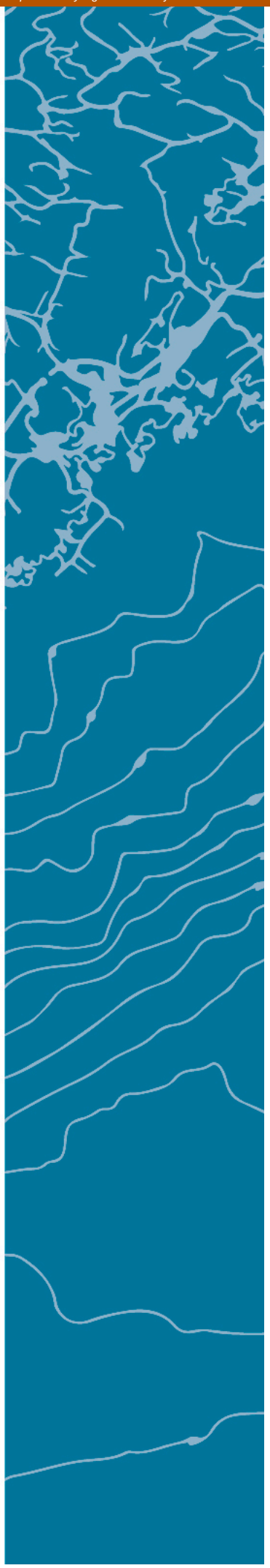
IT-revisjon

Revisors forhold til IT- og informasjonssystemer for regnskapsavleggelse

MILICA COROVIC
IDA KRISTINE OTTOSEN

VEILEDER
Sylvi Nerskogen

Universitetet i Agder, 2017
Handelshøyskolen ved UiA



Forord

Denne oppgaven er skrevet som en avsluttende del av mastergradstudiet regnskap og revisjon ved Handelshøyskolen ved Universitetet i Agder. Oppgaven utgjør 30 studiepoeng og er skrevet i fjerde og siste semester av studiet.

IT-revisjon er en del av studieplanen for faget revisjon på studieprogrammet master i regnskap og revisjon. Det er gjennom disse forelesningene vi har fått interesse for bruk av IT i regnskapsavleggelse. Vi tror at kompetanse om IT-revisjon kommer til å bli mer etterspurt i fremtiden og vi ønsker derfor å finne ut av hvilke utfordringer en revisor møter i skjæringspunktet mellom IT og økonomi.

Da vi begge har tatt bachelor i regnskap og revisjon og kun avlagt nasjonale eksamener, har det å skrive en masteroppgave vært en ny og spennende opplevelse for oss. Det har til tider vært utfordrende å skrive masteroppgave, delvis på grunn av lite faglitteratur og begrenset forskning på området. Derfor ønsket vi å utfordre oss selv ved å velge et tema som vi mener ikke får nok oppmerksomhet. På den måten håper vi at UiA og andre institusjoner retter mer fokus på IT-revisjon i sin utdannelse av fremtidige revisorer.

Vi ønsker først og fremst å takke vår veileder Sylvi Nerskogen for hennes fleksibilitet og kompetanse som hun med glede har delt. Hun har inspirert oss til å være fremtidsrettet i det arbeidslivet vi skal inn i til høsten. Videre ønsker vi også å takke alle revisorene som har stilt opp til intervju og for at de har delt sine erfaringer og sin innsikt med oss.

Kristiansand 01.06

Milica Corovic og Ida Kristine Ottosen

Sammendrag

I dag benytter de aller fleste virksomheter IT- og informasjonssystemer i sine forretningsprosesser. Derfor vil det bli et stort behov for revisorer med kompetanse innen IT- og informasjonssystemer, sikkerhet og risiko ved IT. Formålet med vår masteroppgave er å belyse revisors forhold relatert til IT. Oppgavens problemstilling har følgende formulering:

"Hva gjør revisor for å forstå og håndtere risiko knyttet til IT- og informasjonssystemer relevant for finansiell rapportering?"

Innledningsvis presenteres formålet med revisjon. Det gis en oversikt over revisjonsprosessen og tilknyttede begreper. Ved at vår masteroppgave handler om IT-revisjon gis det en innføring i utviklingen av IT-revisjon som eget fagområdet og vi viser til tidligere forsking.

I teoridelen gis det en innføring i IT-revisjon og hva som menes med IT- og informasjonssystemer. Videre forklares det hvilken funksjon internkontroll har og hvilke oppgaver revisor har i forbindelse med å vurdere de ulike komponentene. Deretter utredes revisors risikovurdering av IT- og informasjonssystemer og hvordan IT-miljø utgjør en del av den interne kontrollen. Derfra går vi videre til å gi en beskrivelse av revisors håndtering og testing av IT- og informasjonssystemer. Kapittelet avsluttes med hvordan eventuelle svakheter ved IT- og informasjonssystemer kan påvirke revisors rapportering og kommunikasjon ved revisjonens slutt og selve revisjonsberetningen.

I kapittelet om metode drøftes ulike datainnsamlingsmetoder og forskningsstrategier. Valg av metode blir presentert og vi utleder vår utvalgsstrategi og fremgangsmåte for rekruttering av intervjuobjekter. Videre forklares gjennomføring av datainnsamling og hvordan oppgaven kan knyttes til prinsippene validitet og reliabilitet.

I kapittel fire gis det en presentasjon av funn og analyse. Analysen er delt opp i kategoriene: revisors forståelse av IT-miljø, revisors håndtering av IT-relaterte kontroller, rapportering og kommunikasjon ved kontrollsvakheter, samhandling mellom revisor og IT-revisor og muligheter og utfordringer for revisor i fremtiden. Her gjør vi rede for hvilke likheter og ulikheter som fremkommer blant våre informanter og vi drøfter eventuelle årsaker som kan føre til dette. Avslutningsvis oppsummerer vi funn og trekker konklusjoner, samt kommer med forslag til videre forskning.

Innholdsfortegnelse

Figurliste

Tabelliste

1. Bakgrunn og forskningsspørsmål

NHOs årskonferanse 2016 tok for seg utfordringene vi står ovenfor i møte med den teknologiske utviklingen. Der ble det konstatert at teknologien endrer jobbene våre raskere enn noen gang. Som følge av informasjonsteknologi har alle fått tilgang til informasjon, vi har fått nye tjenester, nye forretningsmodeller og arbeidsprosesser i omtrent alle bransjer (NHO, 2016). Revisjonsbransjen er intet unntak, og det har vært omfattende omstillinger i arbeidsmetoder for å kunne håndtere disse utfordringene og kunne tilby de beste og mest effektive revisjonstjenestene til sine kunder.

Det kan allikevel virke som at å revidere i kundenes IT- og informasjonssystemer er en utfordrende oppgave for revisor. Utfordringen er særlig tydelig etter hva det amerikanske revisorstilsynet PCAOB kan melde i sine inspeksjoner av de store revisjonsselskapene, der flere svakheter i gjennomføringen av revisjonen kan relateres til dårlige gjennomganger av internkontrollen (PCAOB, 2015). Dette kommer ytterligere frem i boken til Wood, Brown og Howe (2013) der de innledningsvis uttrykker at mange revisorer er av den oppfatning at komplekse IT-miljøer krever spesialister for å forstå teknologien som anvendes. Som følge av dette endrer revisorer sin revisjonstilnærming for å unngå internkontroller der IT-kontroll er en komponent eller kun gjør en overfladisk og lite detaljert vurdering av IT-kontrollene.

Vi mener det er interessant å se på om dette er tilfellet i revisjonsselskaper i dag ettersom det er rettet mer fokus på dette området de siste årene. Derfor stiller vi oss spørsmålet:

"Hva gjør revisor for å forstå og håndtere risiko knyttet til IT-og informasjonssystemer relevant for finansiell rapportering?"

Dette kapittelet skal gi en bakgrunn for teorien i kapittel to. Kapittelet tar for seg konsepter om revisjon, herunder formålet med revisjon og revisjonsprosessen. Ved at vår masteroppgave handler om IT-revisjon gir vi en innføring i utviklingen av IT-revisjon og viser til tidligere forskning på dette området.

1.1 Formålet med revisjon

Ekstern revisjon er prosessen der en uavhengig aktør gjør rede for om et årsregnskap er utarbeidet i samsvar med lover og regler for å øke tilliten til det som rapporteres av finansiell informasjon ovenfor årsregnskapets brukere (Gulden, 2010).

Revisors Håndbok definerer revisors overordnede mål som ”*å oppnå betryggende sikkerhet for at regnskapet totalt sett ikke inneholder vesentlig feilinformasjon, verken som følge av misligheter eller feil, og dermed gjøre det mulig for revisor å gi uttrykk for en mening om hvorvidt regnskapet i alt det vesentlige er utarbeidet i samsvar med et gjeldende rammeverk for finansiell rapportering” (ISA 200, 2016).*

1.2 Revisjonsprosessen

Revisjonsprosessen kan illustreres gjennom følgende figur og forklares nedenfor:

Figur 1: *”Revisjonsprosessen”* hentet fra Geir Haaland sin forelesning ”BE-312 Planlegging og Strategi-PP 5” ved Universitet i Agder høsten 2014

Figuren skal illustrere at selv om revisjonsprosessen består av flere ulike faser, må fasene sees i sammenheng og i relasjon til hverandre. Revisjonsprosessen er en dynamisk prosess der nye forhold og hendelser kan dukke opp underveis i revisjonen og føre til at revisor må foreta nye vurderinger og handlinger i de ulike fasene. Ofte deles virksomhetens regnskapsinformasjon inn i ulike revisjonsområder for å kunne utføre en effektivt revisjon (Gulden, 2010). Det vil si at like transaksjoner systematiseres etter hvor de forekommer i virksomheten. Vanlige inndelinger er salgsområde, innkjøpsområde, lønnsområde og lagerområde.

Fase 1 innebærer at revisor danner seg et bilde av hvor risiko for vesentlig feilinformasjon foreligger i regnskapet. Da er det nødvendig å foreta en risikovurdering av en rekke forhold i og utenfor virksomheten. Dette omfatter å opparbeide en forståelse av virksomhetens art, bransje, reguleringer, eier- og styringsstruktur, finansieringsformer, mål og strategier, og internkontrollen (ISA 315, 2016) . Bruk av IT- og informasjonssystemer utgjør en del av internkontrollen som revisor skal vurdere. Siden internkontroll, herunder kontroller i IT- og informasjonssystemer og revisors forståelse av dem utgjør en vesentlig del av oppgaven, vil dette beskrives og utdypes nærmere i kapittel 2.2.

Risikovurderingshandlinger skal gjøre revisor i stand til å anslå risiko for vesentlig feilinformasjon i det ureviderte regnskapet (Gulden, 2010). I samsvar med revisjonsstandarden ISA 315 (2016) pkt. 6 er revisor pålagt å utføre følgende risikovurderingshandlinger:

- Revisor skal **rette forespørsel** til ledelsen og andre personer som etter revisors skjønn kan ha relevant informasjon for regnskapsavleggelsen. Den eller de som har overordnet ansvar for styring og kontroll kan bidra til at revisor forstår miljøet for utarbeidelsen av regnskapet. Medarbeidere som deltar og har ansvar for regnskapsprosessene kan bidra til at revisor får en forståelse av hvilke regnskapsprinsipper og policyer som ligger til grunn. Andre personer kan være juridiske rådgivere, salgspersonale og IT-personale som alle kan bidra til at revisor får en forståelse av virksomheten.
- **Analytiske handlinger** gjennomføres for at revisor skal kunne avdekke og identifisere forhold og sammenhenger i både finansiell og ikke-finansiell informasjon. Vanlige analytiske handlinger er bruttofortjenesteanalyser, gjennomgang av budsjetter og avviksanalyser, forhold mellom salg og kundefordringer og lønnskostnader i forhold til antall ansatte. Ofte summeres data på et overordnet nivå og gir derfor bare en generell indikasjon på om det foreligger vesentlige feilinformasjon. Derfor er det viktig at revisor også vurderer annen innsamlet informasjon for å kunne vurdere resultatene av de analytiske handlingene.
- **Observasjon og inspeksjon** underbygger informasjon som innhentes fra ledelsen og andre relevante personer. Dette kan for eksempel omfatte å inspisere rapporter og dokumenter og observere virksomhetens drift.

Risikovurderingsfasen gjør revisor i stand til å planlegge revisjonen slik at det er mulig å allokere ressurser der behovet for å revidere er størst slik at revisjonen gjennomføres mål- og kostnadseffektivt (Gulden, 2010).

Fase 2 består i å planlegge revisjonen for å håndtere risiko som revisor identifiserer i fase 1. Derfor kalles denne fasen for risikohåndteringsfasen. Revisor fastsetter en revisjonsstrategi og utformer en revisjonsplan i denne fasen. Revisjonsstrategien er overordnet og tar for seg angrepsvinkelen for revisjonen (Gulden, 2010). Her fastsettes risiko og vesentlighetsgrenser for de ulike revisjonsområdene. Konseptene om risiko og vesentlighet er betydelige for revisjonsprosessen og vil utdypes i kapitlene 1.3.1 og 1.3.3. I denne sammenhengen forstås risiko som risikoen for at det kan foreligge uoppdagede vesentlige feil i regnskapet før det revideres. Fastsettelse av vesentlighetsgrenser vil si at revisor tallfester øvre grenser for hvor mye feilinformasjon regnskapet kan inneholde før det kan antas at det får konsekvenser for de økonomiske beslutningene til brukerne av regnskapet. I revisjonsplanen planlegges detaljene for revisjonen, altså type, omfang og tidspunkt for revisjonshandlingene (Gulden, 2010). Revisjonsplanen oppdateres etter hvert som revisor har gjennomført risikovurderingshandlinger som beskrevet i risikovurderingsfasen.

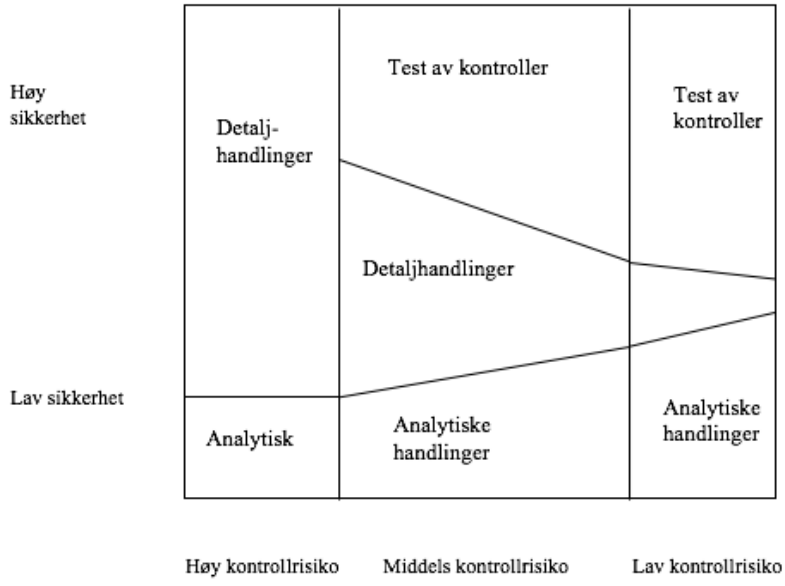
I fase 3 vil revisor gjennomføre risikohåndteringshandlingene som ble planlagt i fase 2. Det betyr at revisor utfører handlinger som skal redusere risiko for at vesentlig feilinformasjon ikke blir avdekket i det reviderte regnskapet (Gulden, 2010). Risikohåndteringshandlinger deles i kategoriene test av kontroller og substanshandlinger. Test av kontroller og substanshandlinger utføres til revisor med betryggende sikkerhet kan bekrefte at årsregnskapet ikke er heftet med vesentlig feilinformasjon. Test av kontroller har som formål å vurdere måleffektiviteten av virksomhetens rutiner og internkontroller som skal forebygge, avdekke og korrigere vesentlig feilinformasjon jfr. ISA 330 (2016) pkt. 4b. Fremgangsmåten er kun hensiktsmessig dersom revisor kan basere seg på at internkontrollen fungerer effektivt (Gulden, 2010).Ulike former for test av kontroller kan være:

- Observasjon av hvordan en kontroll gjennomføres. Dette kan for eksempel være at revisor observerer at en arbeidsdelingsrutine for godkjenning av innkjøp overholdes.
- Inspeksjon av dokumenter der for eksempel revisor gransker rapporter. Dette kan også omfatte fysisk inspeksjon av for eksempel varelageret.
- Gjentakelse av rutiner eller kontroller. Revisor kan for eksempel gjøre en uavhengig utførelse av en kontroll eller prosedyre som opprinnelig utføres av personale.

Substanshandlinger har som formål å avdekke vesentlig feilinformasjon jfr. ISA 330 (2016) pkt. 4a, og skal alltid utføres i et visst omfang. Denne kontrollformen omfatter detaljtester og analytiske substanshandlinger.

- Detaljtester er metoder som for eksempel innebærer fysisk inspeksjon av eiendeler, dokumentgransking, eksterne bekreftelser og kontrollregning.
- Analytiske substanshandlinger omfatter en vurdering av sammenligninger mellom virksomhetens økonomiske informasjon og for eksempel informasjon fra tidligere perioder, forventede resultater i budsjetter og tilsvarende bransjeinformasjon jfr. ISA 520 (2016) pkt. A1. Andre handlinger kan være å vurdere forutsigbare mønstre basert på virksomhetens erfaring, for eksempel bruttofortjeneste i prosent eller forhold mellom finansiell og ikke-finansiell informasjon jfr. ISA 520 (2016) pkt. A2.

En figur som illustrerer hvordan revisor legger opp revisjonens angrepsvinkel vises nedenfor:



Figur 2: ***"Valg av angrepsvinkel/revisjonsstrategi" hentet fra Geir Haaland sin forelesning i BE 312 Revisjonsbevis og handlinger PP 7" ved Universitetet i Agder høsten 2014***

Angrepsvinkelen for revisjonen bestemmes ut i fra revisors vurdering av virksomhetens internkontroll. Effektiviteten i internkontrollen påvirker revisors vurdering av kontrollrisikoen, som er risikoen for at feilinformasjon ikke forhindres, avdekkes eller korrigeres av virksomhetens kontroller. For å forklare figuren gjennom et eksempel kan vi

beskrive tilfellet der revisor vurderer virksomhetens interkontroll som effektiv. Da vurderes kontrollrisikoen som lav fordi virksomhetens internkontroll sørger for at feilinformasjon forhindres, avdekkes og korrigeres. Da befinner revisor seg på høyre side av figuren og angrepsvinkelen til revisjonen vil i stor grad bestå av test av kontroller, noen analytiske handlinger og lite detaljhandlinger for å oppnå høy sikkerhet for konklusjonen på revisjonsberetningen.

Siste fase består av at revisor rapporterer og avgir en formalisert konklusjon vedrørende formålet med revisjonen gjennom en revisjonsberetning (Gulden, 2010). Konklusjonen på beretningen avgjøres av om den totale feilinformasjonen er vesentlig og gjennomgripende for regnskapet. Det er to typer konklusjoner som revisor kan avg. Konklusjonene kategoriseres som umodifisert og modifisert konklusjon. Den umodifiserte konklusjonen er en ren revisjonsberetning som bekrefter at regnskapet i det alt vesentlige er utarbeidet i samsvar med lov og forskrift (ISA 700, 2016). En modifisert konklusjon kan inndeles ytterligere i tre kategorier: konklusjon med forbehold, negativ konklusjon og konklusjon om at revisor ikke kan uttale seg om regnskapet (ISA 705, 2016). ISA 700 (2016) illustrerer revisors skjønnsmessige vurdering av forholdene som fører til modifiserte konklusjoner:

	Revisors skjønnsmessige vurdering av om virkningen eller den mulige virkningen på regnskapet er gjennomgripende	
Typen forhold som ligger til grunn for modifikasjon	Vesentlige, men ikke gjennomgripende	Vesentlige og gjennomgripende
Regnskapet inneholder vesentlig feilinformasjon	Konklusjon med forbehold	Negativ konklusjon
Manglende mulighet til å innhente tilstrekkelig og hensiktsmessig revisjonsbevis	Konklusjoner	Konklusjon om at revisor ikke kan uttale seg om regnskapet

Tabell 1: *"Typer modifiserte konklusjoner"* hentet fra ISA 705 (2016, s. 473)

Variasjoner i utførelsen av revisjonsprosessen kan forekomme på grunn av utøvelsen av revisors profesjonelle skjønn.

1.2.1 Profesjonelt skjønn

Gjennom hele revisjonsprosessen skal revisor anvende sitt *profesjonelle skjønn*. Det er kombinasjonen av relevant opplæring, erfaring, kunnskap og kompetanse som utgjør revisors profesjonelle skjønn (ISA 200, 2016). Revisjonsstandardene kan ikke adressere enhver situasjon som kan oppstå underveis i revisjonsprosessen. Det er her anvendelsen av profesjonelt skjønn kommer inn som supplement for god revisjonsskikk og revisjonsstandardene.

Flere fagorganisasjoner uttrykker at det er svært utfordrende å definere hva som utgjør et velanvendt profesjonelt skjønn og hvordan det brukes (American Institute of Certified Public Accountants; International Federation of Accountants, 2012; KPMG LLP, Glover & Prawitt, 2012).

ISA 200 (2016) tar for seg noen situasjoner der profesjonelt skjønn særlig anvendes. Beslutninger som særlig krever skjønn er ved fastsettelse av vesentlighet og revisjonsrisiko, avgjøre type, omfang og tidspunkt for revisjonshandlinger, bedømme om det er innhentet tilstrekkelig og hensiktsmessige revisjonsbevis, og ved evaluering av ledelsens anvendelse av skjønnsmessige vurderinger. Anvendelse av skjønn går igjen når revisor skal vurdere betydningen av virksomhetens anvendelse av IT- og informasjonssystemer (Gulden, 2010).

Revisors utøvelse av profesjonelt skjønn gir spillerom til å foreta ulike vurderinger og konklusjoner. Dermed kan det være vanskelig å bedømme hvor godt utfallet av profesjonelt skjønn er. En kontroll på revisorskjønnet er imidlertid at en utenforstående revisor, ut i fra revisjonsdokumentasjonen som foreligger, forstår det profesjonelle skjønn som er anvendt for å komme frem til vesentlige vurderinger og konklusjoner (ISA 200, 2016).

1.2.2 Påstander

Det er virksomhetens ledelse som, eksplisitt eller implisitt, påstår at regnskapsinformasjonen som avgis oppfyller visse kvalitative krav, kjent som regnskapspåstander (Gulden, 2010). Ledelsens påstander om regnskapet er også revisors målsetninger i revisjonen. Det vil si at revisor gjennom revisjonen skal fastslå at regnskapet ikke inneholder vesentlig feilinformasjon relatert til alle regnskapspåstandene. Det er revisors profesjonelle skjønn som skal avgjøre hvor sikre bevis som behøves for den enkelte regnskapspåstand (Gulden, 2010).

Revisjonsstandarden ISA 315 (2016) pkt. A124 angir påstandene som revisor skal bekrefte gjennom sin revisjon. Gulden (2010) har bearbeidet formuleringene i revisjonsstandarden for å beskrive hva hver enkelt påstand innebærer.

a) Påstander om registrering av transaksjoner og hendelser i regnskapsperioden som vurderes:
    a. Gyldighet – registrerte transaksjoner og hendelser har forekommet og vedrører enheten.
    b. Fullstendighet – alle transaksjoner og hendelser som skulle ha vært registrert er registrert.
    c. Nøyaktighet – beløp og andre opplysninger knyttet til registrerte transaksjoner og hendelser er riktig registrert i henhold til grunnlaget.
    d. Periodisering – transaksjoner og hendelser er registrert i riktig regnskapsperiode.
    e. Klassifisering – transaksjoner og hendelser er registrert på riktige kontoer.

ISA 315 beskriver også påstander for balansekontoer i hovedboken og påstander om presentasjon og innhold i regnskapet. De blir ikke oppgitt i vår oppgave ettersom vi vil fokusere på de overnevnte påstandene om registrering av transaksjoner og hendelser i regnskapsperioden som vurderes da vi anser de overnevnte påstandene som mest relevante for revisors forståelse og håndtering av risiko knyttet til IT- og informasjonssystemene.

1.3 Revisjonskonseptet

Revisjonen bygger på tre fundamentale konsepter som er av stor betydning for å konkludere på at regnskapet er uten vesentlige feil. De tre konseptene er vesentlighet, revisjonsrisiko og revisjonsbevis (Eilifsen, Messier, Glover & Prawitt, 2014).

1.3.1 Risikomodellen

Det eksisterer alltid en risiko for at en revisor, som reviderer i henhold til god revisjonsskikk, ikke oppdager alle vesentlige feil (Gulden, 2010). Denne risikoen kalles for revisjonsrisiko.

I henhold til ISA 200 (2016) pkt. 13c er revisjonsrisiko definert som: *"Risikoen for at revisor gir utrykk for en uriktig mening i revisjonsberetningen når regnskapet inneholder vesentlig feilinformasjon."*

Risikomodellen er ikke tydelig definert i revisjonsstandardene, men ISA 200 (2016) pkt. 13c viser til følgende sammenheng: *"Revisjonsrisiko er en funksjon av risikoen for vesentlig feilinformasjon og oppdagelsesrisiko"*. ISA 200 (2016) pkt. A37 viser til risikoen for vesentlig feilinformasjon bestående av to komponenter: iboende risiko og kontrollrisiko.

Revisjonsrisiko = Risiko for vesentlig feilinformasjon x Oppdagelsesrisiko

Revisjonsrisiko = Iboende risiko x Kontrollrisiko x Oppdagelsesrisiko

RR = IR x KR x OR

Iboende risiko er definert i ISA 200 (2016) pkt.13n(i) som *"Muligheten for at en påstand om en transaksjonsklasse, kontosaldo eller tilleggsopplysning kan inneholde feilinformasjon som kan være vesentlig, enten enkeltvis eller sammen med annen feilinformasjon, før eventuell tilhørende kontroller tas i betraktning"*.

Kontrollrisiko er definert i ISA 200 (2016) pkt.13n(ii) som *"Risikoen for at feilinformasjon som kan forekomme i en påstand om en transaksjonsklasse, kontosaldo eller tilleggsopplysning og som kan være vesentlig, enten enkeltvis eller samlet med annen feilinformasjon, ikke kan forhindres eller avdekkes og korrigeres i rett tid av enhetens interne kontroll.*

Revisor må alltid vurdere regnskaps- og internkontrollsystemet i virksomheten for å kunne planlegge og utarbeide en effektiv angrepsvinkel (Gulden, 2010). Dersom revisor finner at det ikke foreligger effektiv intern kontroll i virksomheten, vil konsekvensen være at iboende risiko og kontrollrisiko er høy, og følgelig blir det høy risiko for vesentlig feilinformasjon. Videre forklarer Gulden (2010) at høy kontrollrisiko kan skyldes av at det er kostbart og vanskelig å innrette og opprettholde kontrollberedskap internt i virksomheten og at det dessuten kan forekomme menneskelige feil selv i de beste kontrollsystemer dersom ansatte blir distrahert i utførselen av kontroller, misforstår instrukser, slurver eller mangler kunnskap.

Sammenhengen mellom iboende risiko og kontrollrisiko vil ha påvirkning på fastsettelsen av oppdagelsesrisikoen og da omfanget av revisjonshandlinger som må utføres av revisor.

Oppdagelsesrisikoen er definert i ISA 200 (2016) pkt. 13(e) som *"risikoen for at revisjonshandlingene som utføres av revisor for å redusere revisjonsrisikoen til et akseptabelt*

lavt nivå ikke vil avdekke eksisterende feilinformasjon som kan være vesentlig, enten alene eller samen med annen feilinformasjon". Forenklet så kan dette forstås som risikoen for at revisorer ikke oppdager vesentlige feil gjennom sine revisjonshandlinger.

Det foreligger alltid en viss oppdagelsesrisiko, men omfanget, type og tidspunkt av risikohåndteringshandlinger vil redusere risikoen for at vesentlig feilinformasjon ikke blir oppdaget (Gulden, 2010). Det vil være nødvendig for revisor å tilpasse sine revisjonshandlinger og nivå på oppdagelsesrisiko slik at revisjonsrisikoen bringes til et akseptabelt nivå (Gulden, 2010).

1.3.2 Revisjonsbevis

For å underbygge revisjonens konklusjon skal revisor hente inn tilstrekkelige og hensiktsmessige revisjonsbevis. Konseptet defineres i ISA 200 (2016) pkt. 13b som *"Informasjon som brukes av revisor for å komme frem til konklusjonene som revisors mening bygger på. Revisjonsbevis omfatter både informasjon som underbygger regnskapet, og annen informasjon"*.

Tilstrekkelighet viser til kvantitet av revisjonsbevisene. Det vil si at det må vurderes hvor mange revisjonsbevis revisor må innhente for å kunne trekke en konklusjon om regnskapet. Hensiktsmessighet viser til kvaliteten til revisjonsbevisene, altså hvilken styrke beviset har.

1.3.3 Vesentlighet

Gulden (2010, s. 97) definerer vesentlighet som at *"feilinformasjon er vesentlig hvis, og bare hvis, kunnskap om feilinformasjonen ville medføre at en rimelig bruker av årsregnskapet endret sine økonomiske disposisjoner"*.

Revisors vurdering av vesentlighet benyttes til å fastsette vesentlighetsgrenser. Dette er tallfestede øvre grenser for hvor mye feilinformasjon finansregnskapet kan inneholde før det kan antas å få konsekvenser for de økonomiske beslutningene til brukerne av regnskapet.

