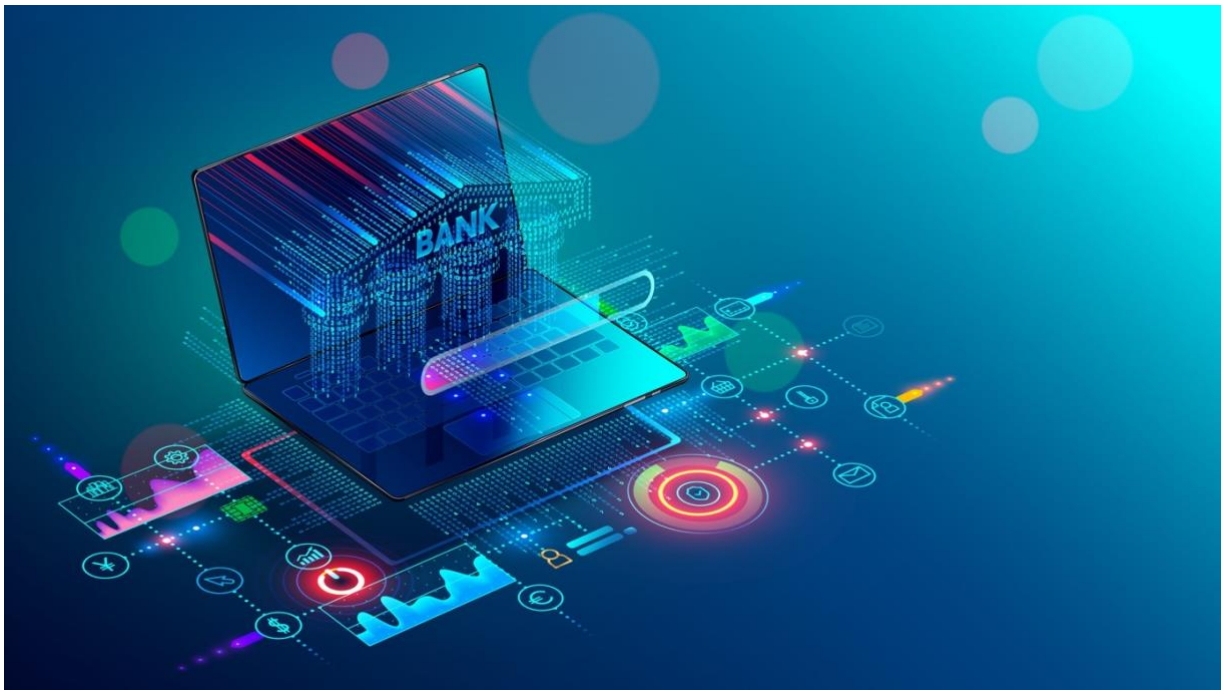
Risiko knyttet til utkontraktering av IKT-tjenester i bank- og finanssektoren



(Cicero, u. å)

«Sikkerheten vår blir ikke bedre enn det svakeste leddet i leverandørkjeden» (NSM, 2023)

Masterstudium i samfunnssikkerhet

Universitetet i Stavanger

Juni 2023

Helene Gibbs og Elida Grønningsæter

DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i samfunnssikkerhet	*Vår*semesteret, *2023* Åpen
Forfatter: Helene Gibbs og Elida Grønningsæter	Helene Gibbs Elida Grønningsæter *(Signatur forfatter)*
Fagansvarlig: Ole Andreas Engen Veileder: Ole Andreas Engen	
Tittel på masteroppgaven: Risiko knyttet til utkontraktering av IKT-tjenester i bank- og finanssektoren Engelsk tittel: Risk Associated with Outsourcing of ICT Services in the Banking and Financial Sector	
Studiepoeng: 30	
Emneord: Utkontraktering, risiko, bank og finans, usikkerhet, sårbarhet, safety og security, trefaktormodellen, risikostyring, NAT, HRO, resiliens	Sidetall: **79** + vedlegg/annet: 106 Stavanger, 14.06.2023

Forord

Det er med stor takknemlighet vi ferdigstiller denne masteroppgaven som en del av masteren i samfunnssikkerhet ved Universitetet i Stavanger. De to siste årene har vært spennene, lærerike og utfordrende. Denne oppgaven representerer avslutningen på flere års arbeid og vi ønsker å takke alle som har bidratt til å gjøre dette prosjektet mulig.

Først og fremst vil vi rette en stor takk til vår veileder Ole Andreas Engen for konstruktive tilbakemeldinger og motiverende ord gjennom hele oppgaven. Vi vil også takke andre akademikere og professorer på fakultetet som har bidratt til å gjøre de siste to årene svært lærerike. Takk til informantene som har bidratt med verdifull data og innsikt i denne studien, uten deres vilje til å dele ville ikke studien vært mulig å gjennomføre.

Vi ønsker å takke våre nærmeste for tålmodighet, oppmuntring og støtte gjennom hele studieløpet. Tusen takk til alle studievenner vi har fått gjennom masteren i samfunnssikkerhet. Dere har alle bidratt til at både motivasjon og humør har holdt seg oppe, i tillegg til at dere mer enn gjerne har delt av deres kunnskap, noe vi har satt stor pris på.

Sist, men ikke minst vil vi takke hverandre for godt samarbeid og felles innsats. Vi er både stolt av å levere denne oppgaven og vennskapet som har utviklet seg. En stor lærdom vi sitter igjen med etter skriveprosessen er at ting tar tid. God lesning!

Stavanger, 14.06.23
Helene Gibbs og Elida Grønningsæter

Sammendrag

Denne studien tar for seg risiko knyttet til utkontraktering av IKT-tjenester i bank- og finanssektoren, samt hvordan denne risikoen håndteres. Rask teknologisk utvikling fører til et økende behov for spesialisert kunnskap, hvor utkontraktering i stor grad brukes som en løsning. Denne utviklingen fører til stadige endringer i risikobildet, noe som kompliserer utkontrakteringsprosessen. Hensikten med studien var derfor å undersøke risikoene som oppstår ved utkontraktering og hvordan sektoren arbeider for å håndtere disse. Følgende problemstilling er belyst:

> *På hvilken måte representerer utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren risiko, og hvordan håndteres den?*

For å besvare studiens problemstilling har vi undersøkt hvilke risikoer utkontrakteringsprosessen representerer, hvordan risikostyringsinstrumenter utvikles, samt hvordan lovverk og krav virker risikoreduserende. Studien bygger på en todelt teoretisk tilnærming. Den første delen omhandler risikobegrepet, dimensjoner ved risiko og risikostyring, mens den andre delen tar for seg organisatoriske aspekter og bygger på teoriene om Normal Accident, High Reliability Organizations og resiliens. Dokumentanalyse av relevante offentlige dokumenter og intervjuer med seks nøkkelinformanter dannet det empiriske grunnlaget for diskusjonen.

Analysen viser at utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren er preget av kompleksitet og tette koblinger, i tillegg til at den representerer ulike typer risiko. Studien har identifisert at hovedrisikoene er leverandørkjedeangrep, avhengigheter, konsentrasjonsrisiko, finansiell stabilitet, operasjonell risiko og systemrisiko. Til tross for dette viser det seg at sektoren er avhengig av å påta seg denne risikoen for å blant annet være konkurransedyktige, få spesialiserte tjenester, redusere kostnader og økte effektiviteten. Som et resultat av dette har sikkerhet og risikostyring derfor høy prioritert. Virksomhetene arbeider kontinuerlig med å kartlegge utfordringer i utkontrakteringsprosessen og benytter ulike risikostyringsverktøy for å håndtere risikoene. Noen av disse er utviklet internt i banken, som eksempelvis en prosess som kalles POPs og et system for leverandøroppfølging. Lovverket spiller også en sentral rolle som et risikostyringsverktøy. Selv om det ikke er enighet om hvorvidt lovverket fungerer etter hensikt, er det enighet om at det fungerer risikoreduserende.

Abstract

This study examines the risks associated with outsourcing ICT services in the banking and finance sector and how these risks are managed. Rapid technological development leads to an increasing need for specialized knowledge, where outsourcing is widely used as a solution. This results in constant changes in the risk landscape, which complicates the outsourcing process. Therefore, the study aimed to investigate the risks that arise from outsourcing and how the sector works to manage them. The following research question is addressed:

> *In what ways does the outsourcing process of ICT services in the banking and finance sector represent risk, and how is it managed?*

To answer our research question, we have examined the risks that the outsourcing process represents, how risk management tools are developed, and how legislation and requirements contribute to risk reduction. The study is based on a two-part theoretical approach. The first part addresses the concept of risk, dimensions of risk, and risk management, while the second part focuses on organizational aspects and builds on theories of Normal Accident, High Reliability Organizations, and resilience. Document analysis of relevant public documents and interviews with six key informants formed the empirical basis for the discussion.

The analysis shows that the outsourcing process of ICT services in the banking and finance sector is characterized by complexity and tight coupling, representing various types of risks. The study has identified that the main risks are supply chain attacks, dependencies, concentration risks, financial stability, operational risk, and systemic risk. Despite this, it is evident that the banking and finance sector is dependent on assuming these risks in order to, remain competitive, obtain specialized services, reduce costs, and increase efficiency. As a result, security and risk management are given high priority. Businesses continuously work to identify potential challenges in the outsourcing process and use various risk management tools to manage risks. Some of these tools are developed internally within the bank, such as a process called “POPs” and a supplier management system. Although there is no consensus on whether the legislation functions as intended, there is agreement that it helps to reduce risk.

Liste over forkortelser

AI	Artificial intelligence
BIA	Business Impact Analysis
DNB	Den norske bank
DORA	Digital Operations Resilience Act
DSB	Direktoratet for samfunnssikkerhet og beredskap
EBA	Den europeiske banktilsynsmyndigheten
EIOPA	Den europeiske tilsynsmyndigheten for forsikring og tjenestepensjon
ESMA	Den europeiske verdipapir- og markedstilsynsmyndigheten
FFI	Forsvarets forskningsinstitutt
GNF	Grunnleddende nasjonale funksjoner
HRO	High Reliability Organizations
IKT	Informasjons- og kommunikasjonsteknologi
KIKS	Kritisk infrastruktur og kritiske samfunnsfunksjoner
Meld. St.	Melding til Stortinget
NAT	Normal Accident Theory
NIFU	Norsk institutt for studier av innovasjon, forskning og utdanning
NIST	National Institute of Standards and Technology
NOU	Norsk Offentlig Utredning
NSD	Norsk senter for forskningsdata
NSM	Nasjonal Sikkerhetsmyndighet
POPs	Produkt- og prosesscoring
PST	Politiets sikkerhetstjeneste
PwC	PricewaterhouseCoopers
SaaS	Software as a Service

Innholdsfortegnelse

1.0 Innledning 1
1.1 Problemstilling og tilhørende forskningsspørsmål 2
1.2 Avgrensning 3
1.3 Oppgavens oppbygning 4
2.0 Kontekst 5
2.1 Utkontraktering 5
2.2 Bank- og finanssektoren i Norge 6
3.0 Teoretisk grunnlag 9
3.1 Risiko 9
3.1.1 Systemrisiko 10
3.1.2 Sårbarhet 11
3.1.3 Usikkerhet 11
3.2 Safety og Security 12
3.2.1 Safety 12
3.2.2 Security 13
3.3 Trefaktormodellen 14
3.4 Risikostyring 16
3.4.1 Risiko – og sårbarhetsanalyser (ROS-analyser) 17
3.5 Normal Accident Theory (NAT) 17
3.6 High Reliability Organisations (HRO) 19
3.7 Resiliens 20
4.0 Forskningsdesign og metodisk tilnærming 23
4.1 Metodisk tilnærming og datainnsamling 23
4.1.1 Kvalitativt forskningsintervju 24
4.1.2 Dokumentanalyse 28
4.2 Forskningskvalitet 30
4.2.1 Reliabilitet 30
4.2.2 Validitet 31
5.0 Presentasjon av empiri og diskusjon 33
5.1 Empiriske funn og diskusjon av forskningsspørsmål 1 33
5.1.1 Risikoidentifisering 34
5.1.2 Utkontrakteringsrisiko 37
5.1.3 Diskusjon av forskningsspørsmål 1 44
5.1.4 Oppsummering av forskningsspørsmål 1 49
5.2 Empiriske funn og diskusjon av forskningsspørsmål 2 50
5.2.1 Risikostyringsverktøy 50

5.2.2 Utfordringer med å styre risiko som følge av utkontrakterte IKT-tjenester 56
5.2.3 Diskusjon av forskningsspørsmål 2 60
5.2.4 Oppsummering av forskningsspørsmål 2 66
5.3 Empiriske funn og diskusjon av forskningsspørsmål 3 66
5.3.1 Føringene lovverket legger 67
5.3.2 Utfordringer knyttet til lovverket 70
5.3.3 Diskusjon av forskningsspørsmål 3 73
5.3.4 Oppsummering av forskningsspørsmål 3 77
6.0 Konklusjon 78
6.1 Forslag til videre forskning 79
Referanseliste 80

Liste over tabeller:

Tabell 1: Oppgavens oppbygning

Tabell 2: Utvalg til intervjuer

Tabell 3: Tidspunkt og tidsbruk på intervjuer

Tabell 4: Utvalg av de mest sentrale dokumentene

Liste over figurer:

Figur 1: Avgrensning mellom safety og security (inspirert av Jore, 2019, s.162)

Figur 2: Visualisering av trefaktormodellen (inspirert av Busmundrud et al., 2015, s.34)

Figur 3: Forskningsdesign

1.0 Innledning

Denne oppgaven omhandler risiko knyttet til utkontrakteringsprosessen av informasjons- og kommunikasjonsteknologi (IKT) i bank- og finanssektoren, og hvordan denne risikoen håndteres. Utkontraktering av IKT-tjenester i bank- og finanssektoren øker stadig grunnet behovet for mer spesialisert kunnskap. En slik organisering blir en sentral del av virksomheters drift og fører med seg muligheter, samtidig som det øker systemenes kompleksitet og skaper utfordringer ved at virksomhetens verdier eksponeres for risiko på nye måter. Det siste tiåret har det skjedd store endringer av trusler, farer og risiko knyttet til cyber, hvor cyberdomene i dag gjennomsyrer finanssektoren (Skjelvik, 2019). Den digitale utviklingen fører med seg nye sårbarheter, spesielt ettersom flere systemer og enheter kobles sammen slik at den samfunnsmessige sårbarheten utvides (NOU 2018:14).

Utkontraktering fører med seg risiko gjennom hele prosessen, fra vurderingsfasen og frem til oppfølging av leverandørene (Norges Bank, 2021a). Leverandørkjedene er tett koplet, noe som medfører at sårbarheter og feil et sted i kjeden kan forplante seg raskere og enklere mellom leddene. Ifølge DSB (2020) representerer dette en strukturell sårbarhet. Lange og uoversiktlige leverandørkjeder bidrar til sårbarheter, noe trusselaktører utnytter for å nå sine egentlige mål (NSM, 2023). Økt kompleksitet, digitalisering, avhengighet, tette koplinger, og hybride trusler synliggjør utkontrakteringens påvirkning på risikobilde (NSM, 2021). En kan derfor anta at det blir vanskeligere å holde oversikt og styre risiko i utkontrakteringsprosessen, spesielt når underleverandører leverer mange av støttetjenestene som virksomhetene er avhengig av (Skjelvik, 2019; Norges Bank, 2021a). Denne prosessen blir dermed en viktig kilde for å kunne oppdage, samt identifisere risiko og håndtere den på best mulig måte for å avverge potensielt sikkerhetstruende virksomhet.

I Sårbarhetsutvalgets rapport (NOU 2000:24) ble IKT-systemene fastslått til å være en av samfunnets bærebjelker. Samfunnet har i den forbindelse blitt mer sårbart for svikt i disse systemene. Samspillet mellom raskere teknologiutvikling og effektivisering, i tillegg til økende kompleksitet og lange verdikjeder, skaper en dynamisk risikosituasjon. Parallelt utvikler den digitale sårbarhetsflaten seg, noe som hverken myndigheter, virksomheter eller enkeltindivider er skjermet for (NSM, 2023). For å kunne håndtere risikoen utkontraktering medfører, er det en forutsetning å etterleve lover, forskrifter og krav. Innføring av lovkrav gjør at bankene må

endre måten de arbeider på, noe som kan medføre økt risiko og sårbarhet (Slettemoen & Ertenstein, 2018).

Ifølge NSM (2023) er det korte tidsrammer for å etablere og opprettholde tilfredsstillende sikkerhetsnivå. Risikovurderinger og sikkerhetstiltak må derfor kontinuerlig tilpasses et risikobilde i stadig endring. I tillegg viser NSM (2023) at Norge har gode forutsetninger for å møte utfordringene dersom tiden *nå* brukes godt, og vektlegger at motstandskraft og robusthet bygges best i fredstid. I utredningen fra Lysne-utvalget (NOU 2015:13) ble det påpekt at komplekse digitale verdikjeder hindrer oss i å kunne fastslå hvilke digitale sårbarheter vi har, og ingen virksomheter vil dermed kunne ha full oversikt over sine egne sårbarheter.

1.1 Problemstilling og tilhørende forskningsspørsmål

Formålet med studien er å se på risiko i en organisatorisk sammenheng, ved å belyse hvordan utkontrakteringsprosessen av IKT-tjenester representerer risiko i bank- og finanssektoren, og hvordan den håndteres. Som vi er kjent med er temaet forsket liten på, noe som motiverte oss til å undersøke dette nærmere. Vi ønsket dermed å finne ut av hvordan ansatte i banker, tilsynsmyndigheter og eksperter forstår og arbeider med risiko i denne sammenhengen. På bakgrunn av dette er følgende problemstilling lagt til grunn:

> ***På hvilken måte representerer utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren risiko, og hvordan håndteres den?***

Vi har formulert tre forskningsspørsmål, som på hver sin måte skal bidra til å belyse problemstillingen. For å forstå hvilke risikoer organiseringen representerer, vil vi undersøke hvilke risikoer bank- og finanssektoren står overfor som følge av utkontrakteringsprosessen av IKT-tjenester. Dette har ført frem til formuleringen av studiets første forskningsspørsmål:

> Hvilke risikoer representerer utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren?

Videre ønsker vi å undersøke hvordan bank- og finanssektoren håndterer risiko knyttet til utkontraktering av IKT-tjenester, og hvilke verktøy de benytter seg av. Dette har ført frem til formuleringen av studiets andre forskningsspørsmål:

> Hvordan blir risikostyringsinstrumenter utviklet i forbindelse med utkontrakteringsprosessen i bank- og finanssektoren?

Utkontraktering av IKT-tjenester i bank- og finanssektoren er sterkt regulert av lovverk i stadig utvikling. Vi vil derfor belyse hvordan det legger føringer for utkontraktering. Studiets siste forskningsspørsmål er formulert slik:

> På hvilken måte virker lovverk og krav risikoreduserende ved utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren?

1.2 Avgrensning

Studiens omfang krever flere avgrensninger da bank- og finanssektoren i Norge er en stor sektor, bestående av en rekke ulike offentlige og private aktører. Derfor er studien avgrenset til å undersøke risiko knyttet til utkontrakteringsprosessen av IKT-tjenester i én bank. Det er fokusert på vurderingene og hensynene som tas fra vurderingen om en tjeneste skal utkontrakteres, til tjenesten er utkontraktert. Vi har valgt å fokusere på IKT-tjenester, da det anses som spesielt utfordrende å sette ut i forhold til etterlevelsen av regelverket. I tillegg har nasjonale risikorapporter identifisert utkontraktering av IKT-tjenester som en kilde til betydelig risiko. Den empiriske datainnsamlingen er avgrenset til dybdeintervjuer av ansatte i én bank, med supplerende intervjuer fra eksterne nøkkelinformanter, samt dokumentanalyse av offentlig tilgjengelige dokumenter. Det teoretiske rammeverket er todelt, hvor første del vil se på ulike dimensjoner av risikobegrepet og risikostyring. Den andre delen vil se på et teoretisk organisatorisk perspektiv med bidrag fra Normal Accident Theory, High Reliabilty Organizations og resiliens. Samlet vil disse teoriene bidra med å svare på hvordan utkontraktering representerer risiko, og hvordan den håndteres.

1.3 Oppgavens oppbygning

Tabell 1 presenterer oppgavens oppbygning med tilhørende kapittelinndeling.

Tabell 1: Oppgavens oppbygning

	Fokusområde
1: Innledning	I det innledende kapittelet presenteres bakgrunn og tema for studien, i tillegg til valgt problemstilling og tilhørende forskningsspørsmål. Studiens avgrensninger og beskrivelse av utforming inkluderes.
2: Kontekst	Begrepet utkontraktering vil her redegjøres for, før det gis en innføring i bank- og finanssektoren i Norge.
3: Teoretisk grunnlag	I det teoretiske kapittelet presenteres relevant teori for å kunne besvare studiens problemstilling. Først vil teori om risiko og risikostyring presenteres, før vi går til kapittelets organisasjonsdel omhandlende NAT, HRO og resiliens.
4: Metode	I oppgavens fjerde kapittelet beskrives forskningsdesign og metodisk tilnærming, med begrunnelse og refleksjon knyttet til foretatt valg. Studiens forskningsetiske betraktninger vil løftes frem.
5: Empiri og diskusjon	Her vil sentrale funn fra empiri presenteres, før innsamlet data knyttes sammen opp mot teorien. Forskningsspørsmålene vil diskuteres og drøftes hver for seg.
6: Konklusjon	I oppgavens siste kapittel skal konklusjon presenteres og avslutningsvis formuleres svar på problemstillingen og forslag til videre forskning.

2.0 Kontekst

I dagens stadig mer digitaliserte samfunn spiller IKT-tjenester en sentral rolle. I dette kapittelet vil vi gi en innføring i begrepet utkontraktering, for å kunne undersøke på hvilken måte denne typen organisering representerer risiko. Vi vil deretter redegjøre for bank- og finanssektoren i Norge, for å kunne undersøke på hvilken måte utkontrakteringsprosessen av IKT-tjenester representerer risiko i denne sektoren.

2.1 Utkontraktering

Når et foretak velger å la en annen juridisk enhet (oppdragstaker) utføre oppgaver på deres vegne, omtales det som utkontraktering (Finanstilsynet, 2021a). Dette gjelder også når foretaket er i samme konsern. Oppdragstaker tar over arbeidsoppgaver som virksomheten tidligere har stått for, og blir dermed leverandør til oppdragsgiveren. Utkontraktering har med årene blitt en helt sentral del av virksomheters drift, og omtales også som tjenesteutsetting, konkurranseutsetting og outsourcing. Vi har undersøkt bruksmengden ved å ta i bruk et tilpasset søk i Universitetsbiblioteket i Stavanger etter norsk materiale. Dette gav «tjenesteutsetting» 13 treff, «utkontraktering» 17 treff, «konkuraseutsetting» 134 treff og «outsourcing» 108 treff. Det er liknende fordeling i resultatene fra Universitetsbiblioteket i Oslo, NTNU Universitetsbibliotek og Universitetsbiblioteket i Bergen. Selv om «outsourcing» og «konkurranseutsetting» er brukt i størst grad, er det valgt å benytte det norske ordet «utkontraktering», som også brukes konsekvent av Finanstilsynet.

Utviklingen innenfor IKT skaper et større behov for spesialisert kunnskap og tjenester. De fleste virksomheter har ikke mulighet til å håndtere alt på IKT-området selv, og er derfor avhengige av å sette ut slike tjenester for å kunne oppnå sine strategiske mål. Utkontraktering kan bidra til enklere drift, kostnadskutt, sikring av nøkkelkompetanse, bedre mobilitet, økt produktivitet og mer automatisert sikkerhet (NSM, 2022). Ved å benytte seg av spesialiserte tjenesteleverandører kan også bank- og finanssektoren få ekstern ekspertise, slik at de heller kan fokusere på sin kjernevirksomhet. Selv om utkontraktering kan ha mange fordeler, er det også sentrale sikkerhetsutfordringer som må tas hensyn til. Organiseringen som utkontraktering representerer fører til lange og uoversiktlige leverandørkjeder, noe som kan føre til utfordringer når risikoen skal kartlegges og håndteres (Norges Bank, 2022b). Leverandørkjeder omfatter “alle ledd i kjeden av leverandører og underleverandører som leverer eller produserer varer, tjenester eller andre innsatsfaktorer som inngår i en virksomhets

leveranse av tjenester eller produksjon av varer fra råvarestadiet til ferdig produkt" (NSM, 2023, s.15). Arbeidet med å identifisere og håndtere risiko i leverandørkjeden er ofte en manuell prosess som er tidkrevende, kostbar og kan gi varierende resultater når det kommer til dens kvalitet.

Leverandørkjedesikkerhet øker i aktualitet etter flere tiår med digitalisering, hvor digitale verdikjeder spenner over flere landegrenser og kontinenter. Farene knyttet til utkontraktering har vært i finanstilsynets søkelys over mange år (Skjelvik, 2019). I rapportene «Risiko 2022» og «Risiko 2023» fra NSM (2022, 2023) påpekes det at gapet mellom det generelle sikkerhetsnivået i norske bedrifter og den reelle trussel de står overfor blir større. Den teknologiske utviklingen har ført til at risikoen for cyberhendelser i bank- og finanssektoren øker, også mot norske foretak (Norges Bank, 2020b). En cyberhendelse kan oppstå ved ulike former for angrep som Nasjonal sikkerhetsmyndighet (NSM) (2022, 2023), Politiets sikkerhetstjeneste (PST) (2021, 2022), og Etterretningstjenesten (2021, 2022) viser til i sine trusselvurderinger. De peker på at statlige aktører blir mer aktive, og fremmer kinesiske og russiske aktører som de mest alvorlige truslene mot norske sikkerhetsinteresser. Statlige trusselaktører viser stor vilje til å utnytte våre sårbarheter gjennom helhetlige og langsiktige tilnærminger, der utførelsen av angrep blir mer sofistikert. NOU (2015:13) viser også til ikke-tilsiktede hendelser, som for eksempel menneskelige feilhandlinger, som årsaker til uønskede hendelser i bank- og finanssektoren.

2.2 Bank- og finanssektoren i Norge

Ifølge «KIKS-rapporten» fra DSB (2016) blir finansielle tjenester betraktet som en kritisk samfunnsfunksjon. I dagens digitaliserte og globaliserte verden er kritiske samfunnsfunksjoner avhengige av lange, og til dels uoversiktlige leverandørkjeder (NOU 2015:13). «KIKS-rapporten» (DSB, 2016) deler de kritiske samfunnsfunksjonene inn i tre hovedområder: *styringsevne og suverenitet, befolkningens sikkerhet* og *samfunnets funksjonalitet.* Innenfor kategorien *samfunnets funksjonalitet* faller systemer og tiltak som indirekte påvirker samfunnets evne til å ivareta befolkningens sikkerhet. Blant disse funksjonene finner vi de finansielle tjenestene. DSB (2016) understeker samfunnets behov for å sikre finansielle tjenester og den økende sårbarheten gitt den pågående digitale utviklingen.

Norsk finanssektor er blant de mest digitaliserte og fremoverlente i bruken av ny teknologi og

digitale løsninger (NOU 2015:13; NOU 2018:14). Denne digitaliseringen bidrar til mer effektiv produksjon av finansielle tjenester, men introduserer også nye risikoer (Meld. St. 12 (2021-2022)). Bank- og finanssektoren er sterkt avhengig av å utkontraktere IKT-tjenester. Ifølge en risikoanalyse fra Den europeiske banktilsynsmyndigheten (EBA) (2021) indikerer større avhengighet til digitale løsninger, økt sårbarhet for mer sofistikerte cyberangrep. Spredning av slike hendelser kan få betydelige konsekvenser for det finansielle systemet. Videre, blir komplekse systemer og lange verdikjeder også identifisert som risikofaktorer i det finansielle systemet.

En alvorlig svikt i IKT-systemet på den finansielle infrastrukturen kan føre til stans eller forsinkelser i transaksjoner, samt tap eller manipulering av sensitiv informasjon (Norges Bank, 2021b). Et cyberangrep kan føre til at IKT-systemer ikke lenger fungerer som forventet og at operatørene ikke lenger kan stole på at dataene er korrekte (Norges Bank, 2021a). En stans i betalingssystemet eller andre sentrale funksjoner i banksystemet kan raskt utvikle seg og få konsekvenser for den finansielle stabiliteten (Norges Bank, 2021b). For å håndtere disse utfordringene kreves det god risikostyring. Finanstilsynet (2021a) vurderer at den samlede risikoen knyttet til digital kriminalitet i sektoren er høy. Samtidig blir det bemerket at arbeidet med cybersikkerhet hos finansforetakene stadig forbedres, og at angrep i stor grad avverges før de får alvorlige konsekvenser.

På internasjonal basis er finanssektoren den sektoren som er mest utsatt for, og hyppigst rammet av, cyberangrep (Meld. St. 12 (2021-2022)). Til tross for denne økningen har det foreløpig ikke vært sikkerhetshendelser med alvorlige konsekvenser for den finansielle stabiliteten (Meld. St. 12 (2021-2022)). Det er virksomheter med funksjoner i finansiell infrastruktur som har ansvar for cybersikkerheten i sine systemer. Dette blir ytterligere komplisert ved at et cyberangrep, eller andre uønskede hendelser, på et enkeltsystem i den finansielle infrastrukturen kan få konsekvenser for andre deler av systemet. I verste fall kan det få alvorlige konsekvenser for hele det finansielle systemet.

