Handelshøyskolen BI

MAN 50151 Governance; risikostyring, compliance og internrevisjon

Term paper 60% - W

Predefinert informasjon

Startdato:	13-09-2021 09:00	**Termin:**	202210
Sluttdato:	20-05-2022 12:00	**Vurderingsform:**	Norsk 6-trinns skala (A-F)
Eksamensform:	P		
Flowkode:	202210||10117||IN17||W||P		
Intern sensor:	(Anonymisert)		

Deltaker

Navn: Henning Blixt Tiller

Informasjon fra deltaker

Tittel *:	Utkontraktering av IKT-tjenester, styring og kontroll
Navn på veileder *:	Flemming T. Ruud

Inneholder besvarelsen konfidensielt materiale?:	Nei	**Kan besvarelsen offentliggjøres?:**	Ja

Gruppe

Gruppenavn:	(Anonymisert)
Gruppenummer:	20
Andre medlemmer i gruppen:	Deltakeren har innlevert i en enkeltmannsgruppe

Prosjektoppgave

ved Handelshøyskolen BI

Utkontraktering av IKT-tjenester, styring og kontroll

Eksamenskode og navn:

MAN 50151 Governance; risikostyring, compliance og internrevisjon

Innleveringsdato:
20.05.2022

Studiested:
BI OSLO

Innholdsfortegnelse

Innhold

Sammendrag

Bank og finansbransjen får stadig flere lover og regler som må følges, både nasjonalt og fra EU. Det er i forbindelse med økt digitalisering innen bransjen sett nødvendig med økt regulering når det gjelder utkontraktering av tjenester innen IKT.
I denne oppgaven vil jeg se nærmere på utfordringer med å følge opp regelverk innen utkontraktering av IKT-tjenester og forsøke finne ut av hva som gjør at dette er krevende.

Innledningsvis vil jeg beskrive hva utkontraktering defineres som, og hvilke avgrensninger som er gjort i denne oppgaven, samt videre forklare hvilke regulatoriske rammeverk som gjør seg gjeldene. Dette for at leseren skal forstå hvor store mengder kunnskap som skal innehas for å kunne være compliant på området.

Videre vil det beskrives verktøy som kan benyttes som rammeverk i virksomheter for å kunne ha en god risikostyring. Jeg vil her beskrive COSO og ISO27001. COSO fordi det er et at de mest anerkjente rammeverkene, og ISO27001 fordi det er et rammeverk som i stor grad kan være et praktisk verktøy for å være compliant i forhold til utkontraktering. Selv om det er mange lover og regler for utkontraktering, så er det ingen av disse som forklarer praktisk gjennomføring. Det vil også være en forskjell i tolkning av lover og regler sett fra Finanstilsynet sitt ståsted og de ulike virksomhetene.

Som grunnlag for analyse av data, vil det bli brukt sekundærdata fra offentlige kilder og foretatt en kvantitativ og kvalitativ analyse for å få innsikt i «hvor skoen trykker» hos virksomheter som har hatt tilsyn fra Finanstilsynet.

Innledning

Det er utkontraktering når et foretak velger å la en annen juridisk enhet (oppdragstaker) utføre oppgaver på vegne av foretaket. Dette gjelder også når foretaket er i samme konsern eller i konsernlignende gruppe som oppdragstaker. (Finanstilsynet, Rundskriv 7/2021, s 4, 2021).

Det er en antakelse at det er en krevende oppgave å følge opp utkontraktering og at det er for lite styring og kontroll på dette. Jeg vil i denne oppgaven forsøke finne ut av om dette er korrekt, og eventuell årsak til dette.

De senere år har det vært en økende tendens at selskaper innen bank og finans utkontrakterer tjenester for å redusere kostnader, øke fleksibilitet og effektivitet. Sett i lys av økende digitalisering og den økende viktigheten av IT og finansiell teknologi (fintech), tilpasser selskaper innen bank og finans sine forretningsmodeller, prosesser og systemer til å omfatte slike teknologier. Tjenester innen IT har blitt det mest vanlige å outsource til underleverandører. Sett bort i fra alle fordeler, så har outsourcing av IT og datatjenester en sikkerhetsmessig risiko og utfordrer risiko og kontrollrammeverk for selskaper, spesifikt på internkontroll, datahåndtering og datasikkerhet.
Tillit til stabilitet rundt systemer for bank og finans er kritisk for korrekt funksjonalitet, og en forutsetning hvis det er systemer som bidrar til økonomien i samfunnet som helhet.
Effektiv intern kontroll er fundamentalt hvis selskaper individuelt og som helhet med andre parter skal fungere på en god måte (EBA, Guidelines on outsourcing arrangements, s6, 2019).

Den økende tendensen til å utkontraktere, spesielt IT-tjenester har vært grunnlag for at Den Europeiske Banktilsynsmyndighetet, EBA har utarbeidet retningslinjer for utkontraktering av tjenester, EBA Guidelines On Outsourcing Arrangements som ble publisert i 2019.

I Norge er retningslinjene fra EBA på utkontraktering ivaretatt i Finanstilsynet sitt Rundskriv 3/20, Veiledning om utkontraktering, som siden er erstattet av Rundskriv 07/21, Veiledning om utkontraktering.

Ettersom det også har blitt mer vanlig med sky-løsninger, hvor data og/eller programvare ikke driftes på selskapers egne fysiske servere, men hvor drift av systemer og lagring av data kan befinne seg geografisk hvor som helst i verden, ser man et økt kontrollbehov for å ivareta sikkerhet, og at drift av systemer er tilstrekkelig stabilt.

Finanstilsynet gir noen eksempler på hva som er utkontraktering av IKT-tjenester

- Hvis foretaket har programvare på egen server, men setter bort driften av serveren til en oppdragstaker, innebærer dette utkontraktering av IKT-virksomhet.
- Avtale om rett til bruk av programvare, plattform og/eller infrastruktur (IKT- systemer og -tjenester) som driftes av oppdragstaker på oppdragstakerens servere, anses som utkontraktering av foretakets IKT-virksomhet. Som eksempler på dette nevnes:
- A. Iaas (Infrastructure as a Service)
- B. Paas (Platform as a Service)
- C. SaaS (Software as a Service)

  Bruk av Iaas, PaaS eller SaaS, innebærer at foretaket også utkontrakterer driften, behandlingen og/eller oppbevaringen av data som registreres i forbindelse med bruken av slike programvarer og tjenester (Finanstilsynet, Rundskriv 7/2021, 2020, s. 5)

I tillegg er det regulatoriske krav til utkontraktering i diverse sektorregelverk som eksempelvis Finanstilsynsloven, Internkontrollforskriften, Meldepliktforskriften, Hvitvaskingsloven samt IKT-forskriften.

Selv om utkontraktering av tjenester også omhandler visse tjenester som ikke er IKT-relatert så gjelder dette et fåtall og jeg vil i denne oppgaven forholde meg til tjenester som gjelder IKT. Dette fordi det er IKT-tjenester som i dag sees som krevende å overholde regelverk og det vil gi et bedre grunnlag for innsikt å bruke

data som gir informasjon om oppfølging av underleverandører på IKT. I data som benyttes i denne oppgaven er det heller ikke nevnt oppfølging på annet enn IKT-tjenester.

Utkontraktering og lovverket

Avtaler om utkontraktering blir regulert i flere regelverk. I Forskrift om risikostyring og internkontroll §5. Utkontraktering, beskrives det slik: Foretaket har ansvar for risikostyring og internkontroll også der deler av virksomheten er utkontraktert. Det skal foreligge en skriftlig avtale som sikrer dette. Avtalen må sikre at foretaket gis rett til innsyn i og kontroll med utkontraktert virksomhet. I Forskrift om meldeplikt ved utkontraktering av virksomhet mv. blir det spesifisert i §1. Samlet oversikt over avtaler om utkontraktering, at alle foretak som er omfattet av finanstilsynsloven §1 skal ha en oppdatert oversikt over alle avtaler om utkontraktering av virksomhet, og som viser til finanstilsynsloven §4, første ledd i forhold til hva oversikten skal inneholde.

- Navn og organisasjonsnummer på oppdragstaker
- Virksomheten/oppgavene som utkontrakteres
- Oppdragstaker driver virksomhet i Norge, i norsk selskap, i filial eller som grensekryssende virksomhet. Dersom oppdragstaker er etablert i utlandet skal det også opplyses hvilket land foretakets hovedkontor er etablert i navn og organisasjonsnummer på underleverandører som oppdragstaker bruker ved utførelse av oppgaver på vegne av foretaket. Dersom underleverandør er etablert i utlandet bes det opplyst hvilket land
- Avtalens oppstarts- og opphørsdato, herunder opplysninger om rullerende avtaleperiode
- Hvordan foretaket vil følge opp sitt ansvar for den utkontrakterte virksomheten, samt foretakets risikovurdering av utkontrakteringen.

I tillegg er det beskrevet spesifikt angående utkontraktering av IKT-virksomhet som også skal inneholde:

- Utkontrakteringsavtalen med vedlegg

- Styremøteprotokoll hvor det fremgår at styret har behandlet utkontrakteringsavtalen og risikovurdering av utkontrakteringen.

I Forskrift om risikostyring og internkontroll §5. Utkontraktering, er det beskrevet slik:
Foretaket har ansvar for risikostyring og internkontroll også der deler av virksomheten er utkontraktert. Det skal foreligge en skriftlig avtale som sikrer dette. Avtalen må sikre at foretaket gis rett til innsyn i og kontroll med utkontraktert virksomhet (Forskrift om risikostyring og internkontroll §5, 2022). Videre er det også spesifisert i Finanstilsynsloven §4 c. at alle foretak som inngår nye eller endrer avtale med oppdragstaker skal melde dette til Finanstilsynet 60 dager før iverksettelse av avtale eller avtaleendring (Lov om tilsynet med finansforetak mv. §4c, 2021).

For å illustrere omfanget av regelverk som må følges og forstås i sammenheng med utkontraktering, vil jeg her gi en oversikt over det mest vesentlige som vil gjelde banker og utkontraktering av IKT-tjenester.

Relevante lover/forskrifter

- Lov om tilsynet med finansforetak mv.(finanstilsynsloven)
- Lov om finansforetak og finanskonsern (finansforetaksloven)
- Forskrift om kapitalkrav og nasjonal tilpasning av CRR/CRD IV
- Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)
- Forskrift om risikostyring og internkontroll
- Forskrift om meldeplikt ved utkontraktering av virksomhet mv.

Relevante rundskriv og publikasjoner

- Modul for operasjonell risiko (Finanstilsynet, 2016)
- Rundskriv 1/2020, Vurdering av egnethetskrav (Finanstilsynet)
- Rundskriv 07/2021, Veiledning om utkontraktering (Finanstilsynet)
- Rundskriv 15/2009, Rapportering av IKT-hendelser til Kredittilsynet (Finanstilsynet)
- Rundskriv (2008), Veiledning for gjennomføring av risiko- og sårbarhetsanalyser, (Finanstilsynet)

- EIOPA-BoS-20/600, Guidelines on information and communication technology security and governance
- EIOPA-BoS-20-002, Guidelines on outsourcing to cloud service providers
- EBA/GL/2019/02, EBA Guidelines on outsourcing arrangements
- ESMA35-36-2319/EBA/GL/2021/06 Guidlines on the assessment of suitability

Ovennevnte lover og rundskriv vil som nevnt i hovedsak være de som gjelder for banker og utkontraktering av IKT. I tillegg ved annen utkontraktering kan flere lover og rundskriv kunne gjøre seg gjeldene, som for eksempel arbeidsmiljøloven, hvitvaskingsloven, personopplysningsloven og tilhørende rundskriv.

Internkontroll, compliance og ansvar

Styrets og daglig leders ansvar

Styret er ansvarlig for at virksomheten drivers i samsvar med lover og forskrifter. Daglig leder har ansvar for å etablere en forsvarlig risikostyring og internkontroll på bakgrunn av de retningslinjer og den risikoappetitt styret fastsetter (IIA Norge, Veileder for Compliancefunksjonen, 2015, s. 8). Dette kommer også frem i Forskrift om risikostyring og internkontroll §3 Styret skal påse at foretaket har hensiktsmessige systemer for risikostyring og internkontroll.

Norsk utvalg for eierstyring og selskapsledelse (NUES) beskriver det i sin anbefaling at, styret skal påse at selskapet har god intern kontroll og hensiktsmessige systemer for risikostyring i forhold til omfanget og arten av selskapets virksomhet (Norsk utvalg for eierstyring og selskapsledelse, 2022).