I tillegg skal revisor vurdere mangler i intern kontroll og om disse er vesentlige i samsvar med ISA 265 (2016). Det er denne vesentlighetsbetraktningen vi tar utgangspunkt i for oppgaven ettersom IT- og informasjonssystemene utgjør en del av virksomhetens interne kontroll. Det er likevel viktig å påpeke at vesentlige feil i internkontrollen kan medføre vesentlige feil i regnskapet

1.4 IT-revisjonens utvikling

Ettersom temaet i vår masteroppgave er IT-revisjon, vil vi gi et innblikk i IT-revisjonens historiske utvikling og hvilke begivenheter som har ført til økt fokus på rammeverk og standarder for IT- og informasjonssystemer, sikkerhet og risiko ved IT.

Utviklingen av teknologi og data på 1960-tallet førte til at samfunnet og næringslivet gjennomgikk en teknologisk revolusjon. Etter hvert som flere virksomheter begynte å benytte IT i sine forretningsprosesser ble det behov for økt kompetanse blant revisorer. Dermed ble IT-revisjon et eget fagfelt innen revisjon. I begynnelsen var konseptet kjent som EDP-revisjon, eller Elektronisk Data Prosess-revisjon. Dette ble starten på EDP-Auditing Association som ble opprettet i 1967 av mennesker som anerkjente behovet for en sentralisert kilde til informasjon for revisjon av kontroller i datasystemer, da dette ble mer kritisk etterhvert som teknologien ble utviklet og mer avansert (Wood et al., 2013, s. 251-252). I dag kjenner vi organisasjonen som ISACA. De er anerkjent innenfor utvikling, innføring og bruk av kunnskap og praksis på områdene informasjonssikkerhet, IT-styring og IT-revisjon (ISACA, u.å-a).

1.4.1 Rammeverk for IT-styring og informasjonssikkerhet

Ettersom ISACA er en av de fremste organisasjonene innen IT-styring, informasjonssikkerhet og IT-revisjon, vil vi trekke frem et rammeverk som de har utviklet. I 1996 utga ISACA det første COBIT- rammeverket som da utgjorde målsettinger for å hjelpe revisorene å manøvrere i kundenes IT-miljøer. Kristoffersen (2014) nevner også dette rammeverket for IKT-styring og kontroll. Det nyeste rammeverket, COBIT 5.0, ble utgitt i 2012 og er ansett som neste generasjon IT-rammeverk (Wood et al., 2013). Rammeverket er internasjonalt anvendt og brukes innenfor områdene revisjon, sikkerhet- og risikostyring, ledelse og IT-operasjoner (ISACA, u.å-c).

COBIT 5.0 tar utgangspunkt i målsettinger og behov i virksomheten for forvaltning og styring av IT-systemer på en optimal og pålitelig måte ved å integrere andre rammeverk og relaterte standarder fra blant annet ISO. Her vil vi særlig trekke frem ISO 27001 og ISO 27002. ISO 27001 omhandler krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av styringssystemer for informasjonssikkerhet i virksomheter (ISO, 2013a). ISO 27002 angir retningslinjer og standarder for informasjonssikkerhet og praksis for informasjonssikkerhets-styring. Standarden inkluderer valg, gjennomføring og styring av kontroller som tar hensyn til virksomhetens risikomiljø for informasjonssikkerhet (ISO, 2013b).

1.4.2 Strengere reguleringer

Det var ikke kun den teknologiske utviklingen som medførte et behov for mer kompetanse på IT og regnskap. I 1985 ble organisasjonen COSO etablert for å undersøke årsaker som førte til uredelig finansiell rapportering. Det viste seg å være et behov for et samlende rammeverk og retningslinjer for virksomhetsstyring slik at den finansielle rapporteringen kunne bli mer pålitelig. I 1992 utga COSO rammeverket COSO 1: Intern kontroll-et integrert rammeverk (COSO, u.å). Allikevel oppstod en rekke amerikanske regnskapsskandaler, som Enron og Arthur Andersen skandalen og WorldCom-skandalen på tidlig 2000-tallet, som følge av sammenbrudd i fundamentale deler av selskapenes internkontroll (Haukerud & Sandanger, 2003; Kristoffersen, 2014). Dette førte til skjerpede reguleringer og The Serbanes-Oxley Act ble iverksatt for å regulere styret og ledelsen i børsnoterte selskaper og revisjonsselskaper som reviderer børsnoterte selskaper. Flere seksjoner av denne reguleringen omfatter IT direkte og vi kan særlig trekke frem seksjon 404 som krever en årlig gjennomgang av effektiviteten av internkontrollen (Wood et al., 2013). For finansnæringen i Norge trådte den nye forskriften om risikostyring og internkontroll i kraft i 2009.

Som en følge av strengere reguleringer ble også behovet for kunnskap og kompetanse om IT- og informasjonssystemer mer viktig for revisors vurdering av internkontrollens effektivitet. Dette har vært medvirkende for IT-revisjonens utvikling.

1.5 Tidligere forskning

Til tross for at IT-revisjon har eksistert siden 1960-tallet er det begrenset med forskning på dette området. Som en del av forberedelsen til vårt teorikapittel utførte vi omfattende søk på tidligere forskning både på internett og i lærebøkene. Vi ble tidlig oppmerksomme på at det å finne grunnlag i tidligere forskning var vanskelig, men fant likevel en interessant studie som læreboken Wood et al. (2013) henviser til. Studien ble utført av Klamm og Watson (2009). De tok for seg 490 virksomheter som rapporterte vesentlige svakheter etter det første året med implementering av The Serbanes-Oxley Act. Dette gjorde de for å vurdere sammenheng mellom svake COSO-komponenter og IT-kontroller.

Rammeverket for internkontroll vil utdypes i kapittel 2.2, men komponentene utgjør: kontrollmiljø, risikovurdering, kontrollaktiviteter, informasjon og kommunikasjon og overvåking. Studiens funn som særskilt trekkes frem er:

- Svakt kontrollmiljø påvirker de andre komponentene. Det vil si at komponentene vil påvirke hverandre.
- IT-relaterte svake COSO-komponenter ”smitter” og skaper flere ikke IT-relaterte vesentlige svakheter og feilinformasjon.
- IT-relaterte svake COSO-komponenter påvirker påliteligheten i rapporteringen negativt, og øker antall rapporterte ikke IT-relaterte vesentlige svakheter.

Deres forskning konkluderte med at IT påvirker overordnet kontrolleffektivitet, og dermed den finansielle rapporteringen. Selv om vår oppgave ikke går ut på å vurdere hvordan implementering og bruk av IT påvirker internkontroll og finansiell rapportering i virksomheten, er studien derimot relevant til å kartlegge og vurdere revisors forhold til IT- og informasjonssystemer for regnskapsavleggelse.

2. Teori

I dette kapittelet skal vi ta for oss teorien som ligger til grunn for vår problemstilling og som videre gir bakgrunn til å vurdere og analysere informantenes svar til problemstillingen:

"Hva gjør revisor for å forstå og håndtere risiko knyttet til IT- og informasjonssystemer relevant for finansiell rapportering?".

Teorien er delt opp etter problemstillingens oppbygning og elementer. Innledningsvis gis det en beskrivelse av IT-revisjon og hva som menes med IT- og informasjonssystemer. Videre forklares hvilken funksjon internkontroll har og hvilke oppgaver revisor har i forbindelse med å vurdere de ulike komponentene. Deretter utredes revisors risikovurdering av IT- og informasjonssystemer og hvordan IT-miljø utgjør en del av den interne kontrollen. I kapittel 2.3 gis det en beskrivelse av revisors håndtering av IT- og informasjonssystemer der generelle IT-kontroller og applikasjonskontroller presenteres. Derfra går vi i dybden av revisors utførelse og håndtering gjennom test av generelle IT-kontroller og applikasjonskontroller og forklarer hvilke konsekvenser ikke-fungerende kontroller medfører for revisjonen. Avslutningsvis i delkapittel 2.4 gis en beskrivelse av hvordan eventuelle svakheter ved IT- og informasjonssystemer kan påvirke revisjonsberetningen og hvordan revisor rapporterer og kommuniserer svakhetene ved revisjonens slutt.

2.1 IT-revisjon

Virksomhetenes bruk av IT i forretningsprosesser blir stadig mer komplekst og gjennomgripende. I takt med denne utviklingen må revisor i større grad forstå hvor virksomhetens finansielle informasjon kommer fra og hvilke prosesser som sikrer at den er pålitelig (Wood et al., 2013). IT-revisjon er dermed en revisjonstilnærming som tar for seg vurderinger av virksomhetens IT-og informasjonssystemer og IT-relaterte kontroller. Fordi revisor i enhver fase av revisjonsprosessen må stille spørsmål ved og svare på hvor den finansielle informasjonen kommer fra og hvilke prosesser som sikrer dens pålitelighet, vil IT revisjon være en naturlig del av den finansielle revisjonen (Wood et al., 2013).

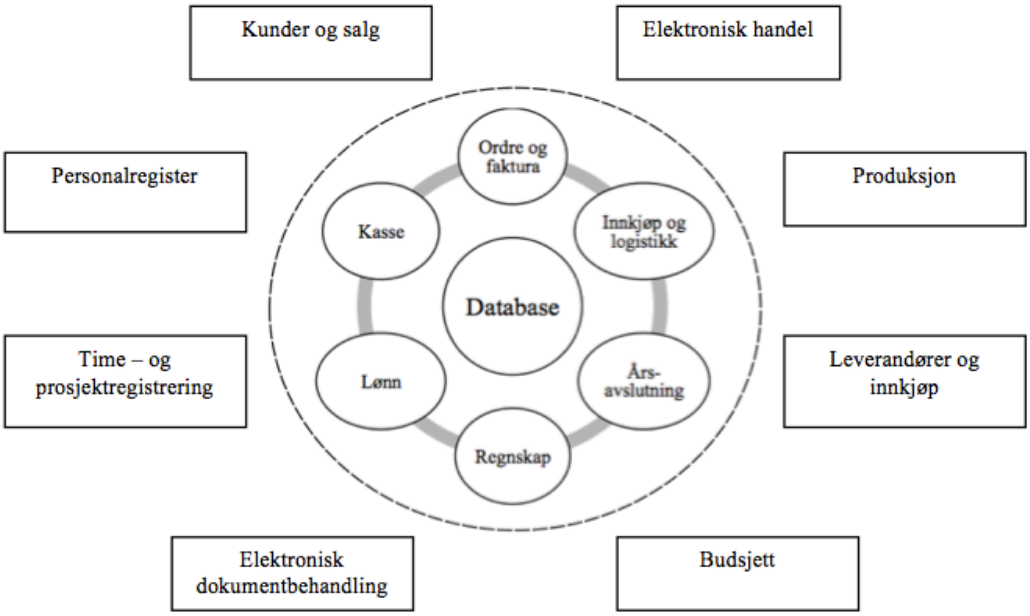
Som følge av omfattende endringer i revisors arbeidsmetoder og en bratt læringskurve kan IT-revisjon medføre en kostnadsøkning det første året. Det er sannsynlig at omfanget og bruken av tid i revisjonsarbeidet reduseres i etterfølgende år da revisor får en utjevnet læringskurve. Dette fører til at revisjoner kan effektiviseres ved å benytte IT-revisjon som revisjonstilnærming (Wood et al., 2013).

2.1.1 IT- og informasjonssystemer

I det følgende tar vi for oss de systemene som er relevant for regnskapsrapportering og tilknyttede forretningsprosesser. Kristoffersen (2014) definerer regnskapssystem som *"system bestående av en eller flere komponenter som benyttes til og som muliggjør produksjon av pliktig regnskapsrapportering og lovbestemte spesifikasjoner, og som er innrettet slik at opplysningsplikten ivaretas"*. Av definisjonen ser vi at det hovedsakelig er to oppgaver et regnskapssystem skal oppfylle. Det første er informasjonsoppgaven, som vil si at systemet skal kunne produsere regnskapet i samsvar med bokføringsloven og være et beslutningsgrunnlag for virksomheten. Det andre er kontrollfunksjonen, som vil si at det skal være mulig å kontrollere informasjonen i ettertid (Kristoffersen, 2014).

Kristoffersen (2014) og Moen og Havstein (2014) har ulike modeller for å fremstille IT- og informasjonssystemer. Fordi modellen til Moen og Havstein (2014) gir en oversikt over elementer som kan inngå i et forretningssystem vil denne være utgangspunkt for hvordan et forretningssystem kan være oppbygd. Kristoffersen (2014) er imidlertid mer på prosessnivå og brukes til å utdype og supplere Moen og Havstein (2014) sin figur.

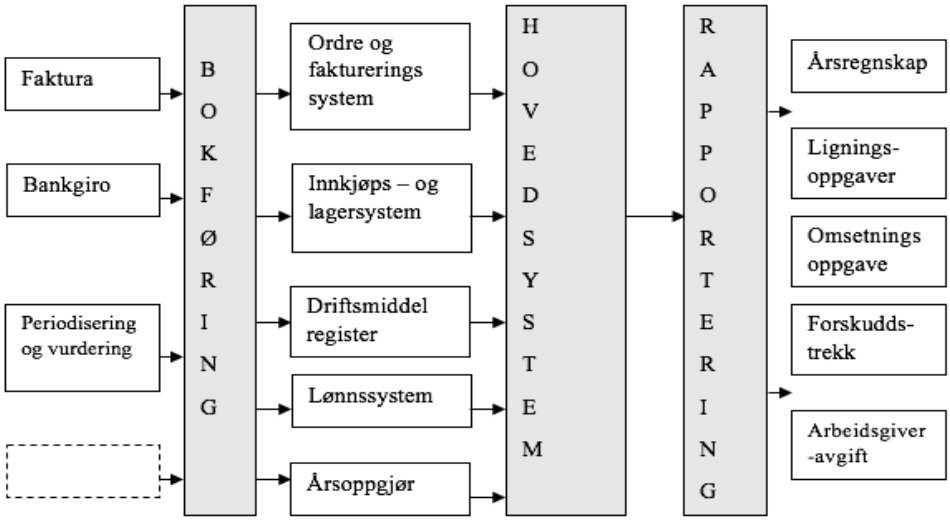
Det er støttesystemene, delsystemene og forretningsprosessene som er byggesteinene i et forretningssystem og kan illustreres gjennom følgende figur (Moen & Havstein, 2014, s. 135)



Figur 3: "Forretningssystemet" av Moen og Havstein (2014, s. 135)

De ytterste boksene er støttesystemene som inneholder opplysninger og informasjon som anvendes ved databehandling som foregår i delsystemene ordre og faktura, innkjøp og logistikk, lønn, kasse og regnskap. Den totale informasjonen som systemene inneholder utgjør selve kjernen i forretningssystemet, nemlig databasen (Moen & Havstein, 2014).

Kristoffersen (2014) fremstiller IT baserte regnskapssystemer på tilsvarende måte, men beskriver at regnskapssystemet ofte består av et hovedsystem som har ett eller flere delsystemer:



Figur 4: ***"IT-basert regnskapssystem" av Kristoffersen (2014, s. 156)***

Prosessen begynner med at input, som kan være både intern og ekstern dokumentasjon, registreres i delsystemene automatisk eller manuelt (Kristoffersen, 2014). Manuelt vil for eksempel si at en ansatt registrerer timene sine på en timeliste som legges inn i systemet, mens automatisk vil for eksempel være skattetrekk, feriepenger og arbeidsgiveravgift som beregnes i lagrede filer, og som sender satsene direkte inn i lønnssystemet når den ansatte registrerer timene sine. Registreringen behandles videre og sendes til hovedsystemet. Hovedsystemet mottar og systematiserer informasjon om alle poster som rapporteres i regnskapet (Kristoffersen, 2014). Dette omfatter eiendeler, gjeld, egenkapital, inntekter, kostnader, transaksjoner med kunder og leverandører og systemgenererte poster. Det sistnevnte er poster som beregnes av regnskapssystemet og kan for eksempel være fordelingsnøkkel for fradragsføring av merverdiavgift (Kristoffersen, 2014). Output fra hovedsystemet kan ta form i ulike rapporter der de vanligste er: bokføringsspesifikasjon, kontospesifikasjon, resultatregnskap, balanse, kunde- og leverandørspesifikasjoner, og grunnlag for offentlige oppgaver (Kristoffersen, 2014).

Hvilke systemer som er relevante for revisor er et forhold som er gjenstand for revisors skjønn, jfr. ISA 315 (2016) pkt. A92. Revisor avgjør hvilke systemer som er relevante basert på hvilke påstander som skal bekreftes for hvilke regnskapsposter, samt hvilke systemer som behandler transaksjonene som havner på disse regnskapspostene (Wood et al., 2013). For eksempel, dersom revisor skal bekrefte gyldigheten for lønnskostnader, vil både et system for timeregistrering og godkjenning av timer, og et system for beregning av lønn understøtte lønnsprosessen. Spørsmålet revisor da må stille seg er i hvilke systemer ligger applikasjonskontrollene og hvilke systemer skal testes for generelle IT kontroller. Svaret i dette tilfellet er i timeregistreringssystemet og lønnssystemet. Generelle IT-kontroller og applikasjonskontroller som omfatter og inngår i virksomhetens IT- og informasjonssystemer vil bli presentert i kapittel 2.3.1 om IT-relaterte kontrollaktiviteter.

2.1.2 IT-revisor

Som tidligere nevnt bruker de fleste virksomheter IT- og informasjonssystemer for regnskapsavleggelse og andre forretningsprosesser. Det er flere momenter som preger kompleksiteten i informasjonssystemene. Det kan være virksomhetstype, standardiserte eller skreddersydde systemer, at de virker alene eller agerer med andre systemer, være store og omfattende eller små. Anvendelsen av komplekse IT- og informasjonssystemer har medført at forventningene til revisors kompetanse har økt og at revisjonstilnærmingen som omfatter IT har blitt en naturlig del av revisjonsprosessen.

I tilfeller der revisjonskunden har omfattende og kompliserte styringssystemer kan det være behov for involvering av en ekspert (Gulden, 2010). En IT-revisor anses som en ekspert eller spesialist. Mange IT-revisorer har bakgrunn som finansielle revisorer. I tillegg bruker de store revisjonsselskapene betydelige ressurser på opplæring og kursing av sine ansatte for å øke kompetansen innen IT-revisjon fordi det ofte vil være en hensiktsmessig tilnærming for å gjennomføre en effektiv revisjon på.

I vår oppgave definerer vi IT-revisor som en som er CISA-sertifisert. Dette er den mest anerkjente tittelen innen IT-revisjon og utstedes av fagorganisasjonen ISACA (ISACA, u.å-b). Sertifiseringen er en kvalitetssikring av IT-ferdigheter, erfaringer og kunnskap om IT-revisjon. En CISA-sertifisert IT-revisor er også i stand til å identifisere sårbarheter og rapportere på virksomhetens etterlevelse av kontroller (ISACA, u.å-b).

Andre typer sertifiseringsordninger som ISACA utsteder er:

- Certified Information Security Manager (CISM).
- Certified in Risk and Information Systems Control (CRISC).
- Certified in the Governance of Enterprise IT (CGEIT).

2.2 Forståelse av IT- og informasjonssystemer

I dette kapittelet retter vi fokuset på revisors forståelse av internkontrollen siden IT- og informasjonssystemene utgjør en del av den. Dette er også en lovfestet plikt gjennom Revisorloven (1999) §5-1 som angir at *"Revisor skal se etter at den revisjonspliktige har ordnet formuesforvaltningen på en betryggende måte og med forsvarlig kontroll"*.

Når revisor gjør en risikovurdering av IT- og informasjonssystemer som er relevant for finansiell rapportering, vil det være mulig å avgjøre hvilke regnskapspåstander/linjer som utgjør størst risiko og dermed utføre de handlingene som er mest hensiktsmessige for å få en effektiv revisjon.

2.2.1 Internkontroll

For at virksomheter skal nå sine mål er det nødvendig med systematisk styring. Dette er en kontinuerlig prosess som foregår fra virksomheten vedtar sine mål til planlegging, gjennomføring og rapportering av resultater. Ledelsen bruker internkontroll som et verktøy for å nå virksomhetens mål (Kristoffersen, 2014). Det er styret som har ansvar for forvaltningen av virksomheten og fastsetter retningslinjer for ledelsen. Ledelsen har ansvaret for all aktivitet, inklusiv risikostyring og internkontroll (Kristoffersen, 2014, s. 61).

Formålene med internkontroll er å sikre målrettet og effektiv drift, pålitelig rapportering og at det overholdes de lover og regler de er underlagt (Kristoffersen, 2014).

Et anerkjent rammeverk for internkontroll, COSO 1: Intern kontroll-et integrert rammeverk, ble publisert og utviklet av COSO i 1992. I 2013 utga de en oppdatert versjon av COSO 1, og siden den gang har de også utviklet rammeverket COSO 2: Helhetlig risikostyring-et integrert rammeverk (Kristoffersen, 2014, s. 34).

2.2.2 COSO 1: Internkontroll-et integrert rammeverk

COSO-modellen er først og fremst et styringsverktøy for virksomhetens målsettinger innen drift, rapportering og etterlevelse av lover og regler. Den består av følgende fem hovedkomponenter: Kontrollmiljø, risikovurdering, kontrollaktiviteter, informasjon og kommunikasjon og oppfølging og overvåking. COSO (2013) har utviklet 17 prinsipper som virksomheter bør etterleve for en god internkontroll. Prinsippene blir presentert under hver komponent de tilhører.

Figur 5: *"The COSO Cube"* hentet fra COSO og McNally (2013, s. 4)

Kontrollmiljø

Kontrollmiljøet er grunnmuren for internkontroll i en virksomhet. Det er ledelsens ansvar å fastsette retningslinjer og skape holdninger som former et godt kontrollmiljø (Kristoffersen, 2014). COSO (2013) har angitt fem prinsipper som et kontrollmiljø bør bestå av.

1. at virksomheten utviser integritet og etiske verdier.
2. at styret er uavhengig og former retningslinjer for gjennomføring av internkontroll.
3. at ledelsen etablerer og strukturerer ansvarsområder.
4. at kompetente ansatte blir og kommer til virksomheten.
5. at internkontroll er enkeltpersonens ansvar innenfor sitt ansvarsområde.

Som beskrevet i tidligere forskning utført av Klamm og Watson (2009) har kontrollmiljø sterk tilknytning til resten av komponentene. Derfor er dette et område i internkontrollen som revisor bør vie tid til å forstå og vurdere da kontrollmiljøet kan gi indikasjoner på hvilken risiko som kan foreligge for resten av internkontrollen. Revisors vurdering av kontrollmiljøet

er også pålagt etter revisjonsstandarden ISA 315 (2016) pkt. 14. Det vil si at revisor må vurdere hvorvidt prinsippene som er nevnt ovenfor fremmer et godt kontrollmiljø ved at det vil ha en positiv virkning på de andre komponentene i internkontrollen.

Risikovurdering

Ved at virksomheter står overfor eksterne og interne trusler, kan dette hindre dem i å nå sine mål. Dette defineres her som risiko. Risikovurdering er dermed en kontinuerlig prosess som tar for seg aktivitetene i virksomheten og skal avdekke interne og eksterne risikofaktorer som kartlegges og analyseres (Kristoffersen, 2014, s. 39). For en god risikovurdering i virksomheten er det følgende prinsipper som bør følges (COSO, 2013):

6. at målsettinger er konkret formulerte og gjør det mulig å vurdere risikoen for at målene ikke blir nådd.
7. at risiko kan identifiseres for hele virksomheten og analyseres for å kunne håndteres.
8. at virksomheten tar høyde for risiko for potensielle misligheter.
9. at virksomheten kan identifisere og vurdere endringer som kan ha innvirkninger på internkontrollen.

Revisor skal opparbeide seg en forståelse av virksomheten og dens prosesser for å identifisere forretningsrisikoer, hvilken betydning de har, sannsynligheten for at de vil forekomme og hvilke tiltak som iverksettes for å håndtere risikoene (ISA 315, 2016). Dette er en prosess som er viktig for å hjelpe revisor med å identifisere risiko for vesentlig feilinformasjon.

Kontrollaktiviteter

Dersom virksomheten har en risikovurderingsprosess der interne og eksterne risikoer er identifisert, kartlagt og analysert, er neste steg å iverksette tiltak for å håndtere risikoene. Kontrollaktiviteter er tiltak utformet som rutiner og retningslinjer som skal sikre at risikohåndtering som ledelsen iverksetter blir utført (Kristoffersen, 2014). Prinsippene for gode kontrollaktiviteter er (COSO, 2013):

10. at virksomheten velger og utvikler kontrollaktiviteter som bidrar til å redusere risikoer til et akseptabelt nivå for at målene blir nådd.
11. at generelle kontrollaktiviteter for teknologi velges ut og utvikles for å støtte målene.
12. at virksomheten iverksetter kontrollaktiviteter i samsvar med vedtatte retningslinjer og prosedyrer.

Det er likevel viktig å påpeke at implementering av kontrolltiltak alltid vurderes opp i mot en kost/nytte-betraktning. Nytten av å iverksette et kontrolltiltak må være større enn kostnaden ved å ha den. Det er lite sannsynlig at en virksomhet iverksetter tiltak for å håndtere enhver risiko. Virksomhetene vil velge ut kontrolltiltak for de risikoene som er lovpålagte å ha, for eksempel knyttet til finansiell rapportering, men også der det foreligger vesentlige risikoer i virksomhetens forretningsprosesser.

Fordi teknologi ofte anvendes i forretningsprosesser, utgjør automatiske kontroller en del av virksomhetens kontrollaktiviteter. En automatisk kontroll er en kontroll som er innebygd i programmet. Det vil si at systemet sørger for at en kontroll utføres (Kristoffersen, 2014). Dette kan for eksempel være at alle obligatoriske felter må fylles ut før informasjonen kan behandles videre, passordkontroll eller at kundenummer er gyldige. Manuell kontroll innebærer at en person utfører kontrollen. Det er vanligvis kombinasjoner av manuelle og automatiserte kontroller i de fleste virksomheter (Kristoffersen, 2014).

Generelle IT-kontroller og applikasjonskontroller inngår som en del av virksomhetenes kontrollaktiviteter dersom de anvender IT- og informasjonssystemer. Siden dette er vesentlige begreper for oppgavens problemstilling vil dette utdypes i kapittel 2.3.

I henhold til ISA 315 (2016) pkt. 20 skal revisor opparbeide en forståelse av kontrollaktivitetene for å kunne vurdere risikoene for vesentlige feilinformasjon på påstandsnivå, og for å utforme revisjonshandlinger for å håndtere de anslåtte risikoene.

Informasjon og kommunikasjon

Informasjon og kommunikasjon muliggjør aktivitetene i virksomheten ved å prosessere, registrere og rapportere informasjon effektivt i rett tid til rett person (Kristoffersen, 2014, s. 54). Informasjon kan være både intern og ekstern. For at informasjon og kommunikasjon skal bidra til en effektiv internkontroll, har COSO (2013) følgende prinsipper:

13. at virksomheten bruker relevant og korrekt informasjon som øker kvaliteten i internkontrollsystemet.
14. at virksomheten bruker intern kommunikasjon, inkludert mål og ansvar for internkontroll som støtter opp under internkontrollen.
15. at virksomheten bruker ekstern kommunikasjon om forhold som påvirker internkontrollens kvalitet.

På dette punktet skiller ISA 315 seg litt fra selve komponenten i COSO-modellen. Mens det omhandler informasjon og kommunikasjon på et operasjonelt nivå i COSO-modellen, er ISA 315 mer innrettet mot revisors forståelse av selve informasjonssystemet som sørger for virksomhetens forretningsprosesser. Dette er angitt i ISA 315 (2016) pkt. 18 ved at revisor skal opparbeide en forståelse av informasjonssystemene, herunder de tilknyttede forretningsprosessene, som er relevant for finansiell rapportering. Dette er for at revisor skal kunne identifisere risiko og relevante kontrolltiltak på påstandsnivå. Derfor må denne komponenten sees i sammenheng med de andre komponentene risikovurdering og kontrollaktiviteter når det kommer til revisors forståelse av virksomhetens internkontroll. Her skal revisor ta for seg rutinene og prosedyrene som angår IT-systemene og kartlegge prosessene i regnskapssystemet. Dette vil beskrives nærmere i kapittel 2.2.3 om IT-miljø.

Oppfølging og overvåkning

Elementene i de andre komponentene kan bli utdaterte eller endret. Dermed kan også internkontrollen bli lite hensiktsmessig eller irrelevant dersom ikke nødvendig overvåking og oppfølging iverksettes for å kontinuerlig påse at internkontrollen er formålstjenlig (Kristoffersen, 2014). COSO (2013) sine prinsipper for god oppfølging og overvåking utgjør:

16. at virksomheten gjennomfører løpende og/eller periodiske evalueringer.
17. at virksomheten evaluerer og kommuniserer avvik slik at korrigerende tiltak kan iverksettes.

Virksomheter kan ha ulike grader av oppfølging og overvåking. I store virksomheter kan det være en egen internrevisjon som gjennomfører vurderinger av kontrollenes effektivitet og rapporterer til styret. I små- og mellomstore virksomheter kan oppfølging og overvåking være en del av den ansattes arbeidsoppgave, der eventuelle avvik rapporteres til ledelsen. I noen virksomheter kan det være ansatt egne controllere. Uavhengig av størrelsen på selskapet er det ledelsens ansvar å sørge for å følge opp rapporteringer. Ledelsen kan også blant annet gjennomføre løpende oppfølgning ved å utføre avviksanalyser og budsjettoppfølging (Kristoffersen, 2014).

Revisors oppgave er å opparbeide en forståelse av de viktigste aktivitetene virksomheten anvender for å overvåke den interne kontrollen som er relevant for finansiell rapportering, herunder tiltak som er relatert til kontrollaktivitetene som er relevante for revisjonen og

hvordan virksomheten iverksetter utbedrende tiltak knyttet til kontrollene med svakheter (ISA 315, 2016) pkt. 20.