Det siste året har vi sett en markant økning i antall sikkerhetstruende hendelser generelt, hvor leverandørkjedeangrep blir fremhevet som en økende risiko (NSM, 2022, 2023). Det finnes flere eksempler på at leverandørkjedeangrep mot IKT-tjenesteleverandører har fått omfattende konsekvenser, noe som gir behov for koordinering og regulering (NSM, 2023). Internasjonalt er det bred politisk enighet om behovet for å styrke motstandsdyktigheten mot cyberangrep i

den finansielle sektoren (Norges Bank, 2021b). Bank- og finanssektoren må forholde seg til et risikobilde i kontinuerlig endring og det er påpekt i «Risiko 2023» at vi ikke er sikrere enn det svakeste leddet (NSM, 2023). Vår største sårbarhet ligger i periferien, der vi er mest eksponert for sikkerhetstruende virksomhet.

3.0 Teoretisk grunnlag

I dette kapittelet vil vi presentere det teoretiske grunnlaget som danner utgangspunktet for drøftingen av det empiriske datamaterialet. Det teoretiske rammeverket er todelt. Først vil vi undersøke begrepet risiko, dets dimensjoner og utvalgte metoder for risikostyring. Deretter vil risiko settes i sammenheng med usikkerhet, sårbarhet, i tillegg til safety og security. Videre vil vi presentere et organisatorisk perspektiv ved å se på bidragene fra NAT, HRO og resiliens. Denne delen presenteres gjennom NAT som forklarer hvorfor ulykker i teknologiske systemer oppstår, og HRO som beskriver hvordan det er mulig å unngå uønskede hendelser i komplekse og høyteknologiske systemer. Til slutt redegjør vi for begrepet resiliens, som kan være en løsning for hvordan bank- og finanssektoren kan håndtere risikoen som utkontraktering av IKT-tjenester representerer. Disse teoriene vil samlet danne grunnlaget for å undersøke risiko i en utkontrakteringssammenheng, samt hvordan disse håndteres i norsk bank- og finanssektor.

3.1 Risiko

Det er ulike definisjoner av risiko i ulike samfunnsområder, og vi vil derfor redegjøre for hvilken forståelse av risiko som blir brukt i denne studien. Den klassiske risikodefinisjonen viser til risiko som et resultat av sannsynlighet og konsekvens (Engen et al., 2021). Denne definisjonen tar ikke høyde for usikkerhetsdimensjonen i tilstrekkelig grad, noe som begrenser dens anvendelighet. Usikkerhet er knyttet til både realisering av hendelser, alvorligheten av potensielle hendelser og tilhørende konsekvenser (Engen et al., 2021). Vi har derfor valgt en definisjon som tar hensyn til ulike dimensjoner av risiko, inkludert usikkerhet, sårbarhet, og safety og security. Av denne grunn ble Aven & Renns (2010) definisjon på risiko valgt, som sier at risiko «refererer til usikkerheten om, og alvorligheten av, hendelser og konsekvenser (eller utfall) av en aktivitet med hensyn til noe mennesker verdsetter» (s.3, egen oversettelse). Med andre ord refererer risiko til fremtidige hendelser eller aktiviteter, og de positive eller negative konsekvensene av disse.

Renn (2008) skiller mellom fire typer risikoer: enkle, komplekse, usikre og tvetydige. Enkle risikoer er kjente, fordi det finnes data som kan brukes for å analysere risikoen ved bruk av kjente og aksepterte metoder. I tilfelle av enkle risikoer betraktes usikkerheten som lav, og skadeomfanget som minimalt (Renn, 2008). Komplekse risikoer kjennetegnes ved at det er vanskelig å skille mellom årsak og virkning noe som krever en mer helhetlig tilnærming for å håndtere dem effektivt. Usikre risikoer kjennetegnes ved at det er vanskelig å forutse hendelser

og deres konsekvenser på grunn av manglede data, upålitelige analysemetoder eller uenighet blant eksperter (Renn, 2008). Tvetydige risikoer kan medføre ulike tolkninger av risikovurderinger eller tilgjengelig informasjon. Slike risikoer kjennetegnes ofte ved kompleksitet. Det skilles mellom disse for å best kunne tilpasse tilnærmingen til risikostyring i henhold til risikoen man står overfor. Som oftest vil en risiko være en blanding av flere av disse typene (Renn, 2008).

Formålet med denne studien er å undersøke risikoen ved utkontraktering av IKT-tjenester i bank- og finanssektoren. Denne risikoen kan omfatte tap av konfidensialitet, integritet og tilgjengelighet av informasjon eller informasjonssystemer, som kan medføre negative konsekvenser (DSB, 2020). Det er også andre tekniske, organisatoriske, finansielle eller juridiske forhold som kan relateres til risikoen. Det er særlig viktig å forstå risikoen og hvilke typer risiko som blir prioriteres, da dette vil ha innvirkning på sikkerhetsarbeidet og risikohåndteringen.

3.1.1 Systemrisiko

Risikoen for forstyrrelser i det finansielle systemet som kan gi alvorlige konsekvenser for realøkonomien og dermed den finansielle stabiliteten, kategoriseres som systemrisiko (Lind, 2016). Bankers sammenkobling, enten direkte eller indirekte, skaper en sårbarhet i systemet ved å tillate spredning av finansiell risiko. Denne sammenkoblingen gir opphav til systemrisiko, der faren er at systemet ikke lengre kan utføre sine funksjoner (Lind, 2016; Norges Bank, 2022c). Kaufmann & Scott (2003) definerer systemrisiko som «risikoen eller sannsynligheten for sammenbrudd i hele systemet, i motsetning til sammenbrudd i individuelle deler eller komponenter, med korrelasjon mellom de fleste eller alle delene» (s.371, egen oversettelse). Ulike typer cyberhendelser har potensial til å true den finansielle stabiliteten og utgjør dermed en kilde til systemrisiko i det finansielle systemet (Meld. St. 12 (2021-2022); Norges Bank, 2021a). Når IKT-tjenester utkontrakteres, oppstår et system preget av tette koblinger, lange leverandørkjeder, mange aktører og lite overordnet styring. En slik organisering kan føre til at svikt i ett ledd påvirker hele systemet.

Systemrisiko knyttes til strukturelle egenskaper som indikerer svakheter i den norske finansielle infrastrukturen og omfanget av systemviktige institusjoner (Norges Bank, 2022c). På denne måten tar systemrisiko høyde for motstandskraften i det finansielle systemet (Norges

Bank, 2022c). Det foreligger et manglende erfaringsgrunnlag for å kunne vurdere nivået på sårbarheten for det finansielle systemet (NOU 2023:6). Håndtering av systemrisiko krever nye tilnærminger, da det er vanskelig å isolere og kan påføre skade på et system som ikke er lett å forutse eller kontrollere. Det kreves større oppmerksomhet rettet mot systemisk cyberrisiko og utvikling av tiltak for å håndtere dette (Norges Bank, 2021a). Det er også behov for et utvidet samarbeid mellom myndigheter og aktører i det finansielle systemet for å overvåke systemrisiko.

3.1.2 Sårbarhet

Utkontraktering av IKT-tjenester representerer avhengigheter og kompleksitet som påvirker systemets sårbarhet (DSB, 2020). Risiko og sårbarhet henger tett sammen, der sårbarhet kan betraktes som et aspekt ved, og en konsekvens av økt risiko. Sårbarhetsutvalget (NOU 2000:24) definerer sårbarhet som «et utrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet» (s.18). På den måten forstås sårbarhet som en forutsetning for at en hendelse kan inntreffe og utfordringen med å gjenopprette ønsket funksjon (Njå et. al., 2020). Sårbarheter i det finansielle systemet kan føre til at ulike forstyrrelser får mer alvorlige konsekvenser for den finansielle stabiliteten (Norges Bank, 2021a).

Ulike reguleringer, tiltak og prosesser gir banker økt motstandsdyktighet og reduserer sårbarhetene. Ifølge Aven (2018) kan sårbarhet beskrives som en faktor som gjør det vanskeligere å stå imot en trussel eller komme tilbake til en stabil tilstand etter trusselhendelsen har inntruffet. Sårbarhet kan betraktes som robusthets motsetning, der sårbarhet er reaktiv mens robusthet er proaktiv. Robusthet refererer til et systems motstandskraft mot uønskede hendelser. Renn (2008) forklarer robusthet ved å se på hvordan det risikoabsorberende systemet vil reagere på stress eller påkjenninger fra risikoagenten. Man kan dermed si at økt sårbarhet reduserer et systems robusthet, mens økt robusthet reduserer et systems sårbarhet.

3.1.3 Usikkerhet

Usikkerhetsdimensjonen er en sentral del av risikobegrepet og refererer til uvissheten om hva som vil skje og hvilke konsekvenser en beslutning eller handling vil føre til (Aven & Renn, 2010). Dette inkluderer blant annet mangel på fullstendig informasjon om fremtidige hendelser, usikkerhet omkring virkningen av beslutninger eller handlinger, samt mangel på kontroll over

omstendigheter som påvirker resultatene. I denne studien tar usikkerhetsdimensjonen ved risikobegrepet for seg den usikkerheten som er knyttet til hvilke risikoer utkontraktering av IKT-tjenester representerer, hvilken man skal akseptere og virkemidlene som skal benyttes (Renn, 2008).

Renn (2008) skiller mellom to typer usikkerhet, kjent som «altory»-og «epistemic uncertainty». De skiller seg ved at aleatorisk usikkerhet er basert på variasjon som kan oppstå som følge av tilfeldige faktorer, mens epistemisk usikkerhet knyttes til manglende kunnskap om fenomener (Renn, 2008). Et velkjent eksempel på aleatorisk usikkerhet baserer seg på tilfeldighet ved terningkast, hvor en kan beregne sannsynligheten. Med epistemisk usikkerhet har personene som er involvert i risikoanalysen ikke tilstrekkelig kunnskap til å forutsi forekomsten av hendelser og eller konsekvensene av dem (Aven & Renn, 2010). Når det gjelder hendelser man har opplevd før, er det mulig å forberede seg på en annen måte enn ved epistemisk usikkerhet (Renn, 2008). For å kunne forstå risikoen knyttet til utkontrakterte IKT-tjenester i bank- og finanssektoren, er det viktig å forstå betydningen av usikkerhet i denne konteksten.

3.2 Safety og Security

Det har foreligget et behov for å skille ulykker fra intenderte ondsinnede handlinger innen risiko og sikkerhet ved språklig differanse. Det benyttes i stor grad de engelske betegnelsene «security» og «safety», da det ikke er like enkelt å fange opp de språklige nyansene på norsk (Jore, 2019). I NOU (2006:6) blir språkbruken rundt begrepene safety og security diskutert ved hjelp av språkprofessor Finn-Erik Vinje. Vanligvis blir safety forstått som «sikkerhet», mens security blir forstått som «sikring». Vinje foreslår å bruke begrepet «trygghet» istedenfor safety, og «sikring» istedenfor security (NOU 2006:6). Safety og security er fortsatt begrepene som brukes i størst grad i fagmiljøet, og som vi derfor ønsker å bruke videre i denne studien. Vi anser at safety-farer og security-trusler utgjør en potensiell risiko for verdier innenfor bank- og finanssektoren, og inkluderer derfor disse dimensjonene for å undersøke hvilke risikoer utkontrakteringsprosessen representerer.

3.2.1 Safety

Sikkerhetsrelaterte hendelser i bank- og finanssektoren kan oppstå grunnet ikke-intenderte hendelser som kan føre til ulykker. Tradisjonelt er det forsøkt å skille mellom begrepene ved å vektlegge intensjonen bak handlingen. Ifølge Jore (2019) er intensjonen alene ikke tilstrekkelig

for å skille mellom begrepene da ulykker sjeldent skjer tilfeldig. Derfor bør skille reflektere den ondsinnede viljen innenfor security-feltet (Jore, 2019). Innen forskning på safety-området er det veletablert at ulykker ikke bare «skjer», og at de på ulike måter kunne vært unngått. Ulykker oppstår gjerne som et resultat av manglende fokus på sikkerhet (Jore, 2019). Safety forsås som handlinger og hendelser som ikke er planlagt, som for eksempel ulykker, komponentsvikt eller feil. Slike hendelser kan oppstå grunnet mangelfull planlegging, utilstrekkelig sikkerhetskultur, manglende risikoanalyser, menneskelig handling eller mangel på handling.

Basert på tilgjengelig forskning kan safety i dag betraktes som en mer etablert vitenskap enn security (Jore, 2019). Sikkerhetsarbeid innenfor safety-feltet handler om å forhindre tap som skyldes handlinger fra ikke-ondsinnede aktører. Utkontraktering kjennetegnes ved mange aktører og lite overordnet styring som har mulighet til å true finansiell stabilitet og er dermed en kilde til systemrisiko. En slik organisering åpner opp for intensjonelle ondsinnede handlinger.

Figur 1: Avgrensning mellom safety og security (inspirert av Jore 2019, s.162)

3.2.2 Security

I denne studien tar vi utgangspunkt i Jore (2019) sin definisjon av security, som er «den oppfattede eller faktiske evnen til å forberede seg på, tilpasse seg, motstå og komme seg fra farer og kriser forårsaket av menneskers bevisste, forsettlige og ondsinnede handlinger som terrorisme, sabotasje, organisert kriminalitet eller hacking» (s.157, egen oversettelse). Et eksempel på en security-risiko er cyberangrep, som er en bevisst og ondsinnet handling utført av en trusselaktør. Slike angrep kan variere i motivasjon, tilgang på ressurser, organisering og metoder som benyttes. Det kan forårsake stor skade på den finansielle infrastrukturen og

resultere i store verditap for virksomheter, kunder og samfunnet ellers. Derfor er det et økende behov for å fokusere på security, samtidig som organisasjoner har begrensede muligheter til å bekjempe truslene alene. Leveson (2020) argumenter for at det er viktig å rette oppmerksomheten mot eget system. Dette henger sammen med diskusjonen omkring utviklingen hvor safety og security flettes inn i hverandre (Jore, 2019; Kongsvik et al., 2018). De to feltene har på mange måter utviklet seg til to ulike miljøer som utvikler egne verktøy og metoder, men det er mange perspektiver som begge feltene deler. Jore (2019) vil i den sammenheng argumentere for et behov for en mer integrert tilnærming mellom feltene. Hvordan man skiller mellom begrepene kan ha betydning for håndteringen av risiko, men grunnet at safety-farer åpner for security-trusler er det relevant at de ses i sammenheng.

3.3 Trefaktormodellen

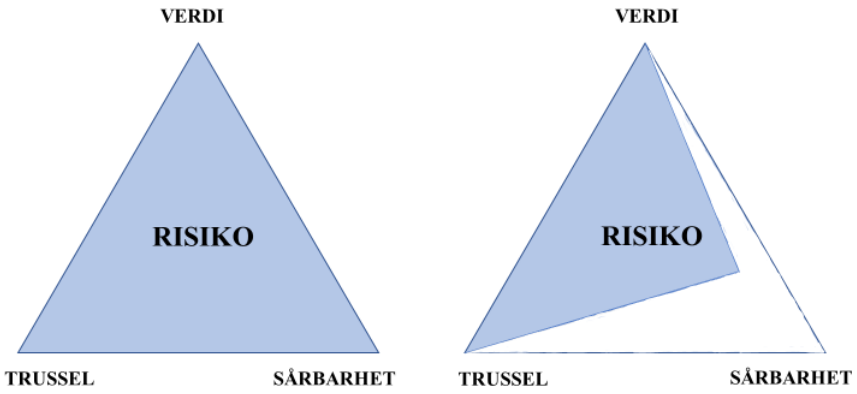
«Trefaktormodellen» blir ofte brukt for å gi en helhetlig vurdering av security-risikoer (Engen et al., 2021). Modellen består av en verdi-, trussel- og sårbarhetsvurdering som samlet kartlegger risikobildet. Ved å se på trusler og sårbarheter knyttet til verdiene man ønsker å beskytte, kan man identifisere risikonivået og peke ut tiltak som kan iverksettes i en beslutningssammenheng (Busmundrud et al., 2015). Risikoen man ønsker å vurdere påvirkes av forholdet mellom de tre faktorene. Denne tilnærmingen til risiko skiller seg fra andre analysemetoder som anvender risiko som et uttrykk for kombinasjonen av sannsynlighet og konsekvens av uønskede hendelser (Engen et al., 2021). Sannsynlighet er med hensyn utelatt eksplisitt i trusselvurderingen, da hendelser som «scorer» lavt, grunnet lav sannsynlighet og høy konsekvens, kan blir gitt lavere prioritet (Busmundrud et al., 2015).

I en risikosammenheng vil det alltid være en viss grad av usikkerhet, men når det gjelder security-trusler, er denne usikkerheten og uforutsigbarhet enda større sammenlignet med safety-risikoer. På grunn av denne uforutsigbarheten av security-hendelser, er det viktig å arbeide kontinuerlig med å identifisere trusselbildet (NSM, 2022). Trefaktormodellen kan benyttes på både safety og security-risikoer, da feltene på mange måter går inn i hverandre og kan være vanskelig å skille fra hverandre (Jore, 2019). Imidlertid har modellen møtt kritikk fordi den ikke tydeliggjør usikkerhetsdimensjonen tilstrekkelig, samtidig som den ikke gir veiledning for prioritering (Busmundrud et al., 2015).

Dersom risikoen som avdekkes i risikovurderingen ikke er akseptabel, må man se på hvilke

muligheter som finnes for å kunne håndtere risikoen (Engen et al., 2021). Formålet med forebyggende sikkerhet i bank- og finanssektoren er å opprettholde den finansielle stabiliteten, i tillegg til å beskytte bankens systemer, informasjon og eiendeler mot uønskede hendelser (Norges Bank, 2022b). Generelt har forebyggende sikkerhet som formål å sikre kontinuitet i bankens tjenester, beskytte bankens omdømme og styrke kundenes tillit. Utover dette har banken også en rekke verdier som er viktige for å kunne drive virksomheten på en ansvarlig og etisk måte.

Figur 2: Visualisering av trefaktormodellen (inspirert av Busmundrud et al., 2015, s.34)



Verdi

Kartlegging av virksomheters verdier er nødvendig for å identifisere konsekvenser av en uønsket hendelse og for å gjøre vurderinger av hvilke skader eller tap man er villig til å akseptere (Busmundrud et al., 2015). Man bør her finne ut hvor kritisk et eventuelt bortfall av denne verdien er, og rangere eller kategorisere disse ut fra kritikalitet (Busmundrud et al., 2015). Bank- og finanssektoren har en rekke verdier som avhenger av virksomhetens spesifikke mål og strategier. For eksempel kan sentrale verdier virksomheten vil verne fra ulike trusler være informasjon, tekniske systemer, økonomi, tillit, materielt utstyr, innovasjon, bærekraft og profesjonalitet. Disse verdiene bidrar til å sikre at banken opptrer på en måte som ivaretar kundenes interesse og samfunnets forventninger.

Trussel

Truslene som verdiene er utsatt for må identifiseres og er avgjørende for risikoen man står overfor (Busmundrud et al., 2015). Med trussel menes en intensjon og evnen en trusselaktør har til å initiere et angrep med hensikt om å påføre skade (Aven, 2020). I bank- og finanssektoren er truslene i stor grad utbredt, med ulike typer aktører med interesse i å utføre ulike typer angrep. Noen av truslene er hacking og phising-angrep, destruktive angrep mot IKT-systemer, spionasje og informasjonstyveri (DNB, 2021). Trusler kan være vanskelig å oppdage grunnet dens påfallende usikkerhetsdimensjon og blir dermed en faktor organisasjoner har begrenset kontroll over (Martin, 2019).

Sårbarhet

Vurderingen av sårbarhet omhandler hvorvidt og i hvilken grad en aktør kan utføre en uønsket handling vellykket (Busmundrud et al., 2015). Det kan for eksempel være snakk om en sikkerhetssvakhet som gjør et system mottakelig for et angrep. På mange måter beskriver sårbarhet muligheten en trussel har for å kunne skade verdiene (Martin, 2019). For å gjennomføre en sårbarhetsvurdering bør virksomheten se på hvilke ressurser de har til rådighet, hva som er iverksatt, og hvilke tiltak de kan iverksette. Man bør også vurdere hvilken mulighet en trusselaktør har for å kunne nå målet (Busmundrud et al., 2015). Ved å øke systemets robusthet kan sårbarheten reduseres, og dermed vil den samlede risikoen minimeres. Samfunnet i dag er preget av digitalisering og avhengighet, noe som bidrar til økt sårbarhet. Man er derfor avhengig av å kartlegge og øke kunnskapen om systemets sårbarheter, for å kunne styrke robustheten (Njå et al., 2020).

3.4 Risikostyring

Kjernen i risikostyring er å oppnå en balansere mellom verdiskapning og beskyttelse mot ulykker, tap og skader (Aven et al., 2004). Aven et al. (2004) definerer risikostyring som «alle tiltak som iverksettes for å oppnå, opprettholde og videreutvikle et sikkerhetsnivå i overenstemmelse med definerte mål» (s. 67). Risikostyringsprosessen handler om å få innsikt i risiko, effekten av tiltak og hvilken grad risikoen kan styres (DSB, 2020). Det handler også om metodene, prosessene og strategiene for å kartlegge og styre risikoens aspekter (Aven et al., 2008). God risikostyring er en forutsetning for å sikre effektive prosesser ved utkontraktering av IKT-tjenester i bank- og finanssektoren. NSM (2023) påpeker at styring av risiko og tiltak må tilpasses et risikobilde i endring, noe som utfordrer en allerede krevende

oppgave. Ved å fokusere på styring, aktører og regler i risikostyringsprosessen, oppnår man en helhetlig forståelse av situasjonen og bidrar til at organisasjoner kan identifisere og vurdere risiko (Aven & Renn, 2010). Det finnes mange metoder virksomheter kan benytte seg av for å identifisere og redusere risiko, samt opprettholde krav. En felles forståelse av hva risikoen innebærer er avgjørende i denne prosessen. Risikostyring av utkontrakterte IKT-tjenester innen bank- og finanssektoren vil ha en reell betydning for IKT-sikkerheten i sektoren, og det er derfor essensielt å kartlegge risikoen en står overfor.

3.4.1 Risiko – og sårbarhetsanalyser (ROS-analyser)

En risiko- og sårbarhetsanalyse (ROS-analyse) er en sentral del av risikostyring og benyttes for å etablere et risikobilde (Aven et al., 2008). Formålet med ROS-analyser er å identifisere potensielle farer og trusler, vurdere deres sannsynlighet og konsekvens, kartlegge risikoreduserende tiltak, samt forbedre virksomhetens motstandsdyktighet. Konsekvensene avhenger av virksomhetenes sårbarhet overfor farene eller truslene (Engen et al., 2021). Analysen inkluderer eksterne og interne faktorer og er derfor sentral når det dreier seg om å analysere utkontrakteringsrisiko. Denne tilnærmingen er proaktiv og bidrar til nødvendig innsikt om risikoer og sårbarheter som kan påvirke virksomheten, slik at man kan håndtere utfordringen på best mulig måte (Aven et al., 2004). En ROS-analyse bidrar til å ta viktige og informerte beslutninger angående virksomhetens sikkerhet og hjelper med å avdekke svakheter, samt forslag til implementering av tiltak. (Njå et al., 2020) Det kan antas at en ROS-analyse spiller en sentral rolle når en bank skal vurdere hvorvidt de skal utkontraktere en IKT-tjeneste eller ikke.

3.5 Normal Accident Theory (NAT)

Normal Accident Theory (NAT) presenterer er en teori om systemer, deres potensiale for feil og deres evne til å komme seg etter feil. Ifølge Perrow (1999) har komplekse systemer med tette koblinger en iboende sårbarhet som fører til uunngåelige ulykker som systemet ikke kan designe seg bort fra. «Mye kan gjøres for å gjøre systemene sikrere, men ulykker kan ikke unngås helt» (Perrow, 1999, s. 330, egen oversettelse).

Bank- og finanssektoren opererer innenfor et omfattende og komplekst system. Gjennom utkontraktering utsettes sektoren for flere potensielle flater for feil og ondsinnede angrep. Ifølge Perrow (1999) kan rask teknologisk utvikling og sammensatte systemer bli for tett koblet

og for komplekse, slik at enkeltfeil eller avvik som oppstår kan forplante seg og medføre alvorlige konsekvenser. Det kan føre til hendelser i mindre deler, flere komponenter eller at det kan få konsekvenser for hele systemet (Perrow, 1999). Lange verdikjeder bidrar ytterligere til kompleksitet, hvor flere aktører fører til økt sårbarhet for hull i systemene. For å redusere risikoen for systemsvikt og ulykker med ukontrollerbare ettervirkninger, bør kompleksiteten og koblingene i systemet minimeres. Perrow (1999) skiller mellom hendelser og ulykker ut ifra om det er mindre deler eller hele systemet som settes ut av spill, avhengig av systemets koblinger og interaksjoner.

Et systems kompleksitet kjennetegnes av hvordan det er koblet og egenskaper ved interaksjoner i systemet (Perrow, 1999). Teorien skiller mellom lineære og komplekse interaksjoner, samt løse og tette koblinger. Interaksjon refererer til hvordan elementene i et system samhandler. Lineære interaksjoner er når systemets enheter og komponenter fungerer enkelt, oversiktlig og som forventet. Komplekse interaksjoner er uforutsigbare ved at interaksjonen mellom elementene kan skje plutselig og uventet, og feil kan spre seg på ukontrollerte måter ved at de er nære hverandre. Ifølge Perrow (1999) kan miljøet systemet operer i være en kilde til komplekse interaksjoner. Koblinger refererer til avstanden mellom elementer i et system. Løse koplinger gir fleksibilitet ved å tillate alternative løsninger, slik at forsinkelser eller endringer ikke forstyrrer systemet (Perrow, 1999). I systemer med tette koblinger er prosessene derimot avhengig av hverandre i tid. Dette innebærer at feil kan spre seg raskt og ikke forsinkes på noen måte, noe som begrenser fleksibiliteten (Perrow, 1999). I slike tilfeller vil det være vanskelig å finne erstatninger i tide. Systemer med løse koblinger og lineære interaksjoner fører vanligvis ikke til alvorlige ulykker, fordi det er begrenset tidsavhengighet og forutsigbarhet som gjør det mulig å håndtere komponentfeil. Imidlertid mer Perrow (1999) at systemer med komplekse interaksjoner og tette koblinger kan oppleve uforutsette ulykker som ikke kan forhindres. Slike ulykker omtaler Perrow (1999) som *systemulykker*. Ifølge Perrow (1999) vil avhengighet til andre systemer bidrar til uventede interaksjoner, noe som øker sårbarhet for systemulykker.

NAT fremhever to strategier for å kontrollere systemer avhengig av organisasjonskompleksiteten, altså hvordan de er koblet og hvordan interaksjonene er. Disse strategiene er sentralisert og desentralisert organisasjonsstyring. I tilfelle av tette koblinger argumenter Perrow (1999) for behovet for sentralisert styring, som innebærer høyere kontroll, standardisering og effektivitet. På en annen side håndteres kompleksitet best ved desentralisert styring, som gir fleksibilitet og mulighet for beslutningstaking på lavere nivå med hensyn til

lokal kunnskap og erfaring (Perrow, 1999). Styring i systemer med tette koblinger og komplekse interaksjoner vil være vanskelig. I systemer med *svært* tette koblinger og høy grad av komplekse interaksjoner hevder Perrow (1999) at det vil være tilnærmet umulig. Desto mer kompleks organisasjonen er, desto større behov vil det være for desentralisert beslutningstaking. Dette skyldes at sentraliserte organisasjoner ofte har problemer med å håndtere økt kompleksitet, mens desentraliserte organisasjoner bedre kan tilpasse seg på en effektiv måte. Ifølge Perrow (1999) oppstår det derfor et dilemma som systemer ikke vil kunne organisere seg ut fra.

Perrow (1999) understreker viktigheten av backup-planer og beredskapsprosedyrer, såkalt redundans, for å håndtere ulykker når de inntreffer. Han peker imidlertid på at slike tradisjonelle sikkerhetsprosedyrer ikke alltid er tilstrekkelig i avanserte teknologisk systemer. Samtidig vil innføring av redundans gjøre systemet enda mer komplekst, med økt ulykkespotensiale, da mulige utvidelser vil kunne ha uforutsette effekter som vil kunne skade systemet. Perrow (1999) argumenterer for økt bevissthet rundt kompleksiteten og tettere samarbeid vil bidra til å forhindre og håndtere fremtidige ulykker. Oppmerksomhet bør også rettes mot mulige interaksjoner mellom teknologiske systemer og organisatoriske rutinger i planlegging og vurdering av risiko. Ved å redusere kompleksitet vil ulykker avverges i større grad. Utfordringen blir at dagens system blir tettere koblet, noe som går imot Perrows (1999) anbefalinger og fører til økt sårbarhet.

3.6 High Reliability Organisations (HRO)

Teorien om High Reliability Organizations (HRO) tar høyde for at man kan håndtere kompleks og krevende teknologi uten å bli utsatt for store ulykker og samtidig opprettholde høy produksjon (La Porte, 1996). Den skiller seg fra NAT ved å hevde at ulykker i høyteknologiske systemer kan unngås ved å fokusere på organisasjonsdesign (Weick & Sutcliffe, 2007; Sutcliffe, 2011). Dette innebærer at sikkerhet må ha høyeste prioritet, og organisasjoner må utvikle redundans eller reservesystemer for å kompensere for eventuelle feil. Videre kreves det effektive reaksjoner på uventede hendelser, mulighet for desentralisert beslutningstaking og kontinuerlig læring for å kunne unngå ulykker (Aven et al., 2004). Læring av feil kan oppnås gjennom øvelser, bruk av tidligere erfaringer og gjennom prøving og feiling. Weick & Sutcliffe (2007) understreker betydningen av effektiv kommunikasjon og samarbeid, samt proaktiv identifisering og håndtering av risikoer. I tillegg preges HROer av en forpliktelse til å redusere

risiko og et kontinuerlig fokus på forbedring. Weick & Sutcliffe (2007) fremhever konseptet «kollektiv oppmerksomhet», som refererer til organisasjoners evne til å ta hensyn til detaljer, miljøet de opererer i, og å reagere på uventede hendelser og skiftende forhold. De fremhever i den sammenhengen viktigheten av fleksibilitet for å kunne tilpasse seg og implementere alternative løsninger for å sikre kontinuitet og omstille seg ved behov (Weick & Sutcliffe, 2007).