Et styre skal altså sørge for den overordnede styringen av virksomheten og ivareta virksomhetens interesser. De skal gjennomføre beslutninger og sørge for tilsyn og kontroll.

For et styre vil det være naturlig å inneha kunnskap om relevante lover og regler som gjelder for virksomheten, og sørge for å oppdatere seg om endringer og praktisering av disse. Hvis et styre feiler med å følge med på endringer i regulatoriske forutsetninger kan det i ytterste konsekvens føre til erstatningsansvar, bøter og straff.

I forbindelse med Daglig leder eller toppledelsens ansvar blir det ofte trukket frem uttrykket «Tone at the top», altså hvor etisk og hvor mye integritet en organisasjon har (Anderson U. , et al.).Uttrykket beskriver altså at holdningene og handlingene fra ledelsen setter standarden for ansatte i organisasjonen når det gjelder å ha en kultur for etikk og integritet rundt intern kontroll og risikostyring. Ledelsen bør altså ha et ambisjonsnivå for intern kontroll som videreføres til mellomledelse og videre til linjen, samt sørge for tilstrekkelige ressurser og kompetanse slik at man har tilstrekkelig kontroll.

Compliancefunksjon

De fleste virksomheter, spesielt innen bank, finans og pensjonsvirksomhet har krav til å overholde og følge et utall lover og regler. Avhengig av størrelse og bransje kan det også være krav til å inneha en compliancefunksjon eller complianceansvarlig.

Ordet compliance har ikke et direkte oversatt norsk ord, men ifølge Norsk Språkråd kan man benytte for eksempel ordene etterleving, regeletterleving eller regeloppfylling som såkalt avløserord på norsk (Språkrådet, 2022).

IIA Norge beskriver compliance på den måten at det innebærer etterlevelse av både eksternt og internt regelverk (IIA Norge, Veileder for Compliancefunksjonen, 2015, s. 5), og beskriver viktigheten av overholdelse av regulatoriske krav. Svikt i rutiner på overholdelse av regulatoriske krav vil føre til økt operasjonell risiko, altså økt risiko for svikt i prosesser knyttet til virksomhetens drift. I praksis vil det eksempelvis føre til økt risiko for svikt i systemer som virksomheten benytter.

Sett opp mot utkontraktering vil det være vesentlig at man har god oversikt over regulatoriske krav og at man har kontroll på at dette er ivaretatt i eksempelvis IT-styringssystemer virksomheten benytter.

Det er ulik praksis på hvordan compliancefunksjonen blir plassert organisatorisk, sett ut ifra type virksomhet og størrelse på virksomheten. I noen tilfeller er det også vanlig å outsource funksjonen, og kjøpe inn denne tjenesten fra for eksempel eksterne konsulentselskap. Dette gjøres hvis virksomheten er veldig liten, eller at de har avdelinger i andre land etc.

IIA Norge presiserer at det som er viktig er at compliancefunksjonen må være tillagt en uavhengighet fra linjen, og ha mulighet til å rapportere direkte til ledelse og styre. Normalt innen bank og finans vil compliance befinne seg i den såkalte andrelinjen, men med mulighet for direkte rapportering til toppleder og styre.

De tre forsvarslinjer

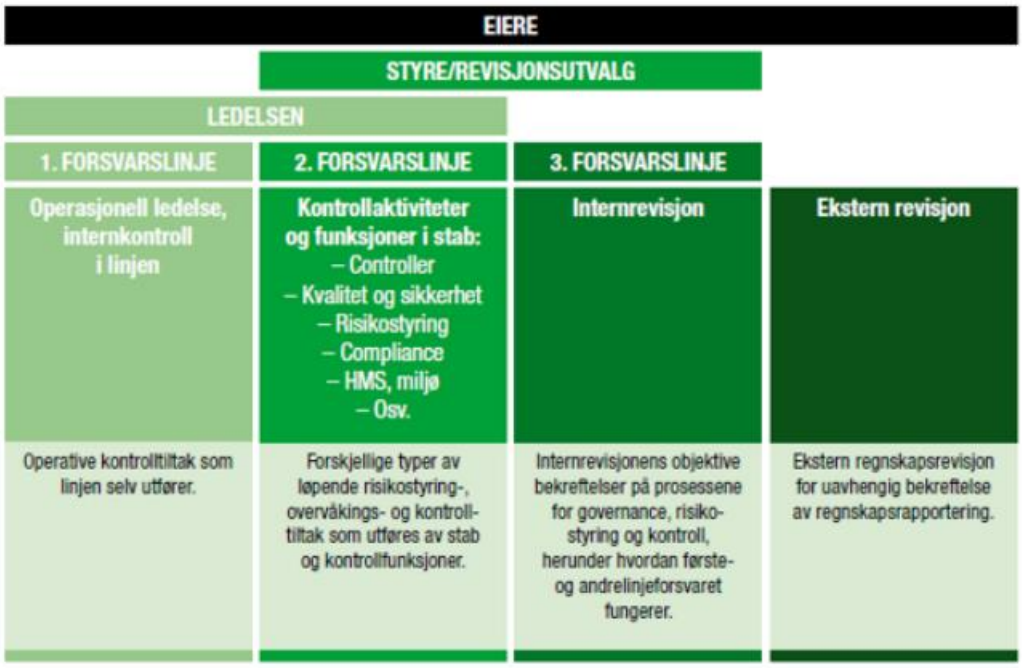
Som en del av styrets og daglig leders ansvar, er det å ha en hensiktsmessig organisering av roller i forhold til kontrollaktiviteter som utføres for å redusere risiko viktig.

For å sikre effektiv ressursutnyttelse, som å unngå at noen aktiviteter ikke er gjenstand for tilfredsstillende kontroll eller duplisering av funksjoner og aktiviteter rettet mot risikostyring og internkontroll. Er det viktig å definere roller og ansvar for de ulike funksjonene på en tydelig måte. Modellen med «de tre forsvarslinjene», gir en oversikt over roller og ansvar for internkontroll og risikostyring på et overordnet nivå, på en enkel og effektiv måte (IIA Norge, Veileder for Compliancefunksjonen, 2015, s. 5).

Modellen viser forslag til en kontrollstruktur for en virksomhet og skille mellom tre grupper som er involver (figur 1)t:

- Første forsvarslinje, som eier og håndterer den operative risiko, og gjennomfører aktiviteter for å identifisere, vurdere, kontrollere og følge opp risiko og gjennomfører korrigerende tiltak hvis nødvendig.
- Andre forsvarslinje, overvåker, veileder og bidrar til å forbedre og rapportere førstelinjekontrollene gjennom å utføre egne kontrollaktiviteter. Andrelinjen har internkontroll som sitt hovedområde.
- Tredje forsvarslinje, utøves av internrevisjonen som gir styrende organer og toppledelsen en høyere grad av uavhengig og objektiv bekreftelse på internkontrollen i virksomheten enn andrelinjen.

Det presiseres at klare mandater og stillingsbeskrivelser er viktig for å kunne skille de ulike funksjonene fra hverandre og hva de har ansvar for.



Figur 1 (IIA Norge, Veileder for Compliancefunksjonen, 2015, s. 7)

Det kan argumenteres for at det er noen svakheter ved denne modellen, på den måten at det forenkler virkeligheten. Virksomheter kommer i mange forskjellige former og med ulike behov. Sett i lys av at alle funksjoner i en virksomhet også bør jobbe for å oppnå virksomhetens strategi vil det også kunne nevnes at terminologien «forsvar» mulig har en negativ vinkling, og at de klare skillene i kategoriene ikke er en modell som oppfordrer til samarbeid på tvers.

Egnethetsvurdering

Felles for styret, daglig leder og nøkkelfunksjoner i finansforetak er at de skal egnethetsvurderes. Egnethetsvurdering går ut på at personer som besitter en av disse rollene skal ha tilstrekkelig erfaring og utdanning samt at det er visse kriterier til økonomiske forhold og adferd som må vurderes for at Finanstilsynet skal godkjenne en vurdering.

Kjernen i egnethetskravene er at vedkommende skal ha den nødvendige kompetansen til å utøve stillingen eller vervet og at vedkommende ikke er dømt for et straffbart forhold eller har utvist en adferd som gir grunn til å anta at stillingen eller vervet ikke vil bli ivaretatt på en forsvarlig måte (Finanstilsynet, Rundskriv 1/2020 Vurdering av egnethetskrav, 2020).

Compliance ansees som en nøkkelfunksjon, og ansatte i denne rollen må også egnethetsvurderes.

Det er vesentlig at personer i nevnte roller skal inneha nødvendig kompetanse, men det er ikke presisert at i et styre så må hver enkelt ha fullstendig kompetanse om lover og regler, men at styrets medlemmer til sammen skal inneha nødvendig kompetanse for å ivareta styrets ansvar.

Etiske overveielser

Etikk er den gren av filosofien som undersøker hva som er rett og hva som er galt, og som setter normer og prinsipper for riktig handling (Filosofi.no, 2022).

Etikk er mer enn lover og regler som er nedfelt i lover og forskrifter. Etikk omhandler holdninger og valg som utføres i en virksomhet i gitte situasjoner. Derfor har ofte virksomheter egne etiske retningslinjer som skal ivareta hvilke holdninger som utvises og valg som foretas i ulike situasjoner, hvor det eksempelvis kan stå om valg mellom å tjene penger eller å bryte regler.

For et styre og daglig leder vil man kunne hevde at det er et spørsmål om etikk i forhold til om det er god nok kontroll på utkontrakterte avtaler. Hvis det ikke er god nok oppfølging og kontroll og dette skulle føre til ulempe for kunder av virksomheten, kan man hevde at de ansvarlige i virksomheten ikke har tilstrekkelig etiske retningslinjer for sitt ansvar.

Finans Norge som er finansnæringens hovedorganisasjon med 240 medlemsbedrifter, har utarbeidet «Finansnæringens etikkplakat».

Punkt nummer 1 på denne er «Løse samfunnsoppdraget på en måte som ivaretar hensynet til alle bedriftens interessenter» (Finans Norge, Finansnæringens Etikkplakat, 2022).

Teori Internkontroll, risikostyring og rammeverk

Definisjon av rammeverk

Et rammeverk er en mengde veiledende prinsipper som danner en mal som organisasjoner kan evaluere en rekke forretningspraksiser mot. Disse prinsippene består av ulike begreper, verdier, forutsetninger og praksiser som er ment å gi en referanse som en organisasjon kan vurdere eller evaluere en bestemt struktur, prosess eller miljø mot, eller en gruppe praksiser eller prosedyrer (Anderson, et al., 2017).

Det finnes flere ulike rammeverk eller standarder man kan benytte for å utarbeide god praksis på internkontroll og risikostyring. Jeg vil her i denne oppgaven ta for meg COSO-rammeverket som er et internasjonalt og anerkjent rammeverk for risikostyring og internkontroll, samt ISO27001 som er internasjonal standard for rammeverk som spesifikt gjelder IT-systemer.

COSO-rammeverket

En av de mest anerkjente rammeverkene for internkontroll er Internal Control – Integrated Framework (COSO), utgitt av the Committee of Sponsoring Organizations of the Treadway Commission.

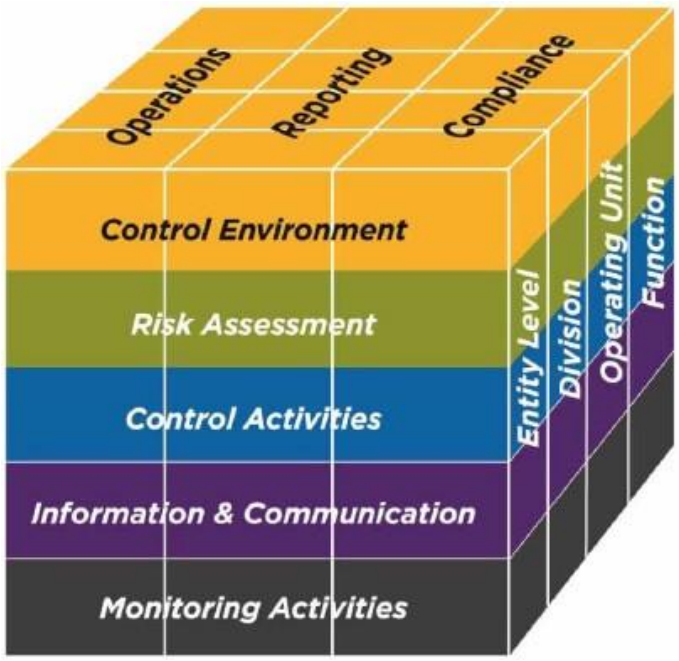
COSO rammeverket er anerkjent som et av det ledende rammeverket for å designe, iverksette og utføre intern kontroll, samt vurdering av effektiv internkontroll (Committee of Sponsoring Organizations of the Treadway Commission, 2013-2014, s. 1).

