-414. https://doi.org/10.1145/162124.162127

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management, 54*(7), 887-901. https://doi.org/10.1016/j.im.2017.01.003

Benbasat, I., Goldstein, D., & Mead, M. (2002). The Case Research Strategy in Studies of Information Systems. i M. Myers, & D. Avison, *Qualitative Research in Information Systems: A Reader.* SAGE Publications, Limited.

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

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548. https://doi.org/10.2307/25750690

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Bansabat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management, 52*(4), 385-400. https://doi.org/10.1016/j.im.2014.12.004

Checkland, P., & Puolter, J. (2020). Soft Systems Methodology. i M. Reynolds, & S. Holwell, *Systems Approaches to Making Change: a Practical Guide.* Springer.

Chen, P.-Y., Kataria, G., & Krishnan, R. (2011). Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quaterly, 35*(2), 397-422. https://doi.org/10.2307/23044049

Chen, X., Wu, D., Chen, L., & Teng, J. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management, 55*(8), 1049-1060. https://doi.org/10.1016/j.im.2018.05.011

Constantinides, P., Chiasson, M., & Introna, L. (2012). The Ends of Information Systems Research: A Pragmatic Framework. *MIS Quaterly, 36*(1), 1-19. https://doi.org/10.2307/41410403
Cram, W., D'Arcy, J., & Proudfoot, J. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quaterly, 43*(2), 525-554. https://doi.org/10.25300/MISQ/2019/15117
Dhillon, G. (2006). *Principles of information systems security: text and cases.* John Wiley Sons.
Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314. https://doi.org/10.1111/j.1365-2575.2006.00219.x
Dlamini, M., Eloff, J., & Eloff, M. (2009). Information security: The moving target. *Computers & Security, 28*(3), 189-198. https://doi.org/10.1016/j.cose.2008.11.007
Donalds, C., & Barclay, C. (2022). Beyond technical measures: a value-focused thinking appraisal of strategic drivers in improving information security policy compliance. *European Journal of Information Systems, 31*(1), 58-73. https://doi.org/10.1080/0960085X.2021.1978344
Drummond, H. (2011). MIS and illusions of control: an analysis of the risks of risk management. *Journal of Information Technology, 26*(4), 259-267. https://doi.org/10.1057/jit.2011.9
Eriksson, V. (den 23 juli 2021). *Efter Coop-hacket - Keseya säger att de fått krypteringsnyckeln*. ComputerSweden: https://computersweden.se/article/1284643/efter-coop-hacket-kaseya-sager-att-de-fatt-krypteringsnyckeln.html
Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. *Journal of the Association for Information Systems, 12*(9), 606-631. https://doi.org/10.17705/1jais.00275
Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quaterly, 30*(3), 611-642. https://doi.org/10.2307/25148742
Guo, K., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49*(6), 320-326. https://doi.org/10.1016/j.im.2012.08.001
Gupta, A., & Zhdanov, D. (2012). Growth and Sustainability of Managed Security Services Networks: An Economic Perspective. *MIS Quaterly, 36*(4), 1109-1130. https://doi.org/10.2307/41703500
Han, K., Choi, J., Choi, Y., Lee, G., & Whinston, A. (2023). Security defense against long-term and stealthy cyberattacks. *Decision Support Systems, 166*, 1-15. https://doi.org/10.1016/j.dss.2022.113912
Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems, 20*(4), 373-384. https://doi.org/10.1016/j.jsis.2011.06.001
Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an