For å opprettholde pålitelighet og håndtere ulike utfordringer, er det nødvendig for HROer å være i stand til å improvisere (Weick & Sutcliffe, 2015). Improvisasjon refererer til evnen til å reagere på uventede situasjoner, ta beslutninger under usikkerhet og press, og tilpasse seg raskt. Fleksibilitet spiller en avgjørende rolle for å håndtere det uforutsette (Weick & Sutcliffe, 2015). Det krever en fleksibel tilnærming i organisasjoners strukturer, prosesser og de ansattes kompetanse (Weick & Sutcliffe, 2007). Erfaring, intuisjon og kreativ problemløsning basert på kunnskap og kompetanse er verdifulle egenskaper i denne sammenhengen. HROer legger vekt på å skape et miljø der de ansatte har tillit og autonomi til å ta avgjørelser i kritiske situasjoner. Mangfold, med hensyn til ekspertise og ferdigheter, er avgjørende for å kunne ta gode beslutninger og håndtere kompleksitet (Weick & Sutcliffe, 2007). Det forutsetter å kjenne til organisasjonens ekspertise, slik at beslutningene tas av de rette personene, og ikke basert på hierarkiske strukturer. Weick & Sutcliffe (2007) påpeker også at organisasjoner må ha muligheten til spontan omstilling gjennom desentralisert beslutningstaking, selv om styrkene ved sentralisert tilnærming understekes. Utkontrakteringsprosessen kan kreve uforutsette endringer, slik som tekniske problemer, leverandørsvikt eller endrede behov. Dette kan kreve improvisasjon og tilpasning for å opprettholde kontinuitet og pålitelighet.

3.7 Resiliens

Resiliens er et sentralt begrep knyttet til effektiv håndtering av risiko og sårbarhet med sikte på at organisasjoner kan opprettholde sine funksjoner og mål selv under ugunstige forhold (Hollnagel, 2014). Det finnes et mangfold av definisjoner på resiliens, men viktige elementer som går igjen er evnen til å absorbere sjokk, transformere seg og tilpasse seg den nye realiteten (Anholt & Boersma, 2018). Aven & Thekdi (2021) definerer resiliens som «systemets evne til å opprettholde eller gjenopprette sin grunnleggende funksjonalitet etter en risikokilde eller en hendelse» (s. 18, egen oversettelse). Hollnagel (2017) understeker at et system må kunne justere sine funksjoner før, under og etter endringer og forstyrrelser. Styrking av resiliens vil

derfor være en viktig strategi for å forbedre systemet, og for å oppnå dette er det nødvendig å være klar over hvilke risikoer en står ovenfor og tilpasse seg dersom en hendelse inntreffer. Bank- og finanssektoren må være bevisst på risikoene som er forbundet med utkontrakteringsprosessen for å kunne håndtere dem på best mulig måte.

Ifølge Hollnagel (2011) er det fire kjennetegn ved resiliens i en organisasjon. Disse inkluderer i) evnen til effektiv og fleksibel respons på både regulære og irregulære trusler, ii) evnen til å overvåke situasjoner og ha kunnskap om hendelser som kan oppstå (innebærer også evnen til å overvåke egne presentasjoner), iii) evnen til å ta lærdom fra hendelser som oppstår, samt fra tidligere hendelser og iv) kunnskap om hva som kan forventes, eller hvordan situasjoner og trusler kan utvikle seg. Med andre ord har resiliente organisasjoner en evne til å respondere, overvåke, lære og forvente hendelser. Hollnagel (2011) understreker at disse fire elementene er gjensidig avhengige av hverandre og danner grunnlaget for en resilient organisasjons evne til å håndtere kompleksitet og uforutsette hendelser på en robust og effektiv måte.

Organisatorisk resiliens handler ifølge Hollnagel (2011) om å bygge et system som kan tilpasse seg og mestre uforutsette hendelser, samtidig som det opprettholder sin kjernefunksjon. Resiliens anses som en dynamisk prosess og en egenskap som organisasjoner skaper gjennom sin tilnærming til arbeidet. Han understreker at det ikke dreier seg om å unngå feil og ulykker, men heller om å håndtere dem effektivt når de oppstår. Resiliente organisasjoner har en klar og felles forståelse av hva som er viktig, og har robuste og fleksible systemer som tillater raske og effektive tilpasninger. En systems evne til å håndtere utfordringer knyttet til utkontraktering og de medfølgende risikoene, er en indikasjon på deres resiliens. Ifølge Hollnagel (2011) oppnås dette gjennom samspillet mellom teknologi, organisasjoner og mennesker, og det krever et systematisk og kontinuerlig arbeid for bygge og opprettholde resiliens. Han oppfordrer, i liket med HRO-teorien, organisasjoner til å fokusere på kontinuerlig læring og forbedring, samt å etablere en kultur som oppmuntrer til læring av feil og forbedring av praksis (Hollnagel, 2011).

Resiliens kan ifølge Martin (2019) betraktes som både passiv og aktiv. Passiv resiliens handler om evnen til å absorbere sjokk og gjenopprette normaltilstand. På den andre siden handler aktiv resiliens om evnen til å tilpasse seg endringer og lære av hendelser for å håndtere fremtidige situasjoner bedre. Martin (2019) påpeker at organisasjoner med et aktivt perspektiv på resiliens ikke bare fokuserer på å gjenopprette normaltilstanden, men også på å komme tilbake i en ny

og forbedret form. På denne måten inkluderer begrepet også mulige ukjente fremtidige hendelser (Aven, 2015).

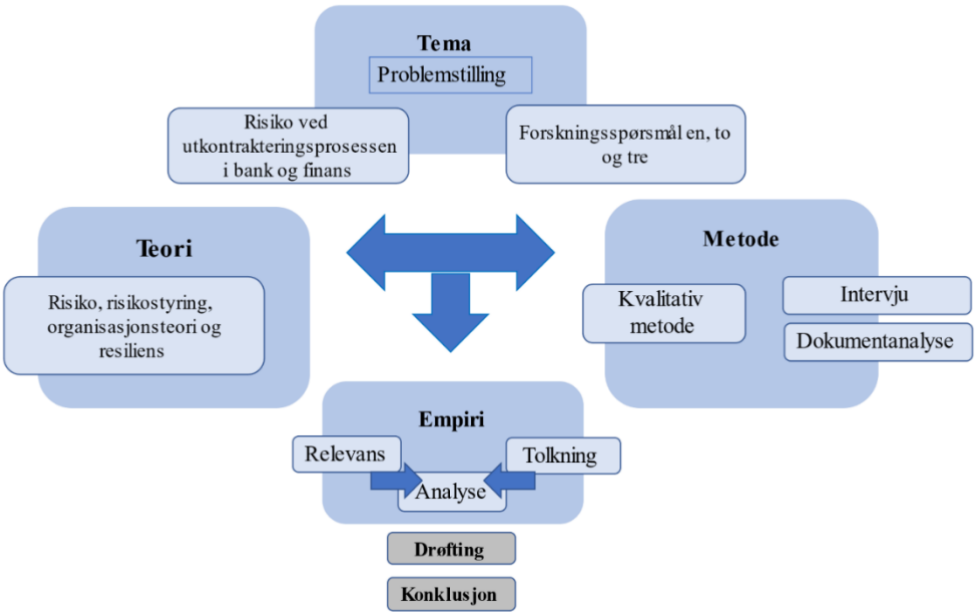
4.0 Forskningsdesign og metodisk tilnærming

Denne studien tar utgangspunkt i en interesse av å undersøke på hvilken måte utkontrakteringsprosessen av IKT-tjenester representerer risiko i bank- og finanssektoren, og hvordan denne håndteres. Problemstillingen har lagt føringer for valg av studiens fremgangsmåte, og bidratt til å avgjøre det mest hensiktsmessige forskningsdesignet (Blaikie & Priest, 2019). For å kunne svare på studiens problemstilling og tilhørende forskningsspørsmål har vi valgt å samle inn data gjennom dokumentanalyse og dybdeintervjuer.

4.1 Metodisk tilnærming og datainnsamling

Vi har tatt utgangspunkt i Danermarks (1997, 2002) beskrivelse av abduksjon for å få en større forståelse av risikofenomenet i en utkontrakteringskontekst i bank- og finanssektoren. Tilnærmingen åpner opp for en problemløsende og kreativ prosess, hvor den abduktive tilnærmingen tillater den empiriske innsamlingen å kunne lede forskningsarbeidet. Formålet med studien er å gi mening til et kjent fenomen for å kunne oppnå en bedre forståelse og forklare det på en ny måte, som samsvarer med Danermarks (2002) måte å forstå abduksjon på. Abduksjon har ikke til hensikt å skape en sannhet, men å øke kunnskap, beskrive, forstå og kunne finne mulige svar hvilket samsvarer med problemstillingens formål (Danermark, 2002). Forskingsdesignet er brukt som en guide for prosjektet, og figuren under viser fremstillingen av hvordan vi har tenkt oss frem til hvordan problemstillingen vil besvares.

Figur 3: Forskningsdesign



Valg av kvalitativ tilnærming fremmer innsikt og søker forståelse ved å gjennomføre intervjuer og studere dokumenter og gav mulighet for et mer fleksibelt forskningsdesign (Blaikie & Priest, 2019; Tjora, 2021). Vi har benyttet primærdata i form av kvalitative dybdeintervjuer, og sekundærdata i form av dokumenter. Dette har blitt gjort for å kunne besvare studiens problemstilling og forskningsspørsmål fra flere innfallsvinkler.

4.1.1 Kvalitativt forskningsintervju

Det ble besluttet å ta i bruk kvalitative forskningsintervjuer, da det er en fleksibel metode som gjorde at informantene ku utrykke seg relativt fritt. Det ble besluttet å ta i bruk kvalitative forskningsintervjuer, fordi dette er en fleksibel metode som gjorde at informantene kunne utrykke seg relativt fritt. Vi la opp til å få fyldige og detaljerte beskrivelser av det vi ønsket å studere slik at problemstillingen kunne belyses fra ulike sider, heller enn å foreta statistiske generaliseringer (Johannesen et al., 2016). Ønsket var å få innsikt i kunnskap og erfaringer for å undersøke risikoen knyttet til utkontrakteringsprosessen. Dette ville bidra til å identifisere ulike risikodimensjoner, utviklingen av risikostyringsinstrumenter og hvordan risikoen håndteres.

Utvalg og utforming av intervjuguide

Tidlig i prosessen hadde vi to kunnskapssamtaler med en parter i PricewaterhouseCoopers (PwC) og en forsker ved Forsvarets forskningsinstitutt (FFI) for å få innsikt og innspill til temaet og prosessen videre. Vi ønsket å komme i kontakt med personer med kunnskap og erfaring knyttet til utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren, noe som gjorde det hensiktsmessig med en strategisk utvelgelse (Tjora, 2021). Det ble tatt systematiske vurderinger på hvilke informanter som ut fra teoretiske og analytiske formål var mest interessante å komme i kontakt med for å belyse studiens problemstilling (Grønmo, 2016).

Vi tok tidlig kontakt med en bank som ønsket å stille med informanter til studien. De aktuelle informantene var ansatte i tre avdelinger som arbeider med ulike deler av utkontrakteringsprosessen. I tillegg til dette ønsket vi også å ha supplerende intervjuer, og gjorde vurderinger på hvem som ville kunne få frem de ulike dimensjonene vi var ute etter, på best måte. Ønsket var å få intervjuet en ansatt ved et myndighetsorgan, en ekspert på utkontraktering av IKT-tjenester og en leverandør av IKT-tjenester inn mot bank- og finanssektoren. Vi fikk avtalt intervju med Finanstilsynet og en ekspert på området fra universitet- og høyskolesektoren. Utover disse var det utfordrende å få tak i andre vi kunne intervjue, herunder blant annet IKT-leverandører. Vi fikk tidlig avtalt to intervjuer med en leverandør som dessverre meldte avbud i slutten av mars. Etter dette ble åtte leverandører og konsulentselskaper kontaktet hvor vi hadde kontakt med flere titalls personer uten å lykkes med å avtale intervju. Avvisningene handlet stort sett om påstander om mangel på kunnskap og tid. Det var noe overraskende for oss at de respektive bedriftene ikke ønsket å stille, fordi de mente de manglet riktig kompetanse for å kunne uttale seg på en god måte. Det endte derfor opp med fire informanter fra en bank, en informant fra Finanstilsynet og en ekspert fra universitets- og høyskolesektoren. Det ble derfor ikke like mange intervjuer som først ønsket, men vi mener likevel kvaliteten på intervjuene i stor grad veier opp for dette.

Vi valgte å benytte oss av semi-strukturerte dybdeintervjuer og utarbeidet en overordnet intervjuguide. Intervjuguiden ble utformet med generelle, åpne og relativt korte spørsmål. Vi ønsket å være søkende slik informantene kunne forklare seg fritt, og dele relevant tilleggsinformasjon som kunne avdekke interessante aspekter ved de aktuelle intervjuspørsmålene. Intervjuguiden ble tilpasset de ulike grupperingene av informanter for å kunne hente ut ønsket informasjon (se vedlegg A, C og C). De ulike intervjuguidene ble også inndelt i tre deler tilhørende studiens ulike forskningsspørsmål, for å enklere kunne sikre at vi

fikk relevant informasjon for å besvare forskningsspørsmålene. Spørsmålene var i stor grad deskriptive, dette fordi mange «hvorfor» spørsmål kan hemme spontanitet, og muligheten til å få fyldige beskrivelser (Drageset & Ellingsen, 2010). Hensikten var at intervjuene skulle være beskrivende i istedenfor forklarende og argumenterende for å oppnå økt kunnskap og innsikt i fenomenet i valgt kontekst. Det ble i tillegg utformet et støttedokument som ble brukt under intervjuene for å sikre at vi fikk svar på alle spørsmålene vi hadde. Utover dette ble det benyttet innslag av snøballmetode som fungerte slik at vi forhørte oss med informanter fra den strategiske utvelgelsen om tips til hvem vi kunne snakke med videre (Grønmo, 2016; Jacobsen et al., 2016). Vi vurderte de innspillene vi fikk, og avtalte intervju med en informant ut fra denne metoden.

Tabell 2: Utvalg til intervju

Utvalg til intervju	**Stilling**	**Funksjon**
Ansatte i bank og finanssektoren	Leder innkjøp og anskaffelser Innkjøp og anskaffelser (informant 1)	Har hovedansvaret for innkjøp i konsernet, i tillegg til inngående og utgående faktura.
	Senior fagspesialist risikostyring og operasjonell sikkerhet Operasjonell sikkerhet (informant 2)	Har stilling for andrelinje i forsvar og er ansvarlig for endringsrisiko i banken. Arbeider ikke direkte med utkontraktering.
	Senior fagspesialist sikkerhet Sikkerhetsavdeling (informant 3)	Arbeider i sikkerhetsavdelingen med blant annet informasjonssikkerhet og POPs-prosessen.
	Fagspesialist sikkerhet Sikkerhetsavdeling (informant 4)	Arbeider i sikkerhetsavdelingen og har ansvar for leverandøroppfølging.
Ansatt i Finanstilsynet	Senior tilsynsrådgiver (informant 5)	Informanten er med som ekspert knyttet til tilsyn og lovverk for å få tilsynsmyndighetens innfallsvinkel.
Ansatt ved universitets- og høyskolesektoren	Ekspertinformant (informant 6)	Informant med ekspertfaglig bakgrunn på området kontrakt og utkontraktering, med et kontrakts- og styringsperspektiv. Bidrar til en alternativ fremstilling og en ekspertfaglig innfallsvinkel.

Gjennomføring av intervjuer

Intervjuguiden ble sendt til de aktuelle informantene på forhånd, slik at informantene hadde mulighet til å forberede seg. Før vi startet intervjuene hadde vi en kort presentasjon av oss selv, før vi deretter presenterte studiens formål og fikk underskrift på samtykkeskjemaet (Vedlegg D). Samtlige av informantene gav samtykke til at deres stillingstittel kunne benyttes i oppgaven, slik at det ble enklere å forstå hvilke ansvarsområder de har, og hvilke deler av utkontrakteringsprosessen de bankansatte arbeider med. Vi informerte informantene i forkant om hvorfor lydopptak ville tas i bruk, med formål om at vi som intervjuere ikke skulle gå glipp av relevant informasjon. Alle informantene samtykket til at opptak kunne benyttes. Appen Diktafon Nettskjema, som er levert av Universitetet i Oslo, ble benyttet slik at vi fikk tatt opptak på en sikker måte. Ettersom at vi var to forskere til stede under intervjuene, tok den ene notater mens den andre stilte spørsmålene. De stikkordsmessige notatene ble brukt både for datagenerering og for å danne oppfølgingsspørsmål knyttet til ytringer av interesse. Etter gjennomføring av intervjuene ble båndopptakene brukt til å transkribere hvert enkelt intervju. Dette skjedde kort tid etter intervjuene, da informasjonen satt ferskt i minnet, og vi enkelt kunne trekke linjer til forskningsspørsmålene. Båndopptakene slettet i henhold til retningslinjer fra Sikt etter transkribering av intervjuene (Sikt, u.å.).

Under intervjuene opplevede vi at informantene i stor grad forklarte fritt og delte tilleggsinformasjon som gjorde at vi enkelt kunne stille oppfølgingsspørsmål, noe som økte fleksibiliteten for å få frem nyanser og variasjoner. Alle intervjuene ble avsluttet med spørsmål hvor informanten kunne gi ytterligere informasjon som kunne være nyttig for studien, i tillegg til muligheten for å stille spørsmål. Intervjuene av de ansatte i banken, og av førsteamanuensis, ble gjennomført på et møterom i deres lokaler. Det at intervjuene ble gjennomført på et grupperom, på deres arbeidsplass, kan tenkes å være mer nøytralt enn om en hadde gjennomført intervjuene på deres egne kontor (Jacobsen, 2015). Intervjuet med informanten fra Finanstilsynet ble gjennomført over Teams.

Tabell 3: Tidspunkt og tidsbruk på intervjuene

Informant:	Stilling	Dato	Tidsbruk
Finanstilsynet	Senior tilsynsrådgiver	6. mars 2023 - Digitalt	60 min
Bank	Leder innkjøp og faktura	10.mars 2023 - Fysisk	30 min
	Senior fagspesialist risikostyring og operasjonell sikkerhet	10.mars 2023 - Fysisk	45 min
	Senior fagspesialist sikkerhet	10.mars 2023 - Fysisk	30 min
	Fagspesialist sikkerhet	10.mars 2023 - Fysisk	35 min
Universitet- og høyskolesektoren	Ekspertinformant	24. april 2023 - Fysisk	40 min

4.1.2 Dokumentanalyse

Det er gjennomført en dokumentanalyse som en metode for å genere og analysere data. Vi har tatt utgangspunkt i generelle offentlige dokumenter som lover, forskrifter, veiledninger, nasjonale trussel- og risikovurderinger, offentlige utredninger, og meldinger til Stortinget. Dokumentene ble valgt på grunnlag av deres relevans for å kunne bidra til å svare på studiens problemstilling. Kriteriene har handlet om utkontrakteringsprosessen, risiko, bank- og finanssektoren, cyberhendelser, digitalisering og leverandørkjeder. Det er benyttet totalt 25 antall dokumenter som grunnlag for dokumentstudiet.

Tabell 4: *Utvalg av de mest sentrale dokumentene*

Innhold	Tittel	Opphav	Publisert
Norske offentlige utredninger (NOU)	NOU 2015:13 *Digital sårbarhet – sikkert samfunn.*	Justis- og beredskapsdepartementet	2015
	NOU 2018:14 *IKT sikkerhet i alle ledd.*	Justis- og beredskapsdepartementet	2018
	NOU 2023:6 *Finanstilsynet i en ny tid – ny lov om Finanstilsynet*	Finansdepartementet	2023
Stortingsmeldinger (Meld. St. NR)	Meld. St. 38 *IKT-sikkerhet. Et felles ansvar*	Justis- og beredskapsdepartementet	2016-2017
	Meld. St. 10 *Risiko i et trygt samfunn*	Justis- og beredskapsdepartementet	2016-2017
	Meld. St.12 *Finansmeldingen 2022*	Finansdepartementet	2021-2022
Lovverk og forskrifter	Lov om nasjonal sikkerhet	Justis- og beredskapsdepartementet	2018
	Forskrift om IKT-systemer i banker mv.	Finansdepartementet	2003
	Forskrift og risikostyring og internkontroll	Finansdepartementet	2008
	Forskrift om meldeplikt ved utkontraktering av virksomhet mv.	Finansdepartementet	2021
Rapporter	Risiko 2023	NSM	2023
	Trusselvurdering 2022	DNB	2022
	Risikostyring i digitale verdikjeder	DSB	2020
	Finansiell stabilitet	Norges Bank	2022
	Finansiell infrastruktur	Norges Bank	2022
	Det norske finansielle systemet	Norges Bank	2022
	Finansiell stabilitet	Norges Bank	2023
	Finansiell infrastruktur 2021	Norges Bank	2021
	Risiko- og sårbarhetsanalyse (ROS)	Finanstilsynet	2022
	Bank og finans	Finanstilsynet	2022
	Risiko- og sårbarhetsanalyse (ROS)	Finanstilsynet	2023
	Trusselvurdering 2022	DNB	2022
	Veiledning om utkontraktering	Finanstilsynet	2021
	IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud	NIFU	2017
	Nasjonal strategi for digital sikkerhetskompetanse	Justis- og beredskapsdepartementet	2019
Totalt antall dokumenter	25 offentlige publiserte dokumenter		

4.2 Forskningskvalitet

Studiens forskningskvalitet kan vurderes ut fra noen kriterier relatert til validitet og reliabilitet. Disse brukes for å vurdere forskningens gyldighet og pålitelighet, og bidrar til å vurdere datainnsamlingens samlede kvalitet (Grønmo, 2016). I utgangspunktet baserer begrepene seg på kvantitativ logikk, men benyttes også innen kvalitativ metode (Thagaard, 2018). Reliabilitet omhandler dataen og kildenes troverdighet. Validitet sier noe om den innsamlede dataens relevans for studiens problemstilling og teori, og om det på bakgrunn av dette kan trekkes slutninger som anses som gyldige (Halvorsen, 2008).

4.2.1 Reliabilitet

Reliabilitet er et grunnleggende spørsmål innen forskning som refererer til påliteligheten av dataene som samles inn og hvordan forskningen er gjennomført (Johannesen, et al., 2016). Det handler om å sikre nøyaktighet i datainnsamling, bearbeiding og tolkning. Reliabilitet er viktig for å kunne gjenta forskning og få tilsvarende resultater (Grønmo, 2003, 2016). Med andre ord er reliabilitet et utrykk for grad av samsvar mellom datasett fra gjentatte datainnsamlinger og av ulike forskere (Golafshani, 2003; Grønmo, 2016). I kvalitativ forskning kan reliabilitet være vanskeligere å oppnå på grunn av variasjoner i tolkningen av dataene. Det er heller ikke alltid er praktisk mulig å gjenta datainnsamlinger av de samme fenomenene på samme måte som i kvantitativ forskning. Sosiale situasjoner kan også endre seg over tid, noe som kan påvirke resultatene (Grønmo, 2016). Fenomenet risiko knyttet til utkontrakteringsprosessen i bank- og finanssektoren og hvordan denne håndteres er i endring, og vil kunne avhenge av hvem man snakker med. Det er derfor lite grunnlag for å anta at en fremtidig studie ville gitt samme resultat, noe som kan sies å svekke studiens reliabilitet. Samtidig vil andre hensyn som kan styrke reliabiliteten vektlegges i større grad slik som en beskrivende forskningsprosess (Golafshani, 2003).

Ettersom datainnsamlingen i stor grad baserer seg på intervjuer, vil det kunne ha stor innvirkning på studiens reliabilitet. For å redusere denne påvirkningen har det blitt brukt god tid og foretatt mange revisjoner av intervjuguiden for å sikre at spørsmålene ikke var ledende. Vi som forskere har vist engasjement og interesse for temaet og informantenes erfaringer ved å legge til rette for at informantene skulle dele så mye av sin kunnskap som mulig. Det har også blitt satt fokus på å gjennomføre kompetanseintervjuer, og dele informasjon med informantene i forkant for å skape trygghet i intervjusituasjonen. Intervjuene ble i tillegg gjennomført på

informantenes arbeidsplass, så langt det var mulig. Oppfølgingsspørsmål har blitt stilt åpent og søkende, og det ble påpekt at lydopptak og notater ble brukt for å ikke gå glipp av viktig kunnskap og erfaring. Det ble i tillegg informert om at vi ikke var ute etter å finne feil, mangler eller eventuelle sikkerhetshull, men vi var ute etter informantenes nøkkelkunnskap. Tanken var at dette ville etablere et trygt utgangspunkt i relasjonen mellom informantene og intervjuerne. Det at to forskere har gjennomført intervjuene og analysert dataene, vil styrke reliabiliteten ved at vi har diskutert og tatt hensyn til nøytralitet i den grad det er mulig i kvalitative studier, hvilket er et omdiskutert tema i seg selv.

4.2.2 Validitet

Validitet handler om datamaterialets gyldighet, samt relevans for problemstillingen og teori som studien ønsker å belyse (Grønmo, 2016). Dette deles inn i *intern validitet* som omhandler troverdighet og *ekstern validitet* som omhandler overførbarheten. Intern validitet handler om hvorvidt vi har studert og målt det studien hadde som formål å måle, og hvorvidt resultatene oppfattes som riktige (Thagaard, 2018). Det skal sikre at studien er en rettferdig presentasjon av fenomenet som studeres (Golafshani, 2003). Dette kan inkludere hvorvidt kildene dataene kommer fra gir riktig informasjon, og om forskernes tolkninger er gyldige (Jacobsen et al., 2016; Thagaard, 2018). Det er satt søkelys på å kontinuerlig forsikre oss om at studiens hensikt samsvarer med forskningsspørsmål, og intervjuguiden. For å sikre den interne validiteten underveis i intervjuene har vi forsikret en felles forståelse mellom informant og forsker ved å spørre: «Har jeg forstått deg rett når du sier at (..)?» (Drageset & Ellingsen, 2010). Empirisk data samlet inn gjennom intervjuer med informanter som besitter omfattende kunnskap om utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren, basert på en intervjuguide utformet ut fra teorien og problemstillingen, bidrar til å styrke gyldigheten. Det samme gjelder dokumentanalysen bestående av sekundærdata av høy relevans for innsamlet primærdata, teori, og problemstillingen. Samlet vil vi argumentere for at dette bidrar til å styrke studiens interne validitet. I tillegg har validiteten vært viktig gjennom hele forskningsprosessen, og problemstillingen er blitt spisset i takt med økt kunnskap og datainnsamling.

Ekstern validitet handler om hvor overførbare forskningsresultatene er til andre sammenhenger, og om hvor generaliserbare funnene er (Halvorsen, 2008; Thagaard, 2018). For å kunne generalisere resultatene, må studien ha en representativ menge

undersøkelsesenheter og helst et tilfeldig utvalg (Jacobsen et al., 2016). Denne studien gir ikke grunnlag for generalisering da mengden undersøkelsesenheter ikke kan sies å være representativ. Hensikten med datainnsamlingen har ikke vært å generalisere fenomenet og fokuset på ekstern validitet har dermed vært mindre relevant. Samtidig er overførbarhet i kvalitativ forskning knyttet til om man kan kjenne igjen meningen, og om denne meningen gir innsikt av betydning (Drageset & Ellingsen, 2010). Studien er utviklet slik at sektoren forhåpentligvis kan dra nytte av funnene, og resultatene kan være med på å gi en indikator på om det samsvarer med det teoretiske rammeverket.

5.0 Presentasjon av empiri og diskusjon

I dette kapittelet vil vi presentere studiens empiriske data innsamlet fra dokumentanalyse og intervjuer. Deretter vil vi diskutere empiri samlet opp mot det teoretiske rammeverket som ble presentert i kapittel 3. Formålet med å samle inn empirisk data fra ulike kilder er å kunne gjennomføre en grundig analyse, og diskusjon av studiens følgende problemstilling: *På hvilken måte representerer utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren risiko, og hvordan håndteres den?*

For å sikre en systematisk og sammenhengende fremstilling har vi valgt å strukturere kapittelet etter studiens tre forskningsspørsmål. Formålet med å presentere kapittelet på en forskningsspørsmålsorientert måte er todelt. For det første gir denne strukturen en tydelig organisering av innholdet, noe som gjør det enklere å følge sammenhengen mellom forskningsspørsmålene og den innsamlede empirien. Dette vil resultere i en klarere og mer fokusert presentasjon av våre funn. For det andre gir en slik strukturering muligheten til å utforske hvert forskningsspørsmål grundig, fra innsamling av empiri til diskusjon og oppsummering. Ved å følge denne tilnærmingen mener vi at vi legger til rette for en grundig analyse av hvert forskningsspørsmål, og presenterer funnene på en konsis måte samtidig som vi opprettholder en sammenhengende fremstilling av problemstillingen.

For å presentere empiri fra henholdsvis dokumenter og intervjuer på en effektiv og klar måte, organiseres det noen hovedkategorier under hvert forskningsspørsmål. Disse kategoriene er utformet for lettere å kunne identifisere og sammenligne funn på en mer systematisk måte, og bidrar til en helhetlig besvarelse av forskningsspørsmålene. I lys av disse hensyn vil vi nå presentere delkapitlene organisert etter våre tre forskningsspørsmål. Hvert delkapittel vil først presentere den innsamlede empirien fra dokumenter og intervjuer, deretter diskusjon av funn opp mot teorien, og til slutt en oppsummering. Vi mener at denne presentasjonen gir en grundig analyse av risiko knyttet til utkontrakteringsprosessen i bank- og finanssektoren, og gir leseren et helhetlig bilde av våre funn og diskusjoner knyttet til hvert forskningsspørsmål.