COSO definerer internkontroll som en prosess som utføres av en enhets styre, ledelse og annet personell, utformet for å gi rimelig forsikring om oppnåelse av mål knyttet til drift, rapportering og etterlevelse (Committee of Sponsoring Organizations of the Treadway Commission, 2013-2014, s. 5) .
Hensikten med å benytte et slikt rammeverk vil være å ha en mal for å redusere risiko for å ikke oppnå mål virksomheten har satt, samt å oppnå god kvalitet, overholdelse av lover og regler og sikre effektiv drift. Man vil altså finne akseptabel risikoappetitt og toleranse og implementere dette i god operasjonell risikostyring som støtter oppunder virksomhetens mål som er bestemt av ledelse og styre.

Videre beskriver COSO at definisjonen er ment å beskrive at internkontroll sett fra COSO sin beskrivelse å omfavne fem punkter:

- Rettet mot oppnåelse av mål
- Pågående oppgaver og aktiviteter
- Menneskelig utførelse
- Tilføre rimelig sikkerhet
- Kunne tilpasses selskapets struktur

COSO har beskrevet en modell for internkontroll for å støtte opp om at organisasjoner skal nå sine mål (Figur 2).



Figur 2 (Committee of Sponsoring Organizations of the Treadway Commission, 2013-2014, s. 5)

Den første dimensjonen av det COSO refererer til som de tre kategorier av mål ledelsen og organisasjonen har i flg COSO rammeverket er:

- Operasjonelle mål
- Rapportering
- Compliance

Operasjonelle mål i følge COSO relaterer til oppnåelse av organisasjonen eller enhetene innen organisasjonen sin etablerte visjon og misjon. Målene vil variere basert på ledelsens valg av driftsmodell, bransjehensyn og prestasjon.
COSO beskriver også at sikring av ressurser bør være en del av operasjonelle mål, det vil si at man beskytter enhetenes ressurser. Ressurser kan være eksempelvis systemer og hvordan man sørger for å redusere risiko for feil eller tap i noen form.

Rapportering viser til rapporter som brukes av organisasjonen og interessenter. Rapportering kan omhandle både finansielle og ikke-finansielle rapporter, samt rapporter for intern og ekstern bruk.
Interne rapporter vil i stor grad være utviklet for å kunne tilfredsstille interne krav, spesielt i forhold til prestasjon, og for å overvåke at man følger strategisk retning.

Sett opp mot denne oppgaven beskriver COSO ekstern ikke finansiell rapportering, vil dette være rapporter som spesifikt omhandler informasjon som for eksempel overholdelse av lover, regler, standarder eller andre forpliktende rammeverk innen bransjen man opererer.
Videre beskriver COSO rammeverket at det er ledelsen, i samarbeid med styret som beslutter rapportenes mål når organisasjonen behøver tilstrekkelig forsikring om oppnåelse av organisasjonens mål.

Mål for compliance er den tredje kategorien av mål for enheter i organisasjonen, og beskriver at enheter i organisasjonen må utføre aktiviteter som ivaretar at lover og regler blir overholdt. Som en del av å spesifisere disse aktivitetene, må man forstå hvilke lover, regler og andre reguleringer som gjelder for enhetene. Som eksempel nevner COSO lover og regler knyttet til eksempelvis skatt, HR og miljø. Som en kommentar her sett opp mot oppgavens problemstilling, kan man nevne at ettersom det er vanlig å lagre data i skyløsninger, vil det være en antatt problematikk for mange organisasjoner at de ikke har kontroll på hvilket land data er lagret, noe som er en aktuell problemstilling i forhold til Shrems II dommen (DigDir, Hva er Schrems II dommen, 2022) hvor det settes lovmessige føringer for lagring av norske data i USA.

De fem komponentene beskrevet av COSO for å støtte oppunder at organisasjonen skal nå sine mål er:

- Kontrollmiljø, menneskene i virksomheten, kunnskap, integritet og etiske verdier i virksomheten.
- Risikovurdering, identifisere og utarbeide analyse på risikoer som eksisterer i tilknytning til virksomheten, og hvilke konsekvenser dersom noen av risikoene inntreffer.
- Kontrollaktiviteter, aktiviteter for å håndtere risikoer som kan hindre virksomhetens måloppnåelse, rutiner for risikohåndtering.
- Informasjon og kommunikasjon, sikre at ledelsen tar ansvar for å kommunisere mål og visjon for virksomheten, samt viktighet av god risikostyring og i tillegg fordele ansvar og beskrive klare roller.
- Overvåkningsaktiviteter, sikre at rutiner og prosesser fungerer gjennom kontinuerlig vurderinger, gjennomføre endringer ved behov og rapportere

videre i organisasjonen. (Committee of Sponsoring Organizations of the Treadway Commission, 2013-2014, ss. 12-14)

Den tredje dimensjonen av kuben representerer enhetene i organisasjonen, som for eksempel produksjon, markedsføring, salg og andre funksjoner avhengig av hva slags type organisasjon det skulle gjelde

COSO-rammeverket spesifiserer at et system for internkontroll aldri kan være fullstendig, men at et effektivt system gir rimelig sikkerhet for oppnåelse for sikring av enhetenes mål, men ikke absolutt sikkerhet.

ISMS, ISO/IEC 27001 og 27002

ISMS er et styringssystem for informasjonssikkerhet, og er en forkortelse for det engelske begrepet «Information Security Management System».
Informasjonssikkerhet i en bedrift handler om å håndtere risiko relatert til informasjonsverdier og behandlingen av data. Uavhengig av hvordan data lagres, må de beskyttes på en god måte.

Det finnes flere slike styringssystemer, men ISO27001 er det som er mest kjent og hvor man kan få en offisiell sertifisering ved å gjennomføre punkter fra standardene.
At man har et styringssystem for informasjonssikkerhet betyr at man skaper en struktur i selskapet som lar ressurser ivareta informasjonssikkerheten i bedriften. Et slikt styringssystem inneholder prosedyrer, sjekklister, sertifikater, policyer, standarder og aktivitetsplaner.

International Organization for Standardization (ISO), er en uavhengig, privat organisasjon som jobber med å lage internasjonale standarder som skal beskrive «best practice» på utførelse av en rekke ting. Organisasjonen er et samarbeid mellom organisasjoner i mer enn 160 land som bidrar til å forbedre og distribuere standarder. ISO utarbeider standarder, såkalt ISO-standarder som beskriver best practice på eksempelvis prosesser innen helse, produktutvikling, kvalitet, mat-sikkerhet og IT-sikkerhet.

Standardene blir i de fleste tilfeller først utarbeidet og godkjent av ISO med innspill fra organisasjoner og forskere verden over, for så å bli tilpasset Den europeiske standardiseringsorganisasjonen i Brussel. Videre i noen tilfeller blir standarder også oversatt og tilpasset enkeltland. ISO standard 27001 og 27002 finnes i norsk utgave. Tittelen i standarden ISO refererer altså til at den er utarbeidet av organisasjonen ISO, mens IEC henviser til at det er den europeiske versjonen av standarden.

ISO/IEC 27000-serien er en standard for ISMS-system, og inneholder en rekke standarder som har til hensikt å sikre virksomheters informasjon og ha et system for dette. Etter hvert som enkeltpersoner, organisasjoner og samfunnet gjør seg mer avhengig av fungerende IT-systemer, er det viktig at man har et bevisst forhold til alle mulige trusler som medfører andre virkninger enn de man vil ha (Standard Norge, IT-sikkerhet - ISO/IEC 27000, 2022).

ISO/IEC 27001 er en spesifikk standard utarbeidet som et ledelsessystem for å ha krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et system for informasjonssikkerhet, mens ISO/IEC 27002 er en mye brukt standard som omhandler sikringsteknikker av informasjonsteknologi, standarden inneholder detaljert beskrivelse av praktisk IT-sikkerhetsarbeid.

ISO/IEC 27001

ISO/IEC 27001 inneholder 114 sikkerhetstiltak, klassifisert i 14 kategorier, blant annet innen personalsikkerhet, tilgangskontroll m.m. ISO/IEC 27001 inneholder ingen beskrivelse av hvordan dette gjennomføres, kun en beskrivelse av selve tiltakene som skal være på plass. Beskrivelsen av hvordan man kan iverksetter de ulike sikkerhetstiltakene finnes i ISO/IEC 27002.
Implementering og benyttelse av ISO/IEC 27001 som rammeverk for ISMS gjøres i 4 faser (Wikipedia - ISO / IEC 27001, 2022):

1. Etableringsplan
2. Implementeringsfase
3. Vedlikeholdsfase

4. Forbedringsfase

Etableringsplan: Her bestemmer man målene for ISMS, og dette deles inn i fire trinn.

Trinn 1: Definer virkeområdet og anvendelsesområde for omfanget av ISMS. Her må man da inkludere alle punkter i ISO/IEC 27001 hvis man skal kunne oppnå sertifisering. Det må også inkludere alle vesentlige eiendeler virksomheten har som er involvert i virksomhetens ISMS. Retningslinjer for hvilket sikkerhetsnivå man vil praktisere må utarbeides, retningslinjene og nivået på sikkerhetsnivå må stå i forhold til de vurderte risikoene.

Trinn 2: Identifiser og vurder sikkerhetsrisiko og etablere sikkerhetspolitikk. Standarden gir ikke retningslinjer for hvilken risikovurderingsmetode man skal benytte, slik at virksomheten står fritt til å bruke metode.

Trinn 3: Behandle risikoen og identifiser gjenværende risiko gjennom en forvaltningsplan. Det er fire mulige behandlinger for hver av de identifiserte risikoene

1. Unngåelse: Hvis risikoen er uakseptabel, velger man å eliminere risiko totalt. Eksempelvis fase ut et system.
2. Reduksjon: Risikoen reduseres til et akseptabelt nivå ved gjennomføring av tekniske og organisatoriske tiltak.
3. Overføring: Den delen av risikoen som ikke kan unngås, altså restrisikoen etter tiltak, overføres til en 3. part eller man tegner en forsikring for å redusere den økonomiske risikoen.
4. Aksept: Man iverksetter ikke ytterligere sikkerhetstiltak fordi konsekvensene av risikoen er akseptabel.

Trinn 4: Velg sikkerhetstiltak. Når alle risikovurderinger er utført og man har besluttet risikotoleranse, implementerer man sikkerhetstiltak iht. ISO-standard for å redusere og kontrollere risiko. Spesifikke tiltak og beskrivelse av dette finner man i ISO/IEC 27002.

Implementeringsfase: Implementeringsfasen har fire stadier

1. Etablere en risikobehandlingsplan
2. Implementere sikkerhetstiltak

3. Generere indikatorer, herunder indikator for om sikkerhetstiltak er effektive og om overholdelse gjør det mulig å vite om ISMS er i samsvar med spesifikasjonene
4. Trene og utdanne personalet

Vedlikeholdsfase: Dette består i den daglige administrasjon av ISMS, og oppdatere hendelser for å reagere raskt. Tre verktøy kan benyttes.

1. Intern kontroll, som består i å kontinuerlig sikre at prosesser fungerer som de skal
2. Interne revisjoner som bekrefter styringssystemets samsvar og effektivitet, både ad hoc og planlagte revisjoner.
3. Vurderinger som med jevne mellomrom garanterer at ISMS er tilstrekkelig med omgivelsene.

Forbedringsfase: Implementere korrigerende, forebyggende eller forbedringshandlinger for hendelser og avvik som er blir observert i vedlikeholdsfasen. Her vil man ha korrigerende tiltak for avvik for at det ikke skal gjenta seg, forebyggende handlinger for å handle før hendelser treffer og forbedringshandlinger for å forbedre ytelsen til ISMS-prosessen.

Begrensninger ved internkontroll og rammeverk

COSO beskriver noen forutsetninger som gjøres gjeldene for at et rammeverk skal ha en forutsetning for å fungere etter hensikten. Det ene er at en svak prosess på utvelgelse av styremedlemmer i en virksomhet, vil føre til en begrensning i muligheten til å ha tilstrekkelig oversikt over internkontrollen. Altså det vil ikke hjelpe å ha et rammeverk, når styret i virksomheten ikke har tilstrekkelig kompetanse. Tilsvarende vil det ved svakheter i strategi, slik som lite spesifisert strategi, urealistisk strategi eller uegnede mål svekke forutsetningene for at rammeverkene vil kunne ha en effektiv nytteverdi (Committe of Sponsoring Organizations of the Treadway Commission, 2013, s.138).

