NORGES HANDELSHØYSKOLE
Bergen, våren 2006

Utredning i fordypningsområdet: Regnskap og Økonomisk Styring
Veileder: Professor Aasmund Eilifsen

Revisjon av intern kontroll, jamfør Sarbanes-Oxley Act of 2002 Section 404

Av

Svein Birger Werring

Forord

Denne utredningen er utarbeidet som en del av 3. avdeling på siviløkonomstudiet ved Norges Handelshøyskole. Formålet med utredningen er å gi en oversikt over hva bestemmelsene om intern kontroll over økonomisk rapportering, jamfør Sarbanes-Oxley Act §404, innebærer. Utredningen tar utgangspunkt i tre sider ved intern kontroll - intern kontroll generelt; intern kontroll som en del av revisors risikovurderingsprosess i revidering av regnskaper; og revidering av intern kontroll over økonomisk rapportering.

Bakgrunnen for valgt av emne ligger i at jeg leste om Enron. Jeg undersøkte hvilke konsekvenser Enron hadde fått, og fikk da kjennskap til Sarbanes-Oxley Act of 2002. Et av de mest sentrale aspektene ved denne loven er bestemmelsene om at alle virksomheter notert på amerikanske børser skal ha intern kontroll over økonomisk rapportering – som ledelsen skal vurdere effektiviteten av – og som revisor skal attestere. Da jeg dessuten skal begynne å jobbe i revisjon høsten 2006 synes jeg det er viktig å ha kunnskap om intern kontroll.

Temaet jeg har valgt er omfattende, og det har vært vanskelig å selektere hva som bør, og ikke bør inngå i utredningen. Bare den amerikanske standarden som nyttes av revisjonsselskaper for revidering av en virksomhets intern kontroll (Auditing Standard 2) er på 161 sider. Derfor er det helt sikkert mye mer som kunne vært inkludert. Likevel føler jeg at utredningen gir en oversikt over hva intern kontroll er, hva som ligger til grunn for revisors forståelse av en virksomhets intern kontroll, og hvordan revisor går frem for å attestere en intern kontrolls effektivitet.

Jeg vil rette en stor takk til veileder, professor Aasmund Eilifsen, for gode kommentarer, rettledning og hjelp underveis.

Bergen, juni 2006

Svein Birger Werring

Sammendrag

Formålet med utredningen er å gi en oversikt over hva bestemmelsene om Intern Kontroll over Økonomisk Rapportering, jamfør Sarbanes-Oxley Act §404, innebærer. For å oppnå dette vil utredningen deles inn i tre hoveddeler.

Intern Kontroll
Denne delen av utredningen vil fokusere på Intern kontroll som begrep. Intern Kontroll vil bli definert, og rammeverktøyet COSO vil bli presentert.

Intern Kontrolls Betydning for Revisjonsoppdraget
Denne delen av utredningen vil fokusere på Intern kontroll i forhold til revisjon av en virksomhets regnskaper. Revisor bør i forbindelse med et revisjonsoppdrag skaffe seg en forståelse av et selskaps interne kontroller, for å vurdere hvilke ytterligere revisjonshandlinger revisor skal foreta.

Intern Kontroll Over Økonomisk Rapportering etter Sarbanes-Oxley.
Denne delen av utredningen vil deles opp i to kapitler.

Først (kapittel fire) vil jeg gi et innblikk i bakgrunnen for Sarbanes-Oxley Act of 2002, gjennom å benytte Enron som eksempel - Deretter vil jeg gi en generell presentasjon av SOX.

Deretter (kapittel fem) vil jeg fokusere på Intern kontroll over økonomisk rapportering etter Sarbanes-Oxley Act (Paragraf 404). Mens intern kontroll presenteres teorietisk i del 1, gjennom rammeverket COSO – og revisors vurdering av intern kontroll i forhold til revisjon av et selskaps regnskaper presenteres i del 2 – vil revisjon av internkontroll (eller attestasjon av internkontroll) bli presentert her. Kapittelet bygger videre på det som allerede har blitt presentert i del 2 og 3, og vil behandle tester av interne kontroller og ledelsens vurdering – som ligger til grunn for revisors attestering av internkontrollens effektivitet. Siden loven er amerikansk vil amerikansk revisjonslitteratur benyttes som utgangspunkt.