5.1 Empiriske funn og diskusjon av forskningsspørsmål 1

I første delkapittel vil vi besvare studiens første forskningsspørsmål: *Hvilke risikoer representerer utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren?* Vi vil her undersøke hvordan risikoen identifiseres og hvilken risiko utkontrakteringsprosessen

representer.

5.1.1 Risikoidentifisering

Resultater fra dokumentanalyse

Finanstilsynets veileder om utkontraktering, også omtalt som rundskrivet, gir retningslinjer for utkontraktering i bank- og finanssektoren. Den definerer hva som regnes som utkontraktering, begrensninger i adgang til å kunne utkontraktere og hvordan risikoen må identifiseres, vurderes og håndteres av foretak under tilsyn (Finanstilsynet, 2021b). I forkant må virksomheten vurdere hvilke IKT-tjenester som kan utkontrakteres og vurdere risikoene, samt ta en beslutning på om dette er en risiko de er villige til å pådra seg. Noen oppgaver kan være av så stor betydning for den operasjonelle virksomheten at det ikke regnes som forsvarlig å sette dem ut. Derfor er det avgjørende å gjennomføre grundige vurderinger tidlig i prosessen for å identifisere risikoene, vurdere sannsynligheten for at hendelser inntreffer og konsekvensene det kan ha for virksomheten (Finanstilsynet, 2021b). Vurderingen må også inkludere muligheten til å terminere avtalen uten for store forstyrrelser. Basert på risikovurderingen må foretaket beslutte om utkontrakteringen skal gjennomføres (Finanstilsynet, 2021b). Punkt fem i rundskrivet har en liste med forhold som vil kunne være av betydning for vurdering av en potensiell oppdragstaker. Dette er noe virksomheten må ta stilling til før en eventuell utkontraktering finner sted.

Ifølge NOU (2018:14) kan anskaffelser av IKT-tjenester i mange tilfeller føre til bedre trygghet, mer stabile tjenester og være et fornuftig IKT-sikkerhetstiltak. Dette vises også i Finanstilsynets «Risiko- og sårbarhetsanalyse 2023» (2023a) hvor de påpeker at sentrale tjenesteleverandører kan ha mer ressurser og kompetanse til å utvikle robuste løsninger enn foretakene enkeltvis. På denne måten kan tjenesteleverandører bidra til å redusere risiko som kan medføre alvorlige hendelser i sektoren. En stor utfordring ved anskaffelser påpekes å være manglende bevissthet om risiko (Finanstilsynet, 2022b; NOU 2018:14). Det er også viktig at virksomheter er bevisste på hvilken kompetanse som ikke bør utkontrakteres (NOU 2015:13). For å iverksette hensiktsmessige sikkerhetstiltak, er det avgjørende at virksomhetene vurderer og identifiserer risikoen ved alle anskaffelser, noe som pålegges av regelverket (NOU 2018:14). Lysneutvalget (NOU 2015:13) bemerket i sin utredning at ingen virksomheter har full oversikt over egne sårbarheter, grunnet kompliserte verdikjeder. Rapporten foreslår et nasjonalt rammeverk for å ivareta en helhetsvurdering av informasjonen som bæres i

verdikjedene, i tillegg til å fastsette et akseptabelt risikonivå for digital sårbarhet (NOU 2015:13). Det påpekes at selv om enkelte risikoer kan være akseptable for den enkelte virksomhet, kan den samlede samfunnsmessige risikoen bli for stor.

Resultat fra intervju

Empiri fra intervjuene viser at banken arbeider ulikt med risikoen ut fra kritikaliteten til tjenesten som settes ut og hvilke tjenester som leveres. Informantene viste til at det er etablerte retningslinjer, rammeverk og standarder for å vurdere risikoen. Det påpekes at de ikke kan følge opp alle utkontrakterte IKT-tjenester og vurderer derfor konsekvenspotensiale for å kunne avgjøre hvem som bør følges opp.

Risikoidentifisering og risikovurdering

På spørsmål om hvordan banken vurderer risikoen knyttet til utkontraktering av IKT-tjenester forklarer informantene at de først må ta en vurdering på om oppdraget er egnet til å settes ut. Dette er fordi det ikke er alle oppdrag de hverken vil, eller kan utkontraktere, grunnet begrensninger i lovverket. «Det er for eksempel ikke lov å utkontraktere risikovurderinger eller noen beslutninger» (informant 2). Oppdraget må defineres godt og blir nøye vurdert før en beslutning tas på om tjenesten skal settes ut. Informantene beskriver prosessen som strukturert med et betydelig fokus på hvilke risikoer som skal belyses, samtidig som informant 1 trekker fram at det har vært utfordrende å forstå risikoen.

Intern virksomhetsstyring forklares av informant 5 som grunnleggende for at man skal oppdage risiko med IKT, og en forutsetning for å kunne ha god oversikt over risikoområdet. Informanten forklarer videre at Finanstilsynet stiller krav til at banken blant annet skal ha tre forsvarslinjer, som alle sitter på ulikt ansvar og rapporterer til hverandre. I intern virksomhetsstyring vurderes også retningslinjer, verktøy, metoder og prosesser som er forbundet med å vedta et foretaks mål og strategier, i tillegg til å styre risiko. Informantene fra banken forklarer at de bruker ulike verktøy og metoder for å identifisere og vurdere risikoen før de inngår avtale med leverandør. Det nevnes blant annet en standard for hvordan de skal gjennomføre risikovurderinger, og en mal som gir retningslinjer for hvordan og hva som bør etterspørres av informasjon. Informant 3 trekker i tillegg frem en matrise som sier noe om sannsynlighet og konsekvens, og en tabell som inkluderer økonomisk tap, regulatoriske krav og eventuelle bøter. «Mye blir regnet om til økonomi hos oss, og den metoden kan utfordres, men da kan man også spørre hva som er akseptabel risiko. Det er nok ganske flytende hvor den ligger, men det knyttes til sannsynlighet

og konsekvens» (informant 3). Informantene forklarer også at de ser på konsekvensene for omdømme dersom det skulle skje en hendelse.

Etter at banken har identifisert og vurdert risikoene tar de en vurdering på hvilken leverandør som er egnet til oppdraget. Innkjøpsavdelingen inkluderes i en tidlig fase der de er med på å vurdere avtalen, leveransen og de juridiske og økonomiske risikoene. De ser også på leverandørens evne til å overleve og til å levere. Andre faktorer som er med i denne vurderingen er ifølge informant 2 om leverandøren har godt nok omdømme, den nødvendige kompetansen og god nok risikostyring. Det ses på om det er mulig for leverandøren å flytte eller gjøre avtaler slik at risikoen som burde være hos leverandøren kommer til banken. "Dette er den optimale prosessen: Vurdering av oppdraget, vurdering av leverandør og deretter vurdering av avtalen» (informant 2). Til slutt vurderes det samlet om avtalen holder mål. Det er her sentralt at det tas en kritikalitetsvurdering på oppgavene hvor vurderingen utvides etter behov.

Selv om prosessen med å kartlegge risiko før inngåelse av kontrakt er svært viktig, må virksomheten også fortsette med å identifisere mulige risikoer gjennom hele samarbeidet. Leverandøroppfølging en sentral del av arbeide med å kunne kartlegge risikoer. Det forklares at banken hele tiden må gjøre vurderinger knyttet til endringer som blir gjort. Grunnet den store datamengden leverandørene mottar fra banken må de være oppdatert på endringer leverandørene gjør. «Vi må vite om alle endringer, og derfor er leverandøroppfølging viktig» (informant 2).

Informanten fra Finanstilsynet forklarte at de tar utgangspunkt i en tilsynsmodul, som har med IKT-sikkerhet å gjøre, når de gjennomfører tilsyn hos bank- og finansforetak. Den baserer seg på NIST-rammeverket (National Institute of Standards and Technology Framework), som amerikanske myndigheter har utformet. Her ser de på blant annet beredskap, i form av forretningsmessig konsekvensanalyse som skal kartlegge effekten en hendelse vil kunne ha på et foretaks forretningsprosesser og tjenester. Informanten forklarer at man her skal finne ut hva som må være oppe til enhver tid, hva som kan være nede i få timer, et døgn eller lenger, og om man eventuelt kan miste data eller hvor lite data man kan miste. Det blir også gått gjennom IKT-sikkerhet og IKT-drift. Verdikjedene er i denne prosessen en «input» til Finanstilsynets tilsyn, som har med hendelsesrapportering å gjøre, ettersom foretakene har krav om å rapportere kritisk eller viktige hendelser, nedetid eller sikkerhetshendelser.

Arbeid med risiko med hensyn til hvordan den vurderes

Informantene forklarte at det arbeides ulikt med risiko med hensyn til hvordan den vurderes ut fra hvilken tjeneste det gjelder, og hvor avhengig banken er av tjenesten. Det at banken ser ulike risikoer ut fra hvilke tjenester som leveres, og hvor kritisk den er, har ifølge informant 4 betydning for hvordan risikoen vurderes og hvilke retningslinjer som følges. «Vi ønsker en lavere risiko med systemer vi er svært avhengig av, og de som vi er mindre avhengig av vil bli vektlagt i mindre grad» (informant 4). Informanten mente at man kan velge å bare ha risikoen, men at man da ikke er så lur. Man kan velge ekstra beskyttelse i form av tiltak, eller velge å akseptere risikoen som den er. «Skulle vi gjort noe med risikoen innebærer det kostnader og utfallet ville kanskje blitt det samme» (informant 4). Det ble påpekt at banken må ta en vurdering hvor de må veie opp en mulig høyere risiko og en mer spesialisering på tjenesten, mot mulig lavere risiko og mindre spesialisert tjeneste.

Informant 4 påpekte også at det arbeides ulikt med risiko avhengig av hvem som er involvert i prosessen, dette fordi ansatte kan ha forskjellige oppfatninger av risiko. Det blir også vist til som en av grunnene til at prosessen er fordelt på ulike avdelinger, med ulike perspektiver og fokusområder. På den måten blir risikoen spredt utover flere ledd, og kan fungere som en slags barriere. Det påpekes likevel at det til syvende og sist er sikkerhetsavdelingen i banken som eier risikoer.

5.1.2 Utkontrakteringsrisiko

Resultater fra dokumentanalyse

Risikobeskrivelse

Utviklingen i samfunnet der «alt henger sammen med alt» utgjør en strukturell sårbarhet på flere måter (NOU 2018:14). Ifølge NSM (2023) er viktige samfunnsfunksjoner avhengige av leverandører, og underleverandører, som potensielt kan ha ukjente og alvorlige sårbarheter. Det pekes på at de mest sårbare områdene er langs flankene (NSM, 2023). Utkontraktering av IKT-tjenester øker risikoen grunnet redusert kontroll over stadig mer komplekse verdikjeder. Leverandørkjeder utgjør sårbarheter som trusselaktører vet å utnytte, for eksempel gjennom leverandørkjedeangrep som kan medføre store konsekvenser.

Det norske finansielle systemet er ifølge Norges Bank (2022b) sårbart for cyberangrep. Slike angrep, beskrevet av både Norges Bank (2021a) og Meld. St.12 (2021-2022), utgjør en kilde

til systemrisiko og kan true den finansielle stabiliteten. Systemrisiko innebærer at det finansielle systemet ikke er i stand til å utføre sine funksjoner, og kan føre til alvorlige økonomiske tilbakeslag. Det er en bred internasjonal politisk enighet om å styrke motstandskraften mot cyberhendelser i bank- og finanssektoren som en vesentlig del av innsatsen for å bekjempe systemrisiko (Norges Bank, 2021b).

Samlokasjon av IKT-virksomhet fra flere foretak eller kjøp av IKT-tjenester fra få leverandører kan medføre konsentrasjonsrisiko (Finanstilsynet 2022b, 2023a). I finanssektoren er IKT-driften i stor grad utkontraktert til et mindre antall sentrale tjenesteleverandører og datasentre, som også ofte leverer tjenester til andre sektorer. Slike aktører er derfor attraktive mål for trusselaktører. Samtidig kan sentrale tjenesteleverandører ha større ressurser og kompetanse til å utvikle robuste løsninger og nødvendig beredskap enn foretakene har. Bruk av tjenesteleverandører kan dermed bidra til å redusere risikoen for at cyberangrep fører til alvorlige hendelser i finanssektoren (Finanstilsynet, 2022b). På den andre siden kan sterke operasjonelle sammenkoblinger og konsentrasjon i systemet forsterke og spre konsekvensene av et angrep, med alvorlige følger (Finanstilsynet, 2022b; Norges Bank, 2022a, 2022b). Manglende robusthet eller lavt sikkerhetsnivå hos en enkelt leverandør kan utgjøre et svakt ledd i de samlede verdikjedene, og skape hendelser som kan smitte over på andre aktører (Finanstilsynet, 2022b). Norges Bank (2022a, 2022b) påpeker at dette gjelder særlig dersom angrepet rammer kritisk infrastruktur eller funksjoner, sentrale IKT-leverandører eller mye brukt programvare. Et potensielt angrep kan føre til at sensitiv informasjon kommer på avveie, og at tilliten til det finansielle systemet svekkes (Finanstilsynet, 2022b). I tillegg kan kritiske funksjoner bli satt ut av spill, noe som kan ramme den finansielle stabiliteten.

Operasjonell risiko, trekkes frem som en risiko forbundet med utkontraktering av IKT-tjenester i rapporten «Det norske finansielle systemet 2022» fra Norges Bank (2022c). Dette refererer til risikoen for tap knyttet til tekniske feil, menneskelig svikt og utilstrekkelige kontrollsystemer. Årsakene til operasjonell risiko kan være mangelfulle prosedyrer, feil i eller angrep på IT-systemer, regelbrudd, bedrageri, brann, terrorangrep eller liknende. Operasjonell risiko kan også forårsake eller forsterke andre risikoer. Dersom en eller flere risikoer blir tilstrekkelig store, kan det bidra til manglede effektivitet og sikkerhet i det finansielle systemet, som kan føre til systemrisiko (Norges Bank 2022c).

Kjennetegn ved risikoene

Sårbarheten kan også beskrives som en karakteristikk av risikoen, der den reflekterer graden av gjensidig avhengighet mellom leddene i en verdikjede et system er bygget på (DSB, 2020). I et system som er preget av utkontraktering med tette koblinger og komplekse interaksjoner, vil ukjente sekvenser oppstå som vil utløse andre følgehendelser, noe som gjør det vanskelig eller umulig å stoppe hendelsesforløpet (DSB, 2020). Slike komplekse systemer er uoversiktlige med mange aktører og fragmentert systemansvar og vil ha betydning for systemets sårbarhet (DSB, 2020). I Lysneutvalgets rapport (NOU 2015:13) fremmes lange og uoversiktlige leverandørkjeder som en utfordring i finanssektoren. I rapporten kommer det frem at større omfang av kjøp av ressurser og kunnskap utenfor Norge på sikt kan føre til utfordringer med å opprettholde tilstrekkelig styring og kontroll. Dette trekkes også frem av Finanstilsynet (2023a) at en av de største risikoene mot stabile finanssystemer er mangel på kontroll av leverandørkjeden til utkontrakterte IKT-tjenester. En av grunnene er at tilgangen på IKT-sikkerhetskunnskap er en stor utfordring på IKT-sikkerhetsområdet (Finanstilsynet, 2022b; Meld. St. 10 (2016-2017); Meld. St. 38 (2016-2017); NOU 2015:13). Manglende kunnskap påvirker utviklingen av IKT-systemer og programvare, samt driften av slike systemer. Det har også betydning for utforming og oppfølgning av lover, forskrifter, råd, veiledere, rutiner og styringssystemer (NOU 2018:14). Konsekvensene av manglende kompetanse kan også føre til svakere oppfølgning og kontroll med kritisk utkontrakterte IKT-tjenester, i tillegg til at problemer eller feil som oppstår blir vanskeligere å løse (Finanstilsynet, 2022b).

NOU (2018:14) poengterer at verdikjedene er sårbare for ulike typer hendelser, både de som skyldes bevisste handlinger og de som skyldes feil eller ulykker. Tilsiktede uønskede digitale hendelser er et økende problem, hvor IKT-systemer kan bli brukt som mellomledd i angrep mot andre egentlige formål (DSB, 2020; NOU 2018:14). Slike hendelser kan være krevende å kartlegge, og kan utgjøre en alvorlig trussel. Angriperne kan ha som mål å skade motparten ved å påvirke, redusere eller ødelegge funksjonaliteten i produksjonssystemer. DNB (2022) anslår i sin trusselvurdering at det er en mulighet for at slike angrep vil øke i takt med den økende sikkerhetspolitiske spenningen. Konsekvensene av et cyberangrep kan gå utover både omdømmet, forholdet til kunder, tilgjengelighet til finansielle tjenester, og føre til tapte inntekter (DNB, 2022). Leverandørkjedeangrep er en betydelig trussel grunnet virksomheters avhengighet av å kjøpe tjenester og programvarer fra underleverandører. Ifølge DNB (2022) må man forvente angrep via tredjeparter, og derfor være i stand til å forsvare seg når det skjer.

«En trend DNB har sett er at tiden det tar fra en sårbarhet blir kjent til trusselaktørene utnytter den blir kortere» (DNB, 2022, s. 9).

Meld. St. 38 (2016-2017) og NOU (2018:14) påpeker at IKT-kriminalitet fører til betydelige økonomiske tap, men at en stor andel av uønskede hendelser er ikke-ondsinnet. Det er vanlig med svikt i IKT-systemer grunnet menneskelige feil, programvarefeil, utstyrsfeil, naturhendelser eller en kombinasjon av disse. Finanstilsynet (2022b) anser sårbarheter knyttet til foretaks forsvarsverk mot digital kriminalitet som den mest sentrale risikoen knyttet til foretakets bruk av IKT, der den samlede risikoen anses å være høy. Når det gjelder sårbarheter knyttet til IKT-drift, tilgangsstyring og informasjonslekkasje anses den samlede risikoen å være middels til høy. Risiko knyttet til sårbarheter ved foretakets leverandørstyring, endringsstyring, styringsmodell og internkontroll, kunnskap- og kompetansestyring, samt datakvalitet anses til å være middels (Finanstilsynet, 2022b).

Resultater fra intervjuer

På spørsmål om hva informantene anser som risiko i en utkontrakteringskontekst av IKT-tjenester i bank- og finanssektoren trekker informantene frem omdømme, økonomiske tap, informasjonstilgang, kunnskap, leverandørkjedeangrep, informasjonsmisbruk, driftssikkerhet, og konsentrasjonsrisiko. Risikoene som påpekes, som følge av utkontraktere IKT-tjenester, relateres både til ikke-ondsinnede hendelser og tilsiktede ondsinnede hendelser. Informantene poengterer at risikoen ved å utkontraktere IKT-tjenester i bank- og finanssektoren er høy, men at gevinsten er større.

Risikobeskrivelse

På spørsmål om hvordan informantene vil beskrive risikoen utkontraktering av IKT-tjenester representerer for bank- og finanssektoren, svarte informant 3 at risikoen er ganske stor og derfor blitt tatt på alvor i stor grad. Informant 4 og 5 mente at risikoen både er høy og lav, men at gevinsten ved å utkontraktere er større. De forklarer at risikoen de står igjen med absolutt må fokuseres på.

Informantene trakk frem ulike risikoer, men påpeker at de sjeldent kan gå på liv og helse. Derimot trekkes omdømme og økonomisk tap frem som de største risikoene av både informant 1 og 3, i tillegg til informasjonstilgang og misbruk av informasjon. Altså at informasjon som kommer på avveie kan føre til tap av omdømme. Dersom banken utkontrakterer en tjeneste til

en underleverandør som begår en feil, kan det føre til at banken blir hacket og angripere får tilgang til kundedata. Det kan resultere i en uheldig situasjon for både kundene og bankens omdømme. «Et produkt vi leverer kan faktisk også ha mye å si for driften av andre systemer i banken. Dette går på Business Impact Anaalysis (BIA), og hva som skjer dersom systemet faller ut» (informant 2).

Andre risikoer som trekkes frem er teknisk risiko og cyberkriminalitet. «Man kan sitte hvor som helst i verden og få eller skape seg tilgang til informasjon» (informant 6). Leverandørkjedeangrep som risiko i en utkontrakteringskontekst blir satt spesielt søkelys på ifølge informant 4. «Vi ser på trusselbildet at det er økt risiko for at hendelser kan komme gjennom leverandører» (informant 4). Når det kommer til driftssikkerhet er det sentralt at banken ikke kun har tilgang til systemet, men også informasjonen som ligger der. Dersom leverandøren skulle gå konkurs kan det hende at banken ikke har tilgang på data som leverandøren har lagret eller behandlet, noe som utgjør risiko for driftssikkerheten.

Konsentrasjonsrisiko trekkes frem som et risikoområde hvor det nå iverksettes risikoreduserende tiltak fra internasjonalt hold. Informant 5 forklarte at Finanastilsynet deltar i et initiativ fra EU-kommisjonen for etablering av et organ med overordnet ansvar over de større aktørene i sektoren for å redusere konsentrasjonsrisiko i sektoren. Det skal sikre at regelverket innen IKT-sikkerhet, risiko og utkontraktering skal være likt for finanssektoren i Europa. De tre europeiske tilsynsmyndighetene, Den europeiske banktilsynsmyndigheten (EBA), Den europeiske verdipapir- og markedstilsynsmydigheten (ESMA) og Den europeiske tilsynsmyndigheten for forsikring og tjenestepensjon (EIOPA), engasjeres som sekretariat i utarbeidelsen av regelverket i samarbeid med representanter fra EØS-landenes myndigheter. Et område som regelverket vil omfatte er «oversight» av kritiske tredjepartsleverandører. Dette inkluderer store tjenesteleverandører som benyttes av mange foretak innen finanssektoren og representerer betydelige konsentrasjoner, slik som Microsoft Office 364 og Google Analythics. Målet med denne funksjonen er å redusere risikoen ved å ha bedre kontroll over løsningene, heller enn å begrense kritiske tredjepartsleverandører. Konsentrasjonsrisikoen blir vurdert gjennom denne «oversight»-funksjonen for å sikre at den er tilstrekkelig robust for å holde risikoen på et akseptabelt nivå. Initiativet er etablert for å styrke tilsynet og reguleringen av de store aktørene i finanssektoren, samt overvåke og håndheve etterlevelsen av regelverket. Målet er å øke stabiliteten og redusere risikoen i sektoren.

Risikoen banken står overfor ble beskrevet ut fra kritikaliteten til systemet som skal utkontrakteres: «Vi har et regelverk og et rundskriv fra Finanstilsynet om hva, og hvordan saker skal vurderes, og de minimumsstandardene må vi alltid møte. Samtidig som kritikalitet må komme inn» (informant 2). Informanten forklarte videre at dersom de har en SaaS-tjeneste (Software as a Service) som kun er informasjonsgivende, men ikke er integrert til noe som helst og heller ikke påvirker beslutningstaking, er den tjenesten ikke *så* viktig og risikoen er dermed begrenset. En slik risiko vil ifølge informant 2 beskrives som risiko for at leverandøren kan bli hacket, og nedetid slik at banken ikke får tilgang på informasjonen. Dersom risikoen ikke er kritisk, vil det være av vesentlig mindre betydning. I situasjoner hvor et system som både er en del av banken og en del av en samfunnskritisk prosess som må være oppe til enhver tid, har man et annet risikobilde og tankesett som banken må ut med.

Kjennetegn ved risikoene

Risikoen knyttet til utkontraktering av IKT-tjenester kjennetegnes ifølge informant 4 av kompleksitet grunnet antall aktører som er involver i en slik prosess. Dette betyr ifølge informanten at desto flere virksomheter som er involvert, desto mer komplisert vil det kunne være å koordinere og overvåke, noe som øker sjanse for feil eller mangler som vil kunne medføre sikkerhetsutfordringer. Informanten fra Finanstilsynet mente at de ikke har annen erfaring enn at risikoen ved utkontraktering av IKT-tjenester kjennetegnes ved at det svekker bankers robusthet og øker sårbarheten. Det samme fremkommer i intervju med informant 6, som mente at utkontraktering ikke nødvendigvis øker risikoen.

> For å ha all nødvendig kompetanse internt, må man være en veldig stor organisasjon, i tillegg til å ha evnen til å kontinuerlig fornye seg på den tekniske siden. Jeg tenker at utkontraktering av IKT-tjenester er helt nødvendig, men det er omfanget og hvordan man gjør det som er den virkelige variabelen i denne sammenheng (informant 6).

Hovedrisikoen med utkontraktering er ifølge informant 6 at de som utkontrakterer ikke får de produktene og tjenestene de trenger. Risikoen handler ikke nødvendigvis om at man ikke får det produktet man ber om, men om man får det produktet man trenger. Ifølge informanten er det helt sentralt at man mestrer samarbeidet mellom kunden og leverandøren. Det pekes også på at det er viktig at leverandøren faktisk gjør det arbeidet som kreves. Informanten forklarer at det er viktig av å vite hva som kreves når man går til innkjøp, for at det skal kunne ivaretas på en god måte. «Kunnskapen som kreves for å ivareta verdiene er helt sentralt, og ikke alltid

like enkelt» (informant 5). Utkontraktering i dag forklares som noe annet enn før, da selskapene det meste av kunnskap «eget hus», eller utkontrakterte til noen i nærheten. «I dag sitter kunnskapen spredt utover hele verden, så en utfordring blir også hvor denne kunnskapen skal komme fra. Det har blitt enda mer komplekst nå enn det var» (informant 6).

Det forklares at små banker er avhengig av å utkontraktere, både grunnet sikkerhets- og rapporteringskrav, og kompetansekrav de skal jobbe med. Informant 5 forklarer at det er stor mangel på kompetanse både innenfor drift og sikkerhet og generelt, og at dette er en risiko av betydning. Informanten peker på at det er særlig de små som er prisgitt å være en del av noe større, og anser dette som svært risikoreduserende. Virksomhetsstyringen innenfor IKT påpekes også som mye bedre hos de store enn hos de små. Informanten påpekte også at risikoen og sannsynligheten innenfor IKT-sikkerhet er vesentlig mye mindre når man er stor, men konsekvensene er større fordi det gjelder flere. Sannsynligheten hadde vært veldig stor om man hadde vært alene, og konsekvensene mindre.

På spørsmålet knyttet til hvilke typer hendelser eller hvilken type risiko utkontrakteringsprosessen av IKT-tjenester representerer, mente alle informantene fra banken at risikoen både er knyttet til tilsiktede ondsinnede handlinger, og ikke-ondsinnede hendelser. Det fremkommer ikke at de arbeider systematisk ulikt med safety og security-risikoer, men heller at de arbeidet med risikoen samlet. Informant 2 forklarer hvordan feil kan skje som følge av leverandørene.

> Vi kan risikere at en leverandør gjør en feil, for eksempel i behandlingen av data. Det kan være menneskelige feil på lik linje som systemfeil, eller at leveransen har en feil innebygget. Vi risikerer på den måten at vår ansatt gjør feil i et system, ikke grunnet at vår ansatt er dårlig opplært eller har liten kompetanse, men feil i leveranse fra leverandør (informant 2).

Videre ble det forklart at type hendelse eller type risiko som utkontrakteringsprosessen representerer kommer an på hvilken utkontraktering man snakker om. Informant 4 spesifiserte at det gjelder både ikke-ondsinnede og tilsiktede ondsinnede hendelser. Noen utkontrakterte tjenester vil ha større safety-fokus, mens andre vil ha økt security fokus. Informant 4 trekker frem brann som en risiko for et datasenter som et eksempel som kan rammes av ondsinnede og ikke-ondsinnede hendelser. Et annet eksempel er en skytjeneste, hvor det vil være fokus på

tilgangsstyring, og rutiner som foreligger for å trykke på linker som vil kunne påvirke banken. Det er altså risikoer som både omfatter safety- og security-risikoer på ulike måter, hvor den ene risikoen kan åpne opp for den andre. Det ble trukket frem at utkontraktering på den ene siden gjør banken mer sårbar fordi det involver flere og det blir da et gap mellom banken og tjenesteleverandørene. Samtidig som tjenestene leverandørene leverer sannsynligvis vil være bedre enn dersom banken hadde produsert det selv. «Sårbarheten øker kanskje på den ene siden, men reduseres på den andre siden. Slik er det med risikoen også, man må velge hvordan man skal forholde seg til den» (informant 4).

5.1.3 Diskusjon av forskningsspørsmål 1

Risikoidentifisering og risikovurdering

Empirien viser at utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren representerer ulike risikoer og at mange av disse kjennetegnes ved kompleksitet. NOU (2015:13) påpeker at ingen har full oversikt over egne sårbarheter grunnet verdikjedenes kompleksitet. Omfattende verdikjeder, med mange aktører skaper et komplekst system som gjør det vanskelig å få oversikt over både svakheter og risikoer knyttet til utkontraktering. NOU (2018:14) viser at den største utfordringen med anskaffelser er manglende bevissthet om risikoen. Dette viser til viktigheten av å ha oversikt over egne leverandører, for å kunne være bevisst på å skaffe oversikt over aktuelle risikoer. For at banksektoren skal kunne vurdere og håndtere risikoen på best mulig måte er det sentralt at de forstår hva risikoen er, hvilke risikoer som må prioriteres og hvorfor, da dette har betydning for sikkerhetsarbeidet og håndteringen av risiko.