Videre beskriver COSO noen andre svakheter ved rammeverket som ikke nødvendigvis dekkes fullverdig av rammeverket. Menneskelig vurdering er alltid

en faktor og rammeverkets betydning vil være avhengig av dette. Eksterne hendelser kan påvirke målene, systemer kan bryte sammen ved for eksempel fraværende personell, ledelse kan overstyre kontrollaktiviteter og det kan også være tilfeller av misligheter hvor ansatte går sammen og samarbeider om å skjule relevante rapporter (Committe of Sponsoring Organizations of the Treadway Commission, 2013, s 139)

Metode

Formål

Jeg vil her beskrive nærmere målet ved oppgaven og hvordan valg av metode, design, innsamling av data, samt om feilkilder og svakheter ved valg av metode.

Målet med denne oppgaven er å finne ut av hvorfor virksomheter ikke har tilstrekkelig kontroll på sin utkontrakterte virksomhet. Kontroll på utkontraktering beskrives i flere lovregler, rammeverk og offentlige veiledere. Likevel er det ut ifra egen observasjon, og i samtaler over årene med kolleger fra bank og finansbransjen en antakelse at det er veldig krevende å ha fullstendig kontroll over utkontrakterte tjenester foretakene benytter. Antatte årsaker kan være mangel på kunnskap, mangel på ressurser, feil ansvarsfordeling, feil prioritering eller annet, noe som jeg vil forsøke finne ut av i denne oppgaven. For å komme nærmere en hypotese vil gjennomgang av kildene som benyttes være grunnlag for å beskrive hva som avdekkes i forhold til antakelser til årsak.
Selv om mangel på oppfølging av utkontraktert virksomhet vil påvirke både compliance, altså å følge opp lover og regler samt risikoprofilen til foretak omtaler jeg her i denne oppgaven som overholdelse av compliance, da å overholde regelverket er en forutsetning for å kunne foreta korrekte risikovurderinger.

Forskningsdesign

For å finne riktig metode for å finne svar på årsak til hvorfor det er krevende å følge opp utkontraktert virksomhet er det viktig å finne tilstrekkelig data på emnet og spesielt da på det som ikke fungerer optimalt, for å systematisere dette for videre analyse.

For å ha den riktige fremgangsmåten må man gå systematisk til verks. Det kan være nødvendig med forskjellige fremgangsmåter for å besvare de enkelte undersøkelsesspørsmålene som er relevante for et bestemt analyseformål. Undersøkelsesdesignet innebærer en beskrivelse av hvordan hele analyseprosessen skal legges opp for at man skal kunne løse den aktuelle oppgaven. Her er det spesielt viktig å vite hvilke typer data man trenger, hvordan disse dataene skal skaffes til veie, og hvordan de skal analyseres (Silkoset, Olsson, & Gripsrud, Metode, dataanalyse og innsikt, 2021, s. 68)

Valget av design avhenger av hvor mye vi vet om et område, og hvilke ambisjoner vi har med hensyn til å analysere og forklare sammenhenger (Silkoset, Olsson, & Gripsrud, Metode, dataanalyse og innsikt, 2021, s. 69).
Det er vanlig å skille mellom tre hovedtyper av design.

- Eksplorerende design
- Deskriptivt design
- Kausalt design

Ved eksplorerende design vil noe av det primære målet med designet på undersøkelsene være å få bedre innsikt og utvikle hypoteser om mulige sammenhenger. En naturlig start i et eksplorerende design er å undersøke om det er skrevet noe om temaet, og om det foreligger data samlet inn av andre, såkalte sekundærdata. Ofte vil det også være aktuelt med visse former for egen datainnsamling (primærdata) (Silkoset, Olsson, & Gripsrud, Metode, dataanalyse og innsikt, 2021, s. 69).
Deskriptivt design krever grunnleggende forståelse av problemområdet som skal utforskes, dette inkluderer å beskrive en enkelt variabel eller en relasjon mellom to eller flere variabler. Når man beskriver en kontekst som inkluderer to eller flere variabler, er det fristende å diskutere dem i tilknytning til årsak og effekt. Med en deskriptivt design har vi imidlertid ingen basis for å kunne påstå at det er en kausal sammenheng. Vi kan bare påstå at variablene endrer seg samtidig på en systematisk måte, noe vi kan referere til som korrelasjon. Vi kan med andre ord ikke påstå at den ene variabelen fører til en endring i den andre variabelen. Så kun

systematisk relatert (Silkoset, Olsson, & Gripsrud, Metode, dataanalyse og innsikt, 2021, s. 72).
Kausalt design bruker an når man ønsker å finne en statistisk årsakssammenheng (kausalitet) mellom to variabler (Sander, 2022).

I denne oppgaven finner jeg det hensiktsmessig å benytte eksplorerende design. Dette med grunnlag i at det finnes få kilder for primærkunnskap tilgjengelig, og at det er antatt utfordrende å få ærlige svar ved eventuelle intervjuer, eller å få noen til å svare på spørsmål da det vil være brudd på taushetsplikt. I tillegg kan det avdekke kritiske svakheter ved drift av virksomheten.

Primær eller sekundærdata

I forbindelse med å finne data og informasjon om temaet, vil det være hensiktsmessig å vurdere om man skal benytte primær eller sekundærdata. Primærdata er nye data som er samlet inn av den eller de som lager undersøkelsen. Sekundærdata er samlet inn av andre (Cappelen Damm, Begrepsbank, 2022).

I forhold til primærkildedata, så kan man anta at direkte intervju og spørsmål som nevnt vil være krevende. Det ene er hvem i bedriften skal man intervjue?
I utgangspunktet burde man intervjue styret som har øverste ansvar, men det vil være risiko for at man kun får overfladiske svar og ikke harde fakta, da de mest sannsynlig bare mottar rapporter, og kvaliteten på rapportene vil avgjøre hvor dyp innsikt i oppfølging av utkontraktering de innehar.
I tillegg vil det være et relativt ømtålig tema å spørre direkte, selv med lovnad om anonymitet, vil antakelsen være at man ikke vil få helt oppriktige svar. Dermed vil det ha liten verdi sett opp mot ønske om å forstå hvorfor det er krevende å følge opp utkontraktert virksomhet, og kjernen i hva som er krevende ved dette.

Slik det er nevnt vurdert vil primærdata være relativt krevende å få samlet inn, og validitet og reliabilitet vil være hensiktsmessig å vurdere i forhold til de to typer kilder.
Derfor er målet å få bedre innsikt og finne hypoteser om mulige sammenhenger når det gjelder svak oppfølging av utkontraktert virksomhet ved bruk av

sekundærdata fra offentlige kilder, da man kan legge til grunn at dette vil være korrekte data som ikke har annet formål enn å dokumentere sannheten.

Validitet og reliabilitet

Dataene som hentes inn for analyse bør ha så god validitet og reliabilitet som mulig for å kunne gi god nok innsikt for å kunne trekke hensiktsmessige konklusjoner.
Validitet dreier seg om hvor godt vi måler det vi har til hensikt å måle. Reliabiliteten refererer til konsistensen på det vi måler (Silkoset, Olsson, & Gripsrud, Metode, dataanalyse og innsikt, 2021, s. 87). Validitet vil altså beskrive hvor gode dataene vi måler vil være, mens reliabiliteten sier noe om konsistensen og stabiliteten av på dataene.

Kvantitativ og kvalitativ data

Kvantitative data er informasjon som enkelt kan måles, mens kvalitative data er informasjon som er beskrivende og ikke nødvendigvis målbart.
Disse to forskningsmetodene er ikke i konflikt med hverandre, men utfyller hverandre (SurveyMonkey, Forskjellen mellom kvantitative og kvalitative undersøkelser, 2022).
I denne oppgaven vil jeg benytte kvalitative data fra offentlige kilder for få dypere innsikt for så å forsøke å kvantifisere variabler som igjen kan benyttes for å forstå sammenhenger.

Teorier og relevant litteratur

Det er vanlig innen bank og finans, at man følger med på rapporter fra Finanstilsynet for å følge trender på hvilke tilsyn som er aktuelle, og hvilke tilbakemeldinger tilsynet kommer med til virksomheter. I bransjen oppfatter man tilbakemeldinger i disse rapportene som signaler fra Finanstilsynet på hvilke forventninger de har og hvordan de tolker regelverk. Dette for å kunne følge opp internt i egen virksomhet mangler man kan identifisere, eller tolkninger av regelverk som i noen tilfeller kan tolkes forskjellig fra Finanstilsynet sitt perspektiv, og i den enkelte virksomhet.

Det er også tilfelle at Finanstilsynet og lovgivende makt har tolket lover og regler forskjellig, noe som igjen kan skape rom for misforståelser når banker og andre finansforetak skal følge nye og endrede regelverk.
I forhold til tilsyn så gjennomfører Finanstilsynet i noen tilfeller «tematilsyn». Det er spesielt interessant når Finanstilsynet utfører såkalte tematilsyn, hvor de har et spesifikt tema for tilsyn som de gjennomfører over et kortere tidsrom i flere tilsvarende virksomheter. Dette gir god innsikt for utenforstående å forstå hvordan konkurrenter overholder regler, hvordan de er organisert og ikke minst hvordan Finanstilsynet tolker lover og regler ut ifra de tilbakemeldingene de gir. Denne informasjonen er som oftest offentlig tilgjengelig, kun i noen tilfeller blir rapportene fra tilsyn sensurert til en viss grad.

For å finne ut om det finnes relevant litteratur i forhold til den aktuelle problemstillingen har jeg tatt utgangspunkt i et tematilsyn fra 2016/2017 hvor Finanstilsynet hadde tematilsyn ved 7 banker. Tematilsynet gjaldt Operasjonell risiko og rapportering av hendelser, og ble publisert 11.07.2017 på Finanstilsynet sine hjemmesider. Formålet med tilsynet var å vurdere bankenes styring og kontroll av operasjonell risiko. Tilsynet hadde i hovedsak søkelys på hendelsesrapportering, det vil si rapportering av uønskede hendelser som inntreffer og kan påføre foretaket tap.
Dette er relevant ettersom utkontraktering er beskrevet som en del av Modul for operasjonell risiko, utgitt av Finanstilsynet i januar 2016. Her blir det i kapittel 2.3 presisert aktuelle vurderingsmomenter som virksomheten må ta i betraktning ved utkontraktering, ettersom utkontraktering kan gi økt eller endrede risikoer.

Finanstilsynet oppgir følgende aktuelle vurderingsmomenter:

- Ansvar kan ikke utkontrakteres, foretaket er ansvarlig for risikostyring og internkontroll også av evt. utkontrakterte deler av virksomheten, jf. finansforetaksloven § 13-4 (3), risikostyringsforskriften § 5 og IKT-forskriften § 12.
- Styret bør fastsette interne retningslinjer for utkontraktering. Retningslinjene bør inkludere rutiner for melding til Finanstilsynet før inngåelse av avtaler om utkontraktering, jf. finanstilsynsloven § 4c.

- Utkontraktering forutsetter en skriftlig avtale som sikrer innsyn, kontroll og revisjon av den utkontrakterte virksomheten, også for Finanstilsynet.
- Avtaler om utkontraktering bør godkjennes av styret og sikre rimelig rett til oppsigelse av avtalen under betryggende forhold til alternativ løsning er etablert. Avtaler om utkontraktering av IKT-systemer som er av betydning for foretakets virksomhet (og endringer i slike) skal behandles av styret, jf. IKT-forskriften § 2. Beslutning om utkontraktering skal tas på grunnlag av en risikovurdering. Foretaket må selv ha kompetanse til å vurdere om oppdragstaker utfører oppdraget tilfredsstillende. Oppdragsgiver må fortløpende ha mulighet til å identifisere og kontrollere de risikoene som er knyttet til utkontraktering av oppgavene (Finanstilsynet, Modul for operasjonell risiko, 2016, s. 8).

Videre har jeg på Finanstilsynet sine hjemmesider funnet 23 tilsynsrapporter fra tidsrommet 26.05.2020 til 04.03.2022 som har temaer som vil omfatte tilsvarende tematilsynet fra 2016/2017.