2.2.3 IT-miljø

ISA 315 (2016) pkt.A62 viser til IT som en fordel for virksomhetens internkontroll ved at det kan bidra til lav kontrollrisiko i virksomheten ved at det er mulig for virksomheten å:

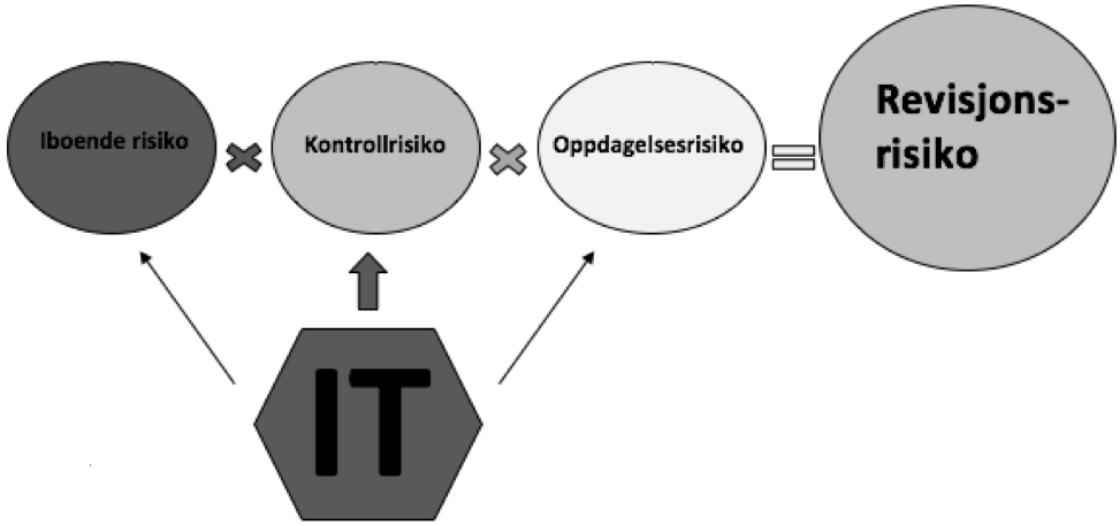
- anvende fastlagte forretningsregler på en ensartet måte og utføre komplekse beregninger ved behandling av store mengder transaksjoner eller data,
- forbedre informasjonens aktualitet, tilgjengelighet og nøyaktighet,
- forenkle videre analyse av informasjon,
- forbedre muligheten til å overvåke hvorvidt enhetens aktiviteter, retningslinjer og rutiner fungerer effektivt,
- redusere risikoen for at kontroller omgås og
- forbedre muligheten til å oppnå en effektiv arbeidsdeling ved å innføre sikkerhetskontroller i applikasjoner, databaser og operativsystemer.

Selv om IT kan være en fordel for virksomhetens interne kontroll skaper den også andre, nye risikoområder og feilkilder. Dette kan medføre høy kontrollrisiko. Risikoforholdene er hentet fra veiledningspunktet A63 i ISA 315 (2016):

- At det bygger på systemer eller programmer som behandler data unøyaktig, behandler unøyaktige data eller begge deler.
- Uautorisert tilgang til data som kan føre til ødeleggelse av eller urettmessige endringer av data, herunder registrering av uautoriserte eller ikke-eksisterende transaksjoner, eller unøyaktig registrering av transaksjoner. Særlige risikoer kan oppstå når flere brukere har tilgang til en felles database.
- Mulighet for at IT-medarbeidere får tilgangsprivilegier ut over de som er nødvendige for å utføre de oppgavene de er blitt tildelt, noe som bryter ned arbeidsdelingen.
- Uautoriserte endringer av faste data.
- Uautoriserte endringer i systemer eller programmer.
- Unnlatelse av å foreta nødvendige endringer i systemer eller programmer.
- Urettmessige manuelle inngrep.
- Mulig tap av data eller manglende tilgang til nødvendige data.

For at revisor skal kunne bekrefte årsregnskapet med betryggende sikkerhet, må revisor identifisere og foreta risikovurderingshandlinger av de områder og aktiviteter hvor det foreligger størst risiko. Revisor opparbeider seg en forståelse av virksomhetens IT-miljø og identifiserer andre elementer som, etter revisor skjønn, vil kunne ha effekt på risikovurderingen av internkontroll og forholdene beskrevet ovenfor.

Figuren under illustrerer IT-miljøets påvirkning av revisjonsrisikoen. IT har en betydelig innvirkning på kontrollrisikoen i tilknytning til regnskapet.



Figur 6: *"IT-miljø påvirker revisjonsrisikoen"* av Kvalvik (2014)

IT-miljø er definert av Den Norske Revisorforeningen (2016) som *"policyene og prosedyrene som enheten implementerer og IT infrastrukturene og applikasjonsprogrammer som den bruker for å støtte sine forretningsoperasjoner og nå sine forretningsmessige strategiske mål"*

Hva som inngår i et IT-miljø er ikke tydelig definert i lærebøkene. Antakeligvis kan IT-miljø forstås som et overordnet begrep og kan inneholde langt mer enn bare policyer og prosedyrer, og hvilke IT-infrastrukturer og applikasjonsprogrammer virksomheten bruker.

Under fremgår noen eksempler på elementer revisor kan innhente informasjon for å kartlegge IT-miljøet.

Elementene er hentet fra Sylvi Nerskogen sin forelesning *"Håndtering av IT-relatert risiko i revisjon, del 1"* holdt ved Universitet i Agder 1. November 2016.

- IT-strategi
- IT-organisering
- Risikovurdering virksomheten selv har utført og i hvor stor grad IT er involvert i dette
- Serviceorganisasjoner/Outsourcet IT-funksjon
- Cloud Computing/Nettskytjenester
- Lokasjoner
- Policyer og prosedyrer
- Applikasjoner og transaksjonstyper
- Endringer i IT-miljø

Revisors identifisering og vurdering av elementene over samt andre elementer ved virksomhetens IT-miljø, gir revisor mulighet til å skape en forventning om virksomhetens interne kontroll. Ved å vurdere IT-miljøet kan revisor lettere identifisere og senere teste relevante kontroller som er iverksatt av virksomheten for å sikre at IT-systemene fungerer hensiktsmessig og at informasjonssikkerheten er opprettholdt. En vurdering av elementene i IT-miljøet vil dermed gjøre det mulig for revisor å innhente nødvendig informasjon og legge til rette en effektiv revisjonstilnærming når revisjonen skal planlegges.

I kapittelet om intern kontroll har vi sett hvordan revisor må vurdere kontrollmiljøet og hvordan ledelsen og de ansattes holdninger til IT- og informasjonssystemer kan ha en innvirkning på revisors risikovurdering. Moeller (2010) viser til en rekke ulike forslag på hvordan revisor kan opparbeide seg en forståelse av virksomhetens kontrollmiljø. Revisor kan innhente tilstrekkelig informasjon om IT-miljøet gjennom samtaler med IT-ledelsen, gjennomgå organisasjonsstrukturer, identifisere hvor IT-ressursene befinner seg og stillingsfordeling for å fastslå om det foreligger hensiktsmessig arbeidsdeling. Det er også mulig å foreta forespørsler om hvorvidt det foreligger ansvarsfordeling for å overholde retningslinjene og rutinene, hvordan disse kommuniseres med ansatte og hvordan overholdelse av retningslinjer og prosedyrer overvåkes. Moeller (2010) forklarer videre at revisor kan gjennom diskusjon med ledelsen vurdere om IT-strategien er i tråd med de overordnede forretningsstrategiene for å forsikre seg om hensiktsmessig drift av IT- og informasjonssystemene. Ved å gjennomgå dokumenterte IT-retningslinjer og prosedyrer for

fullstendighet og relevans, kan revisor vurdere hvorvidt virksomheten legger spesielt vekt på sikkerhet og drift av IT- og informasjonssystemer. Endringer i IT-miljøet, som utskifting av sentrale nøkkelpersoner i IT-funksjonen, stadig endringer av IT-strategi og tjenesteleverandører av IT-systemer, kan gi revisor en indikasjon på hvilken risiko for vesentlig feilinformasjon det er mulig å forvente. Der hvor det ikke er hensiktsmessige IT-strategier og der organiseringen relatert til IT-systemene er ineffektive, vil det som en konsekvens medføre negativ innvirkning på resten av komponentene i virksomhetens interne kontroll. Dette kan videre medføre økt risiko for vesentlig feilinformasjon.

I dag overlater flere virksomheter egne arbeidsoppgaver til uavhengige serviceorganisasjoner. Blant annet har outsorucing av hele eller deler av virksomhetens IT-funksjon til eksterne virksomheter, med bedre kompetanse og flere retningslinjer på kontroll og rutiner, blitt vanligere. Samtidig har også bruken av nettskytjenester, eller Cloud Computing, økt ved å gjøre det mulig for virksomheter å foreta blant annet dataprosessering og datalagring av informasjon på eksterne servere (Løwer & Sanvik, 2015). Felles for outsourcing av IT-funksjoner og nettskytjenester er at det medfører mindre kontrollmulighet av informasjon ved at flere har tilgang til den. Allerede når revisjonen planlegges må revisor skaffe oversikt over hvilken virkning bruk at serviceorganisasjonene kan ha for virksomhetens regnskaps- og internkontrollsystemer (Gulden, 2010). Revisor må påse at det foreligger middels eller lav kontrollrisiko som følge av en overordnet vurdering av hvorvidt serviceorganisasjonen er kompetente til å utføre arbeidsoppgavene og har iverksatt effektive og omfattende kontroller. Dersom revisor finner at kontrollrisikoen til de berørte regnskapsopplysningene er påvirket av serviceorganisasjonen kontrollrutiner, må revisor gjennomføre ytterligere undersøkelser for å anslå kontrollrisikoen (Gulden, 2010). For å underbygge et anslag om lav eller middels risiko hos serviceorganisasjonen er det nødvendig at revisor innhenter en type 1 eller type 2 rapport som er avgitt av revisor engasjert av serviceorganisasjonen:

- Type 1 rapport er en rapport som avgir en beskrivelse og utforming av kontroller hos en serviceorganisasjon jfr. ISA 402 (2016) pkt. 8(b).

- Type 2 rapport er en rapport som avgir en beskrivelse og utforming av kontroller hos en serviceorganisasjon og hvorvidt de fungerer måleffektivt jfr. ISA 402 (2016) pkt. 8(c).

Revisor skal opparbeide en forståelse av virksomhetens egen risikovurdering og hvorvidt de anser IT- og informasjonssystemer som er involvert i deres prosesser som en risiko og eventuelt hvilke tiltak de har iverksatt for å håndtere IT-relatert risiko. For revisor vil det være ressurssparende dersom det er mulig identifisere effektive kontroller og bygge egen revisjonstilnærming på virksomhetens egen risikovurdering eller internrevisjon (Gulden, 2015). Ved å bekrefte kvaliteten og gjennomføringen av virksomhetens interne kontroller og påse at det foreligger en lav kontrollrisiko, vil revisor ha mulighet til redusere omfanget av substanshandlinger (Gulden, 2015).

2.3 Håndtering av IT- og informasjonssystemer

Dersom revisor kommer frem til at virksomhetens bruk av IT- og informasjonssystemer har betydning for den finansielle rapporteringen, vil det som oftest være nødvendig for revisor å teste effektiviteten av virksomhetens kontrolltiltak. I dette kapittelet skal vi ta for oss kontrollaktivitetene som er relevant for IT- og informasjonssystemer. Videre gis en innføring i relevante aktiviteter som sørger for at IT-systemene fungerer hensiktsmessig og at informasjonssikkerheten opprettholdes. Disse er generelle IT-kontroller og applikasjonskontroller.

2.3.1 IT-relaterte kontrollaktiviteter

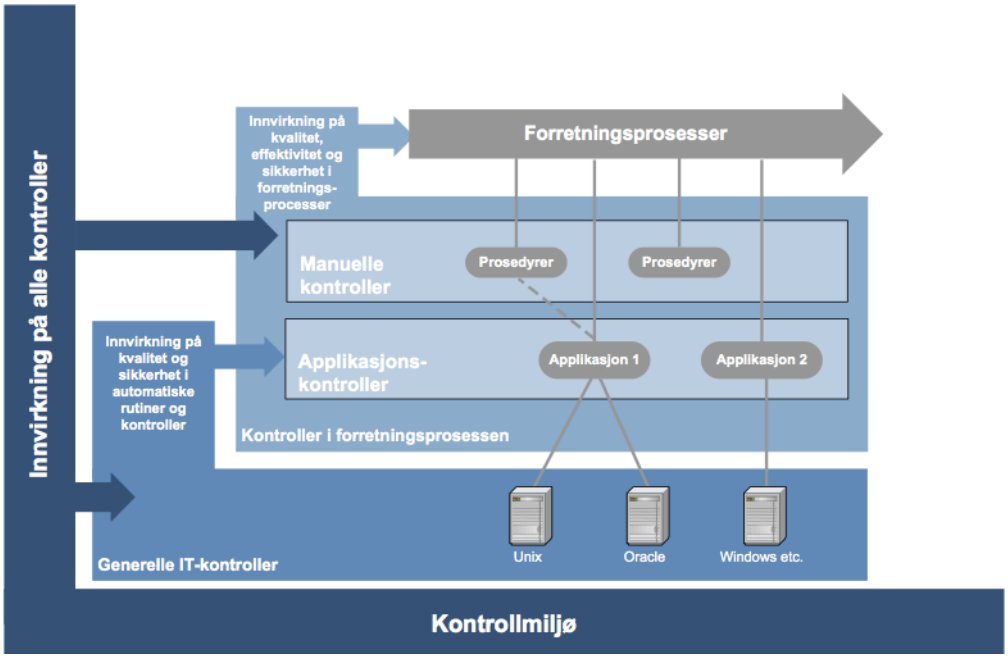
Det er viktig at virksomheten iverksetter nødvendige kontrolltiltak for å redusere risiko som kan oppstå som følge av anvendelse av IT- og informasjonssystemer. Kontrollaktivitetene som iverksettes skal fungere som retningslinjer og rutiner og gi rimelig sikkerhet for at kontrollmålsettinger blir nådd og risikohåndtering blir gjennomført (Kristoffersen, 2014, s. 298). Kristoffersen (2014) viser til seks viktige elementer i prinsippet om iverksetting av kontrollaktiviteter gjennom retningslinjer og prosedyrer:

- Etablering av retningslinjer og prosedyrer for iverksetting av instrukser fra ledelsen.
- Etablering av ansvar og myndighet for gjennomføring av retningslinjer og prosedyrer.
- Gjennomføring til fastsatt tid.
- Iverksetting av korrigerende tiltak.
- Bruk av kompetent personell.
- Evaluering av retningslinjer og prosedyrer.

De internasjonale revisjonsstandardene skiller mellom to kategorier av kontrollaktiviteter som rettes mot IT- og informasjonssystemer. Disse kontrollene er generelle IT-kontroller og applikasjonskontroller, og er en viktig del av kontrollaktivitetene i COSO-modellen.

Lærebøkene til Kristoffersen (2014) og Wood et al. (2013) presenterer generelle IT-kontroller først og deretter applikasjonskontroller. Det bør bemerkes at revisors fremgangsmåte er mer dynamisk enn beskrevet i bøkene og at revisors forståelse og testing av kontrollene kan foregå om hverandre og samtidig. Når revisor foretar en vurdering av enhetens internkontroll, herunder informasjonssystemene og tilknyttede forretningsprosesser, vil revisor først avgjøre hvilke systemer/applikasjoner som er relevante for den finansielle rapporteringen og deretter avgjøre hvilke generelle IT-kontroller som vil være relevante å teste. Mengden av kontroller som bør testes er gjenstand for revisors profesjonelle skjønn, risikovurdering og hva revisjonsmetodikken tilsier at revisor skal teste.

Figuren under viser elementer og sammenhenger i internkontroll. Av figuren kan vi se at kontrollmiljøet har innvirkning på generelle IT-kontroller, applikasjonskontroller og manuelle kontroller. Generelle IT-kontroller har innvirkning på kvalitet og sikkerhet i automatiske rutiner og kontroller, da applikasjonskontroller. Figuren viser videre hvordan applikasjonskontrollene har innvirkning på kvalitet, effektivitet og sikkerhet i virksomhetens forretningsprosesser.



Figur 7: *"Elementer og sammenhenger i internkontroll" hentet fra Sylvi Nerskogen sin forelesning* "Håndtering av IT-relatert risiko i revisjon, del 2" *holdt ved Universitet i Agder 2. November 2016.*

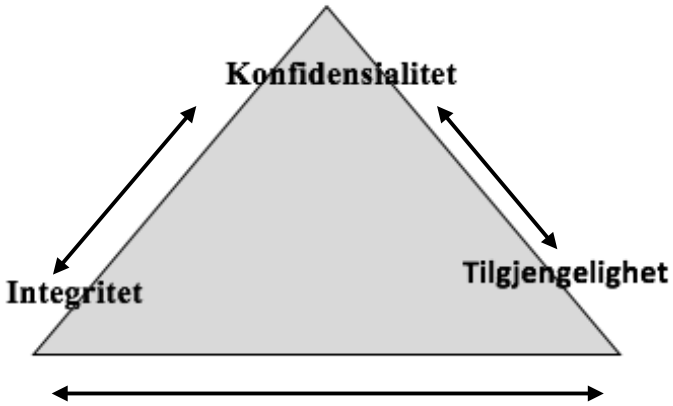
For at data, rapporter og informasjon fra IT- og informasjonssystemer skal være pålitelige for brukerne er det viktig at virksomheten sørger for god informasjonssikkerhet. Mengden og kvaliteten av kontroller som iverksettes for å overholde de tre prinsippene konfidensialitet, tilgjengelighet og integritet, vil avhenge av størrelsen på IT-miljøet og virksomhetens egne særtrekk (Moen & Havstein, 2014).

2.3.2 Konfidensialitet, integritet og tilgjengelighet

De siste årene har det blitt lagt mer vekt på sikkerhet rundt IT- og informasjonssystemer og en rekke tiltak, blant annet standardene ISO 27001 og ISO 27002, har blitt utarbeidet for å øke fokuset på ledelsessystemer for informasjonssikkerhet.

Begrepet ledelsessystem for informasjonssikkerhet kommer fra det engelsket begrepet ”Information Security Management System”, oftest omtalt av forkortelsen ISMS. Den internasjonale standarden ISO 27001 Ledelsessystem for informasjonssikkerhet er utarbeidet for å stille krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av ledelsessystemet for å ivareta konfidensialitet, integritet og tilgjengeligheten av informasjon.

Sikkerhetstriangelet som er illustrert nedenfor er en kjent modell innenfor informasjonssikkerhet og brukes i lærebøkene IT-revisjon av Wood et al. (2013) og Regnskapsorganisering av Moen og Havstein (2014).



Figur 8: *”Sikkerhetstriangel”* av Wood et al. (2013, s. 5)

Konfidensialitet refererer til interne og eksterne brukere av datasystemet. (Wood et al., 2013). Prinsippet baserer seg på at interne brukere bare skal ha tilgang til de systemene og data som er nødvendig for å utføre sine arbeidsoppgaver. Eksternt har konfidensialitet betydning ved at data beskyttes mot uautorisert tilgang ved å iverksette sikringstiltak som brannmurer, kryptering og tilgangskontroller (Wood et al., 2013).

Integritet i regnskapssammenheng er knyttet til ledelsens påstander som beskrevet i kapittel 1.2.2 og konseptet om at årsregnskapet skal gi et rettvisende bilde av virksomhetens eiendeler, gjeld, finansielle stilling og resultat. Integritet skal sikre at regnskapsinformasjonen som fremkommer er pålitelig (Wood et al., 2013).
Tilgjengelighet innebærer at informasjon og data er tilgjengelig til rett tid og på rett sted for ledelsen, ansatte, kunder og andre ved behov. Prinsippet skal også sikre virksomheten mot at data går tapt som følge av avbrudd eller skade (Wood et al., 2013).

Sikkerhetstriangelet viser en sammenheng mellom prinsippene konfidensialitet, integritet og tilgjengelighet. Sammenhengen mellom konfidensialitet og integritet bygger på virksomhetens interne kontroll. Dersom prinsippet om konfidensialitet ikke overholdes kan det medføre integritetsproblemer i dataen eller gi økt potensiale for at regnskapet ikke gir et rettvisende bilde (Wood et al., 2013). Videre bygger sammenhengen mellom konfidensialitet og tilgjengelighet på ledelsens retningslinjer og prosedyrer der data skal være tilgjengelig til rett tid og rett person. Tilgjengelighet og integritet har en sammenheng der det foreligger behov for nødvendig data for å behandle transaksjoner og utarbeide et regnskap (Wood et al., 2013).

Grunnlaget for god styring av informasjonssikkerhet er basert på ledelsens fokus på etablering, overvåking og forbedring av egne styringssystemer og anvendte prosedyrer og retningslinjer for bevare de overnevnte prinsippene (ISO, 2013a).

Læreboken til Wood et al. (2013) illustrerer eksempler på kontroller som virksomheten kan iverksette for å bevare informasjonssikkerheten. Figuren viser sammenheng mellom de tre prinsippene og IT-målene endringshåndtering, drift og sikkerhet.

IT-mål	**Konfidensialitet**	**Integritet**	**Tilgjengelighet**
Endrings-håndtering	Arbeidsdeling og autorisasjon	Nøyaktighet og pålitelighet av endringer	Gjenoppretningsrutiner
Drift	Sikkerhetskopier, tilgang til sikkerhetskopier og adgangskontroller	Systemgjenopprettbarhet	Serverkapasitet, lisenser og sikkerhetskopier
Sikkerhet	Passord, logghistorikk og tillatelser	Art og pålitelighet av iverksatte kontroller	Eksistens av sikkerhetskontroller og passordrutiner

Tabell 2: ”IT Objectives and Domains Mapped to CIA” av Wood et al. (2013, s. 7)

2.3.3 Generelle IT-kontroller

Generelle IT-kontroller er definert i ISA 315 (2016) pkt. A104 som retningslinjer og prosedyrer som skal sørge for at applikasjonskontroller fungerer effektivt. Flere av lærebøkene, blant annet (Eilifsen et al., 2014; Moeller, 2010; Wood et al., 2013) tar utgangspunkt i de internasjonale revisjonsstandardene, og viser til fire kategorier av generelle IT-kontroller:

- Tilgang- og sikkerhetskontroll
- Datasenter- og nettverksdrift
- Kjøp, endringer og vedlikehold av systemprogramvare
- Kjøp, utvikling og vedlikehold av applikasjoner

ISA 315 (2016) pkt. A104 lister også opp *"programendringer"* som en egen generell IT-kontroll.

Styret og ledelsen bør iverksette effektiv organisering av nødvendige generelle IT-kontroller og sørge for at alle ansatte er kjent med virksomhetenes retningslinjer og prosedyrer relatert til systemene som anvendes (Moeller, 2010). Det bør også sørges for at det foreligger retningslinjer og prosedyrer for hvilke rettigheter hver enkelt ansatt har og at oppgaver og ansvar for systemering, programmering og bruk av programmer er adskilt i virksomheter der det er mulig (Gulden, 2010, s. 263). På den måten vil en effektiv arbeidsdeling redusere risikoen for blant annet uautorisert handlinger og misbruk av virksomhetens data.

Det er viktig å understreke at det finnes et stort omfang av sikkerhetstiltak blant de fire kategoriene av generelle IT-kontroller. Blant annet inneholder COBIT, ISO 27001 og ISO 27002 en rekke eksempler på sikkerhetstiltak og sikringsmål.

Under vises en oppstilling og forklaring på noen kontrollaktiviteter og deres sikkerhetstiltak for å skape en bedre forståelse av de fire overordne kategoriene av generelle IT-kontroller. Eksemplene er hentet ISO 27001 og er ikke en uttømmende liste av alle generelle IT-kontroller.

Tilgang- og sikkerhetskontroll

Tilgang og sikkerhetskontroll skal sørge for at det foreligger hensiktsmessig arbeidsdeling og at kun ansatte med brukerrettigheter har tilgang til programmer og data. Kontrollen skal også forhindre tap eller skade på programmer og data som følge av interne og eksterne trusler.

ISO 27001	**Tilgang- og sikkerhetskontroll**	
Pkt.	**Kontrolltype**	**Sikringstiltak**
9.2.1	Registrering og sletting av brukere	En formell prosess for registrering og sletting av brukere skal implementeres for å gi aksessrettigheter.
9.2.3	Styring av privilegerte aksessrettigheter	Tildeling og bruk av privilegerte aksessrettigheter skal begrenses og kontrollers.
9.2.5	Gjennomgang av brukeres aksessrettigheter	Eiere av aktiva skal gjennomgå brukernes aksessrettigheter med jevne mellomrom.
9.2.6	Fjerning eller korrigering av aksessrettigheter	Aksessrettigheter til informasjon og systemer for informasjonsbehandling for alle ansatte og brukere hos eksterne parter skal fjernes ved opphør av ansettelses-forholdet, kontrakten eller avtalen, eller korrigeres ved endringer

Datasenter- og nettverksdrift

Datasenter- og nettverksdrift skal kontrollere driften av systemer for informasjonsbehandling og forhindre uautorisert tilgang til nettverksprogrammer, samt beskytte filer og andre typer dokumenter produsert av IT-systemene mot ødeleggende programvarer ved å ha effektive back-up rutiner og sikkerhetskopieringer.

ISO 27001	**Kjøp, endringer og vedlikehold av systemprogramvarer**	
Pkt.	**Kontrolltype**	**Sikringstiltak**
12.1.1	Dokumentert driftsprosedyrer	Driftsprosedyrer skal dokumenteres og gjøres tilgjengelige for alle brukere som har behov for dem.
12.4.1	Hendelseslogg	Hendelseslogger som registrerer brukeraktiviteter, avvik, feil, og informasjons-sikkhetshendelser, skal produserer, oppbevares og gjennomgås regelmessig.

Kjøp, endringer og vedlikehold av systemprogramvarer

Kjøp, enderinger og vedlikehold skal styrke datafunksjonene og sikre at programmer og applikasjoner fungerer som tiltenkt ved å oppdage og korrigere eventuelle behandlingsfeil gjort av IT-systemene som benyttes. Kontrollen skal sikre integritet av alle IT- og informasjonssystemer ved å påse at alle endringer har blitt testet og godkjent.

ISO 27001	**Kjøp, endringer og vedlikehold av systemprogramvarer**	
Pkt.	**Kontrolltype**	**Sikringstiltak**
12.1.2	Endringsledelse	Endringer i organisasjonen, virksomhetsprosesser, systemer for informasjonsbehandling og systemer som har innvirkning på informasjonssikkerheten, skal være under kontroll.

Kjøp, utvikling og vedlikehold av applikasjoner

Kjøp, utvikling og vedlikehold av applikasjoner er den siste kontrollaktiviteten som inngår i de generelle IT-kontrollene og skal sikre påliteligheten av informasjonen som fremkommer av IT- og informasjonssystemene som anvendes i virksomheten. Kontrolltiltakene må forsikre seg om at alle retningslinjer og prosedyrer for implementering av nye og endringer i eksisterende applikasjoner er fulgt opp, og har vært gjenstand for testing og godkjenning.

ISO 27001	**Kjøp, utvikling og vedlikehold av applikasjoner**	
Pkt.	**Kontrolltype**	**Sikringstiltak**
14.2.7	Utkontraktert utvikling	Organisasjonen skal føre tilsyn med og overføre aktivitet forbundet med utkontraktert systemutvikling.
14.2.9	Systemakseptansetest	Det skal etableres programmer for akseptansetest med tilhørende kriterier for nye informasjonssystemer, oppgraderinger og nye versjoner.

2.3.4 Testing av generelle IT-kontroller

Revisor må opparbeide seg en forståelse av virksomhetens generelle IT-kontroller ved at de er gjenstand for revisors totale risikovurdering og helt nødvendig for at applikasjonene skal fungere effektivt (Wood et al., 2013).

Generelle IT-kontroller skal vurderes og testes på samme måte som andre kontroller i virksomheten som revisor mener er relevant for den finansielle rapporteringen. Test av kontroller er revisjonshandlinger utført for å innhente tilstrekkelig og hensiktsmessig revisjonsbevis for at relevante kontroller fungerer effektivitet og er utformet for å forhindre, oppdage og korrigere vesentlig feilinformasjon i en påstand, jfr. ISA 330 (2016) pkt. A20.

Dersom revisor finner det nødvendig å teste generelle IT-kontroller for å forsikre seg om at informasjonen som fremkommer av IT-systemene gir et rettvisende bilde av regnskapet, vil det være nødvendig å identifisere virksomhetenes generelle IT-kontroller. Det foreligger ingen konkrete retningslinjer for hvordan revisor bør gå frem når han skal identifisere generelle IT-kontroller. Blant annet har flere revisjonsselskap utarbeidet egne revisjonsverktøy og bruker egen revisjonsmetodikk når de skal identifisere og vurdere relevante kontrolltiltak.

Når revisor foretar en vurdering av enhetens internkontroll, herunder informasjonssystemene og tilknyttede forretningsprosesser, vil revisor først avgjøre hvilke systemer/applikasjoner som er relevante for den finansielle rapporteringen og deretter avgjøre hvilke generelle IT-kontroller som vil være relevante å teste. Mengden av kontroller som bør testes er gjenstand for revisors profesjonelle skjønn, risikovurdering og hva revisjonsmetodikken tilsier at revisor skal teste.