Empirien fra intervjuene påpeker at det til tider kan være utfordrende å forstå risikoen, noe som kan knyttes til usikkerhetsdimensjonen. Usikkerheten relatert til utkontraktering av IKT-tjenester kan knyttes til det Renn (2008) omtaler som epistemisk usikkerhet. Ved en slik risiko er det nødvendig å samle inn mer informasjon og kunnskap for å kunne redusere usikkerheten. Likevel er det ikke alle risikoer man kan samle inn nok informasjon om, enten fordi de er nye, eller fordi vi ikke vet noe om dem. Dette er relevante problemstillinger knyttet til utkontraktering av IKT-tjenester, da det stadig kommer ny teknologi med nye utfordringer. Videre skiller Renn (2008) mellom enkle, komplekse, usikre og tvetydige risikoer. Den samlede risikoen utkontrakteringsprosessen representerer kjennetegnes ikke alene av en av kategoriene, noe som samsvarer med det Renn (2008) forklarer. En risiko kan falle inn under

flere av kategoriene ettersom de ikke er helt adskilte og inneholder en blanding av flere typer, noe som også gjelder den overordnede risikoen relatert til utkontrakteringsprosessen. Det er derfor viktig å identifisere og forstå hvilke type risiko det er snakk om, og videre kunne tilpasse risikohåndteringsstrategien og tilnærmingen deretter, noe som ikke alltid er like lett.

Bankens betydelige fokus på sikkerhet gjør at de er avhengig av å gjøre vurderinger knyttet til risiko til enhver tid. Empirien viser at det er mange metoder og verktøy banken benytter for å identifisere og vurdere risiko. Blant disse tilnærmingene er det standarder for risikovurdering, rammeverk og maler som gir retningslinjer, samt vurderinger av sannsynlighet og konsekvens. Banken bruker også en matrise som vurderer sannsynlighet og konsekvens, i tillegg til en tabell som tar hensyn til økonomisk tap, omdømme og regulatoriske krav. Det ble påpekt at det er et fokus på det økonomiske aspektet i banken, da dette naturligvis er en viktig verdi knyttet til deres virksomhet. Denne tilnærmingen viser til avveiningen av ulike hensyn som Aven et al. (2008) beskriver som kjernen i risikostyring.

Det fremkommer i intervjuene at banken har en tilnærming der de arbeider med og vurderer risiko basert på kritikalitet og avhengighet, hvor vurderingen tilpasses ved behov. Dette er den primære metoden de bruker for å vurdere risiko, og et område som vektlegges i stor grad. Hva som er akseptabel risiko knyttet til driften i banken, virker å være flytende og baserer se på samspillet mellom sannsynlighet og konsekvens. En forretningsmessig konsekvensanalyse kan derfor være et sentralt hjelpemiddel for å identifisere og vurdere risikoen knyttet til systemer og tjenester, og kan brukes for å vurdere systemrisiko og iverksette risikoreduserende tiltak. Det er avgjørende å ha en systematisk og kontinuerlig tilnærming for å evaluere risikoen for kritiske systemer.

Risikobeskrivelse

Den innsamlede empirien, som beskriver hva som anses som risiko ved utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren og hvordan den beskrives, er i stor grad sammenfallende. Dokumentanalysen peker blant annet på leverandørkjedeangrep, avhengigheter, konsentrasjonsrisiko, finansiell stabilitet, operasjonell risiko og systemrisiko som de største risikoene. Intervjudataen fremlegger økonomisk tap, omdømme, informasjonstilgang, informasjonsmisbruk, personvern, driftssikkerhet, informasjonssikkerhet og leverandørkjedeangrep som betydningsfulle risikoer. Dokumentanalysen indikerer at manglende robusthet kan utgjøre svakheter i ledd der en

hendelse enklere kan smitte over på andre systemer, noe som kan hemme kritiske funksjoner og potensielt ramme den finansielle stabiliteten (Finanstilsynet, 2022b; Norges Bank, 2022a, 2022b). Selv om informantene ikke nevnte risiko knyttet direkte til den finansielle stabiliteten, la de vekt på at utfallet av et system kan påvirke driften av andre systemer i banken grunnet avhengighet. Dette kan peke mot systemrisiko, som viser til sannsynligheten eller risikoen for sammenbrudd i et helt system, og som i denne sammenhengen kan gi alvorlige konsekvenser og dermed true den finansielle stabiliteten (Lind, 2016; Kaufmann & Scott, 2003).

Informantene viste til økt sårbarhet som følge av risikoen for følgefeil. I tillegg til konsekvenser et leverandørkjedeangrep kan føre til for driften av systemer i banken, herunder nedetid og informasjon på avveie. Dokumentanalysen viser at det finansielle systemet er sårbart for cyberangrep og at det i størst grad er langs flankene sårbarheten ligger (NSM, 2023). Sårbarheten øker i takt med økt risiko, hvor systemets kompleksitet spiller en betydning (NOU 2015:13). Empirien fremmer ikke en konsekvens- og sannsynlighetstilnærmet risikobeskrivelse, men vektlegger heller risikoens usikkerhetsdimensjon ved realiseringen av hendelser, konsekvenser av en eventuell hendelse, i tillegg til alvorligheten og tilhørende konsekvenser (Engen et al., 2021). Risikoene som trekkes frem av empirien gjelder ikke kun for virksomheten, men også dens kunder og samfunnet ellers. Grunnet risikoens usikkerhet, alvorlighet og påvirkningen den kan ha, vil den ene informanten beskrive risikoen ut fra kritikalitet. Med dette mener informanten at man ikke generelt kan beskrive risikoen som høy eller lav. Banken må derfor heller se på hvilken tjeneste risikoen knyttes til, og kan dermed beskrive risikoen ut ifra hvor kritisk den aktuelle tjenesten er.

Kjennetegn ved risikoen

Empiren viser til at det følger en viss risiko ved å utkontraktere IKT-tjenester i bank- og finanssektoren, men informantene påpekte at det er helt nødvendig å organisere seg på denne måten. Noen utkontraktere IKT-tjenester har naturligvis høyere risiko enn andre, grunnet omfanget av tjenester som settes ut. Informantene mente at risikoen anses som både høy og lav, men at gevinsten av utkontraktering er større enn ulempene. Selv om det er enighet om at dette er en risiko man er villig til å ta, er det en betydelig oppmerksomhet relatert til ulempene. Det må derfor vektlegges å arbeide kontinuerlig med risiko, blant annet gjennom identifisering av kritiske områder, risikovurdering og implementering av tiltak for å håndter sårbarhet. Det kan peke mot redundans som ifølge HRO-teorien bidrar til å opprettholde pålitelighet (Weick & Sutcliffe, 2007). NAT-teorien på den andre siden argumenterer for at redundans vil gjøre

systemet mer komplekst, noe som vil være skadelig (Perrow, 1999). Det pekes samtidig på at organiseringen ved utkontrakteringen gjør banken mer sårbar og svekker robustheten. Dette fordi kompleksiteten økes ved at det involverer flere aktører og skaper mer avhengigheter.

Sårbarhet er en faktor som påvirker risiko, og ifølge Aven (2018) bidrar sårbarhet til at det blir vanskelig å stå imot uønskede hendelser. Ut ifra informantene kan det fremstå som at sårbarheten ikke nødvendigvis øker ved å utkontraktere IKT-tjenester, ettersom utkontraktering også reduserer risikoen. Med dette mener informantene at leverandørene ofte har spesialisert kunnskap, og dermed et bedre grunnlag til å holde et godt sikkerhetsnivå rund tjenestene. Det hadde også vært en risiko om banken hadde valgt å ikke utkontraktere og dermed ikke hatt tilgang på spesialkompetansen de trenger. Sagt på en annen måte vil sårbarhet og risiko alltid være til stede, og det foreligger derfor en enighet om at det er en dårlig beslutning å ikke utkontraktere.

Dokumentanalysen fremmer blant annet graden av avhengighet, i tillegg til tap av kontroll og oversikt som kjennetegn ved risikoen, noe som også kom frem i intervjuene. Disse kjennetegnene kan knyttes til den kompleksiteten som Perrow (1999) refererer til, der et systems mange interaksjoner, komponenter og avhengigheter medfører kompleksitet, noe som kan føre til systemfeil. Empirien støtter opp om risikoen for uforutsette feil eller hendelser som følge av organiseringen, slik Perrow (1999) beskriver det. Det at IKT-systemene er koblet sammen på en enda mer uoversiktlig måte, gjør at de trolig utgjør enda tettere koblinger. Dette skyldes at komplekse systemer består av mange ikke-lineære interaksjoner som ofte er skjulte og ikke-oversiktlige. Mange aktører og fragmentert systemansvar, resulterer i flere eksponerte flater som kan være sårbare for feil eller angrep. Til tross for dette har det ikke vært noen hendelser i bank- og finanssektoren som har ført til systemsvikt, eller truet den finansielle stabiliteten i Norge (Meld. St. 12 (2021-2022)). Dette tyder på at det er mulig å organisere seg i et komplekst og tett koblet miljø, og likevel unngå de unngåelige ulykkene som Perrow (1999) refererer til. En slik tankegang presenteres i HRO-teorien, og viser til at selv om det er potensiale for katastrofale feil, kan de unngås ved å ha sikkerhet som høyeste prioritet i organisasjonen (Weick & Sutcliffe, 2007). Det faktum at sektoren ikke har opplevd slike hendelser, kan støtte opp under HRO-tankegangen.

Mangel på kunnskap

Empirien vektlegger kunnskapen som kreves for å utkontraktere IKT-tjenester. Det påpekes at kunnskapen på generell basis er mangelfull, og at denne mangelen representerer risiko ((Meld. St. 10 (2016-2017); Meld. St. 38 (2016-2017); NOU 2013:13). Mangelen på kunnskap kan påvirke graden av kontroll, oppfølging av arbeidet, utviklingen av IKT-systemer, programvare og drift av systemene (NOU 2018:14). Konsekvensene av manglende kunnskap påvirker forskjellige aspekter av utkontrakteringsprosessen. Det kan være utfordrende å velge riktig leverandør i tillegg til å sette realistiske mål og forventninger for kontrakten, samtidig som man forhandler frem en avtale som sikrer at virksomhetens behov blir møtt. Mangel på kunnskap om risikoene utgjør en utfordring, både når det gjelder kjente og ukjente risikoer. Det kan blant annet gjøre administrering og overvåking av tjenester utfordrende. Dette vil kunne by på utfordringer knyttet til identifisering og håndtering av problemer, samt sikring av at leverandører overholder avtalen og oppfyller krav. Det er derfor avgjørende at virksomheten har tilstrekkelig kunnskap om mulige risikoer knyttet til utkontraktering. Dette for at de skal kunne implementere nødvendige tiltak for å fungere som nødvendig, under både forutsette og uforutsette forhold. Det er en forutsetning for at de skal kunne være resilient (Hollnagel, 2011). Når en virksomhet er resilient innebærer det evnen til å kunne tilpasse, omstille og justere seg, noe som krever kunnskap som i dag pekes på som manglende i stor grad. Hollnagel (2017) oppfordrer organisasjoner til å fokusere på kontinuerlig læring og forbedring.

Konsentrasjonsrisiko

Empirien trakk frem konsentrasjonsrisiko som en betydelig risiko ved utkontraktering, som kan forsterke og spre angrep. Hvordan man vurderer og håndterer risikoen er knyttet til denne faktoren (Finanstilsynet, 2022b; Norges Bank, 2022a, 2022 b). Perrows (1999) teori om styring gir innsikt i hvordan ulike organisasjonsstrukturer kan påvirke konsentrasjonsrisiko. Han argumenter for at desentralisert styring kan øke kompleksiteten gjennom å inkludere flere aktører, noe som vil kunne føre til ulykker. Sektorens oppmerksomhet mot å identifisere kritiske områder gjennom initiativ fra EU, risikovurderinger og implementering av tiltak for håndtering av risiko og sårbarhet, kan peke mot redundans i et HRO-perspektiv. HRO-teorien argumenterer for at redundans kan bidra til å opprettholde pålitelighet, øke stabilitet og redusere risiko (Weick & Sutcliffe, 2007). Teorien vektlegger involvering av alle nivåer i organisasjonen gjennom risikovurdering og risikohåndtering for å redusere konsentrasjonsrisiko. En desentralisert styringsstruktur og en HRO-tilnærming kan bidra til å redusere konsentrasjonsrisiko ved å spre beslutningsmyndighet, og ansvar for risikovurdering

og risikohåndtering (Weick & Sutcliffe, 2007). Dette muliggjør tidlig identifisering og effektiv håndtering av risiko, og legger til rette for en fleksibel tilnærming som er viktig ifølge HRO-teorien.

Safety vs. security

Innsamlet empiri indikerer at utkontraktering av IKT-tjenester i bank- og finanssektoren fører med seg risikoer som relateres både til safety og security-dimensjon. I tillegg viser det seg at safety-risikoer også kan åpne for security-risikoer. Intervjumaterialet viser at banken tar hensyn til kritikaliteten, type tjeneste og risikonivået i sitt arbeid. Det er imidlertid ingen indikasjoner på at de arbeider spesifikt ut ifra på *type* risiko. Dette tyder på at banken ikke bruker, eller ikke har behov for, ulike styringsverktøy for å håndtere risiko i henhold til hvordan den identifiseres, ettersom kritikaliteten blir vektlagt i størst grad. Analysen av dokumentene gir ingen indikasjon på at det er vanlig praksis å skille arbeidet basert på hvordan risikoen identifiseres, enten det er i et safety- eller security-perspektiv. I henhold til Jore (2019) er det observert at de samme perspektivene og risikoanalysemetodene i stor grad benyttes både i safety- og security-feltene, uten å nødvendigvis skille mellom dem. Bankens tilnærming kan derfor ses i lys av Jores (2019) poeng angående behovet for en integrert tilnærming mellom disse feltene for å møte dagens, og fremtidens utfordringer. Banken bør likevel være oppmerksom på hvordan safety-risikoer kan åpne opp for security-risikoer, og hvordan de skal identifisere og håndtere slike risikoer. Eksemplene fra banken viser at dette er noe de er oppmerksomme på og tar i betraktning. Det er viktig å erkjenne at det kan være en overlapp eller gjensidig påvirkning mellom dem. Banken bør derfor implementere en helhetlig tilnærming som tar hensyn til begge aspektene for å sikre effektiv risikohåndtering og beskyttelse av verdier i IKT-tjenestene de utkontrakterer.

5.1.4 Oppsummering av forskningsspørsmål 1

Den innsamlede empirien viser at utkontraktering av IKT-tjenester i bank- og finanssektoren bidrar til å skape en kompleks organisering som er utsatt for flere typer risikoer. Denne kompleksiteten resulterer i økte sårbarheter og redusert robusthet, da utkontrakteringen involverer flere aktører og skaper avhengigheter. Risikoene som kommer frem av empirien er leverandørkjedeangrep, avhengigheter, konsentrasjonsrisiko, finansiell stabilitet, operasjonell risiko og system risiko. Risikoene knyttet til utkontrakteringsprosessen karakteriseres som tap av kontroll og oversikt, kompleksitet, avhengighet og manglende kunnskap. Det viser seg også

at det ikke arbeides ut ifra en tydelig skillelinje basert på om risikoen identifiseres innenfor safety- eller security-feltet. Fokuset ligger heller på kritikaliteten, som viser til hvilke risikoer som vektlegges i størst grad. Samlet sett tyder funnene på at risikoen ved utkontraktering betraktes som betydelig. Likevel ville denne risikoen vært like stor, om ikke større, om man hadde valgt å beholde IKT-tjenestene internt. Med andre ord medfører organiseringen av utkontraktering en viss risiko, men risikoene som medfølger anses som nødvendig.

5.2 Empiriske funn og diskusjon av forskningsspørsmål 2

I andre delkapittel vil vi besvare studiens andre forskningsspørsmål: *Hvordan blir risikostyringsinstrumenter utviklet i forbindelse med utkontrakteringsprosessen i bank- og finanssektoren?* Her vil vi undersøke hvilke risikostyringsverktøy som benyttes, samt utfordringer knyttet til styring av risiko.

5.2.1 Risikostyringsverktøy

Resultater fra dokumentanalyse

Lysneutvalget skriver i NOU (2015:13) at finanssektoren representerer en sektor med høy bevissthet rundt de truslene og sårbarhetene knyttet til økt digitalisering sammenlignet med andre sektorer. Dette viser til at sektoren i dag er godt rustet til å kunne håndtere digitale sårbarheter og risikoer (Meld. St.12 (2021-2022)). Operasjonell risikostyring er av stor betydning for finanssektoren for å vurdere risikonivået. Selv om Finanstilsynets stiller krav til regelmessige risikoanalyser, er det ikke nødvendigvis en garanti for kvaliteten. Det er derfor viktig at virksomhetene gjennomfører kvalitativt gode risikoanalyser, gitt kompleksiteten i arkitektur og verdikjeder (NOU 2015:13). Meld. St. 38 (2016-2017) påpeker at samfunnet vårt aldri vil være helt beskyttet mot utfall av eller angrep mot digital infrastruktur eller systemer. «*(...) men vi må evne å iverksette de riktige sikkerhetstiltakene for å redusere risikoen og for å kunne gjenopprette normal funksjon så fort som mulig*» (Meld. St. 38 (2016-2017), s. 11).

Finanstilsynet (2022b) lister opp flere punkter i sin risiko- og sårbarhetsanalyse som foretakene må gjøre for å kunne håndtere risikoen knyttet til utkontraktering. Flere av disse punktene er forankret i lovverket. Det er foretaket selv som bestemmer hvilke risikoreduserende tiltak som skal implementeres etter gjennomført risikoanalyse (Finanstilsynet, 2021b). Med andre ord må de vurdere hvordan de skal styre og kontrollere utkontraktert virksomhet (Finanstilsynet, 2022b). Omfanget av risikovurderinger og risikoreduserende tiltak vil blant annet avhenge av

kompleksiteten i foretakets virksomhet. Det er også avgjørende med IKT-sikkerhetskompetanse ved avtaleinngåelse og oppfølgning. Dersom dette er mangelfullt, må foretaket sørge for å skaffe seg denne kompetansen.

Det er viktig å sikre at leverandøren har tilstrekkelig kapasitet, kompetanse og erfaring til å utføre oppgavene på en forsvarlig måte (Finanstilsynet, 2022b; Forskrift om risikostyring og internkontroll, 2008). Leverandøren må ha etablert tilfredsstillende system for risikostyring og internkontroll, i tillegg til at de må sikre foretakets krav til kontinuitet og beredskap når det gjelder håndtering av avvik i tjenesteleveransen. De må også vurdere ulike risikofaktorer knyttet til oppdragstakeren, som eksempelvis lokalisering, lovgivning, politisk stabilitet, infrastruktur og kulturelle forskjeller (Finanstilsynet, 2022b). I den sammenhengen er det viktig med interne kompetanse innen innkjøp og oppfølgning, noe de kan virke som at foretakene har styrket (Finanstilsynet, 2022b). God innkjøpskompetanse resulterer i bedre leveranser og tjenester fra IKT-leverandører. Anskaffelser kan dermed være et fornuftig IKT-sikkerhetstiltak.

Finanstilsynets ROS omhandler også det de omtaler som *oppfølging av tjenesteleveranser,* og er et viktig aspekt for å sikre helhetlig styring og kontroll over IKT-virksomheten (Finanstilsynet, 2022b). Det anbefales at finansforetakene etablerer en styringsmodell med møteplasser og fora som gjør det mulig å følge opp leverandører på et strategisk (ledelse og styre), taktisk (oppfølging av leverandør) og operasjonelt nivå (daglig oppfølging av leveranser) (Finanstilsynet, 2022b). Styringsmodellen bør inkludere en representant fra oppdragsgiver i alle fora, der samhandling og oppfølging blir bestemt (Finanstilsynet, 2022b). Videre er det viktig at virksomhetens ledelse har bred oversikt over risiko, utfordringer og handlingsalternativer knyttet til utkontrakterte tjeneste (Finanstilsynet, 2022b).

I henhold til Forskriften om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften) må foretak oppfylle en rekke krav til informasjonssikkerhet, også for de deler av IKT-virksomheten som er utkontraktert (IKT-forskriften, 2003, §1). Videre presiserer Forskrift om risikostyring og internkontroll at kontrakten skal sikre at foretaket har ansvar for risikostyring og internkontroll, for de utkontrakterte delene av virksomheten (Forskrift om risikostyring og internkontroll, 2008, §5). For å kunne håndtere risikoene på en forsvarlig måte kreves det systematiske gjennomganger i bank- og finansforetak. Hensikten med IKT-forskriften er å sikre at banksektoren fastsetter overordnede mål, strategier og sikkerhetskrav

for IKT-virksomheten (IKT-forskriften, 2003). Forskriften fungerer som et verktøy for helhetlig sikkerhetsstyring i sektoren. Det er foretaket som skal sikre at organisasjonen besitter tilstrekkelig kompetanse til å forvalte utkontraktering av avtalen. Den inneholder blant annet krav om planlegging og organisering, risikoanalyse, utvikling og anskaffelse, systemvedlikehold, drift, avviks- og endringshåndtering, driftsavbrudd, kriseberedskap, utkontraktering og dokumentasjon (IKT-forskriften, 2003).

I forbindelse med implementering av «Lov om nasjonal sikkerhet» (Sikkerhetsloven) pågår det i Norge en kartlegging av de grunnleggende nasjonale funksjonene (GNF) innenfor det finansielle systemet (Sikkerhetsloven, 2019). Loven krever at alle virksomheter som omfattes av den, må ha et styringssystem for sikkerhet. Ifølge sikkerhetsloven er grunnleggende nasjonale funksjoner «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser» (2019 §1-5 nr.2). Den pågående kartleggingen av de grunnleggende nasjonale funksjonene er en viktig forutsetning for å håndtere systemrisikoen knyttet til cybersikkerhet i Norge. Det er departementet, innenfor sitt ansvarsområde, som er ansvarlig for å fatte om virksomheter er helt eller delvis underlagt Sikkerhetsloven.

Resultater fra intervjuer

For å kunne svare på hvordan risikostyringsinstrumenter utvikles i forbindelse med utkontrakteringsprosessen i bank- og finans, var vi interessert i å undersøke hvordan risikoene håndteres og hvilke verktøy som benyttes i den sammenheng. Informantene svarte at de nyttigste verktøyene var de bankene selv utarbeidet, i tillegg til andre risikostyringsverktøy. Blant de nevnte verktøyene var kunnskap, POPs-prosessen, kontrakter, samarbeid, leverandøroppfølging, uavhengige rapporter og revisjoner. Samtlige av informantene viste til kunnskap og kontrakten som særlig viktige risikostyringsverktøy.

Kompetanse

En av de mest sentrale faktorene, som ble nevnt av samtlige informanter, var tilgangen på kompetanse. Informant 4 fremhevet at banken er avhengighet av å ha kompetanse strategisk fordelt over flere avdelinger. Det involverer flere personer i vurderingsprosessen før en eventuell beslutning om utkontraktering av en tjeneste tas. I tillegg er det mange involverte i selve utkontrakteringsprosessen. Dette sikrer at banken får inn ulike fagkompetanser og ulike syn på risikoene. «Uten kompetanse vil man ikke være i stand til å ta gode vurderinger, noe

som ville føre til økt sårbarhet. Dersom hele utkontrakteringsprosessen var overlatt til innkjøpsavdelingen, ville det vært utfordrende da de ikke har ansatte med sikkerhetsbakgrunn» (informant 4). Informanten mener at utkontrakteringsprosessen i banken fungerer som en risikoreduserende faktor i seg selv, siden inkluderingen av flere personer og avdelinger gir ulike synspunkter på vurderingene. Effektiv virksomhetsstyring og god innkjøpskompetanse ved avtaleinngåelse ble av informant 5 pekt på som kanskje det mest risikoreduserende tiltaket. Gjennom forretningsmessig konsekvensanalyse kan virksomheten identifisere hva som er viktig og hva som ikke er det. «(…) altså hva som er gull og hva som er gråstein?» (informant 5)». Skal man ta vare på gullet påpekte informanten at man må ha en infrastruktur som legger til rette for og tar vare på det.

POPs-prosessen

Informantene forklarte at de har utviklet en produkt- og prosesscoring som kalles POPs, der et tverrfaglig team fra ulike områder som juridisk, innkjøp, compliance og sikkerhet, vurderer og godkjenner nye tjenester eller produkter. «I utgangspunktet skal alle utkontrakteringer gjennom den løypen der, og på den måten fanger vi opp og vil geleide det videre til utkontrakteringsprotokollen. Da vil vi få anledning til å undersøke, spørre og veilede innmelder» (informant 1). Etter at nye tjenester eller produkt er blitt godkjent gjennom POPs-prosessen, inngår banken deretter kontrakt med leverandøren. Banken benytter også en utkontrakteringsprotokoll som er utviklet i banken, hvor alle utkontrakteringsoppgaver skal vurderes. Det er der definert hvilke avtaler som skal brukes og hva de skal inneholde. Denne protokollen er basert på veilederen fra Finanstilsynet og tar hensyn til ulike risikofaktorer som exit-strategi, oppsigelse og muligheten for revisjon fra Finanstilsynet.

Ifølge informant 4 er god risikostyring av utkontrakterte IKT-tjenester kjennetegnet av en prosess som er spredt utover, på samme måte som i banken. Informanten understrekte viktigheten av at de som eier risikoen for en tjeneste også er systemeiere og ansvarlige. Dette skyldes at de som arbeider med systemet og de som har ansvar for det, også er ansvarlig for risikoen da de har en bedre kobling til den. Informant 4 mente at bankens prosess er god, da den dekker hele spekteret fra start til slutt. «Vi har sikkerhetskrav i kontraktene og i prosessen som leverandøren må gjennom før de skal bli godkjent. I tillegg til at vi følger opp i etterkant, for å sikre at alt er som det skal» (informant 4). Hvis det oppdages at noe er glemt eller noe nytt kommer frem i etterkant og ikke er i orden, tar den ansatte kontakt med leverandøren og gir beskjed om hva som må rettes. Dersom leverandøren ikke fikser det den får beskjed om, er

det fare for at banken ikke kan beholde denne leverandøren. «For det er jo vi som til syvende og sist eier risikoen for det er hos oss det kan gå galt» (informant 4). Informant 3 viste også til hvordan man gjennom vurderingen i POPs-prosessen kan få et inntrykk av risikobildet. «I POPs-prosessen er det mange fagpersoner involvert og det viser egentlig hvordan risikobildet er, bare ved å se hvem som sitter i de møtene og skal være med på godkjenningsprosessen» (informant 3).

Kontrakt og samarbeid

Kontrakten mellom banken og leverandøren er retningsgivende for samarbeidet og utkontrakteringsprosessen. Informant 3 vektla viktigheten av å ha gode avtaler med leverandørene, slik at de kan følge opp og ta stikkprøver i henhold til avtalene. Informant 1 nevnte ulike faktorer som er viktig å vurdere før banken inngår en avtale med en leverandør. Blant annet er det essensielt at banken har klare retningslinjer for oppsigelse av avtalen og har gjennomført vurderinger av mulige scenarioer dersom det skulle bli aktuelt. Dersom leverandøren ikke klarer å levere, eller avtalen må sies opp, må banken vurdere exit-strategi og vurdere alternativer. Dette kan inkludere å ta tilbake tjenesten internt eller vurdere andre velfungerende konkurrenter som kan levere den nødvendige tjenesten. Videre påpekte informant 3 at banken gjør spesifikke vurderinger knyttet direkte til leverandøren, og at de har utarbeidet veiledere som leverandørene følger. «Vi har vurderinger av leverandører knyttet til internkontroll, rutiner og prosesser. Vi har også en god veileder som følges hvor det står hvilke risikoer de må vurdere til enhver tid» (informant 1). Informant 6 understreket at med en god kontrakt, spesifikasjoner og god styring kan de fleste risikoer håndteres.

Informantene poengterte at kunden og leverandøren bør være gode samarbeidspartnere. «En leverandør krever at kunden må være «hands on» i betydning av at de må være aktivt med på å lede. Man kan ikke delegere ansvaret i tre år og deretter komme tilbake og spørre hvordan det har gått» (informant 6). Informanten påpekte videre at det er en svært fin balanse, når det gjelder å følge opp leverandørene tilstrekkelig, uten å «jage» dem slik at det oppstår et spenningsforhold. Samarbeidet forutsetter tillitt, uavhengig av hvor god kontrakten er. Det er ikke mulig å lage en fullstendig kontrakt, så den vil derfor alltid inneha noen hull i form av misforståelser eller andre overraskelser som kan dukke opp. «Det må derfor være et tillitsforhold slik at man kan være fleksibel og tilpasningsdyktig» (informant 6). Slike kontrakter er ofte langvarige, og medfører at det vil bli større hull med tiden og kontrakten må derfor kunne tilpasses.

Samtidig som det er sentralt at banken og leverandøren har et godt samarbeid, er det viktig at avdelingene i banken arbeider bra sammen. Informantene forklarer at en del av regimet knyttet til utkontraktering nylig har gjennomgått endringer. «Vi har ikke snakket godt nok sammen og er blitt sittende som siloer» (informant 1).

Leverandøroppfølging

Sikkerhetsavdelingen har ansvar for oppfølgingsarbeid rettet mot leverandørene i driftsperioden. Informant 3 beskrev risikoen til utkontrakteringsprosessen av IKT-tjenester som stor, og at de derfor har fokus på oppfølgingsarbeid rettet mot leverandørene. «I oppstarten har vi mange spørsmål som er mer krevende for leverandørene å fylle ut. De neste to årene er det forenklet oppfølging, der vi sjekker om det er noen endringer som tilsier at risikoen har gått opp eller ned» (informant 3). Informanten påpekte at måten de driver leverandøroppfølging på er påvirket av hvor godt de kjenner til leverandørene. «Til mindre kjente leverandørene er, til mer aktuelt blir leverandøroppfølging, for vi må kjenne dem og deres rutiner» (informasjon 3). Videre nevnte informanten at de har et stort antall leverandører, og de ikke klarer å følge opp alle like godt. Derfor må de vurdere konsekvensmaterialet av data i tillegg til kritikaliteten til leverandørens arbeid. «Vi vurderer konsekvenspotensialet, altså type data, mengde data, sensitivitet på data som avgjør hvilke leverandører vi prioriterer å følge opp. Det er vurdert ut ifra kritikaliteten på det vi gjør og med tanke på konfidensialitet og tilgjengelighet» (informant 3).