Datainnsamling

Rapport for tematilsyn

Tematilsynet hadde tilsyn hos følgende foretak under tematilsynet. Dnb Bank ASA, Skue Sparebank, SpareBank 1 Nord-Norge, SpareBank1 SR-Bank ASA, Sparebanken Sør, Sparebanken Vest og Totens Sparebank.
Det var da totalt 7 stykker, og kun banker.
En oppsummering av tilbakemelding fra Finanstilsynet var:

- Forbedringspotensial på registrering av hendelser og anvende dette i risikovurderinger
- Underrapportering av hendelser
- Manglende policy og rutiner, mangler rammeverk for beredskapsplaner og utkontraktering
- Organisering, compliancefunksjonen er satt som ansvarlig for oppfølging av hendelser. Samt at compliancefunksjonen i flere tilfeller også har annet ledende ansvar som for eksempel juridisk og forretningsutvikling
- Mangler ved rapportering til ledelse, styre og myndigheter

- Lite fokus fra internrevisjon på operasjonell risiko
- Ikke tilstrekkelige ressurser og kompetanse

Av tilbakemeldinger her som er relevant for oppgaven, er at det blir påpekt manglende rutiner for utkontraktering. Ettersom de i rapporten ikke spesifiserer hvem det gjelder så er det utfordring å vite om det gjelder en eller alle. Men på et ett annet punkt som gjelder definisjoner av hendelser, presiseres det at det kun er ett foretak som har dette i orden. Derfor kan man anta at ingen av foretakene har rutine for utkontraktering på plass.

Finanstilsynet påpeker at holdninger fra styret og toppledelsen er avgjørende for risikostyringen ("tonen fra toppen"), og at en forutsetning for en sterk kultur er at mellomledelsen viderefører og tydeliggjør holdningene fra toppledelsen.
Det viktigste signalet Finanstilsynet gir etter tematilsynet er at de forventer at bankene tar operasjonell risikostyring mer på alvor. Det vil si at man har en god "tone fra toppen" som videreføres av mellomledelsen, og har dokumentert ambisjonsnivå og risikotoleranse i sine styrende dokumenter.
I tillegg må man sikre tilstrekkelige ressurser og kompetanse slik at man klarer å benytte operasjonell risikostyring og registrering av hendelser slik at man kan benytte dette til kontinuerlig forbedring (Pwc, Finansbloggen, 2017).

Tilsynsrapporter, enkeltrapporter 2020-2022

For å kunne se utviklingen fra tematilsynsrapporten har jeg videre gått gjennom 23 tilsynsrapporter som er tilgjengelig på Finanstilsynet sine hjemmesider (Finanstilsynet, Nyhetsarkiv, 2022).
Tilsynsrapportene har til felles at de enten har vært omfattet av tematilsyn for IT eller tilsyn som omfatter «Forhold knyttet til styring og kontroll». Disse rapportene er relevante fordi de vil kunne fortelle noe om overholdelse av regelverk for utkontraktering.
For å kvantifisere funn Finanstilsynet har gitt tilbakemelding på har jeg kategorisert tilbakemeldingene på mangler med treff i fire kategorier:

1. Vurdering av oppdragstaker. Vurdering av oppdragstaker viser til kapittel 5 i Veiledning om utkontraktering, hvor det beskrives krav til at foretak

må gjøre en vurdering av oppdragstaker og underleverandører før noe kan utkontrakteres.

2. Utkontrakteringsavtale. Beskrives i kapittel 6. Det er krav til at det foreligger en skriftlig avtale og selve kravene til innholdet i avtalen foretaket har med underleverandør.
3. Risikostyring og internkontroll. Kapittel 8 i veiledningen som beskriver styrets og daglig leders ansvar rundt risikostyring, organisering og tiltak og kontrollfunksjoner ved utkontraktering.
4. IKT forskrift. Viser til tilbakemeldinger fra Finanstilsynet, hvor de påpeker mangler ved overholdelse av Forskrift om bruk av informasjons- og kommunikasjonsteknologi.

Videre analyse av funn i disse kategoriene vil altså beskrives nærmere i ved analyse av disse dataen.

Analyse av data

Kvalitativ analyse, rapport for tematilsyn

Dette viser, selv om det er få antall banker hvor Finanstilsynet har vært på tilsyn at det jevnt over er konkrete mangler på en klar strategi, manglende rapportering, uklar organisering og svak oppfølging av utkontraktert virksomhet. Det er svært få av punktene på tilbakemelding fra Finanstilsynet som nevner at det gjelder «enkelte banker», slik at manglene som nevnes kan antas å gjelde flertallet.
Det skal da være mulig å anta at andre virksomheter innen bank og finans ville gå gjennom rapporten fra Finanstilsynet og måle dette opp mot egen virksomhets praksis på området, og da revidere interne rutiner, organisering og annet som er nødvendig for å overholde retningslinjer.
Ettersom rapporten er fra 2017, kan man anta at mange virksomheter ikke hadde tilpasset seg tilstrekkelig til retningslinjene som var relativt nye på tidspunktet for tilsyn, selv om mange av punktene i retningslinjene kun er presisering eller utdypning av allerede eksisterende lovverk.

Av foretakene som var gjenstand for tilsyn i 2016/2017 var det to av disse som igjen hadde tilsyn i hhv 2021 og 2022, som var Dnb Bank og Sparebank1 SR-Bank.
I tilsynsrapporten fra Sparebank1 SR-Bank oppgis det at det er mangler når det gjelder å utføre en god nok konsekvensanalyse for vurdering av utkontrakterte oppgaver, og mangler på god nok rutine for kriseberedskap som omfattes av rutine for oppfølging av underleverandør. Banken har dermed mangler på to av punktene fra kategoriene jeg har lagt opp til for å kvantifisere mangler. Ved å lese rapporten nærmere oppgir Finanstilsynet at de vurderer rutinene til banken som gode, men at de etterlyser at banken deler rutine rundt konsekvensanalyse med underleverandører. Dette kan man tolke dithen at det egentlig ikke er en alvorlig mangel hos banken, men mer en presisering fra Finanstilsynet som banken bør ta inn i sine rutiner. Det er altså en god forbedring fra tematilsyn i 2016/2017, hvor tilbakemeldingen var at det var manglende policy og rutiner og manglende rammeverk for beredskapsplaner og utkontraktering.

Dnb Bank hadde to tilsyn i 2021, ett på overordnet styring og kontroll som gjaldt Dnb ASA og ett IT-tilsyn som gjaldt Dnb sin filial i London.
Tilsynsrapporten til Dnb ASA fra 30.04.2021 avviker fra de andre rapportene i utvalget på den måten at rapporten oppgis å være et oppfølgingstilsyn fra et tidligere tilsyn i 2018, hvor det ble avdekket vesentlige mangler ved overholdelse av hvitvaskingsregelverket. Rapporten beskriver da i hovedsak ikke konkret noen av de 4 punktene for kvantifisering valgt i oppgaven, men påpeker likevel mangler ved organisering og ressurser samt vesentlige mangler i kompetanse og complianceoverholdelse. Dermed vil det kunne regnes under mangler når det gjelder risikostyring og internkontroll, at det ikke er tilstrekkelig vurdering rundt organisering. Det kan også nevnes at tilsynsrapporten fra 2018 igjen var en oppfølging fra et tilsyn i 2017, hvor formålet i utgangspunktet var å føre tilsyn ved bankens overholdelse av anti-hvitvaskingsregelverk. Slik det leses har altså tilsynet hatt et ekstra fokus på dette regelverket ut ifra tidligere tilsyn når de gjennomførte tilsyn i 2021, noe som preger rapporten og derfor ikke så konkret beskriver forhold til underleverandører. Det skal også sies at Dnb har få underleverandører, da de lager mange av systemene selv, men ettersom det er et

konsern vil det mest sannsynlig foreligge en del konserninterne avtaler som vil ha samme krav når det gjelder utkontraktering og oppfølging.

Ved Dnb sin filial i London og rapporten som er publisert 06.09.2021, er temaet tilsyn av styring og kontroll med IT-virksomheten, og med spesiell vekt på samhandlingen mellom konsern og filial.
Rapporten viser at selskapet har mangler på kategori 1 og 2 i kategoriene som er valgt for denne oppgaven. Mer spesifikt blir det påpekt mangler ved risikovurdering av oppdragstaker, mangler ved kontroll på tilgangsstyring samt oppfølging av avtaler med underleverandører. Det blir påpekt at Dnb Filialen som får leveranser fra IT i Dnb konsern har mer eller mindre overlatt all vurdering og oppfølging av underleverandører til IT konsern. Slik det bør fungere er at Dnb Filial burde hatt kontroll på underleverandører som er en 3. part i flg retningslinjer, selv om dette blir ivaretatt i konserninterne avtaler med avtalte kriterier. Dette fører også til at Dnb Filial ikke har kontroll på hvem hos 3. part som har hvilke tilganger på systemene de benytter. Sett opp mot tidligere tematilsyn, er det da gjentakende at det mangler gode rutiner for oppfølging av utkontraktert virksomhet. Det som kan være verdt å merke seg her, er nok at ettersom det er et konsern, har det antakelig vært kultur for modellen som har vært benyttet ved at det er IT konsern som styrer det som gjelder IT. Det er presisert i Veiledning om utkontraktering kapittel 3, at det er definert som utkontraktering når et foretak velger å la en annen juridisk enhet utføre oppgaver på vegne av foretaket. Dette gjelder også når foretaket er i samme konsern.

Kvalitativ og kvantitativ analyse tilsynsrapporter, enkeltrapporter 2020-2022

Finanstilsynet har i de forskjellige rapportene ulik fremgangsmåte og struktur for hvordan rapporten er utarbeidet, slik at en del av arbeidet har vært å finne den relevante informasjonen for denne oppgaven ved å lese gjennom rapportene. Felles for alle rapportene er at de i en eller annen form gir informasjon om mangler i forhold til overholdelse av regelverk som skal ivareta utkontraktering. Selv om det i stor grad er mye likheter i rapportene på hva de har kontrollert, er det noen forskjeller i temaene som har vært mål for tilsyn. Likevel var det i alle

rapportene med unntak av en, gjort kontroller i forhold til styring og kontroll som omhandler om selskapene har tilfredsstillende kontroll på utkontraktering og underleverandører.

Jeg finner det her derfor hensiktsmessig å først kvantifisere funn etter de fire kategoriene oppgitt under Datainnsamling, for videre å gå i dybden på rapportene for å få mer detaljert informasjon om hvilke tilbakemeldinger på mangler de forskjellige virksomhetene har mottatt fra Finanstilsynet (Vedlegg 1).

Figur 3 viser en oversikt over antall selskaper og hvilke kategorier de har fått tilbakemelding på avvik fra Finanstilsynet, samt sum av hvor mange kategorier de har avvik.

Selskap	Kategori 1	Kategori 2	Kategori 3	Kategori 4	Sum
1	0	0	1	0	1
2	0	1	1	0	2
3	0	0	1	0	1
4	0	1	0	0	1
5	1	1	0	1	3
6	1	1	0	0	2
7	1	0	0	1	2
8	0	0	1	1	2
9	1	0	1	1	3
10	1	1	1	1	4
11	1	1	1	1	4
12	0	1	1	1	3
13	0	0	0	1	1
14	1	1	1	0	3
15	1	0	1	0	2
16	1	0	1	0	2
17	1	0	0	0	1
18	0	1	0	1	2
19	1	0	0	1	2
20	1	0	1	0	2
21	1	0	1	0	2
22	0	0	1	0	1
23	0	0	0	1	1
Sum	13	9	14	11	

Figur 3

Av de 23 selskapene som har hatt tilsyn så er det 100% som har mangler i en eller flere kategorier, slik at man kan konstatere at ingen av selskapene har tilstrekkelig kontroll ifølge Finanstilsynet.

Som figur 4 viser, er det flertallet av selskapene som har mangler i 2 av kategoriene, mens færrest har mangler i alle kategoriene.
Det som peker seg ut her er da de selskapene som har 2 og 4 brudd på overholdelse av kriterier.

Brudd på overholdelse av kriterier av antall kategorier	Antall selskaper	Prosent av utvalg
0	0	0 %
1	7	30 %
2	10	43 %
3	4	17 %
4	2	9 %
Sum	23	100 %

Figur 4

Kategorien hvor flest av selskapene har fått tilbakemelding på mangler er kategori 3 (figur 5), som viser til kapittel 8 i Veiledning om utkontraktering, hvor selskapene da har fått påpekt mangler ved styrets og daglig leders ansvar, organisering og tiltak/ kontrollfunksjoner rundt utkontraktering.
Kategori 1 og 4 har bemerkning på rundt halvparten av utvalget, mens kategori 2 på tilnærmet 40%.