Ved å foreta forespørsler, inspeksjoner, observasjoner og gjennomgang av rutiner og prosedyrer i virksomheten kan revisor identifisere generelle IT-kontroller (Eilifsen et al., 2014). For revisor vil det være rimelig å sørge for at gjennomføringen av test av kontroller dekker de fire kategoriene av generelle IT-kontroller:

- Test av tilgang- og sikkerhetskontroll
- Test av kontroller relatert til datasenter- og nettverksdrift
- Test av kontroller relatert til kjøp, endringer og vedlikehold av systemprogramvare
- Test av kontroller relatert til kjøp, utvikling og vedlikehold av applikasjoner

Ved at generelle IT-kontroller utgjøre en vesentlig del av virksomhetens interne kontroll og understøtter alle aspekter av virksomhetens forretningsoperasjoner utført av IT- og informasjonssystemer, er det viktig at revisor er sikker i sin uttalelse om utformingen og utførelsen av kontrollene. Der hvor revisor kan innhente hensiktsmessige og tilstrekkelig revisjonsbevis for at de generelle IT-kontroller er effektive og er utformet og iverksatt korrekt, vil revisor kunne forvente effektive applikasjonskontroller og planlegge videre revisjon basert på test av kontroller. Dersom det foreligger kontrollsvakheter ved de generelle IT-kontrollene vil revisor lete etter kompenserende kontroller. Det vil si andre kontroller som bidrar til å redusere risikoen for vesentlig feilinformasjon. Eventuelt vil revisor kunne undersøke om kontrollsvakheten faktisk har noen konsekvenser for den finansielle rapporteringen. Revisors vurdering av kontrollsvakheter vil beskrives nærmere i kapittel 2.3.8.

2.3.5 Applikasjonskontroller

Applikasjoner er systemer og programmer som tilfører verdi til datasystemene og understøtter de fleste forretningsprosesser i virksomheter. Applikasjonskontroller er automatiserte eller manuelle rutiner på forretningsprosessnivå og gjelder transaksjonsbehandling i applikasjonsprogrammene (ISA 315, 2016) pkt. 105.

Formålet med applikasjonskontroller er å sikre at fullstendighet, nøyaktighet og gyldighet er oppfylt ved registrering, behandlinger og rapportering av informasjon (Kristoffersen, 2014, s. 300). Flere av disse egenskapene kjenner vi igjen fra ledelsens påstander om regnskapet.

Applikasjoner består av tre komponenter:

- Inndata-input
- Behandlings- og prosesskontroller
- Utdata-output

Inndatakontroller

I dag er inndata ofte generert fra automatiserte kilder, som for eksempel databaser og datafiler. Input kan også legges inn manuelt, for eksempel at en selger legger inn en salgsordre i et ordre- og faktureringssystem. Input kan komme fra andre applikasjoner som er integrert med systemet (Moeller, 2010). Et eksempel på dette er et lønnssystem som får inndata fra et salgssystem for å beregne provisjoner. Dersom data fra salgssystemet utgjør en

vesentlig input for lønnssystemet, bør revisor i tillegg til applikasjonskontrollene i lønnssystemet ta applikasjonskontrollene i salgssystemet i betraktning (Moeller, 2010).

Inndatakontroller skal forhindre og oppdage feil ved registrering av data. Kristoffersen (2014) angir en rekke eksempler på inndatakontroller:

Inndatakontroller	
Kontrolltype	**Eksempel**
Tilgangskontroll: Kun autoriserte personer skal ha tilgang til å utføre en oppgave eller gjennomføre en transaksjon	At det kun er godkjente personer, f.eks. regnskapsansvarlig, som kan registrere lønn til ansatte
Kontrollsiffer: For tallene som registreres tilføyes et kontrollsiffer	KID-nummer (kundeidentifikasjonsnummer)
Ekkokontroll: Kontrollopplysning reflekterer det som registreres	Ved registrering av kundenummer kommer kundenavn opp
Verifisering: Kontrollerer gyldige koder, verdier og grenser	Gyldige datoer, kontonummer, beløp over en visse grenser avvises

Tabell 3: ***"Inndatakontroller" av Kristoffersen (2014, s. 300)***

Behandlings- og prosesskontroller

Det er dataprogrammet som gjennom et sett med instruksjoner sørger for enhver detalj i en behandlingsprosess. Programmering vil ikke utdypes noe videre her, men det er allikevel viktig at revisor forstår hvordan prosessen er oppbygd og hvilke funksjoner den har for å kunne utforme passende revisjonsprosedyrer (Moeller, 2010). Der hvor det foreligger egenutviklede skreddersydde applikasjoner i motsetning til standardiserte applikasjoner, bør revisor være oppmerksom og foreta flere revisjonshandlinger for å bekrefte at applikasjonen fungerer som tiltenkt. Dette skyldes ved at revisor vil i stor grad kunne stole mer på standardiserte applikasjoner utviklet av profesjonelle systemleverandører.

Prosesskontroller skal sikre at behandlingen av data utføres i samsvar med gitte spesifikasjoner og at ingen transaksjoner blir registrert feil (Kristoffersen, 2014).

Kristoffersen (2014) angir noen kontrolltyper for prosesskontroller og tilhørende eksempler.

Prosesskontroller	
Kontrolltype	**Eksempel**
Standardverdier: Automatisk bruk av faste størrelser	Mva-satser eller fast timelønn
Sum totaler: En forhåndsdefinert størrelse blir sammenlignet med registrerte beløp	Mottatt innbetaling mot solgte varer, kontantsalg eller faktura kontrolleres
Balansering: Avvik indikerer feil, test av likhet av verdier i to like poster	Debet = Kredit Saldo ifølge leverandørspesifikasjoner skal tilsvare saldo på leverandørgjeld i hovedboken
Sammenligning: Sammenligner informasjon fra ulike kilder	Mottakslister og innkjøpsordrer sammenlignes med leverandørfakturaer

Tabell 4*: "Behandlings- og prosesskontroller" av Kristoffersen (2014, s. 301 og 302)*

Utdatakontroller

Utdata tar vanligvis form av oppdaterte filer og rapporter. Utdata kan også være integrert til andre applikasjoner (Moeller, 2010). Utdatakontroller skal sikre at registrering av inndata og behandlingen gir gyldige data og utdataen er distribuert til rett person (Kristoffersen, 2014, s. 302) . Kristoffersen (2014) gir eksempler på utdatakontroller:

Utdatakontroller	
Kontrolltype	**Eksempel**
Aldersfordelte lister: Poster sorteres etter dato	Aldersfordeling av saldolister for kundefordringer, avdekker usikre krav
Uavklarte poster eller filer: Kontoer eller filer som krever videre behandling	Restordrer fra kunder som skal effektueres når varene ankommer lager Mottakslister for varer som skal kontrolleres mot bestilling og innkjøpsordre
Avviksfiler: Filer som består av uavklarte poster som er oppdaget av datakontrollen	Kundefordringer som er forfalte skal sendes til rette person for videre behandling. For eksempel purringer og renter

Tabell 5*: "Utdatakontroller" av Kristoffersen (2014, s. 302)*

Det er sjeldent tid og ressurser til å kartlegge og vurdere alle applikasjoner og kontroller i en revisjon. Moeller (2010, s. 239) beskriver en metode for å vurdere risiko for de viktigste applikasjonene fra 1 til 5, der 5 representerer det mest kritiske for revisjonen, på hver av disse kategoriene/spørsmålene:

- Er applikasjonskontrollen sentral for virksomhetens kontroller/funksjoner?
- Basert på tidligere gjennomganger, er internkontroller i applikasjonen effektivt designet?
- Er applikasjonen fra leverandør, eller er den utviklet internt i virksomheten?
- Støtter applikasjonen mer enn én kritisk forretningsprosess?
- Endres applikasjonen ofte, eller er den stabil fra periode til periode?
- Hvor komplisert er det å gjøre endringer i applikasjonen?
- Hvordan påvirker applikasjonskontrollene det finansielle?
- Hva er den overordnede effektiviteten av de generelle IT-kontrollene som støtter applikasjonene?

Applikasjonene som får høyest sammenlagt score vil være gjenstand for testing. Det kan være hensiktsmessig å dokumentere hvorfor noen applikasjoner er valgt fremfor andre i revisjonsdokumentasjonen for å underbygge revisjonsbevisene knyttet til applikasjonskontrollene (Moeller, 2010). Innledende risikovurderingshandling for å kartlegge applikasjonskontroller i de valgte applikasjonene kan gjøres ved å observere sammen med dem som har ansvar for, eller brukerne, av aktivitetene som involverer applikasjonene (Moeller, 2010). I denne delen av prosessen gjør revisor en risikovurdering av applikasjonen ved å vurdere iboende risiko og anslå en foreløpig kontrollrisiko. Noen virksomheter benytter seg av flyt-diagrammer. Diagrammene viser en detaljert oversikt over systemene, tilhørende applikasjoner og prosesser. Dette kan være til hjelp for revisor for å identifisere relevante applikasjonskontroller.

Dersom revisor har vurdert at de generelle IT-kontrollene er effektive og har kartlagt vesentlige applikasjoner, vil revisor gå frem for å teste utvalgte applikasjonskontroller.

2.3.6 Testing av applikasjonskontroller

Hvis de utvalgte generelle IT-kontrollene, som omfatter en applikasjon, fungerer tilfredsstillende vil revisor kunne benytte seg av en metode kjent som ”test of one”. Det vil si at applikasjonskontrollen testes én gang for å bekrefte at den fungerer som den skal. Det er fordi systemer følger logiske prosedyrer og reagerer på samme måte hver gang forutsatt at det ikke er foretatt noen programendringer (Moeller, 2010).

Applikasjonskontroller kan være utfordrende å identifisere, men det som kan være til hjelp er å se etter kontrollpunkter i systemlogikken, og deretter utforme testprosedyrer for å verifisere at de kontrollpunktene er korrekte. Disse kontrollpunktene er hovedkontroller i en applikasjon, og kan være kontroll av fullstendighet av transaksjoner eller nøyaktighet av beregninger (Moeller, 2010). En revisjonsprosedyre som ofte benyttes er walk-through. Metoden skal hjelpe revisor å bekrefte forståelsen som allerede er opparbeidet om kontroller som er etablert, og for å verifisere at kontrollene er implementert. Da går revisor grundig gjennom en bestemt transaksjon der hele regnskapsprosessen spores og behandles ved å foreta forespørsler, observasjoner, inspeksjoner og undersøkelse av underliggende dokumentasjon for å forsikre seg om at nødvendige kontroller er designet og implementert (Arens, Elder, Beasley & Hogan, 2017).

Moeller (2010) utdyper at revisor antakelig må skreddersy gjennomføringen og test av applikasjonskontroller fordi de kan være så forskjellige og varierende fra kunde til kunde. Det er likevel tre kategorier som revisor bør ta høyde for når utforming av test av applikasjonskontroller skal håndteres.

- Tester av applikasjonens inndata og utdata
- Tester av transaksjonsevaluering (behandling og prosesser)
- Andre teknikker for test av applikasjoner

Ved test av applikasjonens inndata og utdata, kan revisor ta utgangspunkt i tilgangskontroller på masterdata. Det vil si at kun autoriserte personer kan endre den viktigste informasjonen som brukes i virksomhetens kjerneaktiviteter. Dette er en kontroll av at riktig inndata blir lagt inn i applikasjonene. Andre tester revisor kan gjøre for inndata er å påse at alle obligatoriske felter må fylles ut for å kunne behandles videre i applikasjonen. For utdata kan revisor ta utgangspunkt i faktura fra en ordre- og faktureringsapplikasjon, og kontrollere for om inndata og beregninger er korrekt fylt og utført (Moeller, 2010).

For test av om transaksjoner blir riktig prosessert og behandlet i applikasjonen kan revisor ta en gjennomgang av spesifikke rapporter mot datafiler. For eksempel i en innkjøpsprosess der applikasjonskontrollen fører til automatisk oppdatering av regnskapet ved registrering av inngående faktura og at varelageret oppdateres automatisk ved varemottak (Moeller, 2010). Andre tester av transaksjonsprosesser kan være at revisor tester om feilsøk-kontroller fungerer som beskrevet. Da vil revisor ta utgangspunkt i en ugyldig transaksjon og følge transaksjonssporet gjennom applikasjonen for å fastslå at det har blitt rapportert korrekt i avviksrapporter (Moeller, 2010). Revisor kan observere hvordan systemet reagerer på feil som bevisst legges inn i applikasjonen. Dette kan for eksempel være å legge inn en innkjøpsordre der en applikasjonskontroll fører til at systemet ikke tillater at samme personer som legger inn innkjøpsordren også kan godkjenne den. Ved å teste denne kontrollen kan revisor verifisere gyldighet av innkjøpskostnadene ved at kostandene har riktig størrelse i regnskapet.

Andre teknikker for test av applikasjonskontroller kan omfatte bruk av kraftige revisjonsverktøy, også kalt ”Computer Assised Audit Tools and Techniques”, kjent som CAATT. Revisjonsverktøyene kan matche filer fra forskjellige perioder, identifisere uvanlige dataposter, utføre sporinger og omberegninger, eller simulere utvalgte funksjoner av en applikasjon.

Andre teknikker Moeller (2010) nevner er:

- Gjentakelse (reperformance) av applikasjonsfunksjoner eller beregninger. Dette er revisjonshandlinger og prosedyrer som kan brukes for både manuelle og automatiserte deler av applikasjonen. For eksempel hvis en anleggsmiddel-applikasjon utfører automatiske avskrivninger, kan avskrivningene beregnes for utvalgte transaksjoner i en compliance test. Compliance brukes for å kontrollere at det er samsvar mellom for eksempel lover og regler og virksomhetens etterlevelse av dem, eller som her at beregninger samsvarer med det systemet produserer av informasjon.
- Observasjon av prosedyrer: Ved observasjon ser revisor på at en kontroll utføres eller når en kontroll inntreffer i et system, eventuelt før og etter den har inntruffet.

Selv om en IT-revisjon kan gi en generell tilnærming til å gjennomføre prosedyrer for de fleste databehandlingsapplikasjoner, er det vanligvis nødvendig å skreddersy tilnærmingen til de spesifikke egenskapene i applikasjonen. Avslutningsvis for test av applikasjonskontroller

er revisors vurdering av dekket risiko. Dersom test og håndtering av applikasjonskontrollene har positive utfall vil det si at applikasjonskontrollene fungerer effektivt og sikrer at fullstendighet, nøyaktighet og gyldighet er oppfylt ved registrering, behandlinger og rapportering av informasjon. Da kan revisor vurdere kontrollrisikoen som lav og dermed redusere omfanget av substanshandlinger i den videre revisjonen. Dersom revisors test av applikasjonskontrollene avslører svakheter i systemet, vil revisor vurdere hvilken effekt det har eller kan ha på regnskapet og utformer videre handlinger som er hensiktsmessige for å vurdere gjenværende risiko.

2.3.7 Systemgenererte rapporter

En prosedyre som har blitt mer vanlig og som det har blitt rettet mer fokus på er revisors bruk av systemgenererte rapporter (PCAOB, 2013; Singelton, 2014). Eksempler på systemgenererte rapporter kan være en systemgenerert liste med kundefordringer som brukes for å bekrefte kundefordringene eller lister med tilganger og logger. Problemet med å bruke systemgenererte rapporter har vært at revisor ikke har bekreftet fullstendigheten og nøyaktigheten av informasjonen som er gitt og at rapporten brukes som et revisjonsbevis. Singelton (2014) beskriver to måter å oppnå sikkerhet for fullstendighet og nøyaktighet. Det første er å verifisere rapportens informasjon ved å sammenligne med ekstern informasjon, og det andre er å sammenligne med virksomhetens interne database. Tester som for eksempel er aktuelle for å verifisere integritet i rapportene, det vil si å bekrefte at rapportene er pålitelige, kan være (Singelton, 2014):

- Å spore et utvalg av transaksjoner til kildedokumentasjonen
- Å teste interne kontroller der formålet er å sikre påliteligheten på en valgt datafil
- Å teste applikasjonskontroller som skal sørge for fullstendighet og nøyaktighet av rapportens innhold
- Utføre beregninger om igjen for å bekrefte rapportens kalkuleringer

Poenget er uansett at det er problematisk å benytte systemgenererte rapporter i revisjonen dersom revisor ikke har testet kontroller i internkontrollen som er relevante for å verifisere at informasjonen i rapporten er pålitelig.

2.3.8 Konsekvenser ved svakheter i kontroller

Dersom revisor avdekker kontrollsvakheter ved test av IT-relaterte kontrollaktiviteter må revisor ta stilling til hvilken risiko det kan utgjøre. Revisor kan rette forespørsel til relevante personer i virksomheten, internrevisjonsfunksjon eller business controlleren, om de kjenner til svakheten og om de eventuelt har gjort noe for å finne ut av hvor stort omfanget av svakheten kan være. Svakheter kan defineres etter tre kategorier (Wood et al., 2013):

- Kontrollsvakhet vil si at kontrollens design eller utførelsen av en kontroll ikke lar ledelsen eller andre ansatte utføre sine oppgaver riktig for å forhindre eller avdekke feilinformasjon i riktig tid.
- Betydelig svakhet er en svakhet som alene eller sammen med andre svakheter påvirker virksomhetens evne til å initiere, registrere, behandle og rapportere økonomisk informasjon på en pålitelig måte etter god regnskapsskikk, slik at det er en sannsynlighet for at det kan foreligge feilinformasjon i regnskapet.
- Vesentlig svakhet foreligger når en betydelig svakhet eller flere betydelige svakheter resulterer i vesentlig feilinformasjon i regnskapet som ikke er forhindret eller avdekket.

Det kan være utfordrende å fastslå vesentligheten og innvirkningen svakhetene kan ha ved at mange svakheter ofte involverer risikohåndtering i virksomheten og ikke et helt spesifikt tall i regnskapet. Når primære kontroller i virksomheten ikke oppnår kontrollformålet, kan revisor påse om det foreligger alternative kompenserende kontroller å teste for å minimere risikoen for vesentlig feil (Wood et al., 2013). Kompenserende kontroller er andre kontroller som er iverksatt av virksomheten for å redusere risikoeksponeringen når de primære kontrollene ikke fungerer (Wood et al., 2013).

Dersom test av den generelle IT-kontrollen ”sletting av brukere” ikke kan bekreftes som effektiv, vil et eksempel på en kompenserende kontroll være en loggføringskontroll av endringer som er foretatt i systemet. Dersom revisor ut i fra loggen kan bekrefte at det ikke er foretatt endringer i systemet av den brukeren som skulle vært slettet, vil ikke risikoen for vesentlig feil i regnskapet øke. På den måten vil kontrollsvakheten i den primære generelle IT-kontrollen ikke få konsekvens for revisjonen. Likevel bør svakheter i generelle IT-kontroller kommuniseres med ledelsen selv om den ikke for betydning for den finansielle rapporteringen.

Dersom revisor finner at de kompenserende kontrollene ikke reduserer risikoen for feil, vil revisor anslå en høyere risiko for den finansielle prosessen svakheten er knyttet til. Da vil kontrollrisikoen vurderes som høy og revisor må øke omfanget av substanshandlinger. Som beskrevet i tidligere kapitler har substanshandlinger som formål å avdekke vesentlig feilinformasjon og omfatter detaljtester og analytiske substanshandlinger. Detaljtester er metoder som for eksempel innebærer fysisk inspeksjon av eiendeler, dokumentgransking, eksterne bekreftelser og kontrollregning. Analytiske substanshandlinger omfatter analyser av nøkkeltall, av forhold i regnskapet som revisor kan ha en forventning til, både finansielle og ikke-finansiell informasjon, og går ned på transaksjonsklassenivå. Substanshandlinger må utføres til revisor med betryggende sikkerhet kan bekrefte at regnskaper ikke er heftet med vesentlig feilinformasjon.

2.4 Rapportering og kommunikasjon

Informasjonssystemet utgjør en del av enhetens interne kontroll, og revisor vil gjøre en totalvurdering av de interne kontrollene og rapportere til de som har overordnet ansvar for styring og kontroll. Dersom revisor etter revisjonen med betryggende sikkerhet kan bekrefte at regnskapet ikke inneholder vesentlige, gjennomgripende feil vil det avlegges en normal revisjonsberetning (ISA 700, 2016) .

2.4.1 Kommunikasjon

I denne oppgaven tar vi høyde for at revisjonskundene er aksjeselskaper som er revisjonspliktige. Selskapet skal ha et styre etter Aksjeloven (1999) §6-1 og kan i tillegg ha en daglig leder jfr. Asl.§6-2. Disse utgjør selskapets ledelse og er ansvarlig for forvaltningen av selskapet. Når revisor skal kommunisere med dem som har overordnet ansvar for styring og kontroll er det hensiktsmessig og identifisere disse spesifikt for hvert oppdrag for å gjøre kommunikasjonsprosessen så effektiv som mulig.

ISA 260 (2016) angir rammeverket som revisor skal forholde seg til når det foreligger forhold som skal kommuniserer med dem som har overodnet ansvar for styring og kontroll.

Standarden angir eksempler på mulige kommunikasjonsformer:

- Presentasjon
- Skriftlig rapport
- Diskusjoner

- Muntlig (men skal inkluderes i revisjonsdokumentasjonen)
- Skriftlig

Ettersom vi skal se litt på kommunikasjonen mellom kunden og revisor i forhold til svakheter i internkontrollen, herunder IT- og informasjonssystemene som støtter opp under regnskapsavleggelsen, vil vi se nærmere på ISA 265 (2016) som angir rammeverket for kommunikasjon av mangler internkontrollen.

2.4.2 Rapportering og kommunikasjon av mangler i intern kontroll

ISA 265 (2016) stiller spesifikke krav til kommunikasjonen av vesentlige mangler i internkontrollen som revisor avdekker i løpet av revisjonen. Revisjonsstandarden skiller mellom mangel i intern kontroll og vesentlig mangel i intern kontroll. Mangel i intern kontroll foreligger når en kontroll er utformet, implementert eller blir gjennomført på en slik måte at den ikke er i stand til å forhindre, avdekke eller korrigere, feilinformasjon i regnskapet i rett tid, eller en kontroll som er nødvendig for å forhindre, eller avdekke og korrigere, feilinformasjon i regnskapet i rett tid, mangler jfr. ISA 265 (2016) pkt. 6a. En vesentlig mangel i intern kontroll er en mangel eller kombinasjon av mangler i intern kontroll som, etter revisors profesjonelle skjønn, er tilstrekkelig viktig til at den fortjener oppmerksomhet fra dem som har overordnet ansvar for styring og kontroll jfr. ISA 265 (2016) pkt. 6b.

Revisor skal skriftlig kommunisere manglene og deres mulige effekt. Ved diskusjon av de faktiske forholdene ved og omstendighetene rundt revisors funn med ledelsen kan revisor innhente annen relevant informasjon for videre vurdering jfr. ISA 265 (2016) pkt. A2, for eksempel:

- Ledelsens forståelse av de faktisk eller antatte årsakene til manglene.
- Avvik oppstått som følge av de manglene som ledelsen kan ha registrert, for eksempel feilinformasjon som ikke ble forebygget av de relevante IT-kontrollene.
- En foreløpig indikasjon fra ledelsen vedrørende dens håndtering av funnene.

Revisor er pålagt å rapportere vesentlige forhold gjennom nummererte brev til ledelsen etter §5-4 i Revisorloven. Dette kan omfatte mangler i plikten til å sørge for ordentlig og oversiktlig registrering og dokumentasjon av regnskap og feil og mangler ved organiseringen av og kontrollen med formuesforvaltningen. Nummererte brev skal oppbevares som en del av regnskapsmaterialet til kunden i fem år, jfr. Bokføringsloven (2006) §13.

3. Metode

I dette kapittelet skal vi gjøre rede for valg av metode for datainnsamling for å besvare masteroppgavens problemstilling. Før vi gjennomfører en datainnsamling er det hensiktsmessig å ta stilling til forskningsdesign, undersøkelsesmetode, utvalgsstørrelse og utvalgsstrategi som del av forberedelsen. Dermed vil vi i dette kapittelet gi et teoretisk kjennskap til den kvalitative metoden der vi bruker dybdeintervju som innsamlingsmetode. I siste del av kapittelet knytter vi opp tilnærmingene validitet og reliabilitet opp mot vår gjennomføring av undersøkelsen.

3.1 Intensivt og ekstensivt undersøkelsesdesign

Når det forskes på ulike fenomener er det en rekke ulike metoder og design å bruke for å belyse en problemstilling. Jacobsen (2005) nevner to måter å gå frem på for å tilnærme seg fenomenet. Disse to er ekstensivt og intensivt undersøkelsesdesign.

Det ekstensive designet tar utgangspunkt i bredden og studerer mange enheter for å beskrive og presisere omfanget av problemstillingen. Designet baserer seg på variasjoner mellom enhetene der målet ved bruk av undersøkelsesdesignet er å se på hyppighet og utstrekningen av fenomenet (Jacobsen, 2005). Ved å bruke et ekstensivt design er det mulig å foreta generalisering av data ved at forskjeller og nyanser blant populasjonen forsvinner og det som er felles vektlegges (Jacobsen, 2005).

Det intensive designet går i dybden av få enheter og samler inn mest mulig informasjon fra hver enhet for å få frem et sammenfallende bilde og en helhetlig beskrivelse av det som studeres (Jacobsen, 2005). I motsetning til det ekstensive designet, vil et intensivt design forsøke å få frem alle nyanser og detaljer av et fenomen eller en hendelse. På den måten kommer individuelle variasjoner og forskjeller frem ved å se på den enkeltes forståelse og fortolkning av fenomenet (Jacobsen, 2005).

Problemstillingen vår er basert på en antakelse om at revisorene foretar en overfladisk og lite detaljert vurdering av internkontroller der IT- og informasjonssystemer er en komponent. Ved å benytte oss av et intensivt design får vi mulighet til å avdekke flere forhold som kan belyse vår problemstilling ved å få tak i den enkeltes forståelse og håndtering av fenomenet. Et intensivt design vil gi oss et mest mulig riktig innblikk i revisors opplevelse i forhold til

fenomenet vi studerer og vi vil ha muligheten til å se på individuelle variasjonen blant revisorene.

3.2 Kvalitativ og kvantitativ undersøkelsesmetode

Når undersøkelser gjennomføres for å belyse en problemstilling kan det benyttes to forskjellige angrepsmetoder: kvalitativ og kvantitativ undersøkelsesmetode. Den store forskjellen mellom disse to metodene er grad av åpenhet og bruk av tall og ord. En kvantitativ metode opererer med tall og størrelse, mens kvalitativ metode operere med meninger formidlet via språk og handlinger (Jacobsen, 2005).

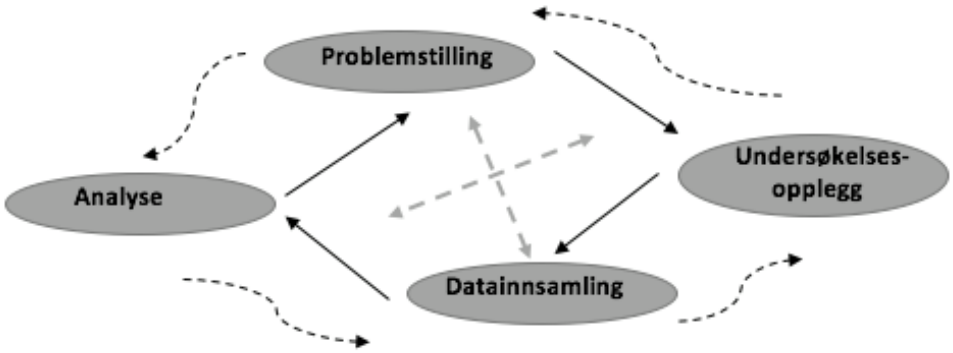
Den kvantitative metoden brukes når et antall observasjoner undersøkes i bredden på bakgrunn av tallfestet informasjon. Dette gjøres for å kunne trekke målbare konklusjoner av den analyserte dataen (Askheim & Grenness, 2008). Ved kvantitativ undersøkelsesmetode er det nødvendig å ha oversiktlige variabler og verdier som kan tilordnes til et tall. Dette medfører at metoden er svært strukturert og lite fleksibel og medfører føringer på hvilken informasjon respondenten kan gi fra seg (Jacobsen, 2005). Noen former for kvantitative undersøkelser er for eksempel eksperiment og spørreundersøkelse (Jacobsen, 2005).

Den kvalitative metoden kjennetegnes ved at data ikke gis i tallverdi, men derimot beholdes som tekst når ett eller flere fenomener skal studeres. Undersøkelsesmetoden er en måte å tilnærme seg virkeligheten på ved å produsere beskrivende data der tolkning brukes som et analyseverktøy (Askheim & Grenness, 2008). Ved den kvalitative metoden er det stor fleksibilitet og åpenhet ved at metoden ikke består av konkrete retningslinjer som bør og må følges (Askheim & Grenness, 2008). Noen former for kvalitative undersøkelser er for eksempel intervjuer og observasjoner (Jacobsen, 2005). Begge metodene tar utgangspunkt i dybden og skaper helhetsforståelse av dataen og fenomenet som studeres.

3.3 Valg av undersøkelsesmetode - kvalitativ metode

Utgangspunktet for bestemmelse av hvilken undersøkelsesmetode som skal benyttes avhenger av sammenhengen mellom undersøkelsens formål og den konkrete problemstillingen i vår masteroppgave. Forskningsspørsmålet i denne masteroppgaven går ut på å finne ut av hva revisor gjør for å forstå og håndtere risiko knyttet til IT- informasjonssystemer relevant for finansiell rapportering. Vi ønsker dermed å se nærmere på menneskelige handlinger ettersom den eksterne revisjonen er påvirket av revisors profesjonelle skjønn. Dermed kan det forventes å foreligge en viss forskjell blant svarene som avgis.

Utbredelsen av IT-revisjon er lite forsket på og det er begrenset omfang om dette temaet i akademisk litteratur. Dette gjør problemstillingen til et undersøkelsesfelt som er sammensatt og komplekst. Derfor vil det være hensiktsmessig å benytte seg av kvalitativ undersøkelsesmetode ved at den beskriver sammenhengen mellom menneskelig erfaring og opplevelser av et fenomen. På den måten vil vi få et intensivt (dypere) innblikk i revisors opplevelse av fenomenet og informantens syn, holdning og perspektiv på virkeligheten. Metoden skaper en nærhet til objektet som studeres og likeverdighet mellom forsker og dem det forskes på (Askheim & Grenness, 2008).