Leverandøroppfølgning forklares som arbeid med å påse at leverandørene opprettholder det arbeidet de har blitt enige om i den innledende fasen, i tillegg til å sikre at leverandøren har samme risikoappetitt som banken. Det er informant 4 som arbeider i siste del av utkontrakteringsprosessen som går på oppfølgning av leverandørene, og spesifiserer at den risikovurderingen som blir gjort er en omfattende prosess. «De leverandørene jeg følger opp har allerede vært gjennom en ganske tung vurdering, der den risikoen som eventuelt har vært, har blitt akseptert, eller så har det blitt gjort tiltak» (informant 4). Informant 2 viste til viktigheten av at banken driver med leverandøroppfølging ved å vise til hva som hadde skjedd dersom en av deres leverandører som mottar store datasett fra banken, hadde startet med ny teknologi. «Dersom en leverandør hadde startet med AI (artificial intelligence) og benyttet vår data, kan den komme på avveie. Vi må derfor vite om alle endringer som leverandørene våre

gjør. God leverandøroppfølging og god kontakt med leverandører er derfor viktig».

Andre risikoreduserende verktøy

Banken benytter ulike hjelpemidler for å håndtere risikoen, i tillegg til de risikostyringsverktøyene banken har utviklet selv. Dette inkluderer å benytte uavhengige rapporter og revisjoner av leverandører utført av revisjonsfirmaer, som ifølge informant 3 bidrar til å få innsikt i leverandørenes status. Videre nevnes det at Finanstilsynets rundskriv og deres tilsyn er til stor hjelp når det gjelder utkontraktering av IKT- tjenester. «I forhold til IKT er prosessen strukturert med et rammeverk og et betydelig fokus på hvilke risikoer som skal belyses. Vi har god hjelp av Finanstilsynet som er vaktbikkje der» (informant 1). Avdelingen for operasjonell risiko arbeider ikke direkte med å redusere risiko, men bistår banken med å finne gode måter for å håndtere, redusere eller akseptere risikoen, ifølge informant 2. «Det er bedre at førstelinje har den forvaltningen av risikoen. Det er de som tar seg av å redusere den. Vi kan sette retningslinjer og informere om hvordan det skal gjøres, men kan ikke følge dem opp» (informant 2). Informanten påpekte at det også kan være risiko banken er villig til å ta fordi fortjenesten er god.

5.2.2 Utfordringer med å styre risiko som følge av utkontrakterte IKT-tjenester

Resultater fra dokumentanalyse

I NOU (2015:13) blir det påpekt at bank- og finanssektoren velger å utkontraktere på grunn av behovet for nøkkelkunnskap fra utlandet. For å sikre effektiv leverandøroppfølgning stilles det krav til at organisasjoner som utkontrakterer må ha tilstrekkelig kompetanse og kapasitet til å ivareta ansvaret. Det er også en oppfatning av usikkerhet i NOU (2015:13) om hvorvidt virksomhetene utkontrakterer for mange oppgaver eller om de har utilstrekkelige ressurser for å kontrollere og følge opp avtalene og leverandørene. Tilgangen på IKT-sikkerhetskompetanse fremstår som en av de største utfordringene på IKT-sikkerhetsområdet, noe som blir påpekt i Meld. St. 10 (2016-2017) Meld. St. 38 (2016-2017), og NOU (2015:13). Disse rapportene legger også det politiske grunnlaget for tiltak som tar sikte på økt kompetanse innen digital sikkerhet og en langsiktig kompetansestrategi, som har resultert i "Nasjonal strategi for digital sikkerhetskompetanse" (Justis- og beredskapsdepartementet, 2019). Ifølge NIFU (2017) vil det innen 2030 være et underskudd på 4100 personer med ønsket kompetanse i det norske samfunnet. I samtaler med Finanstilsynet har foretak og leverandører av IKT-tjenester fremhevet flere viktige forhold knyttet til IKT-virksomheten og gjennomførte tiltak for å

redusere risiko (Finanstilsynet, 2022b). Ressursmangel og utfordringer knyttet til rekrutteringen av IKT-sikkerhetskompetanse fremstår som hovedutfordringen, da der ser ut til å være færre tilgjengelige ressurser enn det markedet har behov for. Ifølge meldingen fra Finanstilsynet peker foretakene på at ressurspersoner foretrekker å knytte seg til foretak som har et etablert sikkerhetsmiljø av en viss størrelse.

Resultater fra intervjuer

Da vi spurte informantene om utfordringer knyttet til håndtering og styring av risiko i utkontrakteringsprosessen, kom noen av temaene som ble nevnt som verktøy for risikostyring også frem her. Informantene kom med ulike refleksjoner om hva de oppfattet som mest utfordrende, men nevnte blant annet mangel på kunnskap, mange involverte og at det er preget av byråkrati. Det ble også påpekt at selve kontrakten kan være en utfordring. I tillegg til at det å være en del av en større allianse kan by på utfordringer på samtidig som det innehar på fordeler.

Mange involverte

En av hovedutfordringene, ifølge informant 4, var den noe uoversiktlige situasjonen som oppstår når det er mange involverte parter som ikke nødvendigvis er like samkjørte. Informanten viste til at de ikke har et system som sier hvordan leverandøren har bli fulgt opp, hvilke vurderinger som har blitt tatt, og at det heller ikke logges i samme system. Dette fører til at banken mangler oversikt fra år til år. Mangelen på oversikt går på sikkerhetsspørsmål, men også andre risikoer som for eksempel bærekraft og økonomi. Informant 4 forklarte at hvis en leverandør plutselig får dårlig økonomi, har de ikke har et system som automatisk varsler om dette. I et tilfelle der økonomien skranter er det fort at sikkerhet blir nedprioritert. Når banken ikke har en totaloversikt over leverandør og den tjenesten de leverer, blir det vanskelig å se det store bilde og hvordan det ene kan påvirke det andre.

Mangel på kompetanse

Ifølge informantene er kompetanse en av de viktigste faktorene for å håndtere risikoen i utkontrakteringsprosessen. Informant 5 trakk frem at det er en stor mangel på drift og sikkerhet, og generelt hele området. Det er viktig å ha kompetanse å forstå behovene, foreta gode innkjøp og å ha innsikt i det som kjøpes inn. Informant 5 mente at bankene ikke har tatt innover seg viktigheten av å ha kompetanse og innsikt for å kunne være dyktige innkjøpere, foreta gode risikovurderinger og kunne følge opp leverandørene. Videre påpekte informanten at det er store

forskjeller mellom store og mindre banker, da de mindre bankene ikke har trappet opp tilstrekkelig for å få god kontroll. Kompetanse er også nødvendig for å kunne ivareta de verdiene man har, noe som ikke alltid er enkelt. Informant 6 mente at dersom man utkontrakterer uten å ha tilstrekkelig med kompetanse og styring, vil sårbarheten øke. Imidlertid kan et valg om å ikke utkontraktere utgjøre en sårbarhet i større grad. Videre påpekte informant 6 viktigheten av å ha nok kompetanse om det produktet man kjøper, og at en god kjøper bidrar til å utvikle leverandøren. «Det er derfor en fordel å ha kompetanse, men ikke overta jobben for dem» (informant 6). Valg av riktig leverandør kan bidra til å bygge opp kompetansen over tid, noe som vil være verdifullt. Forholdet mellom kunde og leverandør kan bidra til gjensidig utvikling gjennom god dialog, men dette krever ressurser fra kundens side til å følge opp tjenesten.

Kontrakt og styring

Hovedutfordringen med utkontraktering av IKT-tjenester var ifølge informant 6 at man mangler kompetansen i «eget hus» til å lede utkontrakteringsprosessen. Mangel på styringsevne vil føre til økt sårbarhet og bidra til å svekke robustheten. Informanten skiller mellom de kontraktsmessige og styringsmessige aspektene og det tekniske, og påpeker at dette er to forskjellige områder. De største kontraktsmessige utfordringene refereres til som et kontinuerlig spenningsforhold, der uenighet oppstår rundt hva leverandøren skal levere og om kunden har fått det de har betalt for. Samarbeidet blir krevende straks tilliten forvitrer, noe som skjer fort dersom man blir utnyttet. I slike tilfeller blir kompetanse, holdninger og fleksibilitet viktige for å tilpasse seg. Ifølge informant 6 er en mindre krevende utfordring å finne riktig leverandør, da tiden man bruker på dette er mye mindre man vil ha leverandøren. «Det er mye viktigere hvordan man klarer å arbeide sammen. Det kan hende at man har valgt feil, og da kan det ende i et legitimt brudd som koster tid og krefter» (informant 6).

Informant 6 viste til at noe av det mest risikoreduserende virksomheten kan gjøre, selv om det er vanskelig, er å utarbeide gode kontrakter og ha god styring. «Å arbeide med å lage spesifikasjoner og kontrakter er veldig vanskelig. Ofte er ikke kunden en god nok kjøper» (informant 6). Med det ønsket informanten å vektlegge viktigheten av at banken er flink til å lage spesifikasjoner i kontrakten, som styrer hva og hvordan leverandøren skal levere tjenestene. Leverandørene er ofte spesialisert og har mer kompetanse enn banken, og det er derfor viktig å samarbeide om utkontrakteringen for å oppnå en vellykket løsning for begge parter. Det å finne den rette tilpasningen er avgjørende. «Faren er at man spesifiserer ting for

detaljert og da får man kun det man har bedt om. Den andre faren er at det blir for løst og at leverandøren da kan gjøre hva som helst» (informant 6). En for stram kontrakt kan begrense leverandørens evne til å bidra med deres ekspertise. Dette er en utfordring da man som kunde ønsker å styre prosessen, men samtidig må være villig til å gi plass til andre med mer kompetanse, samtidig som de selv skal ha tilstrekkelig kompetanse til å styre utkontrakteringsprosessen.

En annen utfordring informant 1 viste til, var at arbeidet kunne oppleves som byråkratisk. De som eier og arbeider i systemene vil ifølge informanten helst bare gjøre det og ønsker ikke forholde seg til for mange krav. Når de banken må følge opp leverandører, avtalen og tjenesten, er dette noe som for mange kan oppleves som byråkratisk. «Det er noe med det pedagogiske her, altså at man ser at det ikke alltid er like enkelt å forstå viktigheten av arbeidet med oppfølgning» (informant 1).

Utfordringer knyttet til alliansen

Ifølge informant 2 er de største utfordringene for banken knyttet til at alliansen er organisert gjennom felleseide selskaper. Det er en felles tjeneste for bankene i samarbeidet som skal gi stordrifts- og kompetansefordeler. Banksamarbeidet eier en stor utvikler som her vil gå under navnet «utvikling». «Utvikling» eier mange av produktene og tjenestene som de bruker på toppen av tjenestebanksystemet. Alliansen bruker samme leverandør for innkjøp av tjenester som banken. «Dersom vi mener vi kan få storhusfordeler ved å kjøpe inn som en allianse eller bare noen få banker, er det ofte slik at «utvikling» benyttes som en innkjøpsallianse. Men leveransen går ikke gjennom «utvikling», men direkte til bankene» (informant 2). Informanten forklarte dette som en utfordring som de arbeider med å få på plass. Problemet kommer av at ingen i «utvikling» føler seg ansvarlig for kontrakten. Oppfølgningen av leverandøren har ikke «utvikling» forutsetningene for å kunne gjøre, dette fordi leveransen ikke går gjennom den kanalen. De vet ikke hva som skjer eller hva som går gjennom den kanalen. Samtidig mener leverandøren at det var «utvikling» som gjennomførte avtalen. «Dersom vi (banken) hadde prøvd å kontakte leverandøren direkte hadde vi fått beskjed om at de ikke har avtale med oss, men har avtale med «utvikling». Den suppen der er en utfordring for oss som vi må ta tak i» (informant 2).

Andre utfordringer

Informant 1 mente på generell basis at rammeverket banken har for hvordan leverandørene skal følges opp ikke er godt nok. «Sikkerhetsavdelingen har sitt eget regime for leverandøroppfølging, men det gjelder kun et fåtall leverandører, da det gjelder de mest kritiske. Fra vår side i innkjøp har vi ikke klare retningslinjer for hvordan leverandører skal følges opp» (informant 1). Videre viste informant 3 til at bevisstheten om utkontraktering av tjenester har gjort at banken bruker mer ressurser på oppfølgning. Dette utgjør ifølge informanten en utfordring, da det kan være vanskelig å sette av nok ressurser og tid til å følge opp leverandørene. «Det er tidkrevende arbeid, og det er klart at vi da prøver å dra nytte av at vi har «utvikling» hvor mange banker spiller på lag, slik at vi slipper å bruke så mye ressurser i hver bank» (informant 3).

5.2.3 Diskusjon av forskningsspørsmål 2

Risikostyring

Utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren krever kontinuerlig vurdering og håndtering av risikoer. Den innsamlede empirien viser til at sektoren utvikler og implementerer ulike risikostyringsinstrumenter. På mange måter omhandler risikostyring de metodene, prosessene og strategiene som kan kartlegge og styre risikoens forhold (Aven et al., 2008). Samtlige informanter vi intervjuet var enige om at man tar en viss risiko når man utkontrakterer IKT-tjenester som følge av komplekse og uoversiktlige leverandørkjeder. Informant 4 nevnte at man enten kan velge å akseptere den risikoen, eller gjøre noe aktivt med den. Det er derfor viktig å håndtere den risikoen som virksomheten velger å eksponere seg for, og dette oppnås gjennom risikostyring. Informant 6 understrekte at god styring er en vesentlig faktor for et vellykket samarbeidet mellom banken og leverandøren. Som det kommer frem av intervjuene og i NOU (2015:13), er risikostyring avgjørende for å forstå risikonivået. Banken er i forkant av utkontrakteringsprosessen avhengig av å få innsikt i risikoene, aktuelle tiltak og i hvilken grad risikoen kan styres. Utkontrakteringsprosessen kan dermed ses på som en risikostyringsprosess. Dette skyldes at risikostyring ikke bare er relevant før beslutningen om å utkontraktere en IKT-tjeneste tas, men at risikostyringsprosessen er en sentral del av hele utkontrakteringsprosessen.

Kompetansen som kreves for å styre risikoen

NOU (2015:13) og informantene understreker at mangel på spesialkompetanse er en sentral årsak til at bank- og finanssektoren utkontrakterer IKT-tjenester. Informanten fra Finanstilsynet utrykte bekymring for at bankene ikke har tatt innover seg hvor mye kunnskap, kompetanse og innsikt som kreves for å kunne være kompetente kjøpere. Dette har også blitt påpekt av Finanstilsynet (2022b). Til tross for at virksomhetene utkontrakterer IKT-tjenester, er det avgjørende at de besitter betydelig kunnskap internt, slik at de kan håndtere prosessen på en effektiv måte. Dokumentanalysen indikerer også et behov for å stille krav til kompetanse og kapasitet hos virksomheten som utkontrakterer, for å at de kan ivareta ansvaret rundt leverandøroppfølging. Intervjuene viser at de ble lagt stor vekt på kompetansen som kreves knyttet til utkontraktering. Dette da nok kompetanse er en sentral faktor for å kunne drive god risikostyring, fra vurderingen av om tjenesten skal utkontrakteres og frem til oppfølging av leverandører. Til tross for at kompetanse er en av de viktigste faktorene for å kunne styre risiko, viser empirien også at mangel på kompetanse er en av de største utfordringene. Informant 6 påpekte at manglende kompetanse i utkontrakteringsprosessen kan øke sårbarheten.

Selv om mangel på kompetanse er en utfordring, er det ikke en uunngåelig risiko, da kompetanse kan bygges gjennom opplæring og erfaring. Fokuset på læring er et sentralt element i HRO-teorien, som vektlegger organisasjoners evne til å håndtere risikoer og unngå store ulykker (La Porte, 1996). Å ha kompetanse om produktet eller tjenesten som skal utkontrakteres, er avgjørende for evnen til å håndtere prosessen på en god måte. Flere av informantene viste til at kompetansen er spredt utover ulike avdelinger i banken. De ansatte i disse avdelingene har spesialkompetansen og har myndighet til å gi innspill og ta avgjørelser innenfor sine fagområder. En slik arbeidsorganisering kan knyttes opp til HRO-teorien, som argumenterer for at spesialisering og bruk av eksperter gjør det mulig å ha desentralisert styring, om det skulle bli nødvendig (Weick & Sutcliffe, 2007). I utgangspunktet kan utkontraktering betraktes som en sentralstyrt prosess, der lovverket legger føringer for gjennomføringen av store deler av prosessen. I denne sammenhengen vil avdelingene som besitter spesialkompetanse knyttet til de ulike delene av prosessen, få siste ordet i ulike avgjørelser. Dette bidrar også til å redusere risikoen, da det ikke er opp til én enkelt avdeling å ta alle avgjørelsene. Utover den interne kompetansen, benytter banken seg også av ekstern kompetanse. Banken bruker uavhengige rapporter og revisjoner gjort av konsulentfirmaer som bidrar til å få oversikt over leverandørene. Videre fremhevet de også at rundskrivet fra Finanstilsynet er til hjelp i risikostyringen. Selv om mangel på kunnskap er en risiko som kan

håndteres, finnes det også situasjoner der det er ikke er mulig å få tilstrekkelig kunnskap om risikoen (Renn, 2008).

POPs-prosessen

Samtlige av informantene i banken refererte til POPs-prosessen, banken har utviklet, som et risikostyringsverktøy de aktivt benytter seg av gjennom utkontraktering. Dette er en prosess som alle leverandører må gjennom før avtaleinngåelse. Gjennom POPs-prosessen kartlegges potensielle risikoer, sårbarheter og usikkerheter, slik at banken har mulighet til å sette inn tiltak om de skulle være nødvendig. Prosessen fungerer som en barriere, da den må fullføres grundig før banken tar beslutningen om utkontraktering. Dette risikostyringsverktøyet bidrar til å gi banken oversikt over mulige risikoer og hvilke tiltak som eventuelt må implementeres.

Prosessen som banken har utviklet har mange likheter med en ROS- analyse, som sektoren er pålagt å gjennomføre regelmessig som en del av risikostyringen. En slik analyse er relevant å benytte seg av når banken skal kartlegge hvilke risikoer som kan oppstå i utkontrakteringsprosessen, og hvordan de skal håndteres. Formålet med en ROS-analyse er å identifisere og kategorisere potensielle farer og trusler, og vurdere deres sannsynlighet og konsekvens, samt iverksette tiltak for å redusere risiko og øke virksomhetens robusthet (Engen et al., 2021). Både POPs-prosessen og ROS-analyser kan knyttes til resiliens, da begge verktøyene har som mål å kartlegge risikoer og implementere tiltak for å opprettholde funksjoner og målsettinger (Hollnagel, 2014). Meld. St. 38 (2016-2017) viste til at samfunnet aldri vil være helt beskyttet mot sikkerhetstrusler, og at det derfor er viktig å sette inn riktige sikkerhetstiltak for å redusere risikoen og gjenopprette normale funksjoner etter en hendelse. Dette viser til at samfunnet er avhengig av at virksomheter er resiliente. Martin (2019) beskriver at aktiv resiliens handler om å tilpasse seg endringer og lære av hendelser, slik at man på den måten blir i stand til å håndtere hendelser. I likhet med aktiv resiliens, beskriver informant 1 POPs-prosessen som endrer seg ut ifra hvilken leverandør det handler om, i tillegg at den endrer seg i takt med risikobildet. Dette viser at prosessen er skapt for å kontrollere risiko, noe som vil kunne bidra til at bedriften blir resilient. Målet med resiliens er at virksomheten skal være motstandsdyktig og håndtere risiko på en effektiv måte, og på denne måte være i stand til å opprettholde sine funksjoner selv under ugunstige forhold (Hollnagel, 2014).

Kontrakt og samarbeid

Godt samarbeid mellom innkjøper og leverandør ble fremhevet som avgjørende for en vellykket prosess. Informant 6 viste til at noe av det viktigste virksomhetene kan gjøre for å få til et godt samarbeid og god risikostyring er å utarbeide gode kontrakter, selv om det er vanskelig. Kontrakten skal sikre at banken har ansvar for risikostyring og internkontroll knyttet til de utkontrakterte delene av virksomheten, og fungerer dermed samtidig som et risikostyringsverktøy (Risikostyring og internkontrollforskriften, 2008, §5). Risikostyring handler om å få innsikt i risiko, kartlegge hvordan risikoen kan styres og hvilke tiltak som kan settes inn (Aven et al., 2008).

Leverandører kan være mer villige til å ta mer risiko enn bankene, og kontrakten blir derfor helt sentral. Det er derfor viktig at kontrakten inneholder tydelige spesifikasjoner, som informant 6 viser til. Den skal ta for seg forventninger til levering, identifisering av risiko, risikoappetitt, krav til sikkerhet, ansvar, leverandøroppfølging og lignende, som alle er sentrale faktorer for risikostyringen. Informanten understekte også viktigheten av å finne en god balanse mellom en for detaljert og en for løs kontrakt. Det er en svært fin balanse mellom å følge opp leverandørene nok og å «jage» dem slik det oppstår et spenningsforhold. I løpet av prosessen vil det dukke opp uklarheter og utfordringer, noe som gjør det vanskelig å utforme en kontrakt uten hull. Derfor la informant 6 vekt på viktigheten av et tillitsforhold mellom kjøper og leverandør, noe som vil gjøre det lettere å være fleksibel og tilpasningsdyktig. Hvis det ikke foreligger tillitt, vil samarbeidet bli vanskelig. Kontrakter med leverandørene er ofte langvarige, derfor er det viktig å oppnå et vellykket samarbeid slik at utkontrakteringen blir gunstig for begge parter.

En annen faktor som kom frem av empirien angående samarbeid, er at det innad i sektoren ikke har vært konkurranse når det gjelder sikkerheten. Lysneutvalget (NOU 2015:13) skriver at finanssektoren representerer en sektor med høy bevissthet om de truslene og sårbarhetene som økt digitalisering medfører, og at sikkerhet aldri har vært en konkurrerende faktor. Dette var også noe informant 5 påpekte, og forklarte det med at sektoren er avhengig av tillitsforhold. Utover samarbeid i sektoren, er det i tillegg viktig med godt samarbeid mellom avdelingene i banken noe informant 3 viste til. De har gjennomført endringer knyttet til samarbeid, med bakgrunn i at kommunikasjonen var for dårlig og at de dermed ble sittende i «siloer». Dette er noe som kan knyttes om til bankens evne til å være resilient. Resiliens, som en egenskap ved komplekse systemer, legger vekt på at samarbeid og tillit er nødvendig for å kunne opprettholde

eller gjenopprette grunnleggende funksjoner etter en risikokilde eller en hendelse (Aven & Thekdi, 2021). Det kan fremstå som at de internt i banken og i sektoren generelt, fokuserer på åpenhet og tillit slik at de sammen kan styrke systemet, noe som tyde på en tilnærming i tråd med resiliens.

Utfordringer

Da vi spurte informantene om utfordringene med risikostyring knyttet til utkontraktering av IKT-tjenester, fikk vi ulike svar. Informant 4 nevnte blant annet at det er mange aktører involverte i prosessen og at alle ikke nødvendigvis er like samkjørte. Dette kan gjøre det vanskelig å få eller opprettholde oversikt, noe som er en sentral faktor i risikostyring. I tillegg nevnte informanten at de ikke har en totaloversikt over kontrakter og vurderinger som blir gjort fra år til år, noe som kan skape utfordringer.

Lange og uoversiktlige leverandørkjeder med mange involverte kan bidra til å øke systemrisikoen. Flere aktører fører også til økt sårbarhet for at hull i systemene vil kunne oppstå (Perrow 1999). Bank- og finanssektoren er spesielt avhengig av verdikjedene som følge av utkontrakterte IKT-tjenester, noe som kan knyttes til *tette koblinger* og viser til hvordan systemet er skrud sammen. Ifølge Perrow (1999) fører rask teknologisk utvikling og sammensatte systemer til tette koblinger og komplekse interaksjoner. Skulle det skje en hendelse et sted i leverandørkjeden, vil det kunne skape utfordringer andre steder i kjeden, noe som kan føre til systemfeil. Det argumenteres for at en slik organisering vil føre til unngåelige ulykker som et resultat av systemets design og vil kunne bidra til at svikt i et ledd vil kunne påvirke hele systemet (Perrow, 1999).

Leverandøroppfølging

Samtlige av informantene var enige i at utkontrakteringsprosessen fører med seg risiko, og at det derfor er viktig at banken har gode prosesser som gjør det mulig å kontrollere disse risikoene. Leverandøroppfølging, eller oppfølging av tjenesteleveranser som Finanstilsynet (2022 C) omtaler det som, er ifølge flere av informantene en svært viktig del av det å styre risikoene. Formålet med oppfølgningen er å bidra til å ivareta helhetlig styring og kontroll over IKT-virksomheten (Finanstilsynet, 2022 C). Kritikalitetsvurdering var et begrep som ble nevnt av alle informantene når det gjaldt leverandøroppfølgning i banken. Det understrekes at banken ikke har mulighet til å følge opp alle leverandørene og at de derfor må gjøre prioriteringer basert på kritikaliteten. Når man skal vurdere kritikaliteten er det viktig å ha kontroll på

virksomhetens verdier. Trefaktormodellen består av en verdi-, en trussel- og en sårbarhetsvurdering som kan brukes for å kartlegge risikonivået og benyttes vanligvis til security-trusler (Engen et al., 2021). Ved å benytte seg av en slik analyse får virksomheten oversikt over verdiene som må beskyttes, truslene som kan true verdiene og verdienes sårbarhet i forhold til truslene (Busmundrud et al., 2015). Man får dermed kartlagt verdier, sårbarheter og trusler, og får på denne måten funnet frem til tiltak som man kan iverksette.

Et samarbeid med en leverandør kan vare i flere år, og som informant 6 snakket om, er det mye som kan endre seg i løpet av denne perioden. Informant 4 har hovedansvaret for leverandøroppfølgingen i banken, og viser til at det er mye som kan endre seg i løpet av kontraktsperioden. Det er derfor er viktig at banken er i kontinuerlig kontakt med leverandørene, og da spesielt de kritiske. Hollnagel (2017) viser til at et system må ha evnen til å justere funksjonene sine i forkant, under og etter endringer og forstyrrelser for å kunne være resilient. Dette kan knyttes opp mot leverandøroppfølging, da poenget er å kunne følge opp leverandørene og være i stand til å gjøre justeringer i god tid, dersom det blir behov for det. Evnen til å i) respondere, ii) overvåke, iii) lære og iv) forvente er fire evner som Hollnagel (2011) identifiserer ved resiliente organisasjoner. Alle disse egenskapene kan knyttes opp til bankens praksis med leverandørfølgingen.

Når en bank utkontrakterer sentrale tjenester, slik som IKT, er deres evne til å respondere avgjørende. Banken er avhengig av å ha et system gjør at de er i stand til å håndtere, og respondere på eventuelle problemer og hendelser. Overvåking av leverandørenes ytelse er sentralt for å kunne opprettholde ønsket kvalitet og pålitelighet. Leverandøroppfølgingen bidrar dermed til at banken er i kontinuerlig kontakt med de mest kritiske leverandørene, og kan på denne måten identifiserer avvik eller risikofaktorer tidlig. De kan dermed håndteres før det får konsekvenser for bankens drift. Læring er også en vesentlig faktor her for å kunne identifisere forbedringsområder og optimalisere samarbeidet med leverandørene. Dette innebærer å evaluere tidligere erfaringer, analysere eventuelle feil eller problemer som har oppstått, og iverksette tiltak for å unngå at det gjentar seg i fremtiden. Læring kan også skje gjennom utveksling av beste praksis med andre organisasjoner som har gjennomført vellykkede leverandøroppfølgingsstrategier. Til slutt er evnen til å forvente mulige risikoer og eventuelle utfordringer viktig for bankens leverandøroppfølging. Dette innebærer å utføre risikovurderinger, holde seg oppdatert på risikobildet og iverksette nødvendige tiltak for å møte fremtidige behov.

Ved å ha realistiske forventninger og proaktiv håndtere risikoer, kan banken lettere forberede seg på endringer og sikre kontinuitet i leverandøroppgavene. Ved å fokusere på leverandøroppfølging gjennom evnene til å respondere, overvåke, lære og forvente vil banken ifølge Hollnagels (2011) teori være en resilient organisasjon. Gjennom arbeidet med leverandøroppfølging vil banken også kunne styrke sin evne til å opprettholde pålitelighet, håndtere uforutsette hendelser og opprettholde en effektiv leverandøroppfølgingsprosess som bidrar til en utkontrakteringsprosess hvor banken har kontroll over mulige risikoer.

5.2.4 Oppsummering av forskningsspørsmål 2

For å styre risikoene som utkontraktering av IKT-tjenester medfører, benytter bank- og finanssektoren flere risikostyringsverktøy. Noen av verktøyene er lovpålagte og andre er utarbeidet av banken selv. POPs-prosessen er et risikostyringsverktøy som informantene fra banken trakk frem, hvor ansatte fra flere ulike avdelinger, med ulik kompetanse, som på mange måter kan speile hvordan risikobildet ser ut. Kontrakten legger grunnlaget for samarbeidet mellom banken og leverandøren, og er en sentral måte å styre risiko på i denne sammenhengen. Kompetanse ble også identifisert som en betydelig faktor for risikostyring. Imidlertid, viste det seg også å være en sentral utfordring, da det oppleves å være stor kunnskapsmangel knyttet til sentrale temaer i sektoren. Mangel på kunnskap var ikke den eneste utfordringen knyttet til å styre risikoene. Leverandørkjedene er lange og utkontrakteringsprosessen innebærer mange aktører, noe som kompliserer prosessen og gjør den i større grad uoversiktlig. Dette skaper utfordringer med risikostyring, og hvilke risikoer banken skal fokusere på. Selv om banken har flere gode verktøy for å styre risiko, er det også store utfordringer og noen av disse er knyttet til elementer for å styre risikoen. Alt i alt, reflekterer dette bankens høye fokus på risiko gjennom hele utkontrakteringsprosessen, noe som kjennetegner HROer som har en kontinuerlig oppmerksomhet på risiko.