	Kategori 1	Kategori 2	Kategori 3	Kategori 4
Antall selskap	13	9	14	11
% av utvalg	57 %	39 %	61 %	48 %

Figur 5

Videre fremgangsmetode som velges er da å gå gjennom tilsynsrapporter og gi en konklusjon på mangler og eventuelle relevante observasjoner og kommentarer som kan gi noe informasjon angående årsaker til mangler.
Først vil jeg gi en noe fyldigere oppsummering fra tilsyn hos foretakene som hadde mest treff, da det i rapportene fra Finanstilsynet er veldig tydelig hva som er årsaken til at foretakene ikke følger opp utkontraktering. Rapportene fra Finanstilsynet er ikke likt strukturert og formulert, slik at beskrivelse av mangler og tilbakemeldinger fra Finanstilsynet varierer både i tekst og tone. Jeg finner det derfor hensiktsmessig å konkludere med en rotårsak som ansees å være hovedårsaken til at foretaket i tilsynsrapporten har måttet svare for mangler.

Gjennomgang av tilsynsrapporter for selskaper med 4 treff:

Harstad kommunale pensjonskasse og Høland og Setskog Sparebank er de i analysen som har flest treff i antall kategorier, og er de foretakene som har mottatt rapporter med mest negativ tilbakemelding fra Finanstilsynet.

Harstad kommunale pensjonskasse sin rapport fra 25.06.2020 (Finanstilsynet, Tilsynsrapport 19/6137, 2020), så viser Finanstilsynet til manglende strategi og retningslinjer generelt. Pensjonskassen sitt strategidokument var fra 2016, og ikke revidert siden. Dette ser ut til å henge sammen med organiseringen, da pensjonskassen i praksis ikke har en egen daglig leder, men leier inn en ressurs fra annen pensjonskasse til 50% stilling. Denne personen har allerede en 100% stilling i annen pensjonskasse.
Pensjonskassen har outsourcet det meste av drift til underleverandører, men har etter hva rapporten beskriver minimum med innsikt hos underleverandørene, og kontraktene ivaretar heller ikke krav til at Finanstilsynet skal kunne føre tilsyn med underleverandører.
På tidspunktet tilsynet ble gjennomført var pensjonskasser enda ikke omfattet i Finansforetaksloven av krav til uavhengig kontrollfunksjon på gjeldende område (kun kapitalforvaltning), noe som har blitt tatt inn i Finansforetaksloven i 2022.

Høland og Setskog Sparebank hadde tilsyn (Finanstilsynet, Tilsynsrapport 21/3377, 2021) som gikk direkte på overholdelse av IKT-forskriften når det

gjelder kontinuitetsledelse. Det vil si å sikre drift ved forretningskritiske uønskede hendelser.
Banken kjøper IT-tjenester av Eika Gruppen, som er en tjenesteleverandør på systemer og produkter til små og mellomstore banker. Eika Gruppen eier få eller ingen systemer selv, men kjøper igjen tjenester fra andre leverandører, som de administrerer og tilbyr videre til selvstendige banker. Dette innebærer blant annet kjernebanksystem, som er kritisk infrastruktur for banker.
Rapporten viser at banken i stor grad ikke følger opp noen av de forpliktelser de har som selvstendig bank, men har overlatt dette fullt og helt til Eika Gruppen. Det bekreftes også i rapporten at de ikke har ressurser som har tilstrekkelig kompetanse, men at de vil sørge for å tilegne seg dette i samarbeid med Eika Gruppen.

Selskaper med 3 treff:
Selskaper i denne kategorien er Credicare, Gjeldsregisteret AS og Invento Kapitalforvaltning

Credicare AS (Finanstilsynet, Tilsynsrapport 20/6760, 2021)
Konklusjon: Selskapet er en del av et konsern. Morselskapet har tatt seg av utkontraktering, og selskapet har ikke hatt egen oppfølging.

Gjeldsregisteret AS (Finanstilsynet, Tilsynsrapport 21/2981, 2021)
Konklusjon: Heleiet datterselskap av TietoEvry AS, få ansatte, ikke tilstrekkelig med ressurser.

Invento Kapitalforvaltning (Finanstilsynet, Tilsynsrapport 20/9363, 2022)
Konklusjon: Organisering av compliancefunksjonen. Compliancefunksjonen har ansvaret for en rekke linjeoppgaver i tillegg. Styret mottar ikke tilstrekkelig med rapporter, samt at Styret ikke ser ut til å forstå kravene i regelverket for utkontraktering.

Selskap med 2 treff

Convene Collection, Dnb Bank Filial London, Eiendomsmegler 1, Experian, Molde kommunale pensjonskasse, MP Pensjon, Odin Forvaltning, Søgne og Greipstad Sparebank, Sparebank1 og Storebrand Livsforsikring.

Convene Collection AS (Finanstilsynet, Tilsynsrapport 20/6670, 2021)
Konklusjon: Selskapet er en del av et konsern. Morselskapet har tatt seg av utkontraktering og selskapet har ikke hatt egen oppfølging fra selskapets egen ledelse.

Dnb Filial London (Finanstilsynet, Tilsynsrapport 19/13577, 2021)
Konklusjon: Selskapet er en del av et konsern. Filialen har ikke egen oppfølging og har overlatt alt til morselskapet.

Eiendomsmegler 1 Midt Norge (Finanstilsynet, Tilsynsrapport 20/7332, 2021)
Konklusjon: Tilbakemelding fra Finanstilsynet på at rutiner ikke omfatter på foretaksnivå, kun på konsernnivå.

Experian Gjeldsregister AS (Finanstilsynet, Tilsynsrapport 21/5133, 2021)
Konklusjon: Experian Gjeldsregister AS er en del av Experian-gruppen. Selskapet har kun 4 ansatte og har ingen oppfølging fra morselskapet, og ingen interne rutiner.

Molde kommunale pensjonskasse (Finanstilsynet, Tilsynsrapport 21/308, 2021)
Konklusjon: Blanding av roller mellom arbeidsgiverforetak og pensjonskasse. Ikke tilstrekkelig kompetanse hos Styret.

MP Pensjon (Finanstilsynet, Tilsynsrapport 19/12784, 2020)
Konklusjon: Blanding av roller mellom arbeidsgiverforetak og pensjonskasse, ikke tilstrekkelig kompetanse hos Styret.

Odin Forvaltning AS (Finanstilsynet, Tilsynsrapport 21/3736, 2021)
Konklusjon: Manglende kompetanse hos Styret og ikke tilstrekkelig IT-kompetanse.

Søgne og Greipstad Sparebank (Finanstilsynet, Tilsynsrapport 21/3380, 2021)
Konklusjon: Selskapet er en del av en allianse med andre banker, og har overlatt ansvar om utkontraktering til alliansen. Styret har ikke kompetanse i tilstrekkelig grad for å forstå krav til IT-området.

Sparebank1 SR-Bank (Finanstilsynet, Tilsynsrapport 21/1606, 2021)
Konklusjon: Mangler i organisering og rollebeskrivelser, ingen ansvarlig MIM (Major Incident Manager) for alvorlige IT-hendelser. Styret har manglende kunnskap om regelverk og gjennomføring.

Storebrand Livsforsikring (Finanstilsynet, Tilsynsrapport 20/4656, 2021)
Konklusjon: Mangler i organisering og rollebeskrivelser. CISO organisert i 1. linjen, men utfører kontrollfunksjoner for 2. linjen på konsernnivå. Compliance og Risk er organisert i konsern, kontrollaktiviteter blir bestemt fra konsern og ikke eget foretak. Finanstilsynet mener internrevisjonen burde vært involvert i arbeidet med involvering og vurdering av konsekvenser på innføring av ny policy for informasjonssikkerhet, «Information Security Management System» (ISMS)

Selskap med ett treff
Aker Pensjonskasse, Dnb Bank ASA, Bergen kommunale pensjonskasse, Kommunalbanken AS, Norsk Gjeldsinformasjon, Trondheim kommunale pensjonskasse og Vipps AS.

Aker Pensjonskasse (Finanstilsynet, Tilsynsrapport 20/12217, 2021)
Konklusjon: Blanding av roller mellom arbeidsgiverforetak og pensjonskasse. Manglende ressurser og kompetanse om utkontraktering og IKT generelt.

Dnb Bank ASA (Finanstilsynet, Tilsynsrapport 19/12479, 2021)
Konklusjon: Mindre relevant da hele rapporten kun omtaler oppfølging av hvitvaskingsstilsyn. Eneste tilbakemeldingen som er relevant er kommentar på uhensiktsmessig organisering av compliancefunksjon

Bergen kommunale pensjonskasse (Finanstilsynet, Tilsynsrapport 19/11247, 2020)

Konklusjon: Knapphet på ressurser og manglende kompetanse både ved Styret og daglig ledelse.

Kommunalbanken AS (Finanstilsynet, Tilsynsrapport 19/8411, 2021)
Konklusjon: Gir svar til Finanstilsynet at leverandøren deres ikke er pliktig til å overholde IKT-forskriften selv om de har utkontraktert en tjeneste. Styret mangler kompetanse på IT og utkontraktering.

Norsk Gjeldsinformasjon (Finanstilsynet, Tilsynsrapport 21/4834, 2021)
Konklusjon: Manglende kompetanse hos Styret og daglig leder. Norsk Gjeldsinformasjon er et selskap som eies i fellesskap av flere banker, blant annet Dnb, Nordea, Sparebank1 og Eika-Gruppen.

Trondheim kommunale pensjonskasse (Finanstilsynet, Tilsynsrapport 20/419, 2021)
Konklusjon: Manglende uavhengighet fra arbeidsgiverforetak. Rutine egnethetsvurdering sist oppdatert 2014. Vesentlig avtaleforhold til en underleverandør sist vurdert i 2009. Manglende kompetanse i Styret.

Vipps AS (Finanstilsynet, Tilsynsrapport 21/808, 2021)
Konklusjon: Mindre foreslåtte rettelser fra Finanstilsynet når det gjelder kriseberedskap, eller er rapporten i hovedsak en oppfølging av tidligere tilsyn på anti-hvitvasking.

Konklusjon

Kravene til å ha kontroll på utkontraktert virksomhet er mange, og befinner seg i flere lovverk, moduler og retningslinjer. Både norske regelverk, og EU-regelverk. Man kan konkludere med at regelverket er uoversiktlig og det er krevende å kunne inneha all kompetanse på området.

I tillegg til alt regelverk, er det også rom for tolkninger slik at selv med full forståelse av regelverket vil det være nyanser av tolkning som vil gi en variasjon i overholdelse av regelverket. Dette kommer klart frem i tilsynsrapportene, hvor Finanstilsynet eksempelvis påpeker at en virksomhet ikke har delt sin kriseplan med underleverandør, selv om det ikke står i noe regelverk at dette er et krav.

I tillegg blir regelverk kontinuerlig oppdatert, og nye tekniske løsninger ser dagens lys og må håndteres praktisk av virksomhetene. Som eksempel er det nå mer og mer vanlig med såkalte skyløsninger, hvor all lagring av data for virksomhetene er lagret hos en leverandør. Dette skaper nye utfordringer og krever kunnskap for å følge opp, og det er ikke gitt at styremedlemmer besitter denne kunnskapen.
Selv om det finnes mye regelverk å forholde seg til, så er det lite materiale tilgjengelig for hvordan man praktisk skal gjennomføre overholdelse av regelverket.

Når det gjelder reliabiliteten på dataene så er det åpenbart at tilsynsrapportene mangler en enhetlig struktur. Rapportene ser i noen tilfeller ut til å være påvirket av tidligere tilsyn hos samme virksomhet, eller av temaer som har vært aktuelle på tidspunktet. Tilsynene er også utført av ulike personer fra Finanstilsynet, så man kan anta at de besitter ulik kunnskap, og har ulik fremgangsmåte. Likevel siden fokuset i denne oppgaven gjelder utkontraktering, vil jeg kunne anta at de har benyttet grunnleggende lover og retningslinjer som grunnlag for tilsynet. Jeg vil derfor konkludere med at tilsynet er gjennomført på en stabil måte, men at konsistensen er variabel. Dette vil i den kvantifiserte delen av analysen tilsi at det kan være svak reliabilitet, men den kvalitative delen vil likevel gi godt innblikk, da man kan se variasjonen i hvor spesifikke og alvorlige tilbakemeldingene fra tilsynet er.
Ettersom antakelsen er at lovverket er likt for alle kontroller, vil man kunne argumentere for at gjennomgangen av kildene som er tilsynsrapportene, at det vil være en gjennomsnittlig sannhet i dataene og funnene som er gjort.
Formålet med datakildene som er benyttet, er å kunne «måle» avvik hos finansinstitusjoner som gjelder utkontraktering. Validiteten vil avhenge av hvor

detaljert vi ønsker å måle, altså hva er godt nok grunnlag for å kunne gjøre en konklusjon.