email authentication service. *Information Systems Journal, 24*(1), 61-84. https://doi.org/10.1111/j.1365-2575.2012.00420.x
Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. https://doi.org/10.1016/j.im.2013.10.001
Jackson, M. (2003). *Systems Thinking: Creative Holism for Managers.* John Wiley & Sons.
Jacobsen, D. (2002). *Vad, hur och varför? Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen.* Lund: Studentlitteratur AB.
Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems, 32*(1), 35-51. https://doi.org/10.1080/0960085X.2022.2088414
Kvale, S., & Brinkmann, S. (2009). *Den kvalitativa forskningsintervjun.* Lund: Studentlitteratur AB.
Kwon, J., & Johnson, M. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quaterly, 38*(2), 451-471. https://www.jstor.org/stable/26634934
Larson, K. (1998). The role of service level agreements in IT service delivery. *Information Management & Computer Security, 6*(3), 128-132. https://doi.org/10.1108/09685229810225029
Lee, C., Geng, X., & Raghunathan, S. (2016). Mandatory Standards and Organizational Information Security. *Information Systems Research, 27*(1), 70-86. https://doi.org/10.1287/isre.2015.0607
Li, W., Leung, A., & Yue, W. (2023). Where is IT in Information Security? The Interrelationship among IT Investment, Security Awareness, and Data Breaches. *MIS Quaterlu, 47*(1), 317-342. http://dx.doi.org/10.2139/ssrn.3581594
Liang, H., Xue, Y., & Wu, L. (2012). Ensuring Employees' IT Compliance: Carrot or Stick? *Information Systems Research, 24*(2), 279-294. https://doi.org/10.1287/isre.1120.0427
Lin, C., Wittmer, J., & Luo, X. (2022). Cultivating proactive information security behavior and individual creativity: The role of human relations culture and IT use governance. *Information & Management, 59*(6), 1-13. https://doi.org/10.1016/j.im.2022.103650
Lindström, K. (den 23 januari 2024). *Attacken mot Tietoevry kan ta veckor att åtgärda*. ComputerSweden: https://computersweden.idg.se/2.2683/1.780804/attacken-mot-tietoevry-kan-ta-veckor-att-atgarda
Lowry, P., & Moody, G. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal, 25*(5), 433-463. https://doi.org/10.1111/isj.12043
Lyytinen. (2011). MIS: the urge to control and the control of illusions – towards a dialectic. *Journal of Information Technology, 26*, 268-270. https://doi.org/10.1057/jit.2011.12

Mani, D., Barua, A., & Whinston, A. (2010). An Empirical Analysis of the Impact of Information Capabilities Design on Business Process Outsourcing Performance. *MIS Quaterly, 34*(1), 39-62. https://doi.org/10.2307/20721414

Moody, G., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quaterly, 42*(1), 285-311. https://aisel.aisnet.org/trr/vol7/iss1/2

Morecroft, J. (2020). System Dynamics. i M. Reynolds, & S. Holwell, *Systems approaches to making Change: A Practical Guide* (2 uppl., ss. 25-88). London: Springer.

Myndigheten för samhällsskydd och beredskap (MSB). (2023). *När kriget kom nära – Årsrapport it-incidentrapportering 2022 (ISBN: 978-91-7927-371-2).* https://rib.msb.se/filer/pdf/30339.pdf

Myndigheten för samhällsskydd och beredskap (MSB). (den 3 april 2023). *Policyöversikt - Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete.* https://www.msb.se/contentassets/270df7e79dea47869bd8bfb50b6629fa/policyoversikt-eucyber_v1.1.pdf

Myndigheten för samhällsskydd och beredskap (MSB). (2024). Cyberangrepp mot samhällsviktiga informationssystem (ISBN: 978-91-7927-459-7). https://rib.msb.se/filer/pdf/30558.pdf

Mähring, M., Wiener, M., & Remus, U. (2018). Getting the control across: Control transmission in information systems offshoring projects. *Information Systems Journal, 28*(4), 708-728. https://doi.org/10.1111/isj.12155

Nazareth, D., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management, 52*(1), 123-134. https://doi.org/10.1016/j.im.2014.10.009

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

Njenga, K., & Brown, I. (2012). Conceptualising improvisation in information systems security. *European Journal of Information Systems, 21*(6), 592-607. https://doi.org/10.1057/ejis.2012.3

Nuijten, A., Keil, M., van der Pijl, G., & Commandeur, H. (2018). IT managers' vs. IT auditors' perceptions of risks: An actor–observer asymmetry perspective. *Information & Management, 55*(1), 80-93. https://doi.org/10.1016/j.im.2017.04.002

Nylén, U. (2005). *Att presentera kvalitativa data: Framställningsstrategier för empiriredovisning.* Malmö: Liber AB.