Figur 9: "*Den kvalitative undersøkelsesprosessen som en interaktiv prosess" av Jacobsen (2005, s. 129)*

Figuren over viser den kvalitative metoden fra en fleksibel side hvor metoden gir mulighet for å endre både problemstillingen, datainnsamlingsmetode og analyse underveis i prosessen av undersøkelsen (Jacobsen, 2005). De brede pilene illustrerer den vanlige, faste forskningsprosessen, mens de stiplede linjene viser at den kvalitative metoden gir mulighet til å endre på den faste rekkefølgen.

Den kvalitative undersøkelsesmetoden har både sterke og svake sider. Fordelene ved kvalitativ metode er at det gir mulighet for å innhente mye informasjon om få enheter ved å ha nær kontakt med den som skal forskes på (Askheim & Grenness, 2008). Metoden gir mulighet til å studere nærmere hvilke faktorer som påvirker informantens opplevelser av fenomenet ved at metoden skaper nærhet mellom den som undersøker og det eller den som undersøkes (Jacobsen, 2005). En kvalitativ metode legger til grunn for en åpen datainnsamling med få begrensninger på de svar som avgis. Metoden vektlegger detaljer, nyanser og det som er unikt for hver enkelt informant (Jacobsen, 2005).

Utfordringene ved den kvalitative metoden er at det hevdes at metoden har begrensede muligheter til å generalisere svarene fra informantene til en hel populasjon. Dette skyldes av at utvalget som undersøkes som regel er lite og ikke-representative (Askheim & Grenness, 2008). Metoden kan være tids- og ressurskrevende og det kan forekomme en undersøkelseseffekt. Det vil si at det er fare for at forsker ender opp med å måle noe han selv har skapt enn å måle hvordan informanten selv opplever fenomenet (Jacobsen, 2005). Nærhet kan også være en utfordring dersom nærheten blir for tett og preger relasjonen mellom forsker og informant (Jacobsen, 2005). Dette kan medføre begrensinger når forsker ønsker å få en tilfredsstillende forståelse av hvordan informanten oppfatter virkeligheten. Anvendelse av kvalitativ undersøkelsesmetode kan også skape fare for at det forekommer en viss mengde ustrukturert data som kan føre til vanskeligheter når en skal analysere, tolke og systematisere den innsamlede informasjonen (Jacobsen, 2005).

I vårt tilfelle anser vi det likevel som hensiktsmessig å benytte oss av den kvalitative metoden for å kunne gi et mest mulig betryggende svar på vår problemstilling. Ved å benytte oss av en denne undersøkelsesmetoden vil vi kunne skape et realistisk bilde av revisors egen oppfattelse av problemstillingen ved at metoden skaper rom for fleksibilitet og åpenhet. Som følge av dette kan vi luke vekk eventuelle forhold som medfører begrensninger og trekke frem det viktigste i svarene som avgis.

3.4 Individuelle intervjuer

Vår oppgave er å se på revisors forhold til IT- og informasjonssystemer for regnskapsavleggelse gjennom forståelse av IT-miljøet og håndtering av IT-relatert risiko. Det individuelle intervjuet, som er en kvalitativ undersøkelsesmetode, egner seg når få enheter undersøkes og vi er interessert i hva den enkeltes personlige erfaring og mening er og hvordan den enkelte fortolker og legger mening i et spesielt fenomen (Jacobsen, 2005).

3.4.1 Dybdeintervju

Dybdeintervju består av et ansikt-til-ansikt intervju mellom intervjuer og informant. Denne metoden er hensiktsmessig for problemstillinger der det er behov for omfattende svar og informasjon (Jacobsen, 2005). Den som intervjuer får mulighet til å stille oppfølgingsspørsmål og oppklare uklarheter i større grad enn ved en generell spørreundersøkelse. Utfordringen er ofte at det er svært tidskrevende å analysere og strukturere svarene i ettertid (Jacobsen, 2005).

For vår oppgave mener vi dybdeintervju vil være den optimale løsningen for å kunne samle inn tilstrekkelige data og identifisere ulike nyanser i revisorenes svar. På den måten vil vi få nok informasjon til å besvare vår problemstilling.

3.4.2 Telefonintervju

Telefonintervju er en metode som egner seg når det er vanskelig å få til et intervju ansikt-til-ansikt. Det vil for eksempel være en god løsning dersom den geografiske avstanden er stor og der det er kostnads- og tidskrevende å få til et møte (Jacobsen, 2005). Telefonintervju gjør det mulig å rekruttere informanter fra ulike regioner uten å være avhengig av fysisk oppmøte. Selve gangen i intervjuet foregår på samme måte som ved ansikt-til-ansikt, men har den svakheten at det ikke er mulig å tolke kroppsspråket på samme måte som ved fysisk tilstedeværelse (Jacobsen, 2005).

Ettersom forståelse og håndtering av IT- og informasjonssystemer er noe informantene i stor grad forholder seg til hver dag og utgjør en betydelig og naturlig del av revisjonen, mener vi at de er like godt rustet til å svare både ansikt-til-ansikt og over telefon.

3.4.3 Strukturert intervjuguide

Et intervju kan gjennomføres på en åpen eller strukturert måte. Et spørreskjema med fast rekkefølge og faste svaralternativer kategoriseres som et veldig strukturert intervju. På den andre siden kan intervjuet bestå av at informanten kun er kjent med temaet fra før, uten strenge retningslinjer for rekkefølge på spørsmål eller svar (Jacobsen, 2005). Et åpent intervju bør ideelt sett være minst mulig begrenset og det er viktig å sørge for at intervjuet oppfordrer informanten til å svare mest mulig utfyllende og ærlig uten at det blir lite konkret og for komplekst å analysere.

Vi har derfor valgt å lage en intervjuguide der intervjuet er delt opp etter revisjonsprosessens faser: planlegging, gjennomføring og avslutning. Likevel vil store deler av intervjuet være åpent slik at vi får med de nødvendige nyansene og kan stille oppfølgende spørsmål.

3.5 Utvalg av intervjuobjekter

Som vi nevnte tidligere er det hensiktsmessig å velge ut informanter som forholder seg til temaet i det daglige. Derfor har vi valgt et stillingsnivå vi mener kan belyse problemstillingen vår. Managere/senior managere innehar tilstrekkelig kompetanse og flere års erfaring. Stillingsnivået gjør at de er sentrale personer og kan være teamledere. Derfor antas det at de

er stødige på revisjonsmetode, kommunikasjon og delegering av oppgaver. Johannessen, Tufte og Christoffersen (2011) viser til tre prinsipper for utvelgelse av informanter: utvalgsstørrelse, utvalgsstrategi og rekruttering av informanter.

3.5.1 Utvalgsstørrelse

Med dybdeintervju som datainnsamlingsmetode er det i utgangspunktet ingen begrensing i utvalgsstørrelse. Ved å velge et tema innenfor regnskap og revisjon er det begrenset hvor mange informanter revisjonsselskapene kan stille med. Første halvåret er tidspunkt for oppgjøret av årsregnskapet og dermed en hektisk periode. Derfor har vi heller tatt utgangspunkt i revisjonsselskaper vi mener kan bidra med å belyse problemstillingen. Da det er fem store revisjonsselskaper som preger bransjen har vi valgt å ta utgangspunkt i informanter fra de fem, samt en informant fra et mindre revisjonsselskap. Totalt utgjør utvalgsstørrelsen seks informanter.

3.5.2 Utvalgsstrategi

Johannessen et al. (2011) beskriver utvalgsstrategi som å velge et utvalg som er hensiktsmessig for det som skal undersøkes. Strategisk utvelgelse går ut på å bestemme på forhånd hvilken gruppe som er relevant for undersøkelsen. Vi mener de store revisjonsselskapene har grunnlag til å ta stilling til problemstillingen da de ofte reviderer kunder som anvender komplekse IT- og informasjonssystemer. Flere av kontorene har sertifiserte IT-revisorer og nok ressurser til kursing og opplæring innenfor IT-revisjon på de finansielle revisorene.

Tidlig i forberedelsesfasen ønsket vi et utvalg av små revisjonsselskaper for å se om det var noen betydelige forskjeller mellom store og små selskaper. Da små revisjonsselskaper ofte reviderer mindre, ikke-børsnoterte selskap, kan IT-revisjon være mindre anvendt. Dermed var det utfordrende å skaffe et utvalg av informanter fra små revisjonsselskap.

3.5.3 Rekruttering av intervjuobjekter

Vanlige måter å rekruttere informanter på er personlig rekruttering, telefonkatalog, annonser eller medlemsregistre (Johannessen et al., 2011).

Da vi rekrutterte informanter brukte vi kontaktnettverket vårt gjennom arbeidsgiverne våre. Da vi skal begynne å jobbe i to av de store revisjonsselskapene fikk vi gode tilbakemeldinger på temaet og de var samarbeidsvillige til å stille med informanter. Disse informantene holder

henholdsvis til i Porsgrunn og Oslo. Et annet stort revisjonsselskap vi har i kontaktnettverket vårt stilte også med en informant. Denne informanten holder til i Kristiansand. Gjennom MRR-studiet har vi blitt kjent med medstudenter som allerede har jobbet noen år i revisjonsbransjen. Av de fikk vi hjelp til å komme i kontakt med de resterende informantene fra de andre store revisjonsselskapene. Dermed fikk vi fem forskjellige informanter fra de fem store selskapene.

Fra de store revisjonsselskapene var det relativt greit å få tak i informanter på stillingsnivået manager/ senior manager som vi var ute etter. Det var noe vanskeligere å rekruttere informanter fra mindre revisjonsselskaper. Dette kom antakeligvis av at vi ikke hadde tilstrekkelig stort nettverk til å få tak i revisorer som kunne stille til intervju. Derimot var det en partner i et selskap i Kristiansand som sa seg villig til å stille opp til intervju.

Vi tok kontakt med flere små og mellomstore selskaper på deres hjemmesider, men det viste seg å være en lite effektiv måte å få tak i dem. Etterhvert fulgte vi opp med telefon. Vi ringte og sendte e-poster til små revisjonsselskaper på Østlandet, men fikk som regel til svar at de var for travle og ikke hadde mulighet til å stille opp. Andre selskaper vi var i kontakt med mente at temaet ikke var relevant for deres virksomhet da de reviderte kunder med IT- og informasjonssystemer som ikke var av den art til å påvirke risikovurderingen.

3.6 Datainnsamling

Datainnsamling er prosessen der informantene gjennom sine svar skaper et grunnlag for å kunne sammenligne, identifisere og analysere de funnene som skal ligge til grunn for en konklusjon til problemstillingen. For denne oppgaven har datainnsamlingen bestått av å intervjue managere, senior managere og en partner. Ved å bruke båndopptaker har det vært mulig å registrere informasjonen riktig og det har vært et nyttig verktøy for datainnsamlingen.

3.6.1 Gjennomføring

Før vi startet datainnsamlingen måtte vi vurdere om behandling av personopplysninger, direkte eller indirekte, kunne brukes til å identifisere enkeltpersoner i oppgaven. Ved å benytte en uformell test på NSD sine nettsider tok vi enklere stilling til utfallet av meldeplikten. Ettersom vi kun oppgir størrelse på revisjonsselskapet, yrkestittel og stillingsnivå skal det ikke være mulig å identifisere informantene. Ut i fra testen ble resultatet at oppgaven ikke er meldepliktig og at vi ikke trenger å sende inn meldeskjema.

Før intervjuene fant sted fikk informantene tilsendt intervjuguiden på forhånd for å kunne forberede seg. Dette var noe informantene selv ønsket da flere mente at temaet var utfordrende. Selv mente vi at det var en god løsning da vi ville at de skulle stille forberedt for å kunne svare utfyllende på spørsmålene. En svakhet med dette kan være at de har gjort undersøkelser i forkant og på den måten forberedt seg på å svare på spørsmål de ellers i hverdagen er usikre på. Vi mente likevel at fordelen ved at de kan stille forberedt veier opp for risikoen for at de velger å ikke være ærlige om sin egen kompetanse. Flere av spørsmålene var utformet slik at de hadde et kontrollformål for å sørge at svarene var konsistente og ikke avvikende. En strukturert intervjuguide var en god måte å gjennomføre intervjuene på da de fikk mulighet til å gi utdypende svar og vi fikk mulighet til å komme med oppfølgende spørsmål.

Siden vi fikk tak i informanter fra Porsgrunn, Kristiansand og Oslo, hadde vi kun mulighet til å møte opp personlig på noen av intervjuene, mens de resterende ble foretatt over telefon. Begge metodene var effektive måter å gjennomføre forskningen på og vi mener det ikke satt begrensninger for å kunne sammenligne funnene. Vi brukte båndopptaker på intervjuene slik at vi i ettertid fikk mulighet til å få med alle detaljer og nyanser som var relevante for problemstillingen og for å være sikre på at intervjuene ble mest mulig analyserbare. Ved å bruke båndopptaker var det lettere å følge opp svarene etter intervjuet dersom noen av dem var utydelig eller ufullstendig. Vi har også tatt visse forhåndsregler ved å benevne hvert intervju med intervju 1, intervju 2 mv. når båndopptaker ble brukt. Informantene identifiserte seg heller ikke på båndopptakene. Opptakene ble slettet i ettertid med hensyn til personvernombudet.

Informantene var meget imøtekommende og vi opplevde at de fleste var interessert i temaet vårt ved at svarte velvillig på alle spørsmål og oppfølgingsspørsmål vi hadde selv om de var usikre på flere av spørsmålene. I forkant estimerte vi å bruke ca.1 time per intervju, men etter gjennomføringen så vi at det varierte blant intervjuene etter vårt behov for mer utfyllende svar eller forklaringer ved bruk av eksempler.

Vi brukte omfattende tid og arbeid på å transkribere intervjuene og analyserte dem i flere omganger. Vår fremgangsmåte bestod i å lytte til opptakene for så å skrive dem ordrett ned. På den måten fikk muntlig data om til skriftlig for å sitere informantene korrekt. Deretter ble intervjuene renskrevet for å trekke ut det vi anså som vesentlig for vår problemstilling. Da dette var gjort sendte vi dem tilbake til informantene for en siste sjekk slik at de fikk mulighet

til å komme med innspill dersom de var uenige i vår utforming og fremstilling av de avgitte svarene. Det var bare en informant som hadde tilbakemelding etter at vi sendte intervjuet. Tilbakemeldingen gjaldt oppklaring av noen begreper som informanten hadde brukt. Før analysen strukturerte vi alle svarene til informantene i et og samme dokument for å se nyansene tydeligere blant svarene som ble avgitt av informantene. Da vi analyserte svarene ble vi overrasket over at noen av spørsmålene gav oss svar på viktige sider ved problemstillingen som vi ikke tenkte da vi utformet spørsmålene.

3.7 Relabilitet og validitet

For at intervju skal kunne betraktes som gyldig og til å stole på er det nødvendig at det overholder prinsippene om validitet og reliabilitet. Begge prinsippene forteller noe om holdbarheten av undersøkelsen ved at de beskriver påliteligheten (reliabilitet) og gyldigheten (validitet) av resultatene som fremkommer av utvalget og fenomenet som har blitt undersøkt.

3.7.1 Reliabilitet

Reliabilitet består i å måle hvor pålitelig den innsamlede dataen er ved å anslå nøyaktigheten av undersøkelsen. Dette gjøres ved å studere eventuelle forhold ved selve undersøkelsen som kan bringe til resultatene vi kommer frem til. Det viser seg at det foreligger sammenheng mellom resultatene som fremkommer og måten undersøkelsen blir gjennomført på. Både innsamling, behandling og fremstilling av datamaterialet kan ha innvirkning på påliteligheten av undersøkelsen (Jacobsen, 2005). En undersøkelse har høy reliabilitet dersom gjennomføringen blir utført korrekt og senere kan bekreftes ved at det er mulig å komme frem til samme resultatet ved samme undersøkelsesmetode (Jacobsen, 2005).

En kvalitativ metode, herunder intervju, stiller andre krav til prinsippet om reliabilitet enn det en kvantitativ metode gjør. Dette skyldes av at en kvalitativ metode kan forklares som en innsamlingsmetode uten bestemte retningslinjer for måling av resultat (Jacobsen, 2005). Alle typer undersøkelser vil utsette undersøkelsesobjektene for ulike stimuli og signaler. Dette er stimuli og signaler som vil kunne påvirke informantene (Jacobsen, 2005). Svarene som avgis av informantene vil avhenge av forhold som dagsform, erfaring og annen kontekst rundt selve intervjuet. Disse forholdene vil kunne påvirke relabiliteten av undersøkelsen og føre til at resultatene kan bli annerledes ved at andre nyanser kan komme frem ved senere undersøkelser.

Ved en beskrivelse av anvendt undersøkelsesmetode og framgangsmåter som utvalgsstrategi, rekruttering av informanter og gjennomføring, vil vi kunne styrke påliteligheten av den innsamlede dataen. I vår undersøkelse gjennomførte vi intervjuer på en åpen måte gjennom en intervjuguide. Likevel stilte vi noen oppfølgende spørsmål der vi mente det var behov. Dette gjorde vi for å få utfyllende svar og oppklare svar som var upresise. Som en konsekvensen av dette kan det være mulighet for at noen av informantene har endret sine svar.

En annen måte å styrke påliteligheten av en undersøkelse på er ved å gi en grundig forklaring av registrering av data og de tolkninger og vurderinger som er tatt når resultatet av undersøkelsen skal fremlegges (Jacobsen, 2005). Dette kommer av at det kan foreligge en risiko for at all data ikke er korrekt registrert og oppfattet. Vår fremgangsmåte bestod av taleopptak, for så å transkribere og deretter renskrive intervjuene for å sende dem tilbake til informantene for en siste sjekk. Dette gjorde vi for å styrke reliabiliteten av resultatene ved presis og korrekt registrering av data. Videre ble alle svarene grundig analysert enda en gang og systematisert med den informasjonen vi mente var viktigst for å besvare vår problemstilling.

3.7.2 Validitet

Validitet beskriver gyldigheten av funnene som fremkommer ved undersøkelsen. En undersøkelse anses som valid når forskerne får tak i det de ønsker og det er mulig å overføre funnen til andre sammenhenger (Jacobsen, 2005, s. 214). Dette omtales som intern og ekstern gyldighet.

Intern gyldighet beror på om det foreligger en rett oppfattelse av resultatene som fremkommer og om fenomenet er beskrevet på en riktig måte. Jacobsen (2005) viser til tre mulige måter å teste den interne gyldigheten på. Dette er ved å validere funnene ved å konfrontere de vi har undersøkt med det som har fremkommet av undersøkelsen, gjennom kontroll mot andre fagfolk, annen teori og empiri eller ved å selv ta en grundig gjennomgang av av informantene og den informasjonen som har fremkommet av deres svar (Jacobsen, 2005).

Ekstern gyldighet går ut på å teste om funnene fra undersøkelsen kan generaliseres (Jacobsen, 2005). I en kvalitativ undersøkelsesmetode er det ikke hensiktsmessig å generalisere funnene fra informantene til en større populasjon. Dette skyldes av at denne metoden heller fokuserer på å kunne forstå og utdype det som undersøkes og de funnene som fremkommer. Deretter generaliseres data fra et mindre utvalg til et mer teoretisk nivå. Dette kalles for teoretisk

generalisering (Jacobsen, 2005). Den andre metoden er generalisering av hyppigheten av fenomenet. Formålet med generalisering av hyppighet er å overføre funnene til en større populasjon (Jacobsen, 2005). I vårt tilfelle er det vanskelig å ta stilling til om undersøkelsen kan generaliseres som følge av liten utvalgsstørrelse. Revisjonsmetodikken innenfor det enkelte revisjonsselskap, i tillegg til opplæring, medfører at det er mulig å anta at revisorer innenfor samme selskap vil avgi nokså like svar. Derfor tar vi utgangspunkt i antall revisjonsselskaper som vi anser som relevante for problemstillingen.

Vår gjennomføring av undersøkelsen bestod av konkrete spørsmål som var laget på bakgrunn av den kunnskapen og teorien vi hadde om temaet på forhånd. Vi brukte god tid på utarbeidelsen av spørsmålene, men fikk likevel oppfattelse av at noen av spørsmålene ikke var tydelige og godt nok gjennomtenkt. Dette tror vi kan skyldes av at spørsmålene ble utarbeidet tidlig i prosessen og at all teori ikke var bekreftet og tatt med. Likevel er det viktig å understreke at vi gjennomførte åpne intervjuer uten faste svarkategorier nettopp for å gi informantene mulighet til å selv velge hvor omfattende de ville svare. På den måten fikk vi høy begrepsgyldighet ved at vi fikk frem informantenes riktige forståelse av problemstillingen.

Utfordringen ved den interne validiteten i vår undersøkelse er at informantene som besvarte spørsmålene var forberedt på at de befant seg i en intervjusituasjon. I tillegg ble spørsmålene tilsendt før selve gjennomføringen av intervjuet. Dette kan ha ført til påvirkning av svarene som ble avgitt da informantene kan ha blitt stimulert til å avgi de svarene de tror at vi ønsker å få. For å øke den interne validiteten og for å være sikre på at det informantene sa samsvarte med virkeligheten, stilte vi enkelte ganger tilleggsspørsmål og andre ganger ba vi dem om å utdype svarene med konkrete eksempler.

En redusert intern validitet kan medføre redusert ekstern validitet ved at det er ikke er mulig å generalisere funnene dersom svarene til informantene ikke samsvarer med virkeligheten. I vårt tilfelle har også utvalgsstørrelsen ført til redusert ekstern validitet ved at vi ikke kan generalisere våre funn fordi det er for få informanter. Vår begrensede utvalgsstørrelse skyldes redusert kapasitet hos revisjonsselskapene ved at det første halvåret er den mest hektiske tiden for dem. Det var derfor en utfordring å rekruttere flere informanter. Likevel vil funnene i vår undersøkelse forhåpentligvis gi en bedre forklaring på revisors forståelse og håndtering av risiko knyttet til IT- og informasjonssystemer relevant for finansiell rapportering.

4. Presentasjon og analyse av funn

I dette kapittelet skal intervjuene presenteres og analyseres. Målet for masteroppgaven er å se på forholdet revisor har til IT- og informasjonssystemer og hvilken innvirkning det har på deres revisjonstilnærming. Vi vil gjøre rede for hvilke likheter og ulikheter som fremkommer blant informantene og videre drøfte eventuelle årsaker som fører til dette. Vi vil sammenligne våre funn med bakgrunn i teorien. Presentasjon og analyse bygger på vår problemstilling:

"Hva gjør revisor for å forstå og håndtere risiko knyttet til IT-og informasjonssystemer relevant for finansiell rapportering?"

Analysen blir delt opp i kategoriene: revisors forståelse av IT-miljø, revisors håndtering av IT-relaterte kontroller, rapportering og kommunikasjon ved kontrollsvakheter, samhandling mellom revisor og IT-revisor og muligheter og utfordringer for revisor i fremtiden. Kapittelet innledes med generell informasjon om yrkestittel og arbeidserfaring informantene har, samt størrelse på selskap.

4.1 Bakgrunnsinformasjon om informantene

Nedenfor presenteres en tabell som illustrerer generell informasjon om informantene. Det er mulig å merke seg at alle informantene har relativt lang arbeidserfaring og derfor et godt grunnlag til å besvare spørsmålene. Informantene tilhører kontorer fra Vest-Agder, Oslo og Telemark.

Informant	Størrelse på selskap	Yrkestittel	Arbeidserfaring	Erfaring fra IT
A	Stort	Senior manager	15 år	Noe kursing
B	Stort	Senior manager	9 år	IT-trained auditor kurs
C	Stort	Senior manager	10 år	Noe kursing
D	Lite	Partner	35 år	Noe kursing
E	Stort	Manager	8 år	Noe kursing
F	Stort	Senior manager	20 år	CISA sertifisering

Tabell 6: Bakgrunnsinformasjon av informantene

4.1.1 Kursing

Vi stiller informantene spørsmål ved om de opplever at revisjonsselskapene de er ansatt i tilbyr tilstrekkelig kursing knyttet til IT-revisjon. Informantene A, C og E svarer at det ikke er direkte mangel på opplæring, men at det er et felt som kan brukes mer tid på. Informantene B og F mener at det er nok intern kursing relatert til IT. Dette er antageligvis fordi informant B uttrykker at IT er et spennende område, mens informant F selv er en IT-revisor.

Informant A mener at det kunne vært bedre opplæring i forhold til å forstå kundens IT-miljø og viktigheten av den. Hun tilføyer at spesielt dette med IT tas litt lett på i små kunder ved at det revideres mye med substanshandlinger for å få god sikkerhet for regnskapet.

"Mer kursing kunne det nok vært, men dette er et tema som alle er sånn "å nei" til".

- Informant A -

Informant C viser til at det er en bølge med fokus på IT nå og at det er enda mer behov for grensedragninger mellom kunnskap om IT og økonomi. Informanten sier at alle må ha en forståelse for IT-revisjon ved at det er det som er fremtiden. Han legger til at de siste to årene har det vært mer kursing generelt på nasjonalt plan om IT-revisjon og hvordan det tilegnes praktisk.

Informant D svarer at han aldri har følt at egen kompetanse ikke har strukket til på noen tilfeller utenom områdene relatert til IT. Videre sier han at dette området er kanskje noe de ikke er flinkest på og at han tror at kursing og mer kompetanse i forhold til IT er noe de kunne trengt mer, men at det er mange andre felt som er mer interessante å bli bedre på. Han trekker spesielt frem skatt og avgifter og generelt regnskapet.

Informant E sier at det ikke står fullt av kurs relatert til IT i kø og at heller ikke Revisorforeningen oppfordrer til bedre kompetanse når det gjelder forståelse av IT. Informanten legger til at de ansatte ved kontoret står fritt til å velge selv.

Svarene til informantene er overraskende da vi forventet at de store revisjonsselskapene fokuserte mer på opplæring og kursing på området. Det kan virke som at i det store revisjonsselskapene velger de ansatte selv i forhold til sine interesser på hvilke områder de vil øke sin kompetanse. Dette gjelder også for IT, men at dette feltet ikke er obligatorisk i like stor grad som for andre kurs. Informant D som har lengst arbeidserfaring av informantene, er den som skiller seg ut og påpeker at andre områder er viktigere for dem. En forklaring på

dette kan være at det er et lite revisjonsselskap, og at de har små kunder og dermed ofte forholder seg til standardiserte systemer.

4.1.2 Rammeverk

Informantene A, B, C, E og F er fra store revisjonsselskaper. Felles for de er at de har egne fagavdelinger som sørger for metodikken. Lover, standarder og rammeverk er sydd inn i revisjonsverktøyet de bruker. Revisjonsmetodikken er utbeidet slik at de danner revisjonshandlinger som skal dekke risiko relatert til IT.

Informant D, som er fra et lite revisjonsselskap, bruker Revisjonsforeningens verktøy Decartes. Dette rammeverket bygger på revisjonsstandardene.

4.2 Revisors forståelse av IT-miljøet

Innledningsvis i masteroppgaven beskriver vi at det råder en antakelse om at revisor kun gjør en overfladisk og lite detaljert vurdering av IT-kontroller. Derfor ønsket vi å se på hva revisorene egentlig gjør når de er ute hos kunden for å opparbeide en forståelse for IT- og informasjonssystemene.

Revisors forståelse inngår som en del av problemstillingen vår. Vi spurte derfor informantene hva de gjør i planleggingsfasen for å vurdere risiko relatert til IT- og informasjonssystemer. For å begrense omfanget av masteroppgaven, har vi valgt å fokusere på kun noen utvalgte elementer i IT-miljøet, deriblant outsourcing og nettskytjenester.

4.2.1 Hvem snakker du med for å forstå og håndtere IT-og informasjonssystemer

På spørsmål om hvem revisorene snakker med for å forstå og håndtere IT-systemene, har vi satt opp en tabell for å illustrere forskjellene og likhetene mellom dem:

Informant/ Størrelse på selskap	IT - ansvarlig	Regnskaps- og økonomi-ansvarlig	Controller	System leverandør	Daglig leder	Ekstern regnskaps-fører
A-Stort	x	x			x	x
B-Stort			x	x		x
C-Stort	x	x		x		x
D-Lite	x	x				x
E-Stort	x	x			x	x
F-Stort	x	x		x		x

Tabell 7: Forstå og håndtere IT- og informasjonssystemer

De vedkommende som revisor henvender seg til er listet opp i tabellen over. De er å anse som personer som revisor forholder seg til gjennom hele revisjonsprosessen og i forhold til vår problemstilling.

Informantene A, C, D, E og F tar utgangspunkt i å snakke med regnskapsansvarlig og eventuelt IT-ansvarlig. Alle informantene henvender seg til ekstern regnskapsfører dersom regnskapsfunksjonen er outsourcet.

Informant B skiller seg ut i sin besvarelse ved å ta utgangspunkt i controlleren på området som revideres og ansvarlige hos systemleverandør ved at de kan mer om det overordnede systembildet enn de som bruker systemene til ordinær regnskapsføring daglig. Informanten reviderer flere børsnoterte foretak og vi tror at dette kan være en årsak til at han går rett på de ansvarlige for systemene og de som utfører jobben. Også C og F retter forespørsel til systemleverandør. Det er kun informantene A og E som opplyser at de retter forespørsel til daglig leder.

I henhold til ISA 315 skal revisor rette forespørsel til ledelsen og andre personer som, etter revisors skjønn, kan ha relevant informasjon for regnskapsavleggelsen. Fordi det anvendes skjønn vil svarene variere blant revisorene, men i noen tilfeller vil de gjøre de samme vurderingene som det fremkommer i tabellen. Variasjonene kan ha sammenheng med størrelse på kundene som revideres ved at i store virksomheter er avstanden mellom ledelsen og de ansatte større enn i små virksomheter.