5.3 Empiriske funn og diskusjon av forskningsspørsmål 3

I dette delkapittelet vil studiens tredje forskningsspørsmål bevares: *På hvilken måte virker lovverk og krav risikoreduserende ved utkontraktering av IKT-tjenester i bank- og finanssektoren?* Det vil besvares ved å undersøke hvordan lovverket legger føringer for utkontrakteringsprosessen, hvordan det følges opp og hvorvidt lovverket fungerer risikoreduserende.

5.3.1 Føringene lovverket legger

Resultater fra dokumentanalyse

Norges Bank (2022c) påpeker på at regulering av det finansielle systemet i første rekke skjer gjennom lover og forskrifter. Målet med reguleringen er å sikre at det finansielle systemet er stabilt og effektivt. Ifølge Norges Bank (2022b) kan reguleringen bidra til at samfunnsmessige gevinster realiseres og risiko reduseres. I NOU (2018:14) har utvalget kartlagt omtrent 150 lover og forskrifter som potensielt angår IKT-sikkerhet på nasjonalt plan, hvor kun et mindretall av disse stiller eksplisitte IKT-sikkerhetskrav. Kartleggingen som har blitt gjort av utvalget viser stor variasjon når det gjelder hvilken grad de stilles krav til IKT-sikkerheten. IKT-forskriften har omfattende og eksplisitte bestemmelser om IKT-sikkerhet, mens andre lover og forskrifter har mer generelle krav om sikring, for eksempel krav om internkontroll som indirekte regulerer IKT-sikkerhet.

Finanstilsynet har tilsynsansvar for alle norske finansinstitusjoner, med formål om å sikre finansiell stabilitet og velfungerende markeder (Finanstilsynet, 2022a). NOU (2023:6) viser til at det i bank- og finanssektoren har vært en generell reduksjon i kostnader og en endring knyttet til risiko som følge av økt bruk av teknologi, og digitale løsninger. Rapporten viser til at tilsyn hos et finansforetak ikke har til hensyn å eliminere risikoen, men heller å påse at risikoen for alvorlige hendelser er innenfor akseptable grenser. I løpet av 2021 gjennomførte Finanstilsynet 21 tilsyn med fokus på IKT og betalingstjenester, hvor ni av disse var banker (Finanstilsynet, 2022b). Disse tilsynene avdekket blant annet at mange foretak mangler en forretningsmessig konsekvensanalyse som grunnlag for sine beredskapsplaner, og dokumentasjon av egen IKT-infrastruktur (Finanstilsynet, 2022b). Dette er viktige deler av sikkerhetsarbeidet og inkluderer krav til dokumentasjon av både internt driftede komponenter, og komponenter driftet av leverandører. Finanstilsynet oppdaget også at foretak manglet dokumenterte risikovurderinger av utkontraktering av IKT-oppgaver, eller anskaffelser av nye IKT-systemer. Bank- og finansforetak er pålagt å gjennomføre regelmessige risikoanalyser som følge av Finanstilsynets krav, som ble nevnt i «resultater fra dokumentanalyse» tilhørende forskningsspørsmål 2.

I en ny forskrift om meldeplikt ved utkontraktering (Forskrift om meldeplikt ved utkontraktering av virksomhet mv., 2021) har det blitt gjort endringer knyttet til hvilke foretakstyper som omfattes av meldeplikten. Retningslinjene fra de europeiske tilsynsmyndighetene EBA, EIOPA og ESMA legger opp til at foretakene selv skal identifisere

de kritiske delene av virksomheten (Finanstilsynet, 2021b). Meldeplikten gjelder for utkontraktering av virksomhet som er kritisk for foretaket, og foretaket kan vurdere dette ut fra kritikaliteten og risikovurderingen som gjøres i forbindelse med avtaleinngåelse. En viktig bestemmelse i forskriften er at alle foretak under tilsyn må ha oversikt over alle sine utkontrakteringsavtaler (Finanstilsynet, 2021b). Dette fordi Finanstilsynet skal kunne følge opp risikoen til utkontrakterte tjenester som ikke er underlagt meldeplikten til Finanstilsynet. Foretak under tilsyn bør forvente økt grad av kontroll ettersom Finanstilsynet vil kunne kreve innsyn i hvordan tjenestene utføres.

I Finanstilsynets rundskriv understrekes viktigheten av utkontrakteringskontrakten og hvordan virksomheter bør utforme den i tråd med gjeldene lovverk (Finanstilsynet, 2022b). Det er mange elementer som bør inkluderes i kontrakten. Virksomhetene må blant annet sikre at oppdragsbeskrivelsen spesifiserer oppdragets omfang, og utarbeide planer for å håndtere eventuell dårlig kvalitet eller andre utfordringer. Det er også viktig å innlemme spesielle krav i avtalen (Finanstilsynet, 2022b). Videre bør avtalen sikre foretakets mulighet til å avslutte kontrakten, enten det skyldes konflikter eller foretakets strategiske valg om en kontrollert avvikling av leverandørforholdet. Avtalen bør også definere partenes plikter tydelig (Finanstilsynet, 2022b). Gjennom avtalen må foretaket sikre at Finanstilsynet har muligheten til å kontrollere oppdragstakers utførelse og etterlevelse av regulatoriske bestemmelser. Videre må oppdragstaker forplikte seg til å ivareta oppgavene som er fastsatt i foretakets beredskaps- og kontinuitetsplaner (Finanstilsynet, 2022b).

Digital Operational Resilience Act (DORA)

Digital Operational Resilience Act (DORA) er et forslag fra EU-kommisjonen som ble lansert i 2020. Forslaget er utarbeidet med hensikt om å skjerpe kravene til IKT-sikkerhet for nettverks- og informasjonssystemer og deres underleverandører av IKT-systemer, grunnet økt risiko for cyberangrep. DORA skal øke motstandsdyktigheten i sektoren for å styrke tillit og øke sikkerheten. Det skal gjøres ved å sikre at alle deltakerne i det finansielle systemet har nødvendige tiltak for å redusere faren for cyberangrep og andre risikoer (Norges Bank, 2023). Implementeringen av DORA legger opp til en helhetlig tilnærming til risikostyring, økt rapportering av alvorlige hendelser, samarbeid mellom tilsynsmyndigheter, krav til godkjente tredjepartsleverandører og krav om testing av beredskapsplaner (Norges Bank, 2023). Kritiske IKT-underleverandører er direkte regulert av DORA, mens andre underleverandører blir indirekte regulert. NSM (2023) vektlegger at økt rapportering av hendelser vil bidra til en bedre

situasjonsforståelse som vil gjøre Norge bedre i stand til å forebygge trusselaktørers bruk av sammensatte virkemidler. Et system for registering og håndtering av sikkerhetstruende hendelser bør være tilgjengelig for å kunne bidra til læring og systematisk prioritering av sikkerhetstiltak (NSM, 2023). Banker som allerede følger retningslinjene satt av europeiske tilsynsmyndigheter er godt forberedt på implementering av regelverket, selv om det krever forbedringsarbeid for å imøtekomme kravene.

Resultater fra intervjuer

På spørsmålet om hvordan lovverket legger føringer for utkontrakteringsprosessen av IKT-tjenester svarer informantene at det legger føringer i stor grad, fordi de er pålagt å følge det. Informant 1 og informant 4 viste til at IKT-forskriften og rundskrivet fra Finanstilsynet legger føringer på hva som bør gjøres når det kommer til IKT-sikkerhet, og utførelsen av arbeidet. Risikostyring er et sentralt fokus for banken, da de er pålagt å være oppmerksom på risikoer til enhver tid. Utover dette nevnte informant 4 DORA, og viste til at det vil stille flere krav til banken i tiden fremover, spesielt på oppfølgingen av underleverandørene til leverandørene. Banken har allerede startet å se på innvirkningen DORA vil ha, og rundskrivet ble trukket frem som et godt hjelpemiddel i den sammenhengen. Informant 5 mente meldeplikten og kravet om at det som skal utkontrakteres må godkjennes av styret, er en premissgiver for kvalitet, da administrasjonen i foretakene må levere i forhold til styrets krav.

Kontrakt

Informant 5 viste til §12 i IKT-forskriften som tar for seg bestemmelser som beskriver hva foretakene skal ha med i avtalene, og hvordan de skal opptre. Videre viste informanten til Finansforetaksloven §13-4 som tar for seg krav til virksomheten i finansforetak, mer spesifikt utkontraktering. Informantene fra banken forteller at de har standardavtaler som benyttes i stor grad, og at disse inneholder kravene som tilsynsmyndighetene stiller, i tillegg til de banken har satt for at de skal føle seg trygge. Informant 4 forklarte at de har et eget vedlegg som dreier seg om sikkerhet i standardkontrakten, som er utarbeidet av «utvikling». Vedlegget trekker frem ulike elementer som for eksempel rett til innsyn, rett til å følge opp og rett til revisjon og så videre. Informant 3 nevnte blant annet at kontrakten sier noe om hvilke hendelser leverandøren må melde inn til dem, slik at banken blir involvert. Dette kan være uønskede hendelser der for eksempel data er på avveie, og det er derfor viktig at banken får beskjed.

Hvordan tilsynsmyndighetene og banken arbeider med å følge opp lovverket og krav

Informanten fra Finanastilsynet forklarte at det hovedsakelig er gjennom tilsyn de arbeider med å følge opp at lovverk og krav blir fulgt. Informanten mente at det å føre tilsyn med IKT er å føre tilsyn med utkontraktert IKT-tjenester. Dette fordi finanssektoren i Norge i stor grad har utkontraktert sine IKT-tjenester helt siden 70-tallet. Informanten forklarte at bankene er så like at et tilsyn hos for eksempel én Eika-bank kan tilsvare 50 tilsyn. «Dersom vi gjennomfører 5-8 tilsyn, vil vi ha dekket en stor del av banksektoren. Vi gjennomfører såpass mange tilsyn at vi har en grei oversikt over hva risikoen er» (informant 5).

Informant 4 viste til at de er en stor bank og at de derfor ofte har tilsyn. Dersom banken ikke følger de lover og krav som de er pålagt, vil det kunne få konsekvenser. Dette er noe de helst vil unngå ettersom det vil kunne få negative følger for omdømme og tillit. Negativt omdømme er noe som selvfølgelig ikke er ønskelig, og de er derfor opptatt av å følge lovene. Internrevisjon på flere områder viser hvordan banken arbeider med å følge opp lovverk og krav. Eksterne konsulenthus kommer da inn for å gjennomføre revisjoner, og for å se på utkontrakteringsprosessen opp mot lovkravene som stilles. Ifølge informant 4 gjør dette at banken selv får mulighet til å gjøre forbedringer på prosessen, uten å få tilsnakk av Finanstilsynet.

Informant 1 og 2 viste til POPs-prosessen for å besvare hvordan banken arbeider med å påse at lovverket følges, og viste til at compliance er en sentral del av denne prosessen. Banken arbeider med å påse at lovverket følges gjennom en strukturert prosess ved innføring eller endringer i alle produkter, systemer og prosesser i banken. Skal det inn med en endring, skal den registreres og det skal tas en risikovurdering. Avdeling for operasjonell risiko sørger gjennom denne prosessen for at alle endringer kommer til dem.

5.3.2 Utfordringer knyttet til lovverket

Resultater fra dokumentanalyse

I NOU (2015:13) ble det påpekt at det er økende trend å utarbeide felles regelverk med EU og andre internasjonale aktører. Rapporten viste til Finans Norges frykt for lavere sikkerhetskrav i Norge, som følge av felles regelverk. Internasjonal konkurranse bidra til å drive kravene mot en nedre grense, selv om Norge i utgangspunktet kan definere strengere minimumskrav. Lysneutvalgets rapport (NOU 2015:13) oppfordrer derfor til å fortsette med det internasjonale

arbeidet, i tillegg til at Finanstilsynet må være oppdatert på beste praksis. Dette kan peke mot en utfordring med regelverket i norsk og europeisk kontekst. Siden 2015 er det gjort oppdateringer i lovverk knyttet til de kravene som stilles, blant annet med tanke på DORA-forskriften, som sikter mot å styrke motstandskraften i det finansielle systemet. For norske banker vil det kunne medføre strengere krav, økte kostander og et enda mer komplekst regelverk som må etterleves, noe som vil kreve større fokus på compliance og risikostyring. Det kan dermed diskuteres hvorvidt felles regelverk medfører lavere sikkerhetskrav, og muligheten for at denne utviklingen er i endring. Det er ikke funnet noe i dokumenter som har undersøkt utfordringene med lovverk og krav i relasjon til utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren, noe som anses som et funn i seg selv. Likevel, løfter NOU (2015:13) frem et element som bør ses på i lys av anbefalingene de fremlegges.

Resultater fra intervju

Innsamlet empiri fra intervjuene viste at det var delte meninger når det gjelder utfordringene med lovverket. Det ble pekt på bruk av standardavtaler og forståelse av lovverket, i tillegg til at kravene som stilles er krevende, mens andre ikke anser eller trekker frem utfordringer. Det var også noe uenighet knyttet til hvorvidt informantene mener regelverket fungerer risikoreduserende og etter hensikt.

Kontraktsinngåelse

Ifølge informantene fra banken er det få utfordringer når det gjelder kontraktsinngåelse, og de mindre utfordringene som dukker opp løses som oftest fint. Informant 1 viste til at det noen ganger kan være utfordrende å få de store internasjonale leverandørene, som eksempel Amazon, til å godta bankens standardavtale. «De er for store og har for mye makt, og vi blir for liten i den sammenheng. De krever og forventer vi skal bruke deres avtaler» (informant 1). Dette kan oppleves som en utfordring da banken er avhengig av å få inn de vilkårene som tilsynsmyndighetene krever, i tillegg til andre vilkår som skal dekke bankens trygghet. Ifølge informant 5 kan det være vanskelig å få avtaleinnsyn ved kontraktsinngåelse, noe som kan by på utfordringer.

Forståelse av lovverk og krav

Informant 1 og 2 trakk frem utfordringer som gjelder forståelsen av lovverket. De viste til at det er et relativt nytt regelverk som fører til mye tolkning, og at denne gjerne er ulik fra virksomhet til virksomhet. Informant 1 trakk frem at lovverket har lite rom for skjønn.

«Veilederen er god og tydelig, men samtidig rigid og gir lite rom for skjønn. Den kunne vært rundere i kantene» (informant 1). Informant 2 pekte på at det er en mangel på klare definisjoner, og at dette byr på store utfordringer siden kravene lovverket stiller i beste fall er krevende. «Det har kostet mye tid, fordi det rett og slett ikke er enkelt å forstå. Et system jeg var sikker på var utkontraktering mente internrevisjon at ikke var det. Det er store utfordringer der, og det mangler mer tydelighet» (informant 2). Informant 4 mente at lovverket ikke er uklart eller har mangler, og finner heller ikke noe som begrenser informantens arbeid knyttet til oppfølgning, men trekker frem elementer i lovverket som kan oppleves som urettferdig. Informanten viste til at de er en stor bank og at det derfor er mulig at deres prosesser er strengere enn prosessene banker av mindre størrelse har. Dette fordi de store bankene oftere får tilsyn, og av den grunn arbeider ut ifra dette.

Hvorvidt lovverket fungerer risikoreduserende

På spørsmålet om informantene mente at lovverket fungerer risikoreduserende og etter hensikt, var det noe ulike meninger. Dette var både knyttet til hvor viktig regelverket er, og hvor godt det fungerer. Informant 2 mente at lovverk og krav egentlig ikke fungerer risikoreduserende ettersom at banken hadde stilt de kravene uansett. Videre mente informanten at reglene er firkantet og at det mangler en mulighet til å ta en risikobasert tilnærming. Utfordringen ifølge informanten var at dersom det brukes mye tid på det som er lite viktig, er det en mulighet for at banken går glipp av sjansen til å identifisere og håndtere hendelser, noe som kan få konsekvenser. På den andre siden mente de andre informantene fra banken og informant 5 at lovverket funger risikoreduserende. «Dersom utkontrakteringer ikke hadde vært regulert i den grad der er, eller det ikke hadde blitt ført tilsyn, ville ikke jeg hatt pengene mine i banken» (informant 5).

Informant 1 resonerte rundt hva som er for mye regulering, før det kan bikke over til å bli for byråkratisk. «Det er risikoreduserende i aller høyeste grad, men noen ganger kan det bli overkill og for mye administrasjon og byråkrati. Det er skjerpende med myndigheter som stiller krav, men hvor balansen går er vanskelig å si» (informant 1). Informant 4 mente kravene knyttet til risikostyring av utkontrakterte tjenester i IKT-forskriften passer veldig godt med det trusselbildet som finnes nå. «Jeg at lovverket fungerer etter hensikt med oss i alle fall. Det håper jeg, og føler at det gjør det med tanke på den prosessen vi har» (informant 4). Samtidig påpekte informanten at lovverket ikke fungerer direkte risikoreduserende, ettersom man kan velge å akseptere den risikoen som følger med. Informant 6 meddelte at det nok er sprikende

erfaringer i bank- og finanssektoren knyttet til hvorvidt lovverket fungerer risikoreduserende. «Det som jeg relativt trygt kan si er at lovverket stort sett vil halte etter» (informant 6).

5.3.3 Diskusjon av forskningsspørsmål 3

Empirien viser at det er noe uenighet om hvorvidt lovverket fungerer risikoreduserende ved utkontraktering av IKT-tjenester i bank og finanssektoren. Likevel indikerer dataen enighet rundt at lovverket legger føringer i stor grad. Noen av informantene argumenterte for at lovverk, spesielt IKT-forskriften og Finanstilsynets rundskriv, har en betydelig innflytelse. Disse reguleringene forklares som en premissgiver for utkontrakteringens kvalitet og danner rammene for utkontraktering. Dette antyder at lovgivning kan bidra til å sikre at foretakene tar hensyn til relevante krav og retningslinjer for å opprettholde pålitelige og robuste IKT-tjenester. Samtidig peker noen informanter på utfordringer knyttet til lovverket, som kan føre til at det ikke fungerer etter hensikt. Eksempel er tolkningen av regelverket og mangel på klare definisjoner og retningslinjer. Dette kan påvirke organisasjonenes evne til å implementere og etterleve lovverket på en konsekvent og effektiv måte, noe som kan påvirke virksomhetens mulighet til å opprettholde pålitelighet og resiliens. Ifølge Hollnagel (2011) handler resiliens om å håndtere feil og ulykker på en effektiv måte når de oppstår, og kan fungere som en strategi for systemet. For at resiliens skal være mulig kreves robuste og fleksible systemer. Even til improvisasjon og fleksibilitet vil kunne bidra til resiliens og evnen til å takle uforutsette utfordringer (Hollnagel, 2017). For at virksomheter i bank- og finanssektoren skal kunne fungere som HROer i komplekse og risikofylte miljøer, og for å kunne oppnå høy pålitelighet og resiliens i utkontrakteringsprosessen, er det viktig at sikkerhet har høyeste prioritet. Det er derfor sentralt at lovverket gir klare og presise retningslinjer slik at tolkningen av regelverket ikke tar opp all tid. Skulle regelverket være utydelig kan dette føre til feilprioriteringer av tid, noe som kan resultere i at fokuset på sikkerhet blir nedprioritert.

Sentralisert og desentralisert styring

Hvorvidt informantene mente at lovverk og krav fungerte risikoreduserende var det noe uenighet rundt. Informant 1 mente lovverket fungerte risikoreduserende, men mente at det går en grense for hvor mye myndighetene skal kunne kreve før det blir for byråkratisk. Informanten fra Finanastilsynet og tre av informantene fra banken mente at lovverket fungerer etter hensikt, mens informant 2 mente det ikke fungerer risikoreduserende. Informant 1 og 2 nevnte at de oppfattet lovverket som rigid, firkantet og at det var lite rom for skjønn. Sistnevnte informant

argumenterte for at banken hadde implementert kravene som står i lovverket, uavhengig om de hadde vært lovpålagt eller ikke, og mente også at banken noen ganger stiller høyere krav. Videre mente informanten at det mangler en mulighet til å ta en risikobasert tilnærming. Det kan dermed oppfattes som at informanten anser at banken ikke har beslutningsmyndighet i stor nok grad til å kunne gjøre vurderinger selv, noe som kan medføre risiko. Banken vil i noen tilfeller ha en annen opplevelse av risikoene, og dermed sette søkelys på risikoer som ikke nødvendigvis er de myndighetene anser som mest relevante.

I følge HRO-teorien er det avgjørende at det er mulighet til å ha en fleksibel tilnærming til styring i organisasjoner. Fleksibiliteten omhandler at det skal være mulig å gå fra sentralisert til desentralisert styring (Weick & Sutcliffe, 2015). Teorien anerkjenner de positive sidene med å ha en sentralisert tilnærming, men understreker behovet for spontan omstilling og desentralisert beslutningstaking. Dette er fordi man ifølge HRO-teorien, krever effektive reaksjoner på uventede hendelser for å kunne unngå ulykker (Aven et al., 2004). Dersom banken opplever lovverket som rigid, og at det begrenser muligheten til å ha en risikobasert tilnærming, kan dette påvirke fleksibiliteten og evnen til å håndtere uforutsette situasjoner. Dersom beslutningsmyndigheten er sterkt sentralisert og begrenset av lovverk, kan det gjøre det vanskelig å tilpasse seg endringer i risikobildet i tillegg til å implementere effektive sikkerhetstiltak. Dette kan også begrunnes med at «(…) lovverket stort sett vil hale etter» som informant 6 viste til.

Dersom banken ikke har muligheten til å ta avgjørelser på eget grunnlag, vil det ifølge informant 2 kunne føre til en sikkerhetsrisiko, fordi de kan gå glipp av hendelser eller ha feil fokus. Perrow (1999) mener en slik desentralisering vil øke kompleksitet og sjansen for at ulykker oppstår. På den andre siden kan det tenkes at en risikobasert tilnærming også vil kunne kreve visse standarder og retningslinjer slik man sikrer at leverandørene oppfyller spesifikke krav. Sentralisert styring kan dermed være mer egnet for å sikre at slike krav blir oppfylt, og kan bidra til å opprettholde en høy grad av sikkerhet og pålitelighet i sektoren (Weick & Sutcliffe, 2007). Balansen mellom risikoreduserende tiltak og fleksibilitet blir vektlagt i HRO-teorien og viser til at det er hensiktsmessig å vurdere en mer balansert tilnærming. En balanser tilnærming her kan for eksempel oppnås gjennom at lovverket legger klare føringer, samtidig som det er rom for at virksomhetene selv kan gjøre vurderinger basert på eget grunnlag.

Informant 4, fra banken, mente at lovverket ikke er uklart eller har mangler, men at tilsyn kan oppleves som urettferdig, og presenterte en hypotese om at mindre banker får tilsyn sjeldnere og derfor ikke følger lovverket like nøye. For at lovverket skal implementeres og fungere etter hensikt, er det viktig at lovverket oppfattes som rettferdig. Om det ikke gjør det, kan det føre til mistillit både til lovverk og tilsyn, noe vil kunne få konsekvenser for systemet i et sikkerhetsperspektiv. En slik tankegang reflekterer en HRO-tilnærming med fokus på tillitt i beslutninger for å håndtere kompleksitet (Weick & Sutcliffe, 2007).

Krav til utkontrakteringskontrakt

Empirien viser at bank- og finanssektoren arbeider på ulike måter for å påse at lovverk og krav følges. Det ble lagt stor vekt på utkontrakteringskontrakten da den utgjør grunnlaget for utkontrakteringsprosessen. Kontrakten reguleres av lovverket, men det viste seg også at banken stiller egne krav som også implementeres i kontrakten. Disse stilles for at bankene skal føle seg trygg på avtalen. De ble påpekt få utfordringer ved kontraktsinngåelse, men det å få de store internasjonale leverandørene til å godta bankens standardavtaler ble nevnt. Utfordringer dette kan medføre i praksis, dreier seg om å få vilkårene som tilsynsmyndighetene krever inn i kontrakten. Det ble også nevnt utfordring med å få avtaleinnsyn ved kontraktsinngåelse. Finanstilsynet arbeider med risikostyring gjennom tilsyn og at det derfor må være avtalefestet i kontrakten (Finanstilsynet, 2022b). Informanten viser videre til at de gjennomfører såpass mange tilsyn at de har grei oversikt over hva risikoen er. Dersom banken ikke følger lover og krav de er pålagt vil dette få konsekvenser som vil kunne påvirke omdømme og tillitt. Det er med andre ord er det tydelig at lovverket som regulerer kontrakten er sentral for å kunne styre risikoen gjennom prosessen.

Kontrakten er sentral for risikostyring av utkontrakteringsprosessen, hvor risikostyring handler om å balansere verdiskapning, samt unngå ulykker, tap og skader (Aven et al., 2004). Informant 2 påpekte som nevnt, manglende mulighet til å ha en risikobasert tilnærming, noe som kan skape begrensninger for verdiskapning. Noen av informantene viste til at risikostyringen som lovverket legger opp til er nødvendig og fungerer etter hensikt, men at balansen kanskje kan gå utover deres mulighet til autonomi i beslutningstaking. Med andre ord kan empiri fra noen av intervjuene peke mot at det mangler mulighet for verdiskapning i stor nok grad på grunn av begrensningene lovverket legger. Det er imidlertid en sektor i stor vekst som samtidig unngår hendelser og feil som påvirker den finansielle stabiliteten, noe som kan peke mot at lovverket som regulerer utkontrakteringen i sektoren i stor grad fungerer etter hensikten.

Digital motstandskraft

DORA-forslaget og IKT-forskriften er utformet med hensikt om å styrke IKT-sikkerheten og den digitale motstandskraften til finansielle tjenester i Europa (Regjeringen, 2020). Regelverket trekkes av informant 4 frem som en utfordring det må jobbes med i tiden fremover. Mye av arbeidet som siktes til handler spesielt om den nye innføringen som tar for seg oppfølgning av underleverandører til bankens leverandører. Ettersom banken i stor grad følger retningslinjer satt av EBA og EIOPA, i tillegg til å ha startet arbeidet med å se på hvilke innvirkninger DORA vil ha for banken, virker det som om de er godt forberedt på implementeringen. DORA utgjør et betydelig tilskudd for å imøtekomme svakheter ved utkontraktering, gjennom å ha et bredere omfang enn IKT-forskriften (Regjeringen, 2020).

DORA stiller krav til godkjente tredjepartsleverandører, mens IKT-forskriften stiller krav til finansinstitusjoners gjennomføring av risikovurderinger av tredjepartsleverandører og avtaler som sikrer informasjonssikkerheten. Reguleringen kan føre til at motstandskraften styrkes, noe som vil øke tillit, sikkerhet og robusthet (Norges Bank, 2023). Denne tankegangen kan knyttes opp mot resiliens. Innføring av DORA vil strekke lengre enn dagens regulering, som kan føre til økt kompleksitet i tillegg til økte kostnader. Det er mulig at innføringen av mer kontroll vil kreve for mye ressurser og at det vil bli for komplisert satt opp mot effekten det vil ha. Dette vil kunne føre til betydelig mer arbeid for å kunne innfri kravene som lovverket krever. DORA-regelverket øker kompleksiteten i bankens arbeid ved å kreve at de har kontroll på egne leverandører og leverandørenes underleverandører (NSM, 2023). Dette utgjør et ekstra ledd som banken må ha kontroll over, noe som vil gjøre arbeidet mer komplekst i et NAT-perspektiv. En mulig effekt av dette kan være mangel på ressurser og feilprioriteringer. Den økte kompleksiteten og arbeidsmengden kan føre til uforutsette hendelser og feil, i tråd med NAT-teorien som vil argumentere for at systemer med høy kompleksitet er mer sårbare (Perrow, 1999).

Bank- og finansinstitusjoner kan ved hjelp av DORA og IKT-forskriften identifisere potensielle risikoer og benytte beste praksis for risikovurdering og håndtering for å oppnå høy pålitelighet og motstandskraft. Dette kan ses i tråd med en HRO-tankegang for en proaktiv risikohåndtering og fokus på kontinuerlig læring (Weick & Sutcliffe, 2007). HRO-prinsippet kan benyttes for å bygge sterke samarbeidsforhold med underleverandører for å forberede bankene på å håndtere uforutsette hendelser i tillegg til å møte endringene i regelverket som vil legge større vekt på samarbeid.

5.3.4 Oppsummering av forskningsspørsmål 3

Samtlige av informantene er enige i at lovverket legger føringer for bankens arbeid knyttet til utkontraktering, men hvorvidt lovverket fungerer risikoreduserende er det delte meninger om. En av informantene påsto at banken ville stilt de samme kravene uavhengig om det sto i lovverket, og at lovverket derfor ikke fungerte risikoreduserende, men at det heller kunne opplevdes som en hindring. En annen informant mente at lovverket var lite tydelig og bidro til å skape usikkerhet, men var i likhet med flesteparten av informantene av den oppfatning at lovverket fungerte skjerpende og at det samlet sett fungerte etter hensikt. Lovverket legger føringer for hvordan banken skal drive utkontrakteringsprosessen, og stiller blant annet krav til hva som skal meldes inn, hva som skal stå i avtalen og hvor ofte det skal gjennomføres risikovurderinger. Alle tiltakene er utarbeidet med hensikt om å minimere risikoene som utkontraktering av IKT-tjenester fører med seg. Lovverket bør legge spesielt til rette for brukervennligheten ettersom omfanget er komplekst, her skal rundskrivet være til hjelp for foretakene. Det kan virke som at det ikke er til nytte i stor nok grad. Implementeringen av DORA-regelverket er noe bank- og finanssektoren må forholde seg til, og kan peke mot økt kompleksitet og krevende arbeid i tiden fremover.