Forord **2**

Sammendrag **3**

1 Innledning **6**

1.1 BAKGRUNN 6
1.2 PROBLEMSTILLING 7

2 Intern Kontroll **8**

2.1 COSOS DEFINISJON AV INTERN KONTROLL 9
2.2 COSOS RAMMEVERK 10
2.2.1 Kontrollmiljø *11*
2.2.1.1 Integritet og Etiske Verdier 12
2.2.1.2 Styret og Revisjonskomiteen 13
2.2.1.3 Kompetanse 14
2.2.1.4 Ledelsesfilosofi og Driftsform 14
2.2.1.5 Organisasjonsstruktur og Fordeling av Ansvar og Myndighet. 15
2.2.1.6 Personalpolitikk 15
2.2.2 Risikovurdering *16*
2.2.2.1 Målsettinger 17
2.2.2.2 Identifisering av Risiko 19
2.2.2.3 Vurdering av Risiko 20
2.2.2.4 Håndtering av Risiko 21
2.2.2.5 Håndtering av Endringer 21
2.2.3 Kontrollaktiviteter *21*
2.2.3.1 Informasjonsbehandling 23
2.2.3.2 Fysisk Kontroll 23
2.2.3.3 Ansvarsfordeling 23
2.2.4 Informasjon og Kommunikasjon *24*
2.2.5 Overvåking *26*

3 Intern Kontrolls Betydning for Revisjon **28**

3.1 FORSTÅELSE AV VIRKSOMHETENS INTERNE KONTROLL 28
3.1.1 Begrensninger i Intern Kontroll *29*
3.1.2 Vesentlighet og Vesentlige Regnskapsposter *31*
3.1.3 Betydelige Selskaper og Forretningsområder *32*
3.1.4 Analyse av Transaksjonsstrømmer og Vesentlige Prosesser *35*
3.1.5 Risiko og Sannsynlighet *36*

4 Sarbanes-Oxley Act of 2002 ..... **39**

4.1 ENRON – DEN AMERIKANSKE DRØMMEN 39
4.1.1 Enron – Skandalene *40*
4.1.2 Markedsverdiprinsippet *40*
4.1.3 Tvilsomme Føringer *41*
4.1.4 Skjule Virkeligheten *41*
4.1.5 Rettslig Etterspill *41*
4.1.6 Arthur Andersen *42*

4.1.7 "Economic Failure" *42*
4.1.8 Svar på Skandalene – Sarbanes Oxley *42*
4.2 HVA ER SARBANES-OXLEY ACT OF 2002 ? 43
4.2.1 Revisjon *43*
4.2.2 Ledelse *44*
4.2.3 Økonomisk Rapportering. *45*
4.2.4 Øvrige Bestemmelser *46*
5 Revisjon av Interne Kontroller over Økonomisk Rapportering. **47**
5.1 MANGLER I INTERNKONTROLL 48
5.1.1 Betydelig Mangel *49*
5.1.2 Vesentlig Svakhet *49*
5.2 PLANLEGGING 49
5.3 EVALUERE LEDELSENS VURDERINGSPROSESS 50
5.3.1 Tester av Kontroller *51*
5.3.3 Ledelsens Rapport *55*
5.3.3.1 Ledelsens Ansvar 55
5.3.3.2 Bruk av Rammeverktøy 56
5.3.3.2 Ledelsens Erklæring Vedrørende Internkontroll Over Økonomisk Rapportering 56
5.3.3.3 Erklæring på Revisors Kjennskap til Ledelsens Vurdering 57
5.4 EVALUERING AV INTERNE KONTROLLERS UTFORMINGSEFFEKTIVITET 57
5.5 TESTING OG EVALUERING AV INTERNE KONTROLLERS IVERKSETTINGSEFFEKTIVITET 58
5.5.1 Valg av Kontroller for Testing *58*
5.5.2 Valg av Metode for Testing *60*
5.5.3 Valg av Tidspunkt for Test av Kontroller *60*
5.5.4 Omfanget av Test av Kontroller *61*
5.5.4.1 Bruk av Statistiske Metoder 62
5.5.4.2 Bruk av Andres Arbeid. 64
5.6 REVISORS VURDERING 65
5.6.1 Revisors Rapport *66*
5.6.1.1 Begrensninger i Revisors Arbeid 66
5.6.1.2 Vesentlig Svakhet 66
5.6.1.3 Revisors Konklusjon. 68
6 Avslutning **69**
Kilder **71**
Vedlegg **75**