4.2.2 Vektlegging av beskrevne rutiner og prosedyrer

På spørsmål om hvordan de vektlegger beskrevne rutiner og prosedyrer, svarer informant A at de tar utgangspunkt i det praktiske. I motsetning svarer informant D at de klart legger vekt på beskrevne rutiner og prosedyrer i virksomheten.

Informant F bemerker at det i praksis ofte ikke er skriftlige rutiner og prosedyrer, men at dersom det er tilfelle, så innhenter de rutinebeskrivelser hvis kunden har det. I utgangspunktet vektlegger informant F det virksomhetene gjør i praksis i det daglige. Denne beskrivelsen er sammenfallende med svarene til informant C og B.

Informant B forklarer at rammeverk for rutiner og prosedyrer vil være et godt utgangspunkt for diskusjon med de systemansvarlige. Informanten sier videre at han innhenter det

overordnede kontrollrammeverket som beskriver de implementerte kontrollene i selskapet siden dette er noe de ikke finner gjennom den vanlige revisjonsprosessen. Informant E svarer at det å forstå rutiner og prosedyrer er noe han i utgangspunktet vektlegger veldig mye for å kunne finne krysningspunktet for hva som er relevant og ikke relevant for regnskapet og revisjonen.

Rutiner og prosedyrer er en del av kundens interne kontroll, men i hvilken grad det er beskrevet kan variere mye. For virksomheter som er underlagt Forskrift om risikostyring og internkontroll er det strengere krav til dokumentasjon av internkontrollen. Revisor skal også bekrefte at virksomheten overholder dette kravet. Ut i fra informantenes svar kan vi tolke det som at hvis det foreligger beskrevne rutiner og prosedyrer vil det være et utgangspunkt for revisor å kartlegge kontroller, men at de også etterser at det fungerer i praksis. Svarene fra informantene kan variere ut i fra revisors skjønn og type kunder de har. Flere påpeker at små kunder sjeldent har skiftelige rutiner og prosedyrer.

4.2.3 Systemer som er relevant for revisjonen

Som tidligere beskrevet må revisor finne systemene som er relevant for revisjonene for å identifisere de generelle IT-kontrollene som skal testes. Derfor stiller vi spørsmål om hvilke systemer som er relevant for revisjonen.

Slik vi tolker informantene A, B, E og F, svarer de relativt sammenfallende at de finner systemer som er relevant for revisjonen gjennom en prosesskartlegging. Ved å gjennomgå vesentlige regnskapsrutiner med regnskapsledelsen avgjør de hvilke systemer som ligger til grunn.

Informant C tar utgangspunkt i hva som er vesentlig for det finansielle og dermed hvilke systemer som påvirker de største regnskapslinjene og hvor det er størst risiko for feil.

Informant D svarer at systemene som går på regnskap, lønn, og ikke minst fakturering er relevant for revisjonen.

Ut i fra revisjonsstandardene skal revisor opparbeide en forståelse av informasjonssystemer og tilknyttede forretningsprosesser som er relevante for den finansielle rapporteringen. Ved å kartlegge systemene som anvendes og elementer i IT-miljøet, vil revisor videre avgjøre om test av IT-relaterte kontroller er hensiktsmessig. Slik vi tolker svarene til informantene er alle sammenfallende med ISA 315.

4.2.4 Outsourcing av IT-funksjonen

I dag har det blitt vanlig å outsource IT-funksjonen og dette kan få konsekvenser for revisors risikovurdering. Derfor stilte vi spørsmålet om hvilken betydning dette har for revisjonen.

Informant A svarer at når IT-funksjonen er outsourcet følger hun opp og stiller de samme spørsmålene til de eksterne systemeierne. Videre utdyper hun at revisorene har krav om å dokumentere på samme måte selv om IT-funksjonen er outsourcet.

Informant B forklarer at dersom IT-funksjonen er outsourcet, spesielt i større selskap, gjør de en ISAE 3402 gjennomgang. Informant E svarer at de på samme måte vil søke etter Type 1 og Type 2 tester. Der vil de få et skriv eller en rapport som tilsier at revisor til dette selskapet kan vedkjenne seg til at systemene og internkontrollen til dette selskapet som regnskapet er outsourcet til fungerer bra.

Informant F svarer at de innhenter en erklæring fra systemleverandøren, men at de uansett må ha en forståelse av hvordan kunden opplever leverandøren som følge av at de uansett har ansvar for å påse at systemet fungerer riktig.

Informant C svarer at dersom IT-funksjonen er outsourcet vil de ha egne prosedyrer og handlinger som skal utføres i tillegg. De kartlegger serviceorganisasjonen ved å vurdere hvor god og pålitelig den er.

Slik vi tolker svarene fra informantene kan det virke som om dette er et område de er kjent med. Alle informantene er enige om at en outsourcet IT-funksjon fører til en kartlegging av serviceorganisasjonen. Hensikten er å få bekreftelse av virksomheten selv, eller deres revisor, om at deres systemer er pålitelige. Dette samsvarer med det vi har beskrevet i teorien.

4.2.5 Risikovurdering i forhold til IT-outsourcing

Videre stiller vi spørsmål om informantene mener at outsourcing av IT-funksjonen kan medføre en annen risikovurdering av kunden.

På spørsmålet er informantene nokså samstemte i at outsourcing av IT-funksjonen kan være en styrke for selskapet og dermed ha en positiv innvirkning på regnskapsavleggelsen. Både informant A, C og F forklarer at dette spesielt vil være positivt for de små kundene de reviderer. Dette kommer av at kompetansen i en outsourcet IT-funksjonen er bedre og at det foreligger flere formelle retningslinjer med tanke på kontroll og rutiner. Informant A utdyper

dette ved å forklare at kompetansen er avgjørende for risikoen, mens informant C svarer at dersom noen av kundene har skreddersydde programmer og gjør mye av arbeidet selv, så vil risikoen øke.

Noen av informantene eksemplifiserer svaret ved å ta utgangspunkt i generelle IT-kontroller. Informant A legger til at dersom IT-funksjonen er ”in-house” så vektlegger de enda mer arbeid knyttet til back-up, sikkerhet, og rutiner relatert til tilgang.

Likevel viser informant B til noen svakheter ved outsourcet IT-funksjonen. Informanten forklarer at dersom IT-funksjonen er outsourcet gjennom profesjonelle kan man risikere at flere har tilgang til systemene og informasjon enn det virksomheten er komfortable med. I tillegg påpekes det at det virkelige komplekse er når man ikke får en type to bekreftelse fra serviceorganisasjonen funksjonen er outsourcet til.

Informant E er uklar i hvilken betydning dette kan ha, men sier at det kan telle positivt uten å utdype mer.

Informantene virker nokså samstemte i forhold til risikovurdering av en outsourcet IT-funksjon. Vår oppfattelse er at de er enige om å se etter at den interne kontrollen i serviceorganisasjonen er god og belyser hvilke utfordringer de ofte står ovenfor i forbindelse med dette. Det ser ut som at å innhente type 1 og type 2 bekreftelse er den sentrale handlingen her.

4.2.6 Nettskytjenester

På spørsmålet om informantene har bekjentskap med nettskytjenester og hvilken betydning det kan ha for revisjonen, opplever vi at informantene avgir noe ulike svar. Alle informantene er enige om at dette er en tjeneste som begynner å bli mer vanlig. Likevel varierer svarene informantene avgir med tanke på hvilken nytte en slik tjeneste har.

Informant D forklarer at flere av deres kunder benytter seg at dette og utdyper at store deler av revisjonen basere seg mer på skanning og mindre papirarbeid ved at all informasjon ligger på en felles server oppe i en sky. Informant A svarer at mange regnskapssystemer er nettskybaserte, men innrømmer at de ikke har helt kontroll på hvordan disse agerer med andre systemer. Informanten er usikker på hvilken betydning dette har for revisjonen og legger til at hun tror de kartlegger på samme måte, men at nettskytjenester er noe hun ønsker å ta med seg videre å undersøke mer.

Informant B viser til egne nettskytjenester og svarer at deres regnskapsavdeling tilbyr slik regnskapsføringstjeneste. Selv har han ikke vært bort i dette før med sine kunder. Han mener at nettskytjenester sier noe om hvordan informasjonen er lagret. Dersom informasjonen ligger i en sky fokuserer de mer på sikkerhet med tanke på kartlegging av back-up rutiner.

Informant E svarer at bruk av nettskytjenester har en innvirkning på revisjonen på et eller annet vis, men mener at det å benytte seg av nettet på den måten er en helt naturlig del av den tiden vi er i dag. Informanten forklarer at det viktigste er at man håndterer sikkerheten til informasjonen, men er usikker på hvor relevant informasjonssikkerheten er for det totale regnskapet som revisorene skal bekrefte.

Informant C kan ha tolket spørsmålet annerledes ved at han ikke svarer på om hans kunder benytter nettskytjenester. Han svarer derimot på hvordan han som revisor utveksler informasjon og dokumentasjon med sine kunder i en nettsky. Han forklarer at enkelte i revisjonsselskapet benytter seg av det på større kunder. Selv har han ikke dette på noen av sine kunder og begrunner det med at han opplever det som lite effektivt. Han sier videre at det tar like lang tid å få all nødvendig informasjon på en minnepenn. På store kunder, med mange ansatte spredt rundt på forskjellige lokasjoner, kan det være effektivt å benytte seg av slike tjenester. Han forklarer at det da lages en strukturert liste på hva som trengs og ønskes av revisjonsdokumentasjon og at dette lastes opp av kunden i nettskyen.

Informant F mener at nettskytjenester får samme betydning for revisjonen som med outsourcing av IT-funksjonen. De etterser likevel at kunden har tilgangskontroller, rutiner for oppfølging og datasikkerhet. Informanten legger til at de spesielt ser på hvilke rutiner kunden har dersom de sier opp avtalen ettersom regnskapsloven tilsier at det skal oppbevares i x antall år.

Ut i fra svarene informantene avgir kan det virke som om de har ulikt forhold til nettskytjenester og at dette var et spørsmål alle informantene, utenom F, ga ustødige svar på. De viser kjennskap til tjenesten, men hvilken konsekvens bruk av nettsky har, er flere av dem usikre på. Dette er en overraskende observasjon da vi forventet at flere av informantene kunne avgi tydeligere svar på dette ettersom flere av dem sier at nettsky har blitt vanlig. Vi vil allikevel trekke frem informant B som nevner at de er ekstra påpasselige med back-up, mens informant F utviser meget godt kjennskap til revisjon av nettskybaserte systemer.

4.2.7 Oppsummering

Revisors forståelse av IT-miljøet bærer preg av revisors profesjonelle skjønn. Selv om flere av informantene har relativt lik bakgrunn, er det flere av spørsmålene under dette området som får ulike utfall. Dette kan komme av informantenes kompetanse, interesse, erfaring og selskapets egen revisjonsmetodikk. Informantenes svar tilsier at risikovurderingen av systemer, samt elementene i IT-miljøet, vil ha betydning for revisors håndtering av IT-relaterte kontrollaktiviteter.

4.3 Revisors håndtering av IT-relatert risiko

På bakgrunn av spørsmålene om forståelse av IT-miljøet vil vi at informantene skal beskrive hvordan de håndterer IT- og informasjonssystemene når de gjennomfører sin revisjon. En generell oppfattelse for denne delen av problemstillingen er at revisor endrer sin tilnærming til revisjonen for å unngå IT-kontroller i internkontrollen.

4.3.1 Kartlegging av generelle IT-kontroller og applikasjonskontroller

Nedenfor har vi systematisert informantenes svar etter kategoriene av generelle IT-kontroller vi presenterte i teoridelen:

Informant	Tilgangs-kontroller	Kjøp, endringer og vedlikehold av systemprogramvare	Kjøp, utvikling og vedlikehold av applikasjoner	Datasenter og nettverksdrift (sikkerhet og back-up)
A	x	x (endringshåndtering)		
B	x	x (systemendring)	x (program development)	x (computer operations)
C	x	x(endringshåndtering)		x
D		x		x
E	x			
F	x	x (endringshåndtering)	x	x

Tabell 8: Kartlegging av generelle IT kontroller

Det er informantene B og F som kan opplyse om at de kartlegger alle de fire kategoriene av generelle IT-kontroller. Informant A svarer basert på erfaring, og forklarer at det er tilgangskontroller og endringshåndtering som er de vanligste IT-kontrollene. Tilsvarende opplyser informant C at tilgangskontroller, endringshåndtering og IT-sikkerhet med back-up, er de pliktige til å kartlegge et minimum av. Informant D nevner back-up rutiner, kapasitet,

fysisk sikring, vedlikehold og anskaffelse av systemer som eksempler på generelle IT-kontroller.

Informant E er noe upresis i forhold til det vi forventet å få til svar. Informanten forklarer at tilgangsstyring er viktig, men at det er først og fremst programmets bruk inn mot regnskapet som er vesentlige her. Videre utdyper informant at hva han anser som viktig vil avhenge av revisors profesjonelle skjønn hvor man vurderer hva som er relevante IT-kontroller knyttet til regnskapet.

Tidligere omtalte vi tilgangskontroller, kjøp, endring og vedlikehold av systemprogramvare, programendring, og kjøp, utvikling og vedlikehold av applikasjoner som hovedkategorier for generelle IT-kontroller. Vi opplyste ikke informantene om noen av disse i forkant for å ikke påvirke deres svar. Dermed fikk vi også litt varierende svar. Som vi kan se av tabellen er det informantene B og F som hovedsakelig nevner at de kartlegger alle fire kategoriene for generelle IT-kontroller. Informant B var veldig tydelig på at deres metodikk besto av å teste alle fire kategoriene. Ut i fra vårt inntrykk var også dette noe som han var veldig opptatt av og hadde forberedt seg godt på. Svaret fra informant F, som er IT-revisor, stemmer med vårt bilde av hans kompetanse på område. Slik vi tolker de andre informantene er svarene deres mer sprikende som følge av erfaring og skjønnsmessige vurderinger, særlig da informanten A, C, D og E.

For å grave dypere inn i informantenes forståelse av kontrollaktiviteter relater til IT- og informasjonssystemer, stiller vi etterfølgende spørsmål om hvordan de identifiserer applikasjonskontroller.

Informantene A, B, D, E og F svarer at de identifiserer applikasjonskontroller gjennom rutinekartlegging av transaksjonsstrømmene. Det er likevel mulig å belyse noen nyanser blant svarene som avgis. Informant B påpeker at applikasjonskontrollene kan oppleves som usynlige, men at det beste verktøyet er en grundig walk-through av prosessen. Informant F svarer tilsvarende at de først kartlegger ved å høre med kunden om hvilke applikasjonskontroller de har og deretter vurderer om de skal teste dem. Informant D sier at de kartlegger de mest sentrale rutinene for selskapet og at disse ofte er rutiner knyttet til salg, innkjøp og lønn. På lik linje som informant D, svarer informant E at dersom de i rutinekartleggingen oppdager en rutine som påvirker et område i regnskapet, går de inn og prøver å danne seg en formening om hvordan dette fungerer i praksis.

Her er det i midlertidig informant C som skiller seg ut og svarer at i større selskaper har de egne kart for applikasjonskontroller som de kan basere tester på, og disse er ofte nøyaktige.

Slik vi tolker svarere som informantene avgir har de alle vært borti identifisering av applikasjonskontroller og at kartlegging av disse kontrollene gjøres ved å benytte walk-through og flow-charts.

4.3.2 Testing av generelle IT-kontroller

På spørsmålet om hvordan informantene tester generelle IT-kontroller, svarer B, C og E at dette bestemmes hovedsakelig av revisjonsmetodikk og egne revisjonsverktøy de benytter.

Informant A går gjennom rutinene for de generelle IT-kontrollene med personen som har ansvaret for rutinen. Målet er å få innblikk på systemene som har innvirkning på regnskapsavleggelsen for så å kontrollere dem videre.

Informant B viser til eget revisjonsverktøy med fire punkter som danner rammeverket for generelle IT-kontroller. Dette verktøyet har egne restriksjoner på at arbeid relatert til generelle IT-kontroller må bekreftes etterhvert som arbeidet utføres. Noen eksempler som informanten beskriver er test av ansattes tilgang, passordrutiner og arbeidsdeling. Informanten stiller også spørsmål ved virksomhetens systemendringer ved å foreta tester før endringer implementeres. Dersom alle de fire punktene er testet og er på plass, vil de ha nok grunnlag til å si at kun autoriserte personer har tilgang, alle endringer er kontrollert, testet for implementering og alt opereres på en hensiktsmessig måte.

Informant C opplyser at revisjonshandlingene som er laget i deres revisjonsverktøy, er laget på en måte som tvinger dem til å få svar på enkelte spørsmål relatert til generelle IT-kontroller av kunden. Han eksemplifiserer med å sjekke tilgangskontroller og hvem som har endringsmuligheter.

Informant E svarer at deres metodikk hele tiden er på jakt etter relevante generelle IT-kontroller. Ved å følge sjekklister og svare på spørsmål revisjonsverktøyet stiller, vil det kanskje tilsi at det foreligger et komplekst IT-miljø. Da må IT-revisor involveres dersom det ikke kan oppnås sikkerhet på andre måter.

Informant D utdyper at deres selskap tester generelle IT-kontroller via forespørsler rettet mot ledelsen, observasjoner og annen dokumentasjon.

Informant F forklarer at de vurderer kontrollenes design i internkontrollen og vurderer implementeringen for å teste de generelle IT-kontrollene. For tilgangskontroller sjekker de rutiner og kontroller for etablering av brukere, hvem som har tilgang til hva, og hvilke rutiner de har for oppfølging av tilganger. Når det gjelder drift hører revisor med kunden om hvilke back-up rutiner de har, hvor ofte de tar back-up og om de har enbkatastrofeplan. For endringshåndtering ser informanten på hvilke kontrollrutiner de har i forhold til nye versjoner av applikasjoner og at de kjører tester på dem.

Spørsmålet om testing av generelle IT-kontroller stilte vi relativt åpent da vi ville at informantene selv skulle beskrive hvordan de tester generelle IT-kontroller. Det vi kan se her er at informantene har valgt å utdype dette spørsmålet ulikt. Flere av informantene støtter seg på revisjonshandlinger som revisjonsverktøyet angir, men at de ikke forklarer konkret hvordan disse handlingene utføres. Informant B gir noe mer utdypende svar enn de andre. Slik vi tolker det kan det ha sammenheng med informantens interesse for området og hvilke kunder informanten har. Her kommer det tydelig frem at informant F er en IT-revisor da svaret er det mest detaljerte i forhold til hvilke tester som gjennomføres.

4.3.3 Testing av applikasjonskontroller

Etter at informantene gav en beskrivelse av hvordan de testet generelle IT-kontroller, spør vi videre om hvordan de går frem for å teste applikasjonskontroller. Som tidligere beskrevet utgjør applikasjonskontroller en del av kontrollaktivitetene i internkontrollen, derfor er påstanden fra Wood et al. (2013) om at revisor endrer sin tilnærming til revisjonen for å unngå internkontroller der IT-kontroll er en komponent eller kun gjør en overfladisk og lite detaljert vurdering av IT-kontrollene, særlig knyttet til spørsmålet rundt test av applikasjonskontroller.

Informantene A og B opplyser at test av applikasjonskontroller baserer seg på en tilnærming om at de generelle IT-kontrollene er effektive og testet tidligere.

Informant A fastslår at dersom generelle IT-kontroller er effektive, skal det holde å ta gjennomgang av rutiner gjennom en såkalt walk-through test. Da går informanten gjennom rutinen og tester om alle kontrollene i rutinene er effektive. Dersom dette er tilfelle vil det holde å teste én applikasjonskontroll for å se om den fungerer.

Informant B forklarer at de bruker noe som de kaller for ”test of one”, og utdyper at applikasjonskontrollene er helautomatiske. Dersom generelle IT-kontroller er testet tidligere og godkjent, og det videre skal testes en applikasjonskontroll, vet de at systemet vil gjøre det samme på den samme måten hver gang. ”Test of one” er en revisjonsprosedyre hvor de tester en applikasjon en gang. Med rammeverket i bakhånd og effektive generelle IT-kontroller kan de konkludere at applikasjonskontrollene fungerer som de skal.

Informant B uttaler:

”Sånn praksis, så må vi ofte inn i test-systemet til kunden. Det er her vi kan ha det litt gøy med tanke på applikasjonskontroller ved at vi kan prøve å kjøre gjennom ting som ikke skal være mulig.”

- Informant B -

Informant E tar utgangspunkt i et flow-chart som de lager med kunden. Der identifiserer de kontroller på et område i regnskapet som de fysisk tester.

Informant D viser lite kjennskap med akkurat testing av applikasjonskontroller. Han uttaler at de som regel prøver å finne kontroller hos kunden, enten det er manuelle eller automatisk kontroller, og teste kontrollene for å kunne bekrefte fullstendigheten, nøyaktigheten og gyldighetene av data.

Informant F tar utgangspunkt i transaksjonsstrømmen og følger den fra input og eventuelt beregninger til output i form av enten rapporter eller overføringer til andre systemer. Ved at kunden forklarer hvilke kontroller de har, gjennom prosessen, vurderer de om de er hensiktsmessige eller om noe mangler.

Informant C avgir ulikt svar enn de andre informantene. Han forklarer at dersom man snur litt på det vil en kunne tilnærme seg revisjonen på en annen måte og dermed unngå å teste applikasjonskontroller. Dersom man ønsker å bekrefte effektivitet og nøyaktighet av noen regnskapslinjer eller noen transaksjoner fra hovedboken, vil en ved eventuell tall-testing, etterregning og organisering av informasjonen kunne unngå å teste applikasjonskontrollen. I dette tilfellet forstås det slik at revisjonstilnærmingen informant C prøver å forklare her baserer seg mer på substanskontroller enn test av kontroller.

Svarene til informantene varierer fra å ikke teste applikasjonskontroller i det hele tatt, til å utdypende forklare hvordan applikasjonskontroller testes. Siden spørsmålet ble stilt *"hvordan tester du identifiserte applikasjonskontroller?"* gav det ingen retningslinjer for hva eller hvor mye de skulle svare. Dette var noe av poenget med hvorfor spørsmålet ble stilt åpent og det kan være en mulig årsak til at svarene er varierende. Informantene A og B er tydelig inne på at det er effektive generelle IT-kontroller som danner grunnlag for å kunne teste applikasjonskontrollene. Dette samsvarer med teorien som vi har beskrevet tidligere. Informantene E og D gir etter vår vurdering en overfladisk beskrivelse av hvordan de tester applikasjonskontroller. Informantene F og B gir derimot en mer detaljert beskrivelse av hvordan applikasjonskontrollene testes. Ved at informant F er en CISA-sertifisert IT-revisor, er dette sannsynligvis forklaringen til et tydeligere svar som samsvarer med teorien på hvordan applikasjonskontroller skal testes. Årsakene til at svarene fra de andre informantene varierer, kan være at det er begrenset omfang av applikasjonskontroller som er hensiktsmessige å teste i deres kunder. Likevel kan informantene litt om prosedyrene rundt dette.

Det som er mest overraskende her er imidlertid informant C som velger å beskrive hvordan applikasjonskontroller kan unngås. Informanten gir en beskrivelse av hvordan han identifiserer applikasjonskontroller, men gir ikke en forklaring på hvordan han tester dem. Ut i fra svaret til informanten er han opptatt av å lete etter den mest effektive revisjonstilnærmingen og at substanshandlinger kan være mer hensiktsmessig enn test av kontroller i noen tilfeller.

4.3.4 Verifisering av rapporter

Verifisering av integritet i rapporter har som tidligere nevnt vært i fokus de siste årene. Derfor stiller vi spørsmål ved hvordan de verifiserer integriteten i rapporter. Informantene svarer følgende:

Informant A bruker resultatrapporter som et eksempel og sier at de verifiserer ved å avstemme dem mot regnskapet og kontrollsummere. Hun sier at dersom du har en effektiv IT-revisjon er også det en kontroll.

Informant B forklarer at dette er ekstremt på agendaen den siste tiden. Han definerer rapporter i to kategorier: standardrapporter fra systemet og Custom-rapporter, som er rapporter laget eller tilpasset av selskapet slik at det ikke lenger er standard rapporter laget av systemutvikler.

Videre sier han at ved standardrapporter i systemene, forutsatt at de har testet GITC (General IT-Controls) og at det er på plass, er terskelen for å stole på at de er fullstendige og nøyaktige mye lavere. Informanten forklarer at de da har kontroll på endringene som er gjort gjennom årene og vet at rapportene genererer likt hver gang. Han legger til at det kan være nødvendig å teste og avstemme mot saldobalanse. Videre sier han at hvis der er en Custom-rapport må de inn i det de kaller for IPE-testing – ”Information produced by the entity”, og gjøre egne handlinger. Hvilke handlinger som gjøres avhenger av rapporten for å kunne verifisere at den er komplett og nøyaktig. Der er det ikke nok å avstemme mot saldobalanse. Han eksemplifiserer rapporten som en aldersfordeling av kundereskontroen hvor de har egne matriser på hvor mye de må teste. Han forklarer at de går inn og tester spesifikt at de dataene som kommer i rapporten er i henhold til fakturaen som er utsendt, at data er lagt inn korrekt og beløpene er korrekt. Informanten avslutter med å si at ved Custom-rapporter som kunden har laget selv, må de gjøre en utvalgsbasert testing i henhold til matriser.

Informant C sier også at det har vært veldig stort fokus på verifisering av rapporter. Han forklarer at han kan få IT-revisoren til å sjekke rapporten for seg eller sjekke systemet, og må teste applikasjonen selv. Videre sier han at noen rapporter må testes hver gang den tas ut, men hvis ingen tukler med systemet og det er likt hver gang, kan han teste den én gang. Da er ITGC (IT generelle kontroller) i bunnen. Alternativt, hvis rapporten bygger på en applikasjonskontroll må han kartlegge de mest grunnleggende ITGC (IT generelle kontroller) og gå inn å detalj-teste den. Informanten bruker også kundereskontro som eksempel. Hvis han skal teste den, tar han et utvalg fra lista og ser om riktig dato er inne i systemet, forfallsdato, hvor gamle de utestående fordringene er, sjekker det fysisk og gjør mer substanshandlinger.

Informant D sier at dersom det kommer rapporter ut i fra systemet, og de ikke har andre indikasjoner på at de inneholder feil, aksepterer de rapporten som riktig. Informanten bruker også kundelister som et eksempel hvor de kritisk går gjennom den og tar den opp hvis det skulle være noen åpenbare feil. Han bruker avstemming med eksterne kilder ved saldoforespørsel som en måte å verifisere kundeliste på.

Informant E synes også dette er viktig. I deres metodikk kalles dette for ”information prepared from entity” eller IPE. Dette går ut på hvordan de skal teste at det som de får fremlagt er ekte. De løser seg fra systemene og utfører substanstester, som for eksempel hvordan ting beregnes. Videre bruker han årsoppgave fra bank som eksempel og sier at denne kan manipuleres og se ekte ut hvis man er god i PDF. For å kunne stole på den rapporten som

er levert, henvender de seg direkte til banken for kunne få en kilde fra ekstern aktør. For systemgenererte rapporter, der det beregnes automatiske snittpriser, kalkuleringer og avsetninger, sier han at de må inn å finne interne kontroller i systemet som gjør det mulig å vurdere om rapporten er ekte. De identifiserer og ser at test av kontroller gjennomføres på den biten. Videre sannhetsverifiserer de den ved at kunden forklarer og viser hvordan de utfører kontrollen. Dersom kontrollen stemmer vil det bekrefte at test av kontroller fungerer og at de kan bruke det som test av generelle IT-kontroller i revisjonen.

Informant F sier at den enkleste måten å verifisere integritet i rapporter er å gjøre en ”reperformance”. Han viser til et eksempel hvor han får en liste fra et system hentet ut fra databasen. Ved å summere hele rapporten på nytt og få samme resultat, vil det være den sterkeste testen for å sjekke integritet i rapporter.

Det kommer tydelig frem at dette spørsmålet har vært en aktuell problemstilling for informantene fra de store revisjonsselskapene, og slik vi tolker svarene har særlig informantene B, C, E og F god forståelse for hvordan de skal gå frem for å håndtere verifisering av integritet i rapporter som brukes i revisjonen. Vi vurderer det som at informant D tar lettere på denne problemstillingen i sitt svar. Informanten er fra et mindre revisjonsselskap. Dette kan være en mulig årsak til at denne problemstillingen ikke har vært like aktuell som i de store revisjonsselskapene.

4.3.5 Oppsummering

Som vi tidligere oppsummerte vil informantenes svar tilsi at risikovurderingen av systemer samt elementene i IT-miljøet har betydning for revisors håndtering av IT-relaterte kontrollaktiviteter. I dette kapitelet om håndtering av IT-relaterte kontroller ser vi tydeligere hvordan informantenes kompetanse, interesse, erfaring og selskapets egen revisjonsmetodikk understøtter svarene som avgis.

Det vi anser som den viktigste betraktningen her er bekreftelsen av informant C om at substanshandlinger i noen tilfeller er den mest effektive revisjonstilnærmingen. Samtidig er det viktig å påpeke at de resterende informantene utviser kjennskap til og forståelse av hvordan de håndterer IT-relaterte kontrollaktiviteter.

4.4 Rapportering og kommunikasjon ved kontrollsvakheter

Rapportering er en viktig del av revisjonsprosessen uansett om det foreligger vesentlige svakheter eller mindre kritiske svakheter i IT- og informasjonssystemene. Dette følger også av lovbestemmelsen i Revisorloven (1999) §5-1 som angir at *"Revisor skal se etter at den revisjonspliktige har ordnet formuesforvaltningen på en betryggende måte og med forsvarlig kontroll"*.