Validiteten i datagrunnlaget antas også være noe redusert på den måten at form og fremgangsmåte på rapportene varierer. Likevel sees det som at man kan trekke gyldige slutninger om det som var formålet med undersøkelsen.

Dette ville være meningsfullt å gå mer i dybden, men som nevnt er tilsynsrapportene utformet på forskjellige måter, så det vil antatt skape dårligere validitet. Et eksempel er at tilsynet kun i to av rapportene nevner at foretakene ikke er compliant med IKT-forskriften §12 som omhandler utkontraktering, mens de samtidig har gitt tilbakemelding til andre foretak i datagrunnlaget på at utkontraktering ikke følges opp, men ikke vist til §12 i IKT-forskriften. Hvis rapportene til tilsynet var konsekvente så skulle nesten alle foretakene i datagrunnlaget hatt tilbakemelding på avvik i forholdt til §12 i IKT-forskriften. Hvis vi legger til grunn at absolutt alle foretakene som er omhandlet av dataene har fått en tilbakemelding om avvik i forhold til Finanstilsynets forventninger. Vil det være grunnlag for at datagrunnlaget er vurdert valid for å måle overholdelse av regelverk for utkontraktering, men den kvantitative målingen av data vil kun gi noen indikatorer og ikke fullstendig fakta. Likevel ser det ut til at de som har flest treff i analysen har minst kontroll på utkontraktering, og de med minst treff har kun mindre tilbakemeldinger fra tilsynet på rettelser, men ikke fullstendige mangler. Dermed har det fungert etter hensikt.

Noen observasjoner som er gjort ved gjennomgang av rapportene er interessante:

- Alle foretakene har utkontrakterte oppgaver som omhandler IKT
- 10 av foretakene i undersøkelsen er enten en del av en allianse eller konsern, og utkontraktering blir i hovedsak administrert av alliansen eller morselskap
- Flere av pensjonskassene får tilbakemelding på sammenblanding av roller mellom arbeidsgiverforetak og pensjonskasse, og manglende rutine for interessekonflikt

- Alle tre gjeldsopplysningsforetakene (som er alle vi har i Norge) får tunge tilbakemeldinger på vesentlige mangler. Disse virksomhetene har alle eiere som er store konsern
- 12 av selskapene har mangler ved vurdering av oppdragstaker
- 8 av selskapene kan ikke dokumentere tilfredsstillende kontrakter med leverandører
- 10 av selskapene har ikke tilfredsstillende rutiner for oppfølging av underleverandører
- 13 av selskapene har mangler ved risikostyring og internkontroll

Ettersom tilsynsrapportene alltid vil være adressert til styret i virksomheten er det enkelt å konkludere med at det er manglende kompetanse eller oppfølging fra styret som er årsaken til at utkontraktering ikke blir fulgt opp iht. regelverket. Det er vanlig innen bank og finans, at det er «administrasjonen» som utfører de faktiske oppgaver. Med administrasjonen menes øverste ledelse og 2. linje. Det tilhører sjeldenheten at et styremedlem utformer en rutine eller retningslinje. I praksis vil et styre bare be om dokumenter eller tilsvarende fra administrasjonen, og komme med rettelser eller godkjenne dokumentasjon.

Det som er en rød tråd gjennom alle rapportene med unntak av noen få, er at tilbakemeldinger fra Finanstilsynet, og tilsvar fra virksomhetene vitner om mangel på kompetanse og/eller mangel på forståelse og innsikt i virksomheten. Dette i tillegg til mangel på internkontroll og eventuelle rammeverk.

- Ingen av foretakene viser til at de har rammeverk for internkontroll
- Ingen tilsvar inneholder noe om at foretakene eksempelvis har en uavhengig 3. part som foretar revisjon av virksomhetens IKT-systemer.
- Ingen av foretakene viser til at de benytter rammeverk for IKT-systemer, slik som ISO27001 eller andre tilsvarende rammeverk.

Som tidligere beskrevet i oppgaven, angir COSO-rammeverket noen forutsetninger for at et rammeverk skal fungere etter hensikten, nemlig at det forutsetter en god prosess på utvelgelse av styremedlemmer. Det vil altså ikke hjelpe å ha et rammeverk, hvis de som beslutter ikke har kompetanse til å forstå hensikten med å benytte et rammeverk.

Etter tematilsynet i 2016/2017 gav Finanstilsynet veldig tydelige signaler at de forventer at bankene tar operasjonell risikostyring mer på alvor. Det vil si at man har en god "tone fra toppen" som videreføres av mellomledelsen, og har dokumentert ambisjonsnivå og risikotoleranse i sine styrende dokumenter. I tillegg påpeker de at man må sikre tilstrekkelige ressurser og kompetanse i virksomheten.
Ut ifra gjennomgang av enkeltrapporter fra 2020-2022 kan det virke som at dette ikke er absorbert og tatt inn i hverken styrende dokumenter eller i praksis i flertallet av virksomhetene som har hatt tilsyn i nevnte periode.

Det kan derfor være logisk å konkludere med at det ikke er tilstrekkelig egnethetsvurdering når man rekrutterer styremedlemmer innen bank og finans, og at det ikke er tilstrekkelig kunnskap blant styremedlemmer til å kunne følge opp regelverket rundt utkontraktering av tjenester. Det ser også ut til at de ulike virksomhetenes styre, i liten grad har ansatt ressurser som kan tilbringe kunnskap og opplæring om det aktuelle tema. Kun en av virksomhetene oppgir til Finanstilsynet at de skal foreta kunnskapsheving.
Det kan også stilles spørsmål ved om compliancefunksjonene eksisterer, og hvis det er en rolle som finnes (krav til banker), om de foretar hensiktsmessige kontroller, og har god nok rapporteringsvei til styret.

Avslutning og oppsummering

Grunnen til at jeg valgte temaet for denne oppgaven, er at jeg har hatt en teori om at det er for lite styring og kontroll med utkontrakterte leverandører. Regelverket er mangfoldig og det er mange kilder av lover og regler man skal forholde seg til, både nasjonalt og gjennom EU-regelverk. I tillegg er det ingen av retningslinjene fra offisielle kilder som sier noe om hvordan man praktisk skal kunne utføre oppgavene som regelverkene pålegger.

I tillegg så er det ikke bare på utkontraktering at virksomheter innen bank og finans har krevende regelverk de skal forholde seg til, og som innehar samme

utfordring med praktisk utførelse. Eksempelvis kan nevnes praktisk fremgangsmåte ved oppfølging av kapitalkrav, forskrift om boliglån, anti-hvitvasking og finansiell rapportering.

At oppfølging av styring og kontroll med utkontrakterte avtaler ikke blir fulgt opp som nødvendig, er god grunn til bekymring. I analyse av data som blant annet omhandler en av bankene i Eika-gruppen, var ansvaret ikke ivaretatt på noen måte. Det er i beste fall total fraskrivelse av ansvar for internkontroll, men ikke minst i forhold til de titusenvis av kundene som er avhengig av at underleverandørenes funksjoner fungerer. Eika-Gruppen er en allianse på ca 50 banker og benytter SDC som leverandør for kjernebanksystem. Kjernebanksystemet er systemet som er grunnlag for lønnsinngang, regningsbetaling, nettbank og kortbetaling for kundene. 26. april 2022 var det en teknisk feil hos SDC som førte til at lønnsutbetalingen til mer enn 100.000 kunder som har lønnskonto hos banker som benytter SDC, ble reversert (E24.no, 2022). Om dette ikke hadde skjedd hvis den nevnte banken hadde oversikt over sin underleverandør vites ikke, men hvis de fulgte retningslinjene ville de i alle fall hatt en beredskapsplan.

Tilfeldighetene skulle ha det til at mens jeg skrev denne oppgaven ble det kommunisert fra Finanstilsynet i media, at de «Ser at det kan være behov for å minne om krav til styremedlemmer» (Finanswatch.no, Finanstilsynet: – Ser at det kan være behov for å minne om krav til styremedlemmer, 2022). Finanstilsynet refererer til flere saker som har vært i media hvor det har vært flere aktuelle styresaker som gjelder bank og finans den siste tiden. Spesifikt gjelder det Askim & Spydeberg Sparebank og MyBank, hvor hhv. Administrerende Banksjef og styreleder har foretatt handlinger som er i strid med retningslinjer og regelverk.

I tilfellet med MyBank har til og med Finanstilsynet fattet vedtak på at styret skal byttes ut. Tilsynets vedtak er basert på en vurdering av styremedlemmenes egnethet (E24, Finanstilsynet krever store endringer i MyBank-styret, 2022).

Det kan virke som den generelle oppfatningen når det gjelder styrearbeid er å sørge for virksomhetens lønnsomhet, og at det glemmes at bank og finansinstitusjoner har et kritisk samfunnsoppdrag. Det hadde vært interessant å se videre på virksomheters etiske retningslinjer, og om de samsvarer med oppfølging av lover og regler og om de hensyntar annet enn «ting som er i vinden». Ved noen raske stikkprøver så ser etiske retningslinjer kun å dreie seg om bærekraft. Høland og Setskog Sparebank, som ellers ikke hadde noen oppfølging av utkontraktering. Har som eksempel kun linket til Eika sine retningslinjer for bærekraftige investeringer (Eika - Etiske Retningslinjer for Eika Kapitalforvaltning, u.d.), slik at det er ukjent hvordan de forholder seg til etikk ovenfor kunder.

Det kunne vært interessant å forhøre seg hva styremedlemmer i virksomhetene som er nevnt i oppgaven tenker om «Finansnæringens etikkplakat», punkt nummer 1. «Løse samfunnsoppdraget på en måte som ivaretar hensynet til alle bedriftens interessenter» (Finans Norge, Finansnæringens Etikkplakat, 2022).

Man kan anta at kunder av virksomhetene burde være relativt store interessenter.

Litteraturliste

Anderson, U. L., Head, M. J., Ramamoorti, S., Riddle, C., Salamasick, M., & Sobel, P. J. (2017). *Internal Auditing.* Internal Audit Foundation.

Anderson, U., Head, M., Ramamoorti, S., Riddle, C., Salamasick, M., & Sobel, P. (u.d.). *Internal Auditing, Assurance & Advisory Services.*

Cappelen Damm, Begrepsbank. (2022). *Mangfold*. Hentet fra https://mangfold.cappelendamm.no/vgsamf/tekst.html?tid=1006552

Committe of Sponsoring Organizations of the Treadway Commission. (2013, s 139). *Internal Control - Integrated Framework.*

Committe of Sponsoring Organizations of the Treadway Commission. (2013, s.138). *Internal Control - Integrated Framework.*

Committee of Sponsoring Organizations of the Treadway Commission. (2013-2014). *Internal Control - Integrated Framework.* American Accounting Association.

Committee of Sponsoring Organizations of the Treadway Commission. (2013-2014). *Internal Control - INtegrated Framework.* Committee of Sponsoring Organizations of the Treadway Commission.

DigDir, Hva er Schrems II dommen. (2022). *Hva er Schrems II-dommen*. Hentet fra Erfaringsrapport om handlingsplanen 2020: https://www.digdir.no/handlingsplanen/hva-er-schrems-ii-dommen/2581

E24, Finanstilsynet krever store endringer i MyBank-styret. (2022). https://e24.no/boers-og-finans/i/Or01Kb/finanstilsynet-krever-store-endringer-i-mybank-styret. Hentet fra https://e24.no/boers-og-finans/i/Or01Kb/finanstilsynet-krever-store-endringer-i-mybank-styret

E24.no. (2022, 04 26). *Teknisk feil hos flere banker – lønninger reversert*. Hentet fra https://e24.no/norsk-oekonomi/i/1OJBoG/teknisk-feil-hos-flere-banker-loenninger-reversert

EBA, Guidelines on outsourcing arrangements, s6. (2019). EBA Guidelines on outsourcing arrangements. *EBA Guidelines on outsourcing arrangements*. European Bank Authority. Hentet fra

https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

Eika - Etiske Retningslinjer for Eika Kapitalforvaltning. (u.d.). *Etiske Retningslinjer for Eika Kapitalforvaltning*. Hentet fra https://eika.no/spare/fondssparing/etiske_retningslinjer?_gl=1*qfx59j*_ga*MTU4ODU1NzU4My4xNjUyODY2NzU4*_ga_6TCCNDDC9W*MTY1MzAyNjUzNi4yLjAuMTY1MzAyNjUzNi4w

Filosofi.no. (2022). *Etikk*. Hentet fra https://filosofi.no/etikk/#:~:text=Etikk%2C%20eller%20morall%C3%A6re%2C%20er%20den%20gren%20av%20filosofien,at%20det%20er%20i%20strid%20med%20visse%20moralnormer.