1 Innledning

1.1 Bakgrunn

De første årene i det nye millenniet vil av flere bli husket for de mange finansskandalene som ble rullet opp rundt om i verden. Skandaler rundt selskaper som *Enron*, *WorldCom*, *Adelphia, Tyco* og *Global Crossing* rystet USA, mens Europa fikk sitt å henge fingrene i med *Royal Ahold*, *Vivendi International* og *Parmalat*. Norge var heller ikke fritt for problemer, med *Finance Credit* og *Sponsorservice.* Felles for selskapene var at det var gjort noen tvilsomme føringer, ja i flere tilfeller kunne en del føringer være direkte i strid med god regnskapsskikk.

John Thain, CEO I New York Stock Exchange, var en av mange som hevdet at den viktigste oppgaven det amerikanske aksjemarkedets hadde, var å gjenvinne investorers tillit. ”Restoring investor confidence is the most important issue today for US equity markets” (Thain, 2004). I et forsøk på å gjenvinne denne tillitten, ble **Sarbanes-Oxley Act of 2002** (heretter også kalt SOX) undertegnet av president George W. Bush i Juli 2002.

Det blir sagt at Sarbanes-Oxley Act er den mest omfattende regnskaps- og selskaps-lovgivningen i USA, siden innføringen av Securities Act og Securities Exchange Act i begynnelsen av 1930-årene. Dette fordi Sarbanes-Oxley Act innebærer skjerpede bestemmelser innenfor områdene **Revisjon, Corporate Governance**, og **Økonomisk Rapportering** for selskaper registrert hos SEC (U.S. Securities and Exchange Commission). Spesielt har **Paragraf 404** blitt viet mye oppmerksomhet, i det den stiller krav til ledelsen om implementering, og påfølgende evaluering av effektiviteten av **Intern Kontroll over Økonomisk Rapportering**, samt krav til revisors attestering av ledelsens evaluering. Kravene har vist seg å medføre betydelig arbeid og betydelige kostnader for berørte selskaper.

Bestemmelsene om intern kontroll over økonomisk rapportering vedrører også en rekke ikke-amerikanske selskaper. Norske selskaper som Norsk Hydro, Smedvig, Statoil og Telenor er alle registrert på børs i USA, og er derfor pålagt å følge bestemmelsene. I tillegg vil kravene få virkning for norske datterselskap av selskaper notert på amerikanske børser.

Det har vært diskutert hvorvidt lignende bestemmelser bør innføres i EU og Norge. FEE (The European Federation of Accountants) har imidlertid argumentert for å vente å se hvordan

implementeringen fungerer i USA. Min subjektive oppfatning er at Europa antakeligvis ikke tåler flere skandaler av typen Parmalat og Royal Ahold, og dersom en eller flere lignende saker rulles opp, vil det bli fortgang i prosessene også i Europa.

Intern Kontroll over Økonomisk Rapportering jamfør SOX er dermed et høyst aktuelt tema også her hjemme, da utvikling og regulering i USA vil påvirke en rekke norske virksomheter både direkte og indirekte, på samme måte som at amerikansk praksis og regulering historisk sett har hatt stor påvirkning for utviklingen i Europa (Christiansen, 2003). Enkelte norske selskaper er som nevnt allerede berørt av bestemmelsene, det gjelder både norske konsern og datterselskaper av utenlandske konsern. I tillegg forbereder revisjonsselskapene mulige krav om lignende bestemmelser her hjemme.