Näringsdepartementet. (2018). *Granskning av Transportstyrelsens upphandling av it-drift (Ds 2018:6).* Elanders Sverige AB,. https://data.riksdagen.se/fil/FB3C8AF9-BE36-4E7F-A09B-80D12887C189

Ogbanufe, O., Kim, D., & Jones, M. (2021). Informing cybersecurity strategic commitment through top management perceptions: The role of institutional

pressures. *Information & Management, 58*(7), 1-18. https://doi.org/10.1016/j.im.2021.103507
Ohlin, J. (den 6 mars 2019). *Transportstyrelsen – detta har hänt*. SVT Nyheter: https://www.svt.se/nyheter/inrikes/transportstyrelsen-detta-har-hant
Ormond, D., Warkentin, M., & Crossler, R. (2019). Integrating Cognition with an Affective Lens to Better Understand Information Security Policy Compliance. *Journal of the Association for Information Systems, 20*(12), 1794-1843. https://doi.org/10.17705/1jais.00586
Pang, M.-S., & Tanriverdi, H. (2022). Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of U.S. federal government. *Journal of Strategic Information Systems, 31*(1), 1-19. http://dx.doi.org/10.2139/ssrn.2933577
Paul, J., & Wang, X. (2019). Socially optimal IT investment for cybersecurity. *Decision Support Systems, 122*, 1-12. https://doi.org/10.1016/j.dss.2019.05.009
Posey, C., Roberts, T., Lowry, P., & Hightower, R. (2014). Bridging the divide: A qualitative comparison of information security Bridging the divide: A qualitative comparison of information security professionlas and ordinary organizational insiders. *Information & Management, 51*(5), 551-567. https://doi.org/10.1016/j.im.2014.03.009
Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quaterly, 34*(4), 757-778. https://doi.org/10.2307/25750704
Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems, 55*(1), 156-164. https://doi.org/10.1016/j.dss.2013.01.001
Schneider, A., Wickert, C., & Marti, E. (2017). Reducing Complexity by Creating Complexity: A Systems Theory Perspective on How Organizations Respond to Their Environments. *Journal of Management Studies, 54*(2), 182-208. https://doi.org/10.1111/joms.12206
Shiau, W.-L., Wang, X., & Zheng, F. (2023). What are the trend and core knowledge of information security? A citation and co-citation analysis. *Information & Management, 60*(3), 1-21. https://doi.org/10.1016/j.im.2023.103774
Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information management & Computer Security, 22*(3), 279-308. https://doi.org/10.1108/IMCS-05-2013-0041
Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quaterly, 34*(3), 487-502. https://doi.org/10.2307/25750688
Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security "De Jure" Standard in a Government Organization. *MIS Quaterly, 34*(3), 463-468. https://doi.org/10.2307/25750687

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302. https://doi.org/10.1016/j.im.2011.07.002

Spears, J., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quaterly, 34*(3), 503-522. https://doi.org/10.2307/25750689

Stahl, B., Doherty, N., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal, 22*(1), 77-94. https://doi.org/10.1111/j.1365-2575.2011.00378.x

Straub, D., & Welke, R. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quaterly, 22*(4), 441-469. https://doi.org/10.2307/249551

Swedish Institute for Standards (SIS). (2014). Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security (ISO/IEC 27036-3:2023, IDT). Svenska institutet för standarder. https://www.sis.se/en/produkter/information-technology-office-machines/it-security/ss-isoiec-27036-32024/

Temizkan, O., Kumar, R., Park, S., & Subramaniam, C. (2012). Patch Release Behaviors of Software Vendors in Response to Vulnerabilities: An Empirical Analysis. *Journal of Management Information Systems, 28*(4), 305-337. https://doi.org/10.2753/MIS0742-1222280411

THE EUROPEAN PARLIAMENT AND THE COUNCIL. (den 14 december 2022a). *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554&qid=1680197942535