6.0 Konklusjon

Norsk bank- og finanssektor har utkontraktert IKT-tjenester i flere tiår, og risikoene dette medfører er svært aktuelt i dagens risikobilde. Utkontraktering av IKT-tjenester legger til rette for betydelige muligheter for spesialisering, teknologisk utvikling og kostnadskutt. Det kan også bidra til økt sikkerhet, men kommer ikke uten utfordringer. Problemstillingen som skal besvares er følgende:

> *På hvilken måte representerer utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren risiko, og hvordan håndteres den?*

De mest vesentlige risikoene viser seg å være leverandørkjedeangrep, avhengigheter, konsentrasjonsrisiko, finansiell stabilitet, operasjonell risiko og systemrisiko. Disse risikoene relateres til utkontrakteringens organisering, som skaper et komplekst system bestående av uoversiktlige leverandørkjeder med mange involverte, og kjennetegnes ved manglende kontroll og oversikt. Risikoene knyttes til dimensjoner relatert til safety og security, i tillegg til stor grad av usikkerhet og sårbarhet. Samlet sett utgjør utkontraktering av IKT-tjenester i sektoren en betydelig risiko som på mange måter er vanskelig å komme utenom. Fordelene med utkontraktering anses til å være større enn ulempene, og risikoen hadde trolig vært høyere dersom banken ikke hadde utkontraktert. Studien viser at banken er avhengig av å utkontraktere IKT-tjenester for å holde seg konkurransedyktig og er derfor villig til å ta risikoene det medfører. Det er derfor avgjørende at sektoren har et høyt sikkerhetsfokus.

Norsk bank- og finanssektor arbeider kontinuerlig med å håndtere ulike risikoer ved bruk av forskjellige tilnærminger og risikostyringsverktøy. I dette arbeidet prioriterer sektoren i størst grad ut fra tjenestenes kritikalitet, noe som gjenspeiles i både lovpålagte reguleringer og bankens internt utviklede verktøy. Overholdelse av lovverk og krav spiller en viktig rolle i håndteringen, men grunnet et stadig skiftende risikobilde kan lovgivningen ofte være på etterskudd. Det kreves derfor en helhetlig tilnærming til risikohåndtering for å møte risikoen på en effektiv måte. For å opprettholde tilstrekkelig kontroll, er det nødvendig med bedre håndtering av utkontrakteringsprosessen. Mangelen på tilstrekkelig kunnskap og kompetanse blir dermed en betydelig utfordring, noe som utgjør en sikkerhetsutfordring på IKT-området. Det antydes at innføring av supplerende regelverk vil medføre mer omfattende prosesser, blant

annet knyttet til leverandøroppfølging. Hvilke implikasjoner det faktisk vil føre til er derimot for tidlig å konkludere med.

6.1 Forslag til videre forskning

Temaet som har blitt diskutert er av høy aktualitet. Det er flere områder innenfor temaet som har behov for forskning for å kunne møte fremtidens utfordringer, bedre rustet enn i dag. I en forlengelse av studien oppfordres det til videre forskning på digitalisering av bank- og finanssektoren, spesielt med tanke på organiseringen knyttet til omfattende utkontraktering av IKT-tjenester. Kunnskap og kompetanse for teknologisk utvikling i bank- og finanssektoren er avgjørende for å håndtere risikoen, samtidig som de positive sidene utnyttes. Ved å kartlegge risikofaktorer og sikkerhetsstrategier kan man møte utfordringene, i tillegg til å sikre en stabil og trygg digital infrastruktur, som er av avgjørende betydning. Slik forskning kreves for å kunne styrke motstandsdyktigheten i møte med fremtidens teknologiske fremskritt.

Referanseliste

Anholt, R., & Boersma, K. (2018). *From Security to Resilience: New Vistas for International Responses to Protracted Crises*. IRGC.

Aven, T. (2015). *Risikostyrin: grunnleggende prinsipper og ideer (2.utg., p.192)*. Universitetsforlaget.

Aven, T. (2018). *The Call for a Shift from Risk to Resilience: What does it Mean?* Society for Risk Analysis, *39*(6), 1196–1203. https://doi.org/10.1111/risa.13247

Aven, T., Boyesen, M., Njå, O., Olsen, K. H. & Sandve, K. (2004). *Samfunnssikkerhet.* Universitetsforlaget.

Aven, T. & Renn, O. (2010). *Risk Mangagement and Goverance. Concept, Guidelines and Applications*. US: Springer. https://doi.org/10.1007/978-3-642-13926-0

Aven, T., Røed, W., & Wiencke, H. (2008). *Risikoanalyse – prinsipper og metoder, med anvendelser* (p.237). Universitetsforlaget.

Aven, T. & Thekdi, S. (2021). *Risk science; An introduction.* Routledge.

Blaikie, N. & Priest, J. (2019). *Designing social Research.* (Third edition.). Polity Press.

Busmundrud, O., Maal, M., Kiran, J.H., & Endregard, M. (2015). T*ilnærminger til risikovurderinger for tilsiktede uønskede handlinger.* (FFI-rapport 00923). Forsvarets forskningsinstitutt. https://publications.ffi.no/nb/item/asset/dspace:2503/15-00923.pdf

Cicero. (u.å.). *Tradisjonelle bankfilialer må gjennom en digital transformasjon.* Cicero. https://www.cicero.no/tradisjonelle-bankfilialer-ma-gjennom-en-digital-transformasjon/

Danermark, B. (1997). *Att förklara samhället.* Studentlitteratur.

Danermark, B. (2002). *Explaining Society: critical realism in the social sciences*. Routledge.

DNB. (2021). Trusselvurdering 2021. DNB. https://www.dnb.no/dnbnyheter/no/samfunn/trusselvurdering-2021

DNB. (2022). Trusselvurdering 2022. DNB. https://www.nsr-org.no/uploads/documents/Publikasjoner/DNB_Trusselvurdering-2022_LOWRES.pdf

Drageset, S., & Ellingsen, S. (2010). *Å skape data fra kvalitativt forskningsintervju*. *5*(4), 332-335. Sykepleien forskning (Oslo). https://doi.org/10.4220/sykepleienf.2011.0027

DSB. (2016). *Samfunnets kritiske funksjoner: Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* (KIKS 2-rapport). Direktoratet for samfunnssikkerhet og beredskap https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

DSB. (2020). *Risikostyring i digitale verdikjeder.* Direktoratet for samfunnssikkerhet og beredskap. https://www.dsb.no/globalassets/dokumenter/rapporter/risikostyring-i-digitale-verdikjeder.pdf

EBA. (2021). *Risk assessment of the European bankning system.* European Banking Authority. https://www.eba.europa.eu/sites/default/documents/files/document_library/Risk%20Analysis%20and%20Data/EU%20Wide%20Transparency%20Exercise/2021/1025102/Risk_Assessment_Report_December_2021.pdf

Engen, O.A., Kruke, B. I., Lindøe, P., Olsen, K. H., Gould, O. E., & Gould, K. A. P. (2021). *Perspektiver på samfunnssikkerhet* (2. utgave.). Cappelen Damm akademisk.

Finanstilsynet. (2021a). *Risiko- og sårbarhetsanalyse (ROS). Finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT).* Finanstilsynet. Risiko- og sårbarhetsanalyse (ROS) 2021 (finanstilsynet.no)

Finanstilsynet. (2021b). *Veiledning om utkontraktering.* Finanstilsynet. https://www.finanstilsynet.no/contentassets/9f76ac1a390a44218b285b61bb13e19a/veiledning-om-utkontraktering.pdf

Finanstilsynet. (2022a). *Bank og finans.* Finanstilsynet. https://www.finanstilsynet.no/forbrukerinformasjon/bank-og-finans/

Finanstilsynet. (2022b). *Risiko- og sårbarhetsanalyse (ROS) 2022.* Finanstilsynet. https://www.finanstilsynet.no/contentassets/d6c5910b41044d1b89f7a50a7b7315db/ros-2022.pdf

Finanstilsynet. (2023a). *Risiko- og sårbarhetsanalyse (ROS) 2023.* Finanstilsynet. https://www.finanstilsynet.no/contentassets/fbbc7ef2a0c9499fbb6fa68867ad697c/risiko-og-sarbarhetsanalyse-2023.pdf

Finanstilsynet. (2023b). *Finanstilsynets strategi 2023-2026.* Finanstilsynet. https://www.finanstilsynet.no/om-finanstilsynet/styringsdokumenter/strategi/

Forskrift om IKT-systemer i banker mv. (2003). *Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)* (FOR-2003-05-21-630). Lovdata. https://lovdata.no/dokument/SF/forskrift/2003-05-21-630

Forskrift om meldeplikt ved utkontraktering av virksomhet mv. (2021). *Forskrift om meldeplikt ved utkontraktering av virksomhet mv.* (FOR-2021-09-15-2777). Lovdata. https://lovdata.no/dokument/SF/forskrift/2021-09-15-2777

Golafshani, N. (2003). *Understanding reliability and validity in qualitative research.* The qualitative report, 8(4), 597-607.

Grønmo, S. (2016). *Samfunnsvitenskapelige metoder*. (2.utg.). Bergen: Fagbokforlaget.

Halvorsen, K. (2008). *Å forske på samfunnet.* Cappelen Akademisk.

Hollnagel, E. (2011). *Epilogue: RAG – The Resilience Analysis Grid.* In Resilience Engineering in Practice (1st ed., pp. 275–296). CRC Press. https://doi.org/10.1201/9781317065265-19

Hollnagel, E. (2014). *Safety-I and safety-II: The past and future of safety management* (p. 187). Ashgate. https://doi.org/10.1201/9781315607511

Hollnagel, E. (2017). *Safety-II in Practice: Developing the Resilience Potentials.* UK: Routledge. https://doi.org/10.4324/9781315201023

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode* (3. utg.). Cappelen Damm Akademisk.

Johannsen, A., Tufte, P.A., & Christoffersen, L. (2016). *Introduksjon til samfunnsvitenskapelig metode (*5. Utg.). Abstakt forlag.

Jore, S. (2019). *The Conceptual and Scientific Demarcation of Security in Contrast to Safety.* European Journal for Security Research. https://doi.org/10.1007/s41125-017-0021-9

Justis- og beredskapsdepartementet. (2019). *Nasjonal strategi for digital sikkerhetskompetanse.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf

Kaufman, G. G., & Scott, K. E. (2003). *What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?* The Independent Review, 7(3), 371–391. http://www.jstor.org/stable/24562449

Kongsvik, T., Albrechtsen, E., Antonsen, S., Herrera, I., Hovden, J., & Schiefloe, P. M. (2018). *Sikkerhet i arbeidslivet.* Bergen: Fagbokforl.

La Porte, T. R. (1996). *High Reliability Organizations: Unlikely, Demanding and At Risk.* Journal of Contingencies and Crisis Management, 4(2), 60-71. https://doi.org/10.1111/j.1468-5973.1996.tb00078.x

Leveson, N. (2020). *Safety and Security Are Two Sides of the Same Coin. I The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*. Springer International Publishing. https://dspace.mit.edu/handle/1721.1/137069

Lind, Ø. A. (2016). *Smitte mellom banker – systemrisiko som følge av bankenes sammenkobling nr.13*. Norges Bank. Smitte mellom banker - SYstemrisiko som følge av bankenes sammenkobling nr. 13 (Norges-bank.no)

Martin, P. (2019). *The rules of security: staying safe in a risky world*. Oxford University Press.

Meld. St. 12. (2021-2022). *Finansmarkedsmeldingen 2022.* Finansdepartementet. https://www.regjeringen.no/contentassets/0142ad0157fc48a5a6283c9945feb82a/no/pdfs/stm202120220012000dddpdfs.pdf

Meld. St. 9. (2022-2023). *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/d256b455415c4cae8a710f62cc97d4f9/no/pdfs/stm202220230009000dddpdfs.pdf

Meld. St. 10. (2016-2017). *Risiko i et trygt samfunn.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/

Meld. St. 38. (2016-2017). *IKT-sikkerhet. Et felles ansvar.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf

NIFU. (2017). *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud.* Rapport 2017:32. Justis- og beredskapsdepartementet. https://nifu.brage.unit.no/nifu-xmlui/bitstream/handle/11250/2490041/NIFUrapport2017-32.pdf?sequence=6&isAllowed=y

Norges Bank. (2021a). *Finansiell stabilitet 2021.* Norges Bank. https://www.norges-bank.no/contentassets/c4ffd169504b47249d646ed5753b0da0/finansiell_stabilitet_2021.pdf?v=11/10/2021110512

Norges Bank. (2021b). *Finansiell infrastruktur 2021.* Norges Bank. *https://www.norges-bank.no/contentassets/12681d7ba8744ff59176cd54544469c9/fi_finansiellinfrastruktur_2021.pdf?v=05/19/2021222251&ft=.pdf*

Norges Bank. (2022a). *Finansiell infrastruktur 2022*. Norges Bank. https://www.norges-bank.no/contentassets/7437af41dbd94dbfaee9e7f0d231a3ba/finansiellinfrastruktur_2022.pdf?v=08/08/2022123229

Norges Bank. (2022b). *Finansiell stabilitet 2022*. Norges Bank. https://norges-bank.brage.unit.no/norges-bank-xmlui/bitstream/handle/11250/3030880/finansiell_stabilitet_2022.pdf?sequence=1&isAllowed=y

Norges Bank. (2022c). *Det norske finansielle systemet 2022.* Norges Bank. https://www.norges-bank.no/contentassets/33185319a0ca4b069c3c0e9e9656e773/dnfs_2022_web.pdf?v=06/30/2022150342

Norges Bank. (2023). *Finansiell stabilitet 2023 – 1.halvår.* Norges Bank. *https://www.norges-bank.no/contentassets/c4de63c7ee654f7fa99e7f37e075d5b2/finansiell-stabilitet-1-23.pdf?v=05/10/2023085735*

NOU 2000:24. (2000). *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf

NOU 2006:6. (2006). *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf

NOU 2015:13. (2015). *Digital sårbarhet - sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NOU 2018:14. (2018). *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/0d408600df2f4738a9bbb85040b02b59/no/pdfs/nou201820180014000dddpdfs.pdf

NOU 2023:6. (2023). *Finanstilsynet i en ny tid – ny lov om Finanstilsynet.* Finansdepartementet. https://www.regjeringen.no/contentassets/b34c128f2e174a67afa97035baea7679/no/pdfs/nou202320230006000dddpdfs.pdf

NSM. (2021). *Nasjonalt digitalt risikobilde 2021.* Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/137495-1635323653/NSM/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf

NSM. (2022). *Risiko 2022. Økt risiko krever økt årvåkenhet.* Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/137798-1644424185/NSM/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

NSM. (2023). *Risiko 2023. Økt uforutsigbarhet krever høyere beredskap.* Nasjonal sikkerhetsmyndighet. https://nsm.no/getfile.php/1312547-1676283421/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies*. Princeton University Press.

PST. (2021). *Nasjonal trusselvurdering 2021*. Nasjonal trusselvurdering 2021 (pst.no)

PST. (2022). *Nasjonal trusselvurdering 2022.* Nasjonal trusselvurdering 2022 (pst.no)

PwC. (2023). *Digital Operational Resilience Act (DORA).* Digital Operational Resilience Act (DORA) – Alt du trenger å vite (pwc.no)

Regjeringen. (2020). *Forslag til forordning om digital operasjonell motstandsdyktighet i finanssektoren*. Regjeringen. Forslag til forordning om digital operasjonell motstandsdyktighet i finanssektoren (regjeringen.no).

Renn, O. (2008). *Risk Governance: Coping with uncertainty in a complex world* (pp.455). UK: Earthscan.

Sikkerhetsloven. (2019). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-01-24

Sikt. (u.å). *Fylle ut meldeskjema for personopplysninger.* Hentet fra: 4.2.23 fra: Meldeskjema for personopplysninger i forskning (sikt.no)

Skjelvik, A. (2019). *Cyber-risiko i den norske finanssektor* (Masteroppgave). Universitet i Stavanger. https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/2628889/Skjelvik_Alvhild.pdf?sequence=1&isAllowed=y

Slettemoen, J., M., & Ertenstein, S. (2018). *Informasjonssikkerhet i banknæringen* (Masteroppgave). Universitetet i Stavanger. https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/2565691/Ertenstein_Stine_Slettemoen_Julia.pdf?sequence=4&isAllowed=y

Sutcliffe, K. M. (2011). *High reliability organizations (HROs). Best Practice & Research Clinical Anaesthesiology*, *25*(2), 133-144. https://doi.org/10.1016/j.bpa.2011.03.001

Thagaard, T. (2018). *Systematikk og innlevelse: en innføring i kvalitativ metode* (5.utg., p.222). Bergen: Fagbokforlaget.

Tjora, A.H. (2021). *Kvalitative forskningsmetoder i praksis* (4. Utg.). Gyldendal akademisk.

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in the age of uncertainty* (2nd ed.). Jossey-Bass.

Weick, K. E., & Sutcliffe, K. M. (2015). *Managing the Unexpected: Sustained Performance in a Complex World* (3rd ed.). John Wiley & Sons. https://doi.org/10.1002/9781119175834

Vedlegg

Vedlegg A: Intervjuguide til ansatte i bank

Vedlegg B: Intervjuguide til ansatt i Finanstilsynet

Vedlegg C: Intervjuguide til ansatt i universitets- og høyskolesektoren

Vedlegg D: Informasjons- og samtykkeskjema

Vedlegg E: Vurdering av behandling av personopplysninger fra Sikt

Vedlegg A

Intervjuguide til ansatte i bank

Del 1.

- Presentasjon av studiens formål og fokus og studiens problemstilling
- Informasjon om taushetsplikt og informantenes anonymitet
- Signering av samtykkeskjema

Del 2.

Generelt

1. Hva er din stilling (tittel) og hva innebærer den?
2. Hvilke deler av utkontrakteringsprosessen arbeider du med?

Risiko knyttet til utkontrakteringsprosessen av IKT-tjenester

3. Kan du fortelle om din bakgrunn og erfaring med risiko knyttet til utkontraktering av IKT-tjenester?
4. Hva anser du som risiko i en utkontrakteringskontekst?
5. Hvordan vurderer banken risiko, og foreligger det retningslinjer som dere tar utgangspunkt i?
6. Hvordan går dere frem for å vurdere om risikoen knyttet til utkontraktering er akseptabel?
7. Hvordan vil du beskrive risikoen tilknyttet utkontraktering av IKT-tjenester?

Styringsinstrumenter i forbindelse med utkontraktering

8. Hvordan arbeider dere med leverandører av IKT-tjenester gjennom utkontrakteringsprosessen?
9. Hvordan arbeider dere med å redusere risikoen som utkontraktering av IKT-tjenester representerer?

10. Arbeides det ulikt med risiko med hensyn til hvordan de identifiseres/kategoriseres?
11. Hva tenker du kjennetegner god risikostyring av utkontrakterte IKT-tjenester i banken?
12. Hva opplever dere som utfordringer når det kommer til kontraktsinngåelse mellom innkjøper og leverandør?
13. Hvor ligger utfordringene med å styre risikoen utkontraktering av IKT-tjenester medfører?

Lovverk og krav

14. På hvilken måte legger lovverket føringer for utkontrakteringsporsessen?
15. Hvilke lovkrav anser dere som viktigst i forbindelse med utkontrakterte IKT-tjenester?
16. På hvilken måte arbeider dere med å påse at lovkrav og veiledninger ved utkontrakterte IKT-tjenester følges?
17. Er det noen faktorer som dere mangler i dagens lovverk (som burde vært inkludert)? Eller eventuelle uklarheter?
18. Hva tenker dere rundt bruk av standardisering? (at standardisering ikke er lovpålagt)
19. I hvilken grad mener dere lovverk og krav fungerer etter hensikt?

Del.3

- Noe informanten vil legge til som kan være av interesse for studien eller spørsmål?
- Vi ønsker å komme i kontakt med andre (eksterne, men også mulig interne) informanter med kunnskap og erfaring om tema. Har du noen forslag til andre vi kan intervjue i denne sammenheng?

Vedlegg B

Intervjuguide til ansatt i Finanstilsynet

Del 1.

- Presentasjon av studiens formål og fokus og studiens problemstilling
- Informasjon om taushetsplikt og informantenes anonymitet
- Signering av samtykkeskjema

Del 2.

Generelt

1. Hva er din stilling (tittel) og hva innebærer den?

Risiko knyttet til utkontrakteringsprosessen av IKT-tjenester

2. Kan du fortelle oss om din bakgrunn og erfaring med risiko knyttet til utkontraktering av IKT-tjenester?
3. Hva legger du i begrepet risiko?
4. Hvordan anser Finanstilsynet risikoen for ulike farer og tusler i norske finansforetak (relatert til utkontraktering av IKT-tjenester)?
5. Hvordan opplever Finanstilsynet at utkontraktering kan svekke robusthet og gi økt sårbarhet?

Styringsinstrumenter i forbindelse med utkontraktering

6. Hva opplever Finanstilsynet som utfordringene når det kommer til kontraktsinngåelse mellom innkjøper og IKT-leverandør?
7. Hvordan forholder Finanstilsynet seg til risiko ved tilsyn, og hvilke risikoer er det dere her tar høyde for?
8. Hvordan vurderes risikoene?
9. Hvordan opplever Finanastilsynet samarbeidet og informasjonsflyten med bank og finansforetak?

10. Hva mener Finanstilsynet bør gjøres for å kunne håndtere risikoen ved å utkontraktere IKT-tjenester på best mulig måte?

Lovverk og krav

11. På hvilken måte legger lovverket føringer for utkontrakteringsporsessen?
12. Hvilke lovkrav anser du som viktigst i forbindelse med utkontrakterte IKT-tjenester?
13. Hvilke erfaringer har Finanstilsynet med tilbakemeldinger fra finansforetak som blitt gjennomført tilsyn hos?
14. På hvilken måte arbeider dere med å påse at lovkrav og veiledninger ved utkontrakterte IKT-tjenester følges?
15. Er det noen faktorer som dere mangler i dagens lovverk (som burde vært inkludert)? Eller eventuelle uklarheter?
16. I hvilken grad mener dere lovverk og krav fungerer etter hensikt?

Del.3

- Noe informanten vil legge til som kan være av interesse for studien eller spørsmål?
- Vi ønsker å komme i kontakt med andre informanter med kunnskap og erfaring om tema. Har du noen forslag til andre vi kan intervjue i denne sammenheng?

Vedlegg C

Intervjuguide ansatt i universitets- og høyskolesektoren

Del 1.

- Presentasjon av studiets formål
- Informasjon om taushetsplikt og informantenes anonymitet
- Signering av samtykkeskjema

Del 2.

Generelt

1. Hva er din stilling og hva innebærer den?

Risiko knyttet til utkontrakteringsprosessen av IKT-tjenester

2. Kan du fortelle om din bakgrunn og erfaring relatert til utkontraktering av IKT-tjenester?
3. Hva anser du som risiko i en utkontrakteringskontekst? Og hva kjennetegner den?
4. Hvordan anser du risikoen for ulike farer og trusler i utkontrakteringsprosessen av IKT-tjenester, og hvilke farer og trusler anser dere som mest relevante?
5. Hvordan tenker du at utkontraktering av IKT-tjenester generelt kan svekke robusthet og gi økt sårbarhet?

Styringsinstrumenter i forbindelse med utkontraktering

6. Hvordan opplever du samarbeidet mellom innkjøper og leverandør IKT-tjenester gjennom utkontrakteringsprosessen?
7. Hva opplever du som kontraktsmessige utfordringer?
8. Hva tenker du er nyttige verktøy for å kunne styre risikoen som utkontrakteringen av IKT-tjenester representerer?

9. Hva mener du kan gjøres for å håndtere risikoene ved å utkontraktere IKT-tjenester på best mulig måte?
10. Hva anser du som utfordringene når det kommer til kontraktsinngåelse mellom innkjøper og leverandør?
11. Hvor tenker du at utfordringene ligger med å styre risikoen utkontraktering av IKT-tjenester medfører?

Lovverk og krav

12. På hvilken måte tenker du at lovverket legger føringer for leverandører av IKT-tjenester i en utkontrakteringsprosess?
13. Hvilke lovkrav anser du som viktigst i forbindelse med utkontrakterte IKT-tjenester?
14. Er det noen faktorer som du mener mangler i dagens lovverk (som burde vært inkludert)? Eller eventuelle uklarheter?
15. I hvilken grad mener du lovverket og krav fungerer etter hensikt?

Del 3.

- Er det noe informanten vil legge til som kan være av interesse for studien? Eller har informanten andre spørsmål?
- Vi ønsker å komme i kontakt med andre informanter med kunnskap og erfaring om temaet. Har du noen forsalg til andre vi kan intervjue i denne sammenhengen?

Vedlegg D

Informasjons- og samtykkeskjema til informanter

Vil du delta i forskningsprosjektet

"Risiko ved utkontrakteringsprosessen av IKT-tjenester i bank og finans"?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å se på risiko knyttet til utkontrakteringsprosessen av IKT-tjenester i bank- og finanssektoren. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Problemstillingen for masteroppgaven er «På hvilken måte representerer utkontrakteringsprosessen av IKT-tjenester risikoer for bank- og finanssektoren, og hvordan håndteres disse risikoene?»

Forskningsspørsmålene vi skal analysere omhandler hvilke type risikoer som oppstår, hvordan banken utarbeider risikostyringsinstrumenter i forbindelse med utkontraktering og på hvilken måte lovverk virker risikoreduserende for utkontrakteringsprosessen.

Hvem er ansvarlig for forskningsprosjektet?

Institutt for sikkerhet, økonomi og planlegging ved Universitetet i Stavanger (UiS) er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Du er invitert til å delta i prosjektet for å kunne bidra med relevant innsikt knyttet til risiko i forbindelse med utkontrakteringsprosessen av IKT-tjenester i bank og finans. Du kan bidra med kunnskap og erfaring som vil være relevant for vårt prosjekt.

Hva innebærer det for deg å delta?

Det vil benyttes dybdeintervjuer som vil ca. vare i 30-45 minutter. Opplysningene vi ønsker å samle inn handler som arbeidsoppgaver og hvordan du arbeider med risiko knyttet til

utkontrakteringsporsessen og relevant lovverk. For å få med all relevant informasjon så vil vi benytte oss av lydopptak.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

De som vil ha tilgang på lydopptakene som blir gjort er Elida Grønningsæter og Helene Gibbs.

Opptakene blir gjort med diktafon appen som tilhører Nettskjema. Nettskjema.no er Norges sikreste og mest brukte løsning for datainnsamling til forskning. Vi er ikke interessert i navn eller andre personopplysninger annet enn stillingstittel. Informanten vil derfor være anonymiserte og vil kun bli henvist til ved stillingstittel i oppgaven. Navn og andre kontaktopplysninger vil heller ikke være tilgengelig i lydopptakene.

Lagring av datamaterialet vil skje på via nettskjema der en trenger passord for å få tak i opptakene. Når prosjektet er ferdig, vil lydopptakene bli slettet.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Prosjektet vil etter planen avsluttes når oppgaven leveres, 15. juni 2023. Etter endt prosjekt vil lydopptakene slettes og de eneste opplysningene som vil være tilgjengelig er det som blir skrevet i masteroppgaven. Informasjonen som vil benyttes i oppgaven vil være anonymisert.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Stavanger har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende

- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Universitetet i Stavanger ved Ole Andreas Engen, ole.a.engen@uis.no , tlf. 92467852
- Vårt personvernombud: Rolf Jegervatn personvernombud@uis.no

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:

- Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen

Ole Andreas Engen

(Veileder)

Helene Gibbs og Elida Grønningsæter

(Studenter)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *risikoer ved utkontraktering av IKT-tjenester i bank- og finanssektoren*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i et personlig intervju
- ☐ at det vil bli tatt lydopptak på bånd
- ☐ at stillingstittel kan inkluderes i oppgaven

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Vedlegg E

Vurdering av behandling av personopplysninger fra Sikt

Referansenummer: 841865

Vurderingstype: Standard

Dato: 07.03.2023

Prosjekttittel: Risiko knyttet til utkontrakteringsprosessen av IKT-tjenester i bank og finans

Behandlingsansvarlig institusjon: Universitetet i Stavanger / Det teknisk-naturvitenskapelige fakultet / Institutt for sikkerheit, økonomi og planlegging

Prosjektansvarlig: Ole Andreas Engen

Student: Helene Gibbs

Prosjektperiode: 02.01.2023 - 15.06.2023

Kategorier personopplysninger

- Alminnelige

Lovlig grunnlag

- Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 15.06.2023.

Meldeskjema

Kommentar

Vår vurdering er at den planlagte behandlingen i dette prosjektet er lovlig, hvis den gjennomføres slik den er beskrevet i meldeskjemaet med dialog og vedlegg og vurderingen her.

OM VURDERINGEN

Sikt har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

FØLG DIN INSTITUSJONS RETNINGSLINJER

Vi har vurdert at du har lovlig grunnlag til å behandle personopplysningene, men husk at det er institusjonen du er ansatt/student ved som avgjør hvilke databehandlere du kan bruke og hvordan du må lagre og sikre data i ditt prosjekt. Husk å bruke leverandører som din institusjon har avtale med (for eksempel ved skylagring, nettspørreskjema, videosamtale eller liknende). Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

MELD VESENTLIGE ENDRINGER

Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Se våre nettsider om hvilke endringer du må melde: https://sikt.no/melde-endringar-i-meldeskjema

OPPFØLGING AV PROSJEKTET

Vi vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet. Lykke til med prosjektet!