Det vi ønsker å se på her er hvordan revisor rapporterer og kommuniserer funn i revisjonen til de som har overordnet ansvar for styring og kontroll i virksomheten. Tidligere beskrev vi at revisor kan avgi to ulike typer konklusjoner basert på hvor vesentlig og gjennomgripende feilinformasjonen eller svakheten er. Dersom revisor kan bekrefte at regnskapet og internkontrollen ikke er heftet med vesentlig feilinformasjon eller svakheter, vil det avgis en umodifisert revisjonsberetning. I motsatt tilfelle vil det avgis en modifisert beretning.

4.4.1 Konfidensialitet, integritet og tilgjengelighet

For å bygge revisjonen på test av IT-relaterte kontroller må IT-og informasjonssystemene overholde prinsippene om integritet, konfidensialitet og tilgjengelighet. Dermed stiller vi spørsmål om hvilke konsekvenser det får for den videre revisjonene og hva de gjør for å dekke denne risikoen dersom systemene som anvendes ikke overholder prinsippene.

Informant A sier at det blir mer arbeid og at de tester alle kontroller som om de er manuelle. Videre sier hun at de ikke kan stole på applikasjonskontrollene og det blir mer substansarbeid. Alternativt tester de ikke kontroller i det hele tatt, men går rett på substanshandlinger fordi den kombinerte risikovurderingen blir høyere. Utvalgsstørrelsen blir også mye høyere når risikoen vurderes som høyere.

Informant B forklarer at dersom det foreligger svakheter knyttet til GITC – testingen deres, vil det føre til høyere risiko og det blir mer omfattende arbeid. Han bruker et eksempel ved at kunden ikke har implementert arbeidsdelingsrutiner. Da ville de foretatt en test om det i løpet av året forelå tilfeller hvor en person har gjort to eller flere kritiske steg flere steder.

Informant C mener at det kommer an på hvor graverende tilfellet er og om man eventuelt må revurdere revisjonsstrategien eller revisjonsprogrammet. I tilfelle kan man ikke bygge like mye på IT-systemet og rapportene som planlagt. Informanten avslutter med at det kan i verste

fall føre til at man ikke kan avgi en ren revisjonsberetning eller ikke har grunnlag til å uttale seg om regnskapet.

Informant D sier at de utvider med andre substanskontroller hvis det viser seg at test av kontroller indikerer at systemene ikke fungerer.

"Jeg føler ofte at det kanskje ikke er systemene som svikter, men heller manglende manuell oppfølging av kontroller."

- Informant D -

Informant E sier at dersom kontrollene viser seg å ikke fungere og det ikke er spor av kontrollen i noen situasjoner, kan han ikke bruke test av kontroll eller bruk av IT som en angrepsvinkel. Videre sier han at det er mulig å se om det er andre kontroller som kan brukes eller at det må brukes mer substansangrepsvinkel for å verifisere tallene.

Informant F sier at det kommer an på hva konsekvensen er av at systemene ikke overholder de tre prinsippene. Hvis det er et komplekst system og han ikke kan stole på tallene, må han gjøre andre revisjonshandlinger for å verifisere informasjonen. Som et eksempel bruker han et tilfelle hvor man ikke kan stole på outputen fra systemet. Da må han vurdere om han kan gå på transaksjonsnivå og få summert opp og testet transaksjonene. Han utdyper at hvis det er enkle transaksjoner, for eksempel kjøp-salg, så bør det være mulig å verifisere den finansielle informasjonen. Der det er kompliserte transaksjoner og beregninger kan det få større betydning for den finansielle revisjonen. Dette kan medføre et punkt i en revisjonsrapport og eventuelt vurderes i revisjonsberetningen.

Ut i fra informantenes svar kan vi se en tydelig tendens til å øke omfanget av substanshandlinger som en konsekvens av at IT- og informasjonssystemene ikke overholder prinsippene om integritet, konfidensialitet og tilgjengelighet. Dette er sammenfallende med det vi forventet å få til svar da vi stilte spørsmålet. Informantene fikk mulighet til å svare på spørsmålet uten at vi la noen føringer. Som det fremkommer her har informantene tillagt ulik vekt på spørsmålet ved at noen gir en beskrivelse på et overordnet nivå, mens andre utdyper med eksempler og gir en mer detaljert beskrivelse.

4.4.2 Vurdering av vesentlige svakheter i IT- og informasjonssystemer

Siden revisorene skal anvende sitt profesjonelle skjønn for å avgjøre hvilke tilfeller som anses som vesentlige svakheter, stiller vi spørsmål ved hvordan de vurderer vesentlige svakheter i IT- og informasjonssystemer.

Både informant A og E forklarer at feil relatert til IT- og informasjonssystemer vurderes opp mot en vesentlighetsgrense som er satt. For å vurdere om det foreligger vesentlige svakheter i informasjonssystemet, svarer informant A at det må være feil av den betydning at det fører til vesentlig feil i regnskapet. Dette er sammenfallende med svarene til informantene B, C, D, E og F som påpeker at det er en skjønnsmessig vurdering om det får en gjennomgripende effekt på regnskapet. I tillegg sier informant F at internkontroll knyttet til transaksjonsflyten og overføring av data til økonomisystemene er et område der det bør være kontroll.

Informant B eksemplifiserer en vesentlig svakhet som et gjennomgående problem med arbeidsdeling og tilganger til systemene, og at dette utgjør en risiko for revisjonen. Informant E kan fortelle at dersom de er usikre på om det er vesentlig svakhet, går de tilbake for å utføre mer revisjon og kan måtte endre strategien. Informant A bruker tap av data som eksempel og forklarer at de da ikke kan bekrefte tallene og konkludere på regnskapet.

I samsvar med revisjonsstandarden ISA 265 og tidligere beskrevet teori er en svakhet vesentlig når den får betydning for risikoen for vesentlig feilinformasjon eller at det foreligger kontrollsvakheter i internkontrollen som er viktige for dem som har overordnet ansvar for styring og kontroll. Dette stemmer godt med våre funn ved at slik vi tolker svarene til informantene er de enige om at en vesentlig mangel må ha en gjennomgripende effekt på regnskapet.

I tillegg stiller vi spørsmål om de vil påpeke ovenfor de som har overordnet ansvar for styring og kontroll, om sikkerheten i IT-systemene er mangelfullt. Alle informantene er enige om at mangler på sikkerhet i IT- og informasjonssystemene er en del av håndtering av internkontroll og at dette er noe de rapporterer på. Informant B hadde i tillegg en mening om viktigheten av informasjonssikkerhet:

”Cyber – security vil jeg si er på topp ti liste, kanskje topp fem, av alle risikoer i norske børsnoterte foretak. Så gjennomgående problemer eller mangler i IT-systemene, det vil havne opp på konsernnivå ettersom det er noe kundene bryr seg om.

- Informant B -

Informant F skiller mellom vesentlige sikkerhetssvakheter og mindre sikkerhetssvakheter. Alle svakheter rapporteres til oppdragsansvarlig revisor. Han eksemplifiserer skille slik:

”For eksempel hvis du skulle hatt seks tegn i passordet, i stedet for fem. Okei, da er det kanskje ikke at du har passord som det burde vært, men det har ikke nødvendigvis noe å si for den finansielle informasjonen umiddelbart. Det blir en vurderingssak mot hvordan det vil påvirke den finansielle rapporteringen, at det mangler en intern kontroll”.

- Informant F –

Utformingen av spørsmålet gav ikke informantene noen indikasjon på å forklare hvordan de kartlegger og håndterer informasjonssikkerheten i revisjonskunden. Ut i fra svarene fra informantene er det allikevel mye fokus på informasjonssikkerhet og at dette er noe de rapporter på dersom det er mangefult. Informant B har i tillegg nevnt at informasjonssikkerhet er viktig for børsnoterte foretak. Dette tror vi har sammenheng med regionen og kundegruppene han reviderer i. Informant F har også mye å tilføye på dette spørsmålet. Dette mener vi kan ha en sammenheng med at han er IT-revisor og dermed retter mer oppmerksomhet mot informasjonssikkerhet.

4.4.3 Kommunikasjon og rapportering av vesentlige svakheter

Under spørsmålet om vesentlige svakheter vil vi at informantene skal utdype til hvem de kommuniserer og rapporterer til. Nedenfor presenterer vi en tabell med svarene informantene avgir.

Informant	Rapporter til ledelsen	Presentasjoner til styret	Nummererte brev	Diskusjon med revisjonsteamet
A	x	x	x	x
B	x	x	x	x
C	x	x	x	x
D	x		x	
E	x	x	x	x
F	x	x	x	x

Tabell 9: Kommunikasjon og rapportering av vesentlige svakheter

Som vi kan lese av tabellen ovenfor svarer samtlige av informantene at vesentlige svakheter relatert til informasjonssystemer kommuniseres gjennom rapportering til ledelsen og gjennom nummerte brev. Informantene fra de store revisjonsselskapene, da A, B, C, E og F, bruker presentasjoner der de deltar på styremøter for å formidle svakhetene de observerer. Informantene opplyser at de også bruker diskusjon i revisjonsteamet.

Informant E forklarer at nummerert brev blir først og fremst aktuelt når det foreligger lovbrudd eller andre alvorlige svakheter knyttet til ledelseshierarkiet. Han påpeker videre at nummererte brev er et offentlig dokument som skal oppbevares og skal fremlegges ved kontroller.

Informant D, som holder til i et mindre revisjonsselskap, sier at i små kunder er det tett dialog med eiere og styret via møter. Han sier også at nummererte brev er lovpålagt dersom det er vesentlige forhold.

Som antatt er svarende fra informantene like. I forbindelse med dette kan det være relevant å trekke inn at det er lovpålagt å rapportere om vesentlige forhold i samsvar med Revisorloven (1999)§5-2. Vi mener at informantenes bruk av presentasjoner kan ha sammenheng med størrelse på kundene, og at det foreligger et større behov for å kommunisere med styret. Det er derfor rimelig at dette også kan ha noe å i si for informant D sitt svar. Etter vårt inntrykk forholder han seg til mindre kunder enn de andre informantene og bruker dermed ikke presentasjoner, men heller personlige møter til å kommunisere og rapportere vesentlige svakheter.

4.4.4 Vurdering av mindre kritiske svakheter i IT- og informasjonssystemer

Som en oppfølging til spørsmålene om vesentlige svakheter følger vi opp med hva de regner med som mindre kritiske svakheter i IT- og informasjonssystemer.

Både informant A, D og E svarer at mindre kritiske svakheter, er svakheter som ikke får konsekvens eller påvirker regnskapstallene vesentlig. Informant B eksemplifiserte mindre kritiske svakheter som ansatte som bytter avdeling og ikke får fjernet tilgangsmuligheter fra den forrige avdelingen. Informant C gir også et eksempel der en mindre svakhet kan være et undersystem til et faktureringssystem som utgjør en liten del av inntektsprosessen.

Informant E forklarer at en ren revisjonsberetning er det beste å få og at det er revisor sin plikt å påse at alt er i orden. Videre mener informanten at revisor kan tre inn i en rolle som rådgiver for å rette opp i mindre kritiske svakheter slik at virksomheten kan lære i ettertid.

Informant F begrunner mindre kritiske svakheter med at de ikke får umiddelbare konsekvenser for den finansielle informasjonen, men at det blir en vurderingssak om mindre mangler i internkontrollen påvirker den finansielle rapporteringen.

Slik vi tolker svarene til informantene mener alle at mindre svakheter er svakheter som de kan dekke på andre måter for å redusere revisjonsrisikoen og som ikke medfører vesentlig feil i regnskapet.

4.4.5 Kommunikasjon og rapportering av mindre kritiske svakheter

Videre stiller vi spørsmål om hvem de kommuniserer mindre kritiske svakheter til. Dette gjør vi for å se om det foreligger noe forskjell mellom kommunikasjon av vesentlige svakheter og mindre kritiske svakheter. På samme måte presenterer vi en tabell med svarene informantene avgir.

Informant	Rapporter til ledelsen	Presentasjoner til styret	Systemeiere
A	x	x	
B	x	x	x
C	x	x	
D	x		
E	x	x	
F	x	x	

Tabell 10: Kommunikasjon og rapportering av mindre svakheter

Der det foreligger mindre kritiske svakheter i informasjonssystemene ser vi at alle informantene rapporterer til ledelsen. Informantene A, B, C, E og F opplyser om at presentasjoner til styret brukes også for mindre kritiske forhold.

Det som skiller seg ut i dette tilfellet er informant B som påpeker at de gir beskjed til systemeierne om mindre kritiske forhold, men at slike forhold uansett kommenteres som en tilbakemelding til ledelsen gjennom en presentasjon.

”Du vil gjerne komme med innspill til forbedring, ellers vil det jo være likt neste år hvis ingen tar tak. Hvis du sier ifra til styret vil de presse på til ledelsen å frigi tid og penger til å fikse på det.”

- Informant C –

På samme måte som ved kommunikasjon av vesentlige svakheter ser vi at svarere på kommunikasjon av mindre kritiske svakheter er relativt sammenfallende. Vårt inntrykk er at alle informantene er opptatt av å bidra til å forbedre kundens aktiviteter ved å opplyse om mindre operasjonelle svakheter i internkontrollen. Som merket i tabell 6 er det informant B som kan fortelle at mindre kritiske svakheter også kan kommuniserer til systemeiere. Dette mener vi er et godt eksempel på anvendelse av skjønn.

4.4.6 Betydning for revisjonsberetning

Alle informantene er enige om at dersom IT- og informasjonssystemene ikke fungerer tilfredsstillende, vil det få betydning for revisjonsberetningen. Dette utdyper alle informantene ved å forklare at IT- og informasjonssystemene er en viktig del av internkontrollen. Derfor er det overraskende at informantene B, C og F opplyser at de aldri har gitt en modifisert beretning på bakgrunn av svakheter i IT- og informasjonssystemene. De andre informantene A, D og E påpeker ikke dette i sine svar.

”Det er veldig uvanlig at selskaper ikke har ting på stell. Vi kan godt finne ting som er lite effektivt, at de ikke bruker så mye av systemet de trenger eller at de har feil systemer, men at veldig mye er feil, er sjeldent”

- Informant C -

Informant E forklarer at dersom den interne kontrollen, herunder IT- og informasjonssystemene, ikke er i orden, skal revisor gjøre en vurdering om det er av den art at det bør påpekes ovenfor styret og eventuelt avgi en modifisert revisjonsberetningen.

Informant B forklarer at for at det skal ha betydning for revisjonsberetningen må det typisk være en svikt som medfører at de ikke får gjennomført revisjonen med tilstrekkelig sikkerhet.

” I revisjonsberetningen konkluderer vi også på om ledelsen har tilrettelagt for en god intern kontroll. Hvis det er så gjennomgående feil, går vi rett på det punktet”

- Informant B -

Informant D sier at dersom det er gjennomgripende feil vil det få konsekvenser dersom de ikke kan oppnå sikkerhet ved andre kontroller. Dette kan medføre til presisering eller forbehold i beretningen.

4.4.7 Oppsummering

På spørsmålet om prinsippene konfidensialitet, integritet og tilgjengelighet, ser vi at konsekvensen er gjenstand for revisors profesjonelle skjønn. Informantene forklarer at revisjonsarbeidet blir mer omfattende gjennom økt substanshandlinger, kompenserende handlinger og at de kanskje til og med må revurdere revisjonsstrategien dersom systemene ikke overholder prinsippene. Hvilken konsekvens det vil medføre for rapporteringen avhenger av hvor vesentlig svakheten er og om den har gjennomgripende effekt på regnskapet. Likevel er vårt inntrykk at alle informantene er opptatt av å bidra til å forbedre kundens aktiviteter ved å opplyse om mindre operasjonelle svakheter i internkontrollen.

Alle informantene er enige om at svakheter i IT- og informasjonssystemene er en del av håndtering av internkontroll og at dette er noe de rapporterer på. Flere av informantene oppgir at de aldri har gitt en modifisert beretning på bakgrunn av dette. Ut i fra dette svaret kan det virke som om ingen av revisjonskundene til informantene har hatt svakheter i internkontrollene relatert til IT- og informasjonssystemer. Vi stiller oss selv spørsmål ved om det kan være knyttet til at kontrollsvakhetene ikke er vesentlige nok eller gjennomgripende til å få betydning for revisjonsberetningen og at det derfor sjeldent er med.

4.5 Samhandling mellom revisor og IT-revisor

I kapittelet om IT-revisor ga vi uttrykk for at forventningene til revisorenes kompetanse har økt ettersom kompleksiteten og anvendelse av IT- og informasjonssystemer er blitt vanlig. Allikevel er det tilfeller som tilsier at det er behov for involvering av en ekspert når systemene utgjør en risiko i revisjonskunden. Derfor stiller vi informantene spørsmål ved hvilke oppdrag og hvilke vurderinger de foretar når de involverer en IT-revisor. Informantene A, B, C, E og F er revisorer på managernivå, mens informant D er partner. Det er kun informant F som har en CISA-sertifisering og som kan benevnes som IT-revisor.

4.5.1 Involvering av IT-revisor

Informant A påpeker at dersom kunden de reviderer har flere regnskapssystemer eller forsystemer involveres en ekspert som IT-revisor for å kartlegge rutinene. IT-revisor brukes

også som rådgiver for revisjonsteamet ved at han har bedre forutsetninger der systemene er mer komplekse.

Informant B svarer at det først og fremst er revisjonsteamet som drar ut til kundene. Det er partner som vurderer hvorvidt oppdraget tilsier at det trengs å involvere eksperten, da IT-revisor. IT-revisors involvering er veldig vanlig i planleggingsfasen for å finne ut hvordan man hensiktsmessig kan tilnærme seg IT-miljøet og legge til rette et riktig revisjonsprogram. På det tidspunktet kommer de finansielle revisorene inn og gjør den store jobben, men IT-revisoren er med i hele prosessen ved at det er de som er ansvarlige for IT-revisjonene. De tar en gjennomgang av den jobben som blir gjort av de finansielle revisorene.

"Hvis vi skal basere oss på IT-systemene, kommer det an av at de har positive konklusjoner, og da er det litt for sent dersom de kommer med negative funn litt ute i januar. Deres høytid er høsten."
- Informant B -

Informant C legger til grunn at det vil avhenge av om de skal ha internkontrollfokus og dermed bygge revisjonen på eventuelle IT-rapporter eller om de skal ha ren substansrevisjon. Han utdyper at noen ganger er IT-revisor med første året, selv om det er mindre selskap. Hvis det neste året, etter vi har revidert, ikke er mye endringer i IT, kan vi bruke hans informasjon og utføre samme tester og handlinger som han gjør. IT-revisoren brukes i planleggingen og kartlegger på høsten i interimsperioden.

Informant F svarer at revisjonsteamet er først ute å gjør en vurdering. Dersom de er i tvil involverer de samtaler med en IT-revisor, men at bruk av IT-revisor er mest relevant i kunder der systemene er spesialtilpasset. I kundene som benytter standardsystemer vil revisjonsteamet håndtere systemene selv.

Informant D sier at det mest naturlig er å trekke inn IT-revisor på de store oppdragene. Fordi dette revisjonsselskapet ikke har en IT-revisor, kunne han ikke utdype dette nærmere.

Informant E har noe sammenfallende svar med informant C og forklarer at dersom det ikke er endringer i systemene fra tidligere år, kan de basere den fremtidige revisjonen på IT-revisors tidligere handlinger. Det er vanskelig å tolke hva informantene mener her og det kan skyldes av at informantene tolker spørsmålet annerledes enn det som var tiltenkt. Likevel tror vi at det informantene prøver å si er at de ikke kan unngå å teste kontroller, men at de tester de samme

kontrollene som ble utført i fjor. Videre svarer E at involvering av IT-revisor er mer revisjonsteamets vurdering for å kunne få hensiktsmessig og tilstrekkelig revisjonsbevis. Dersom revisjonsmetodikken deres i planlegging- og kartleggingsfasen av rutinene kommer frem til at det foreligger et komplekst IT-miljø, vil man vurdere å involvere en IT-revisor for å kunne verifisere transaksjonene. Informanten forklarer at involveringen av IT-revisor vil bidra med å *"mette"* revisjonsteamet slik at de oppnår tilstrekkelig revisjonsbevis. Videre sier informanten at de som regel klarer å innhente nødvendig revisjonsbevis uten å benytte seg av IT-revisor.

Behovet for å involvere en IT-revisor er gjenstand for vurdering når revisor planlegger revisjonen. Slik vi tolker svarene fra informantene har de både like og ulike, men interessante betraktninger om når en IT-revisor bør involveres. Dette tror vi kan ha sammenheng med at informantene tilhører ulike regioner og har ulike kundeporteføljer. Derfor er det også mulig å stille seg spørsmål ved om det kan være en sammenheng mellom tilgjengelige IT-revisorer og hvor ofte de brukes og for hvilke deler av prosessen.

4.5.2 Samhandling og kommunikasjon mellom finansiell revisor og IT-revisor

På oppdragene der IT-revisor involveres stiller vi spørsmål ved hvordan de tilrettelegger for at IT-revisors funn blir fulgt opp og hvordan de kommuniserer seg imellom.

Informant A og E svarer at IT-revisoren er i utgangspunktet en del av revisjonsteamet og det er her eventuelle funn diskuteres. IT-revisoren deltar på alle planleggingsmøter før oppstart av revisjonen på høsten, og er med ut på revisjonen og gjør sin del. Videre sier informant A at det ofte er finansiell revisor som tester mange av kontrollene, hvor flere av disse er applikasjonskontroller. Informant E legger til at dersom IT-revisor oppdager funn som kan ha innvirkning på revisjonen, ber de han om å lage et notat som kan benyttes som revisjonsbevis ved senere anledning.

"På oppdrag der han brukes mer som ekspert, er han inne kort for å kartlegge noe og komme med sin anbefaling."

- Informant A -

Informant B sier derimot at IT-revisoren som regel gjør egne handlinger og finner sine konklusjoner. Deretter gir vedkommende en tilbakemelding om det foreligger noen

kontrollsvakheter og eventuelt forslag til forbedringer. I møte med IT-avdelingen og systemeier diskuteres funn og konklusjoner.

Tilsvarende svarer informant C at IT-revisor jobber i en egen revisjons-fil og at det er der han noterer sine funn. Informanten opplyser om at han ofte må snakke med IT-revisor først om hva som er nødvendig å kartlegge. Videre sier han at dersom den finansielle revisoren skal bygge på spesielle rapporter, teste applikasjonskontrollene og vurdere om rapportene er til å stole på, må han snakke med IT-revisoren i forkant. I etterkant er kommunikasjonen skriftlig og muntlig der både operasjonelle og finansielle funn kommuniseres videre til selskapet.

Informant F forteller at IT-revisor og finansielle revisor dokumenterer i samme revisjonssystem. IT-revisoren rapporterer sine funn til oppdragsansvarlig revisor som skal vurdere hvordan funnene skal håndteres videre, om det er et punkt som skal i en revisjonsrapport eller om det er innspill til kunden som ikke er nødvendig å ta med i en revisjonsrapport.

På informant D sitt kontor er det ingen IT-revisorer. Derfor er informanten utelatt fra dette spørsmålet.

Ut i fra vår vurdering av informantenes svar kan det virke som at samhandlingen mellom IT-revisor og finansiell revisor foregår mest i planleggingen og innimellom på enkelte deler av revisjonen som ekspert. Nyansene i svarene er etter vårt inntrykk preget av informantenes revisjonsmetodikk og hvorvidt denne metodikken tilsier at IT-revisor er nødvendig.

4.5.3 IT-revisors effekt på den totale revisjonen

Tidligere beskrev vi at IT-revisjon og involvering av IT-revisor kan bidra til en effektiv revisjonstilnærming. Vi ønsker å se nærmere på hvilken verdi dette kan ha for revisjonen og stilte derfor spørsmålet om hvilken effekt informantene tror involvering av IT-revisor kan ha for den totale revisjonen.

Alle informantene er enige om IT-revisor kan bidra til en effektiv angrepsvinkel for den totale revisjonen.

"Effektiv gjennomføring er et nøkkelord her. På oppdrag som er komplekse, er det å teste kontroller den raskeste veien til en effektiv revisjon. Ellers vil man teste seg ihjel og må

gjøre masse substanshandlinger, og omfanget blir enorm. Da er IT kjempe viktig og hvis ikke IT-systemene fungerer, er risikoen for feil mye større"

- Informant A -

Informant B og F presiserer at der det foreligger omfattende transaksjonsmengder vil de ikke klare å oppnå tilfredsstillende sikkerhet ved vanlig type kontrolltesting og avanserte substanshandlinger. IT-revisor bygger et fundament som de finansielle revisorene kan bygge videre på. Informant F tillegger at det er noen kunder de ikke kan revidere uten en IT-revisor.

Informant D slår fast at en IT-revisor, i tillegg til effektiv gjennomføring, også kan bidra til å sette opp kontroller som er effektive.

Informant E svarer at dersom det foreligger et kompleks system der det er vanskelig å gjøre jobben fordi kalkyler, snittpriser, kostnader og tilganger ligger "back-office", må de inkludere en IT-revisor. Informanten sier at det ville hatt stor betydning her.

"Dersom vi skal involvere en IT-revisor er det også en kostnadsspørsmål, hvor mye dette vil koste og hvor mye sikkerhet det gir oss. Gir det oss sikkerhet, kan vi la være å gjøre andre ting. Hvis vi må ha en IT-revisor inn og vi må inn å gjøre like mye jobb, er sannsynligheten stor for at vi sier at vi føler at de kontrollene vi gjør kompenserer for IT-revisor, og at vi nødvendigvis ikke trenger å ha IT-revisor inne."

- Informant E -

Alle informantene er enige om at involvering av IT-revisor vil bidra til å skape en effektiv revisjon. Verken lærebøkene eller informantene er inne på om involvering av IT-revisor kan bidra til økt kvalitet på revisjonen. Dette er en interessant observasjon ettersom IT-revisjon kan bidra til en ny dimensjon i revisjonen som kan antas å øke revisjonens kvalitet.

4.5.4 Oppsummering

Behovet for å involvere en IT-revisor er gjenstand for vurdering når revisor planlegger revisjonen og hva deres revisjonsmetodikk tilsier. Det kan virke som at involvering av IT-revisor bidrar til en effektiv revisjon, men på grunn av kost/nytte betraktninger involveres de i stor grad som eksperter i planleggingsfasen og ikke som en del av revisjonsteamet gjennom hele revisjonsprosessen.

4.6 Muligheter og utfordringer for revisor i fremtiden

Som tidligere nevnt blir IT-systemene stadig mer integrert og altomfattende. Den teknologiske utviklingen har ikke bare medført at virksomhetene må holde seg oppdatert, men også revisorene. Vi har derfor valgt å stille informantene spørsmål om de ser for seg noen fremtidige utfordringer for revisjonsbransjen i forbindelse med teknologi. Dette ga oss noen svært interessante svar, syntes vi.

4.6.1 Hvilke utfordringer står revisjonsbransjen ovenfor i forbindelse med teknologi?

Informantene er alle enige om at det foregår enorm digitalisering og at teknologien vil forandre hele revisjonsbransjen og stille andre krav til revisor.

Informant B presiserer at teknologien vil forandre hele bransjen i de nærmeste fem-ti årene. Videre viser informanten til begrepet Big Data og at de siste tre årene etter at begrepet ble implementert, har det vært mer fokus på GITC-testing. Mer datatesting har kommet på agendaen for å kunne håndtere de enorme mengdene av data.

Informant A, B og E forklarer at det er naturlig at de vil måtte oppdatere sine egne rammeverk og systemer ettersom teknologien vil bli avansert. Informant E legger til at dersom man tenker ti år frem i tid vil det bli mer IT-fokus, og at delen som revideres finansielt med substanstester nå, vil bli mindre.

"Å ta i bruk de mulighetene det gir, tror jeg gir utfordringer for at vi skal bli mer effektive. Næringslivet forøvrig tror jeg er glad i å ta IT i bruk, så hvorfor skal ikke revisor også, eller regnskap på en måte, ta de tingene i bruk og gjøre det effektivt og gjøre de riktige tingene"

- Informant E -

Informant F kan også bekrefte at de ser muligheter i forbindelse med teknologi og mener at IT-revisor trolig vil få en del å gjøre, også i fremtiden. Informant D ser ikke på utviklingen som en utfordring for sitt selskap, men påpeker at hvis det ikke hadde vært for Revisorforeningen ville de ikke hatt noe metodikk. Han uttaler:

"Vi er nok avhengige av at vi har en forening som er i front og oppdatert med dette med teknologi"

- Informant D -

Informant C er mer kritisk til fremtiden og utviklingen av revisjonsbransjen. Han sier at det er spådd at revisjon er en bransje som vil dø ut sammen med regnskapsførere fordi roboter vil ta over. Dette utdyper han ved å forklare at etter hvert vil roboter sjekke alle transaksjonene og da vil det kun være nødvendig med en programmerer. Informant A opplyser om det samme, og forklarer at robotisering testes i stor grad ut for tiden i de store revisjonsselskapene. Informant C påpeker at fremtidige konkurrenter antas å være rene IT-selskaper. Han legger til at i revisjonsselskapet jobber de med å bli enda mer aktuelle, ikke bare på det finansielle, men også på det operasjonelle ved å skape merverdi for kundene.

"Vi er utsatt"
- Informant C -

Ut i fra svarene til informantene kan det se ut som noen av dem er mer optimistiske enn andre. Vi synes det er interessant å se at informant D trekker frem revisorforeningens rolle for små selskap, og at de er helt avhengige av at foreningen holder seg oppdatert med den teknologiske utviklingen. Den teknologiske utviklingen har medført utfordringer for flere bransjer. At informant A og C påpeker at robotisering vil ta over for regnskapsførere og revisorer, er en interessant belysning for spørsmålet vi stiller. Vårt inntrykk av svarene er at behovet for IT-revisorer vil bli større i fremtiden og at IT-revisjonstilnærmingen vil bli mer vanlig. I forbindelse med dette kan det antas at behovet for mer forståelse av IT-miljøet og mer testing av IT- relaterte kontrollaktiviteter vil øke.