THE EUROPEAN PARLIAMENT AND THE COUNCIL. (den 14 december 2022b). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Tietoevry. (den 21 Januari 2024). *UPDATE: Ransomware attack affecting Tietoevry's services for some customers in Sweden*. https://www.tietoevry.com/en/newsroom/all-news-and-releases/other-news/2024/01/ransomware-attack-in-sweden-update/

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(1), 38-58. https://doi.org/10.1057/ejis.2013.27

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*, 190-198. https://doi.org/10.1016/j.im.2012.04.002

Vedadi, A., & Warkentin, M. (2020). Can Secure Behaviors Be Contagious? A Two-Stage Investigation of the Influence of Herd Behavior on Security Decisions. *Journal of*

the Association for Information Systems, 21(2), 428-459. https://doi.org/10.17705/1jais.00607
Vishwanath, A., Neo, L., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems, 128*, 1-11. https://doi.org/10.1016/j.dss.2019.113160
von Solms, R., van der Haar, H., von Solms, S., & Caelli, W. (1994). A framework for information security evaluation. *Information & Management, 26*(3), 143-153. https://doi.org/10.1016/0378-7206(94)90038-8
Vuorinen, J., & Tetri, P. (2012). The Order Machine – The Ontology of Information Security. *Journal of the Association for Information Systems, 13*(9), 695-713. https://doi.org/10.17705/1jais.00306
Wall, J., Lowry, P., & Barlow, J. (2016). Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess. *Journal of the Association for Information Systems, 17*(1), 39-76. https://doi.org/10.17705/1jais.00420
Wang, T., Wang, Y.-Y., & Yen, J.-C. (2019). It's Not My Fault: The Transfer of Information Security Breach Information. *Journal of Database Management, 30*(3), 18-37. https://doi.org/10.4018/JDM.2019070102
Williams, C. (2011). Client–vendor knowledge transfer in IS offshore outsourcing: insights from a survey of Indian software engineers. *Information Systems Journal, 21*(4), 335-356. https://doi.org/10.1111/j.1365-2575.2010.00354.x
Xiao, J., Xie, K., & Hu, Q. (2013). Inter-firm IT governance in power-imbalanced buyer–supplier dyads: exploring how it works and why it lasts. *European Journal of Information Systems, 22*(5), 512-528.
Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems, 92*, 36-46. https://doi.org/10.1016/j.dss.2016.09.009
Yoo, C., Goo, J., & Rao, H. (2020). Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness. *MIS Quaterly, 44*(2), 907-931. https://doi.org/10.25300/MISQ/2020/15477

Bilagor

Bilaga 1 – Information till potentiella respondenter

Hej!

Jag har påbörjat en uppsats för Linnéuniversitetet där syftet är att öka kunskapen kopplat till DORA-införandet och mer specifikt IT-riskhantering inom IT-leverantörskedjorna. Utgångspunkten är att ett DORA-införande innebär att flera intressenters världsbilder behöver medlas för att få fram rimliga lösningar som ger ett värde och som verkligen stärker organisationens och Sveriges digitala motståndskraft. I samband med det skulle jag väldigt gärna få med ditt perspektiv!

Min önskan är att få hålla en intervju på distans med dig och om möjligt boka upp 1 timme för detta. Intervjun skulle innebära inspelning för att kunna sedan efter samtliga intervjuer analysera de sammantagna insikter som kan dras. Det finns bifogat en intervjuguide som jag tänkt utgå ifrån. Tanken är inte att behöva förbereda något innan intervjuerna och om det finns frågor som man upplever inte kunna svara på så är det helt ok. Det är helt enkelt ett stöd för oss att utgå ifrån.

Intervju är naturligtvis frivillig. Själva intervjuerna kommer även hållas anonymt. Det vill säga att både respondent och organisation inte namnges i uppsatsen. Under själva granskningen av uppsatsen kommer jag dock att behöva ange namn till min handledare samt slutlig betygssättande granskare inom Linnéuniversitet. Intervjufiler osv kommer att efter avslut att tas bort och lagras fram till dess skyddat.