Finans Norge, Finansnæringens Etikkplakat. (2022). Finansnæringens Etikkplakat. Hentet fra https://www.finansnorge.no/siteassets/politikk/finansnaringens-etikkplakat-oppdatert-aug2018.pdf

Finanstilsynet. (2021). *Tilsynsrapport.* Hentet fra https://www.finanstilsynet.no/contentassets/c87b0a58516a4e0c81c94663c38704bf/tilsynsrapport-molde-kommunale-pensjonskasse.pdf

Finanstilsynet. (2021). *Tilsynsrapport 19/8411*. Hentet fra https://www.finanstilsynet.no/contentassets/1adff534dfcb4b389da036e94666fd26/tilsynsrapport-kommunalbanken-as.pdf

Finanstilsynet. (2021). *Tilsynsrapport 20/12217*. Hentet fra https://www.finanstilsynet.no/contentassets/4b07ec80ed48420594b1281ab7810496/tilsynsrapport.pdf

Finanstilsynet, Modul for operasjonell risiko. (2016). *Modul for operasjonell risiko.* Finanstilsynet.

Finanstilsynet, Nyhetsarkiv. (2022). *Nyhetsarkiv*. Hentet fra https://www.finanstilsynet.no/nyhetsarkiv/?l=no&t=104&s=13&s=14&s=20&s=24

Finanstilsynet, Rundskriv 1/2020 Vurdering av egnethetskrav. (2020). *Rundskriv 1/2020 Vurdering av egnethetskrav.* Hentet fra

https://www.finanstilsynet.no/contentassets/87b33d0010ca4498ac280532c2b4592c/rundskriv-1-2020.pdf

Finanstilsynet, Rundskriv 7/2021. (2020). *Rundskriv, Veiledning om utkontraktering.* FInanstilsynet. Hentet fra https://www.finanstilsynet.no/contentassets/9f76ac1a390a44218b285b61bb13e19a/veiledning-om-utkontraktering.pdf

Finanstilsynet, Rundskriv 7/2021, s 4. (2021). *Rundskriv 7/2021 Veiledning om utkontraktering.* Finanstilsynet. Hentet fra https://www.finanstilsynet.no/contentassets/a09cc0bbacb943af995ee29c4db180d9/veiledning_utkontraktering.pdf

Finanstilsynet, Tilsynsrapport 19/11247. (2020). *Tilsynsrapport 19/11247.* Hentet fra https://www.finanstilsynet.no/contentassets/e9d904e60cd84f76a8e3d3377dfb0cfd/tilsynsrapport---bergen-kommunale-pensjonskasse-pdf

Finanstilsynet, Tilsynsrapport 19/12479. (2021). *Tilsynsrapport fra stedlig tilsyn i DNB Bank ASA 4. til 7. februar 2020 19/12479.* Hentet fra https://www.finanstilsynet.no/contentassets/550b0e46fc8542ce85844550f8298df4/tilsynsrapport_dnb.pdf

Finanstilsynet, Tilsynsrapport 19/12784. (2020). *Tilsynsrapport 19/12784.* Hentet fra https://www.finanstilsynet.no/contentassets/eb395d1d9a904c49805d6d6cf11ffdad/tilsynsrapport---mp-pensjon-pk-pdf

Finanstilsynet, Tilsynsrapport 19/13577. (2021). *Tilsynsrapport 19/13577.* Hentet fra https://www.finanstilsynet.no/contentassets/c5dd4bdf1bae474eba5a4322c79cac49/tilsynsrapport-dnb-bank-asa.pdf

Finanstilsynet, Tilsynsrapport 19/6137. (2020). *Tilsynsrapport 19/6137.* Hentet fra https://www.finanstilsynet.no/contentassets/ce439879240f4ef9adcb2a53ca45e340/tilsynsrapport---harstad-kommunale-pensjonskasse.pdf

Finanstilsynet, Tilsynsrapport 19/8411. (2021). *Tilsynsrapport 19/8411.* Hentet fra https://www.finanstilsynet.no/contentassets/1adff534dfcb4b389da036e94666fd26/tilsynsrapport-kommunalbanken-as.pdf

Finanstilsynet, Tilsynsrapport 20/12217. (2021). *Tilsynsrapport 20/12217*. Hentet fra https://www.finanstilsynet.no/contentassets/4b07ec80ed48420594b1281ab7810496/tilsynsrapport.pdf

Finanstilsynet, Tilsynsrapport 20/419. (2021). *Tilsynsrapport 20/419*. Hentet fra https://www.finanstilsynet.no/contentassets/a2682bf002194cf2bc7788884f18ee68/tilsynsrapport---trondheim-kommunale-pensjonskasse.pdf

Finanstilsynet, Tilsynsrapport 20/4656. (2021). *Tilsynsrapport 20/4656*. Hentet fra https://www.finanstilsynet.no/contentassets/06181addb747481f93d01f7934686839/tilsynsrapport-storebrand-livsforsikring2.pdf

Finanstilsynet, Tilsynsrapport 20/6670. (2021). *Tilsynsrapport 20/6670*. Hentet fra https://www.finanstilsynet.no/contentassets/294708b809304bc0bb1a1ba74a7430f2/tilsynsrapport_convene-collection-as.pdf

Finanstilsynet, Tilsynsrapport 20/6760. (2021). *Tilsynsrapport 20/6760*. Hentet fra https://www.finanstilsynet.no/contentassets/09be4716b89e40ee8f8bd4876b5c1e28/tilsynsrapport-credicare-as.pdf

Finanstilsynet, Tilsynsrapport 20/7332. (2021). *Tilsynsrapport 20/7332*. Hentet fra https://www.finanstilsynet.no/contentassets/e475c4fd6117416fa2d07df81cce3ac8/tilsynsrapport-eiendomsmegler-1-midt-norge-as.pdf

Finanstilsynet, Tilsynsrapport 20/9363. (2022). *Tilsynsrapport 20/9363*. Hentet fra https://www.finanstilsynet.no/contentassets/304dbd090b4d47718ce37277498157df/tilsynsrapport---invento-kapitalforvaltning-as.pdf

Finanstilsynet, Tilsynsrapport 21/1606. (2021). *Tilsynsrapport 21/1606*. Hentet fra https://www.finanstilsynet.no/contentassets/845a271cd57f4290935401e3337e5ed2/tilsynsrapport-sr-bank-asa.pdf

Finanstilsynet, Tilsynsrapport 21/2981. (2021). *Tilsynsrapport 21/2981*. Hentet fra

https://www.finanstilsynet.no/contentassets/8d45b1275b08400983d88d4a0d25f58e/tilsynsrapport-gjeldsregisteret-as.pdf

Finanstilsynet, Tilsynsrapport 21/308. (2021). *Tilsynsrapport 21/308.* Hentet fra https://www.finanstilsynet.no/contentassets/c87b0a58516a4e0c81c94663c38704bf/tilsynsrapport-molde-kommunale-pensjonskasse.pdf

Finanstilsynet, Tilsynsrapport 21/3377. (2021). *Tilsynsrapport 21/3377.* Hentet fra https://www.finanstilsynet.no/contentassets/93284c53adbe4d0ca8c7b1bba2eb2b9c/tilsynsrapport-holand-og-setskog-sparebank.pdf

Finanstilsynet, Tilsynsrapport 21/3380. (2021). *Tilsynsrapport 21/3380.* Hentet fra https://www.finanstilsynet.no/contentassets/c14a9adb4cdb41ed9bdbd82d9ce262d4/tilsynsrapport-sogne-og-greipstad-sparebank.pdf

Finanstilsynet, Tilsynsrapport 21/3736. (2021). *Tilsynsrapport 21/3736.* Hentet fra https://www.finanstilsynet.no/contentassets/dbdf729ed0ab4d939100f246631870c9/tilsynsrapport---odin-forvaltning-as.pdf

Finanstilsynet, Tilsynsrapport 21/4834. (2021). *Tilsynsrapport 21/4834.* Hentet fra https://www.finanstilsynet.no/contentassets/8d45b1275b08400983d88d4a0d25f58e/tilsynsrapport-norsk-gjeldsinformasjon-as.pdf

Finanstilsynet, Tilsynsrapport 21/5133. (2021). *Tilsynsrapport 21/5133.* Hentet fra https://www.finanstilsynet.no/contentassets/8d45b1275b08400983d88d4a0d25f58e/tilsynsrapport-experian-gjeldsregister-as.pdf

Finanstilsynet, Tilsynsrapport 21/808. (2021). *Tilsynsrapport 21/808.* Hentet fra https://www.finanstilsynet.no/contentassets/3c00dc49317a45a38d2afde3cc0db33e/tilsynsrapport-vipps-as.pdf

Finanswatch.no, Finanstilsynet: – Ser at det kan være behov for å minne om krav til styremedlemmer. (2022, 05 12). Finanstilsynet: – Ser at det kan være behov for å minne om krav til styremedlemmer. Hentet fra https://finanswatch.no/nyheter/bank/article14014918.ece

Forskrift om risikostyring og internkontroll §5. (2022, 03 01). Norge: Finansdepartementet.

IIA Norge, Veileder for Compliancefunksjonen. (2015). *Veileder for Compliancefunksjonen.*

IIA Norge, Veileder for Compliancefunksjonen. (2015). *Veileder for Compliancefunksjonen.* IIA Norge.

IIA Norge, Veileder for Compliancefunksjonen. (2015). *Veileder for Compliancefunksjonen.* IIA Norge.

Lov om tilsynet med finansforetak mv. §4c. (2021, 01 01). Norge: Finansdepartementet.

Norsk utvalg for eierstyring og selskapsledelse. (2022). *Den norske anbefalingen om eierstyring og selskapsledelse*. Hentet fra https://nues.no/eierstyring-og-selskapsledelse/

Pwc, Finansbloggen. (2017). *Finanstilsynets funn fra tematilsyn innen operasjonell risiko er nå tilgjengelig.* Hentet fra https://blogg.pwc.no/finansbloggen/finanstilsynets-funn-fra-tematilsyn-innen-operasjonell-risiko-er-n%C3%A5-tilgjengelig

Sander, K. -K. (2022). *estudie.no*. Hentet fra Kausalt design: https://estudie.no/kausalt-design/?msclkid=c10b37cacf8511ec8b3e088eb3f70d12

Silkoset, R., Gripsrud, G., & Olsson, U. (2021). *Metode, dataanlyse og innsikt.* Cappelen Damm akademisk.

Silkoset, R., Olsson, U., & Gripsrud, G. (2021). *Metode, dataanalyse og innsikt.* Cappelen Damm akademisk.

Silkoset, R., Olsson, U., & Gripsrud, G. (2021). *Metode, dataanalyse og innsikt.* Oslo: Cappelen Damm akademisk.

Silkoset, R., Olsson, U., & Gripsrud, G. (2021). *Metode, dataanalyse og innsikt.* Capellen Damm.

Språkrådet. (2022). *På godt norsk - avløserord*. Hentet fra https://www.sprakradet.no/sprakhjelp/Skriverad/Avloeysarord/

Standard Norge, IT-sikkerhet - ISO/IEC 27000. (2022). *IT-sikkerhet - ISO/IEC 27000*. Hentet fra https://www.standard.no/fagomrader/ikt/it-sikkerhet/

SurveyMonkey, Forskjellen mellom kvantitative og kvalitative undersøkelser. (2022). *SurveyMonkey*. Hentet fra Forskjellen mellom kvantitative og kvalitative undersøkelser: https://no.surveymonkey.com/mp/quantitative-vs-qualitative-research/

Wikipedia - ISO / IEC 27001. (2022). *Wikipedia*. Hentet fra https://no.frwiki.wiki/wiki/ISO%2FCEI_27001

Wikipedia. (2021, Oktober 15). *Wikipedia*. Hentet fra Wikipedia: https://no.wikipedia.org/wiki/Utkontraktering