5. Avslutning og konklusjon

”Hva gjør revisor for å forstå og håndtere risiko knyttet til IT- og informasjonssystemer relevant for finansiell rapportering?”

5.1 Konklusjon og avsluttende betraktninger

Hvilken betydning IT- og informasjonssystemer har for den eksterne revisor og utførelsen av revisjonen, er begrenset i norsk akademisk litteratur om revisjon. Dette kommer ytterligere frem ved at de internasjonale revisjonsstandardene, ISAene, kun gir overfladiske beskrivelser av revisors forståelse og håndtering av IT-relatert risiko. Teorien i vår masteroppgave er dermed basert på en rekke ulike kilder som gir en mer detaljert og grundigere innføring av IT-revisjon. Ved å ta utgangspunkt i engelsk litteratur og informasjon fra internasjonale aktører, herunder PCAOB, ISACA, COSO og ISO, har vi bygd opp kapitlene i vår teori. Derfor er det viktig for oss å konstanter at det er enkelte områder vi har usikkert grunnlag til å trekke konklusjon på.

Risikobildet i revisjon er preget av at forretningsprosesser i stor grad understøttes av IT- og informasjonssystemer. Derfor er ikke lenger teknologi forbeholdt IT-revisorer, men bør inngå som en naturlig del av den finansielle revisjonen uavhengig av virksomhetstype og størrelse. Det er nettopp dette vi har ønsket å belyse i vår masteroppgave. Vi ser at fokuset på dette har variert blant våre informanter. Det kan virke som et paradoks at alle informantene er enige om at de står ovenfor utfordringer og muligheter knyttet til IT- og informasjonssystemer, men at bruken av en IT-revisjonstilnærming varierer så mye som det fremkommer her. Vi beskrev innledningsvis at Wood et al. (2013) uttrykker at revisor kun gjør en overfladisk og lite detaljert vurdering av IT-kontroller, og endrer sin tilnærming for å unngå internkontroller, der IT-kontroller er en komponent. Det er denne antakelsen vi utfordrer våre informanter på ved å stille dem spørsmål ved hvordan de forstår og håndterer IT- og informasjonssystemer relevant for finansiell rapportering. Ut i fra svarere informantene har avgitt og vår analyse av dem, er det vanskelig å trekke ut en entydig konklusjon på denne antakelsen. Under intervjuene kommer det frem at informantenes kompetanse, interesse for IT-revisjon og erfaring er svært varierende blant informantene, selv om de er på samme stillingsnivå og har hatt noe kursing i IT. Det vi kan trekke frem er at informanten som er CISA-sertifisert IT-revisor utviser høy forståelse for IT-revisjon og den grunnleggende teorien i oppgaven. Blant de andre informantene i de store revisjonsselskapene er svarene mer varierende, og slik vi har tolket

dem har de absolutt tilstrekkelig kompetanse for forståelse og håndtering av IT- og informasjonssystemer, men utviser ikke noe særlig interesse utover det selskapet pålegger dem å kunne. Unntaket her er imidlertid informant B som finner IT-revisjon mer interessant. Alle informantene mener at IT-revisjon vil bli en økt revisjonstilnærming i fremtiden og at de vil oppleve økt konkurranse i å tilby de beste og mest effektive revisjonstjenestene til sine kunder. Derfor synes vi det er rart at det ikke mer interesse fra informantenes side for dette området i dag. Informant D fra et mindre revisjonsselskap utviser noe mer begrenset forståelse. Dette er en interessant betraktning ettersom informanten benytter Den Norske Revisorforeningens revisjonsverktøy, Decartes, som metodikk. I hvilken grad vi mener informantene har besvart problemstillingen, illustreres nedenfor

Figur 10: Grad av forståelse og håndtering av IT- og informasjonssystemer

Vi kan derfor konkludere med at revisors forståelse og håndtering av IT- og informasjonssystemer for finansiell rapportering er svært varierende, men at årsakene til dette kan være mange, for eksempel revisjonsselskapets metodikk, tilgang og fokus på kursing i IT, kompleksiteten i kundenes systemer, kompetanse, interesse og erfaring. Det er viktig å påpeke at dette er en kvalitativ studie med begrenset utvalgsstørrelse. Dermed bør vi være forsiktige med å generalisere våre funn, men at dette gir et godt grunnlag for videre forskning.

5.2 Forslag til videre forskning

Forslag til videre forskning i forbindelse med revisors forhold til IT- og informasjonssystemer for regnskapsavleggelse kan være en studie som kartlegger behovet for kompetanse innen IT-revisjon i fremtiden. Dette gjelder både behovet for kompetanse blant revisorer i dag, men også for fremtidige høyere utdanninger.

Ettersom vår oppgave har et begrenset utvalg, ville det være interessant med en studie der utvalget i større grad kan generaliseres gjennom en kvantitativ analyse.

Et annet forslag er å ta for seg mindre revisjonsselskap og undersøke hvordan Decartes tilrettelegger, eller ikke, for IT-revisjon. Dette stiller også noen spørsmål ved om Revisorforeningen følger utviklingen og om revisjonsstandardene er gode nok rammeverk for å ta høyde for fremtidens revisjoner der IT- og informasjonssystemer utgjør en større og mer betydningsfull rolle i virksomheter.

Vårt siste forslag er en studie som tar for seg hvilke prioriteringer som går foran i en revisjon, der kvalitet og effektivitet er det som blir målt. Som vi kan se i vår studie er informantene enige om at en effektiv revisjon er viktig, men hva med kvalitet? Det kan dermed være interessant å se på hvilke hensyn som tas i forbindelse med revisjonens kvalitet.

Litteraturliste

Aksjeloven. (1999). *Lov om aksjeselskaper (aksjeloven)*.

American Institute of Certified Public Accountants. Professional Judgement Hentet fra https://www.aicpa.org/InterestAreas/FRC/Pages/professional-judgment.aspx

Arens, A. A., Elder, R. J., Beasley, M. S. & Hogan, C. E. (2017). *Auditing and assurance services : an integrated approach* (16th ed., global ed. utg.). Upper Saddle River, N.J.: Pearson.

Askheim, O. G. A. & Grenness, T. (2008). *Kvalitative metoder for markedsføring og organisasjonsfag*. Oslo: Universitetsforlaget.

Bokføringsloven. (2006). *Lov om bokføring (bokføringsloven)*.

COSO. (2013). COSO Internal Control - Integrated Framework Principles Hentet fra https://www.coso.org/Documents/COSO-ICIF-11x17-Cube-Graphic.pdf

COSO. (u.å). About Us Hentet fra https://www.coso.org/Pages/aboutus.aspx

COSO & McNally, J. S. (2013). The 2013 COSO Framework & SOX Compliance Hentet fra https://www.coso.org/documents/COSO McNallyTransition Article-Final COSO Version Proof_5-31-13.pdf

Den Norske Revisorforeningen. (2016). *Stikkordsregister*. Revisors Håndbok.

Eilifsen, A., Messier, W. F., Glover, S. M. & Prawitt, D. F. (2014). *Auditing & assurance services* (3rd ed. utg.). London: McGraw-Hill.

Gulden, B. P. (2010). *Revisjon: Teori og Metode*. Oslo: Cappelen Akademisk Forlag.

Gulden, B. P. (2015). *Den eksterne revisor* (9. utg. utg.). Oslo: Gyldendal akademisk.

Haukerud, A. & Sandanger, K. (2003). Ny renessanse for internkontroll. *Magma, 6*(6), 43-51.

International Federation of Accountants. (2012). A Professional Judgement Framework for Financial Reporting - An international guide for preparers, auditors, regulators and standard setters Hentet fra https://www.ifac.org/system/files/uploads/PAODC/A-Professional-Judgement-Framework-for-Financial-Reporting.pdf

ISA 200. (2016). *Overordnede mål for den uavhengige revisor og gjennomføringen av en revisjon i samsvar med de internasjonale revisjonsstandardene*. Revisors Håndbok 2016.

ISA 260. (2016). *Kommunikasjon med dem som har overordnet ansvar for styring og kontroll*. Revisors Håndbok 2016.

ISA 265. (2016). *Kommunikasjon av mangler i intern kontroll til dem som har overordnet ansvar for styring og kontroll, samt ledelsen*. Revisors Håndbok 2016.

ISA 315. (2016). *Identifisering og vurdering av risikoene for vesentlig feilinformasjon gjennom forståelse av enheten og dens omgivelser*. Revisors Håndbok 2016.

ISA 330. (2016). *Revisors håndtering av anslåtte risikoer*. Revisors Håndbok 2016.

ISA 402. (2016). *Særlige hensyn ved revisjon av en enhet som bruker en serviceorganisasjon*. Revisors Håndbok 2016.

ISA 520. (2016). *Analytiske handlinger*. Revisors Håndbok 2016.

ISA 700. (2016). *ISA 700 Konklusjon og rapportering om regnskaper*. Den Norske Revisorforening.

ISA 705. (2016). *ISA 705 Modifikasjoner i konklusjonen i den uavhengige revisors beretning*. Den Norske Revisorforening.

ISACA. (u.å-a). History of ISACA Hentet fra http://www.isaca.org/About-ISACA/History/Pages/default.aspx

ISACA. (u.å-b). Sertifiseringer Hentet fra http://www.isaca.org/chapters2/Norway/certification/Pages/default.aspx
ISACA. (u.å-c). Why use COBIT 5? Hentet fra https://cobitonline.isaca.org/about
ISO. (2013a). ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements Hentet fra https://www.iso.org/standard/54534.html
ISO. (2013b). ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls Hentet fra https://www.iso.org/standard/54533.html
Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. Kristiansand: Høyskoleforlaget AS - Norwegian Academic Press.
Johannessen, A., Tufte, P. A. & Christoffersen, L. (2011). *Forskningsmetode for økonomisk-administrative fag* (vol. 3). Oslo: Abstrakt forlag.
Klamm, B. K. & Watson, M. W. (2009). SOX 404 Reported Internal Control Weaknesses: A Test of COSO Framework Components and Information Technology. *Journal of Information Systems, 23*(2), 1-23. doi: http://dx.doi.org/10.2308/jis.2009.23.2.1
KPMG LLP, Glover, S. M. & Prawitt, D. F. (2012). Enhancing Board Oversight - Avoiding Judgment Traps and Biases Hentet fra https://www.coso.org/documents/COSO-EnhancingBoardOversight_r8_Web-ready %282%29.pdf
Kristoffersen, T. (2014). *Virksomhetsstyring og regnskapsorganisering*. Bergen: Fagbokforlaget Vigmostad & Bjørke AS.
Kvalvik, K. M. E. (2014). *IT er ikke bare for IT-revisorer*. Paper presentert på Nasjonal Fagkonferanse i offentlig revisjon, Oslo. http://www.nkrf.no/filarkiv/File/Kurs_og_konferansepdf-er/Nasj-fagkonf-2014/T-1620-Kvalvik.pdf
Løwer, C. & Sanvik, E. (2015). Cloud computing - Rettslige utfordringer ved bruk av nettskyen. *Nr. 2*, 8. doi: http://www.revregn.no/asset/pdf/2015/2-30-6.pdf
Moeller, R. R. (2010). IT Audit, Control and Secutiry Lastet ned fra https://ebookcentral.proquest.com/lib/agder/reader.action?docID=624573
Moen, T.-G. & Havstein, B. (2014). *Regnskapsorganisering Bokføring og Intern kontroll*. Oslo: Cappelen Damm Akademisk.
NHO. (2016). Er vi klare for nye utfordringer? Hentet fra https://www.nho.no/arskonferanser/remix/forside/nyhetsarkiv/derfor-er-det-annerledes-denne-gangen/
PCAOB. (2013). Staff Audit Practice Alert No. 11 Hentet fra https://pcaobus.org/Standards/QandA/10-24-2013_SAPA_11.pdf
PCAOB. (2015). Staff Inspection Brief Hentet fra https://pcaobus.org/Inspections/Documents/Inspection-Brief-2015-2-2015-Inspections.pdf
Revisorloven. (1999). *Lov om revisjon og revisorer (revisorloven)*.
Singelton, T. (2014). IS Audit Basics: What Every IT Auditor Should Know About Computer-generated Reports. *ISACA Journal, 5*, 11-12.
Wood, T. J., Brown, W. C. & Howe, H. (2013). *IT Auditing and Application Controls for Small and Mid-Sized Enterprises*: Wiley Corporate F&A.

Vedlegg

Vedlegg 1. Intervjuguide

Informasjon om informantene:

Størrelse på selskap

Yrkestittel

Erfaring

Erfaring fra IT

I planleggingsfasen:

1. Hvem snakker du med når du skal forstå, vurdere og håndtere enhetens IT systemer?
2. Hvor mye vekt tillegger du de beskrevne rutiner og prosedyrer for enhetens håndtering av systemene som er relevante for finansiell rapportering?
3. Når involveres en IT revisor i oppdrag?
4. Hvilken effekt mener du IT revisor har for den totale revisjonen?
5. Hvordan kommer du frem til hvilke systemer som er relevant for revisjonen?
6. Hvilke rammeverk mener du er nødvendige å støtte seg på?
7. Hvilken betydning får det for revisjonen dersom IT funksjonen er outsourcet?
8. Hvilken betydning får det for revisjonen dersom bedriften bruker nettskytjenester?
9. Hva brukes ellers IT revisorer til?
10. Hvor stort oppdrag og hvor komplekst må det være før du involverer en IT revisor?
11. Hvordan legger dere til rette for kommunikasjon og samhandling mellom funn fra IT revisor til finansiell revisor?
12. Har du noen andre kommentarer til planleggingsfasen?

I gjennomføringsfasen:

1. Hvilke generelle IT kontroller kartlegger du?
2. Hvordan tester du generelle IT kontroller?
3. Hvordan identifiserer du applikasjonskontroller?
4. Hvordan går du frem for å teste applikasjonskontroller?
5. Hvordan verifiserer du integritet i rapporter som brukes?
6. Hvilke tilfeller anser du det som mest hensiktsmessig å gjøre manuelle gjennomganger?

7. Vil du som revisor påpeke overfor de som har overordnet ansvar for styring og kontroll om sikkerheten i IT systemet er mangelfullt?
8. Dersom test av kontroller viser at IT systemene ikke overholder prinsippene om integritet, konfidensialitet og tilgjengelighet, hvilke konsekvenser får det videre for revisjonen?
9. Hvilken betydning har det for den øvrige revisjonen at IT revisor avdekker svakheter?
10. Har du noen andre kommentarer til gjennomføringsfasen?

I avslutningsfasen:

1. Har det betydning for revisjonsberetningen om hele eller deler relevante informasjonssystemer ikke fungerer tilfredsstillende?
2. Hvordan avgjør du om det foreligger vesentlig svakhet i enhetens interne kontroll, herunder informasjonssystemer som er relevant for finansiell rapportering og hvordan kommuniserer du disse?
3. Hvordan avgjør du om det kun foreligger mindre alvorlige svakheter i internkontrollen, herunder informasjonssystemer som er relevant for finansiell rapportering og hvordan kommuniserer du disse?
4. Har du noen andre kommentarer til avslutningsfasen?

Andre spørsmål:

1. Hvilke utfordringer mener du revisjonsbransjer står ovenfor i forbindelse med teknologi?
2. Har du kjennskap til COBIT-rammeverket
3. Er det tilstrekkelig kursing i IT

Vedlegg 2. Refleksjonsnotat av Milica Corovic

Dette refleksjonsnotatet er skrevet i forbindelse med min avsluttende masterstudie innen Regnskap og Revisjon – Siviløkonomi ved Universitetet i Agder 2017. Målet med dette refleksjonsnotatet er å reflektere over den kunnskapen og erfaringen jeg har opparbeidet meg gjennom mitt masterstudie. I notatet vil jeg presentere oppgaven og diskutere avhandlingens funn opp mot tre temaer universitet anser som en viktig del av utdannelsen av revisorer. Disse temaene er internasjonalisering, innovasjon og samfunnsansvar.

Jeg og min partner Ida har skrevet en masteroppgave innenfor fagfeltet revisjon, herunder IT-revisjon. Revisjon har vært et emne på bachelorstudiet og siste semester av masterstudiet ved Universitetet i Agder. Det er gjennom disse forelesningene vi har fått interesse for bruk av IT- og informasjonssystemer for finansiell rapportering og da revisors forståelse og håndtering av risiko relatert til dette. IT-revisjon er lite omdiskutert tema ved studiet, men likevel særdeles viktig og spennende område. De aller fleste bransjer i næringslivet tar i bruk komplekse IT-systemer og er dermed avhengige av en velfungerende intern kontroll for å redusere risikoen for vesentlig feilinformasjon. Behovet for en revisors kompetanse og forståelse av IT-systemer som anvendes for regnskapsavleggelse bør antas å være en viktig forutsetning for at revisor kan være sikker i sin uttalelse om den interne kontrollen og legge til rette for en effektiv revisjonstilnærming preget av kvalitet. Det er nettopp av den grunn jeg og min partner har funnet dette temaet som svært interessant og spennende.

Sammendrag

Vi ønsket å undersøke hva revisorer gjør for å forstå og håndtere risikoen relatert til IT-og informasjonssystemer og dermed undersøke indirekte nivået av kompetanse og erfaring av dette område blant revisorer. Et av formålene med oppgaven var å se om revisorer anser det som en utfordring å revidere kundenes intern kontroll med tanke på IT- og informasjonssystemer. For å gjennomføre undersøkelsen benyttet vi oss av åpent intervju som datainnsamlingsmetode. Den kvalitative metoden ble valgt som undersøkelsesmetode først og fremst da vi har lite forhåndskunnskap om IT-revisjon fra vår utdanning, samt som det ikke er det mest omdiskuterte temaet i lærebøkene om revisjon. Ved å gjennomføre intervjuer fikk vi mulighet til å få et helhetlig bilde av fenomenet vi studerte, samt identifisere eventuelle nyanser som fremkom av systematiseringen og analysen av den innsamlede dataen. Vi gjennomførte intervjuer av fem revisorer fra de fem store selskapene i Norge, samt en revisor fra et lite selskap. Spørsmålene i intervjuet var bygd opp etter temaene forståelse og

håndtering av IT-og informasjonssystemer og inneholdt blant annet spørsmål om revisors vektlegging av beskrevne rutiner og prosedyrer for enhetens håndtering av IT-systemer, identifisering av systemer som er relevant for revisjonen og test av generelle IT-kontroller og applikasjonskontroller. Som en avslutning stilte vi spørsmål om hvilke konsekvenser ikke-fungerende IT- og informasjonssystemer kan medføre for beretningen og hvordan og til hvem eventuelle svakheter rapporteres til. På bakgrunn av vår analyse og tolkninger konkluderte vi med at revisors forståelse og håndtering av IT- og informasjonssystemer for finansiell rapportering er svært varierende, og at årsaken til dette kan være mange, men at det som regel vil være som følge av egen revisjonsmetodikk, tilgang og fokus på kursing i IT, kompleksitet av kundenes systemer, kompetanse, interesse og erfaring.

Internasjonalisering

IT- og informasjonssystemer utgjør en del av virksomhetens internkontroll og dermed er en velfungerende intern kontroll en viktig forutsetning for at virksomheten skal sikre en målrettet og effektiv drift samt sikre påliteligheten av regnskapsinformasjonen som fremkommer av systemene som anvendes. For å redusere risikoen og opprettholde sikkerhet i regnskapsinformasjonen er det nødvendig at revisor er sikker i sin uttalelse om IT- og informasjonssystemer og gjennomfører nødvendige vurderinger og handlinger for å redusere risikoen for feilinformasjon. I dag skal revideringen av revisjonspliktiges årsregnskap foretas i samsvar med bestemmelensen i Revisorloven samt de internasjonale standardene for kvaliteskontroll (ISA) utarbeidet av IAASB. Flere revisorer støtter seg også på revisorforeningen. Revisorforeningen er en interesse- og kompetanseorganisasjon for godkjente revisorer i Norge og deltar blant annet aktivt i IFAC (The international Federation of Accountants) og Accountancy Europe som representerer den europeiske regnskap- og revisorprofesjonen i forhold til EU-systemet. Ved at all utdanning og etterutdanning for revisorer bygger på lovene og standardene utarbeidet av de overnevnte organene, vil det være helt avgjørende at de utvikler seg i takt med teknologien og legger opp til en god og kvalitetsmessig revisjon av intern kontroll, herunder virksomhetenes IT- og informasjonssystemer. Konsekvensen av dårlig internkontroll kan medføre store utfordringer for brukerne av regnskapet samt økonomiske utfordringer for virksomheten både regionalt, men også internasjonalt dersom det foreligger samarbeid blant virksomheter.

En redusert tillitt til regnskapsinformasjon fremkommer som regel av dårlig intern kontroll eller svekket moral blant ansatte i virksomheten. Gjennom de senere årene har dette påvirket flere virksomheters økonomi negativt og blant annet medført finansskandaler. Enron og Arthur Andersen-skandalen og WorldCom-skandalen , samt krisene i de norske selskapene Finance Credit og Sponsorservice, er gode eksempler på skandaler som oppstod som konsekvens av redusert tillit til kvaliteten av regnskapet. Uten å gå nærmere inn på alle mekanismer som kan ha vært med på å utløse disse skandalene, kan det likevel argumenteres for at mangel på intern kontroll og brukerens tillit til selskapenes styring, kontroll og rapportering har spilt en vesentlig rolle.

Innovasjon

Innovasjon handler i stor grad om fornyelse eller nyskapning, eller annerledes tankegang i håp om å skape verdi for en innbygger, virksomheten eller samfunnet. Som tidligere nevnt handlet vår oppgave om revisor sin forståelse og håndtering av IT- og informasjonssystemer, hvorvidt vi konkluderte med at det er varierende blant revisorene og hvorav deres håndtering er preget av blant annet profesjonelt skjønn, kompetanse og erfaring på området. Det er av den grunn hensiktsmessig å foreslå økt fokus på akkurat dette med IT-revisjon og hvordan dette tilegnes praktisk. Dette gjelder både i utdanningen av fremtidige revisorer, men bør også være en viktig del av etterutdanning for eksisterende revisorer. Den enorme digitaliseringen medfører endringer av revisjonsbransjen, hvorav mer kunnskap innen IT revisjon vil kunne bidra til en effektiv revisjon. En revisor vil kunne skape merverdi i form av for eksempel konkurransefortrinn for virksomheter dersom de er godt kjent med IT-og informasjonssystemer og hvordan det påvirker risikoen for feilinformasjon. Ved senere undersøkelser kan det for eksempel være relevant å bruke case-studiet der problemstillingen er knyttet til komplekse IT-systemer. Ved undersøkelsen kan en prøve å se på hvilke eventuelle nyanser som vil være mulig å identifisere som følge av forståelse og håndtering av IT- og informasjonssentret blant finansielle revisor med begrenset kunnskap om IT-revisjon kontra en IT-revisor som har en eller annen form for sertifisering innen IT- og informasjonssystemer. På den måten vil det kanskje være mulig å trekke noen konklusjoner basert på om revisorenes kunnskap på området har en betydning for problemstillingen og videre konkludere på om det foreligger behov for mer IT-revisjon i utdanning og senere kursing.

4.

Samfunnsansvar

Som en avslutning for dette refleksjonsnotat skal jeg vurdere vår masteroppgave opp mot samfunnsansvar. Samfunnsansvar handler om å ta sosial og miljømessig ansvar utfor det som er pålagt av lover og regler. Revisors forståelse og håndtering av risiko relatert til finansiell rapportering er veldig individuelt og kan bestå av varierende handlinger og holdninger blant revisorene. Som regel vil revisorens revisjonstilnærming være et resultat av revisjonsmetodikken i virksomheten han eller hun er ansatt i. Revisjonsmetodikken vil i de fleste tilfeller bygge på de internasjonale revisjonsstandardene (ISA) som vil danne grunnlag for at revisor overholder de lover og regler som de er underlagt. For min egen del vil det være vanskelig å reflektere og diskutere om revisorens forståelse og håndtering av IT-systemer ivaretar samfunnsansvar på en god måte uten undersøke deres revisjonsmetodikk og de retningslinjer som revisorene er underlagt nærmere. Revisjon bygger i stor grad på profesjonelt skjønn, men det er allikevel viktig å understreke at revisorer er allmenhetens tillitsperson og at beretningene som avgis er et resultat av revisorloven og de internasjonale revisjonsstandardene, blant annet DNRS om etikk, som de er underlagt. Det bør igjen allikevel diskuteres om det vil være nødvendig å øke fokuset av IT-revisjon i utdanningen og om det vil være nødvendig for eksisterende revisorer å delta på flere kurs relatert til IT. Blant annet kan man øke fokuset på for eksempel COBIT-rammeverket og ISO 27 001 og ISO 27 002 standardene som nettopp behandler dette med IT-styring og ledelsessystemer for informasjonssikkerhet. Det er mulig å anta at bedre kompetanse på området vil styrke samfunnsansvaret blant revisorene, men også føre til nyttig risikoreduksjon og konkurransefortrinn på lengre sikt. Likevel bør det kunne anerkjennes at revisorloven og ISAene ivaretar samfunnsansvaret på en god nok måte og at brukeren av regnskapet av den grunn kan ta beslutninger på bakgrunn av nøyaktig grunnlag.

Vedlegg 3. Refleksjonsnotat av Ida Kristine Ottosen

I dette refleksjonsnotatet skal jeg ta for meg hvordan vår masteroppgave kan relateres til begrepene internasjonalisering, innovasjon og samfunnsansvar ved å trekke inn relevant kunnskap og erfaring som jeg har fått gjennom masterstudiet regnskap og revisjon ved UiA.

IT-revisjon er en del av faget Revisjon 2 på MRR studiet, men er tillagt lite vekt i norsk akademisk litteratur om revisjon. Jeg og min medstudent Milica synes at IT-revisjon er et spennende tema som vi tror vil ta større del av revisjonslandskapet i fremtiden. Det var da vi undersøkte nærmere om IT-revisjon at vi fant ut at dette er et tema som flere revisorer synes et utfordrende å forholde seg til, og ble dermed opphavet til oppgaven vår og problemstillingen "Hva gjør revisor for å forstå og håndtere risiko knyttet til IT- og informasjonssystemer relevant for finansiell rapportering?".

Med bakgrunn i antagelser om at denne revisjonstilnærmingen benyttes i begrenset omfang og at revisorene reviderer rundt IT- og informasjonssystemene i kunden i stedet for i dem, har vi funnet ut at denne antagelsen stemmer til en viss grad. Det vi si at i vår masteroppgave har vi analysert svarene fra informantene og på grunnlag av det kan se at det fremdeles er en vei å gå i forbindelse med å forstå og håndtere risiko knyttet til IT- og informasjonssystemer for finansiell rapportering. Selv om de store revisjonsselskapene har begynt å benytte seg av IT-revisjon på enkelte oppdrag, kan det virke som at det er interessen for IT-revisjon og revisors ønskede kompetanse på området som avgjør om IT-revisjon anvendes som revisjonstilnærming. Det er også et tydelig skille i oppgaven vår mellom de store revisjonsselskapene og det mindre revisjonsselskapet. For det mindre revisjonsselskapet var problemstillingen vår svært utfordrende.

Internasjonalisering

Oppgaven vår kan relateres til internasjonalisering ved at det er internasjonale aktører, som COSO, ISACA og PCAOB som er blant de ledende standardsetterne, også for revisjonsselskapene i Norge. Flere av disse er vi allerede kjent med gjennom flere fag vi har hatt på masteren, blant annet finansregnskapsfagene og revisjonsfagene. Aktørene samarbeider også på tvers av landegrenser og PCAOB fører også tilsyn med revisjonsselskapene sammen med Finanstilsynet. Revisjonsselskapene er også globale aktører med kontorer over hele verden, og dermed er også selskapene vi har tatt informanter fra knyttet til et internasjonalt nettverk. Norsk lovgivning begynner å rette seg mer inn mot internasjonal lovgivning. Et eksempel på dette som vi tar opp i oppgaven er The Serbanes-

Oxley Act og internkontrollforskriften, og ikke minst er ISAene som ligger til grunn i Revisors Håndbok et resultat av internasjonal lovgivning. I tillegg kan vi påpeke at det i stor grad er benyttet engelsk akademisk litteratur i denne masteroppgaven.

Innovasjon

Det kommer tydelig frem i det siste spørsmålet vi stiller informantene at det er ventet store utfordringer i fremtiden knyttet til konkurransesituasjonen og revisjonsmetodikken som følge av teknologisk utvikling. Problemstillingen kan knyttes til innovasjon ved at den tar for seg hvordan revisjonsselskapene benytter seg av den nye teknologien som allerede eksisterer, men også hvilke holdninger de har til den som kommer i fremtiden. Ved å rette oppmerksomhet mot hvordan revisorene håndterer nye innovative løsninger, som for eksempel bruk av nettskytjenester er dette et eksempel på hvordan innovasjon også påvirker revisjonsbransjen. Innovasjon er et tema som ble introdusert for oss gjennom strategifaget på masterprogrammet.

Samfunnsansvar

Når det kommer til samfunnsansvar, vil jeg påpeke at gjennom revisjonsfaget har vi fått inngående kunnskap om revisors etiske og moralske problemstillinger. Dette mener jeg er viktig å ta med seg videre i arbeidslivet. Samtlige av informantene mener at IT-revisjon er en revisjonstilnærming som kommer til å vokse i fremtiden, og behovet for kompetanse på dette området vil bli større. Jeg mener vi er med på å skape et ansvar overfor utdanningsinstitusjonene og andre aktuelle aktører, ved å belyse at det fremdeles er behov for økt kompetanse, ikke bare for nyutdannede som oss, men også blant de som har lang arbeidserfaring.