Hoppas det går att lösa en intervju!

Hälsningar,

Christian Dohrendorf

Linnéuniversitetet
Institutionen för informatik

351 95 Växjö / 391 82 Kalmar
Tel 0772-28 80 00
Lnu.se

Bilaga 2 – Intervjuguide

Inledning/orientering

- Finns det något som är oklart som behöver lyftas innan det att den inspelade intervjun påbörjas?

Är begreppen IT-leverantörskedja och digital motståndskraft tillräckligt definierade?

- Hur skulle du definiera begreppet digital motståndskraft?
- Hur skulle du definiera begreppet IT-leverantörskedja?

Vad innebär DORA-kraven kring IT-leverantörskedjor?

- Hur ser du på krav på att hantera IT-risker genom hela IT-leverantörskedjor, är det en större skillnad mot tiden innan DORA?
- Hur ser du på krav att tillsynsmyndighet ska kunna följa upp risken i IT-leverantörskedjor, är det en större skillnad mot tiden innan DORA?
- Ser du något annat som DORA innebär för förhållande mellan företag och IT-leverantör (direkt eller indirekt)?

Vilka hinder finns det att införa DORA-kraven utifrån riskhanteringen inom IT-leverantörskedjorna?

- Ser du något som kan vara extra utmanande med DORA när det gäller kraven på riskhantering eller rapportering till tillsynsmyndighet utifrån IT-leverantörskedjorna?

Vilka skillnader finns det i att hantera koncerngemensamma IT-leverantörer i förhållande till helt externa leverantörer?

- Finns det skillnader i hanteringen av koncerngemensamma IT-leverantörer mot externa leverantörer?
- Vad behöver beaktas mer specifikt i att hantera koncerngemensamma IT-leverantörer med tanke på DORAs krav?

Linnéuniversitetet
Institutionen för informatik

351 95 Växjö / 391 82 Kalmar
Tel 0772-28 80 00
Lnu.se

Vilka råd bör ges till organisationer för att uppnå hög grad av informationssäkerhet för att hantera risker som kopplas till IT-leverantörskedjorna?

- Vad tror du är framgångsfaktorer för att säkra kraven på hantering av IT-leverantörskedjor enligt DORA? Exempel på åtgärder återfinns i tabellen nedanför.
- Vad tror du ger mest värde i att förändra?
- Vad är viktiga perspektiv för dig i införandet av DORA?

Genomföra analys över leveranskedjor	Uppdatera avtal med leverantörerna
Incidenthantering	Relevant gränssnitt med leverantör
Kontinuitet- och återställningsförmåga	Samarbeta med andra aktörer
Tydliga definitioner	Threat Intelligence
Styrning för IT-upphandling och erbjuda stöd till upphandlarna	Riskhantering
Uppföljning mot leverantör	Finansiering av IS
Höjd säkerhetsmedvetenhet genom utbildning	Oberoende granskning och certifiering
SLA per leverantör	Holistisk styrning
Ledningssystem	Ledningens engagemang i IS-relaterade frågor
Tydliga klausuler vid upphandling om informationsplikt	Moderniserad IT

Leder väldigt detaljerade regleringar till att det blir bättre förutsättningar att öka Sveriges digitala motståndskraft?

- Ser du att införande av DORA leder till högre digital motståndskraft i IT-leverantörskedjor?

Linnéuniversitetet
Institutionen för informatik

351 95 Växjö / 391 82 Kalmar
Tel 0772-28 80 00
Lnu.se

- Ser du att det finns en risk att DORA och andra omfattande regleringar leder till att det blir svårt med att prioritera rätt åtgärder utifrån ett helhetsperspektiv?

- Tror du det finns alternativ till DORA-kraven och att hantera det på annat sätt än en reglering?

Uppföljning/avslut

- Finns det något annat du skulle vilja lyfta upp innan det att vi avslutar den inspelade intervjun?

Linnéuniversitetet
Institutionen för informatik

351 95 Växjö / 391 82 Kalmar
Tel 0772-28 80 00
Lnu.se