1.2 Problemstilling

Jeg vil, med utgangspunkt i revisjonslitteratur, se på hva intern kontroll innebærer, både som eget begrep, og i forhold til revisjon av regnskaper. Dette vil jeg benytte for å se på hvilke forhold og hvilke prosesser som leder fram til ledelsens og revisors evaluering av effektiviteten av intern kontroll over økonomisk rapportering, etter Sarbanes-Oxley Act §404.

2 Intern Kontroll

Intern kontroll er den prosessen som er utformet og som gjennomføres av dem som har overordnet ansvar for styring og kontroll og av andre medarbeidere, for å gi rimelig sikkerhet for at foretaket når sine mål med hensyn til pålitelig økonomisk rapportering, effektiv drift, og for at gjeldende lover og forskrifter blir overholdt. Derav følger at intern kontroll blir utformet og implementert for å håndtere identifiserte forretningsrisikoer som truer oppfyllelsen av disse målsettingene.

- (RS315, §42)

Når begrepet ”Intern Kontroll” diskuteres er det vanskelig å komme utenom Committee of Sponsoring Organizations of the Treadway Commision (COSO) og dens rapport ”Intern Kontroll – Et Integrert Rammeverk”. COSO-rapporten, publisert i 1992, bygger på et samarbeidsprosjekt mellom amerikanske regnskaps- revisjons- og ledelsesorganisasjoner. På bakgrunn av teoretiske studier og praktisk erfaring fra sentrale ledere skulle en hjelpe bedrifter med å finne et felles grunnlag for evaluering og forbedring av systemer for intern kontroll. Dette skulle oppnås gjennom å etablere en felles definisjon av begrepet, samt gjennom å angi en standard for hvordan virksomheter kan vurdere sine interne kontrollsystemer og foreta forbedringer (COSO, 1992 / COSO, 2005). Resultatene har etter hvert blitt godt innarbeidet i revisjonsbransjen. Både Securities Exchange Commission, Public Company Accounting Oversight Board, og The European Federation of Accountants, så vel som Den Norske Revisorforening bygger på COSOs arbeid når intern kontroll defineres og beskrives.

2.1 COSOs Definisjon av Intern Kontroll

Intern kontroll defineres som en prosess som er iscenesatt og gjennomført av de ansatte i en virksomhet, og utformet for å nå fastsatte målsetninger.
- (COSO, 1992)

Gitte definisjon inneholder tre viktige momenter. Intern kontroll en **Prosess**, Intern kontroll er **Iscenesatt og Gjennomført av de Ansatte**, og til sist: Intern kontroll bygger på **Fastsatte Målsettinger**.

Prosess

Intern kontroll er beskrevet som en *Prosess*. Intern kontroll bør dermed forstås som en **serie med handlinger**, snarere enn én enkelt operasjon. Videre forstår en med en *prosess* at handlingene foregår over tid.

Iscenesatt og Gjennomført av de Ansatte

Generelt vil en med intern kontroll forstå at det dreier seg om noe som skal foregå innad i en bedrift. Innad i bedriften inkluderer alle ansatte; det være seg ledelsen, styret, internrevisor, ansatte i økonomiavdeling, ansatte i produksjonsavdeling, etc. Derimot er ikke eksterne interessenter slik som selskapets eiere, politikere, eller ekstern revisor ansvarlig for selskapets interne kontroll. Til syvende og sist vil det være ledelsen i selskapet som har ansvaret for at Intern Kontroll er iscenesatt og gjennomført.

Fastsatte Målsettinger

Med fastsatte målsettinger forstår en at det er essensielt med forhåndsetablerte målsetting for at intern kontroll i det hele tatt skal ha noen mening. Disse målsettingene kan deles inn i tre områder:

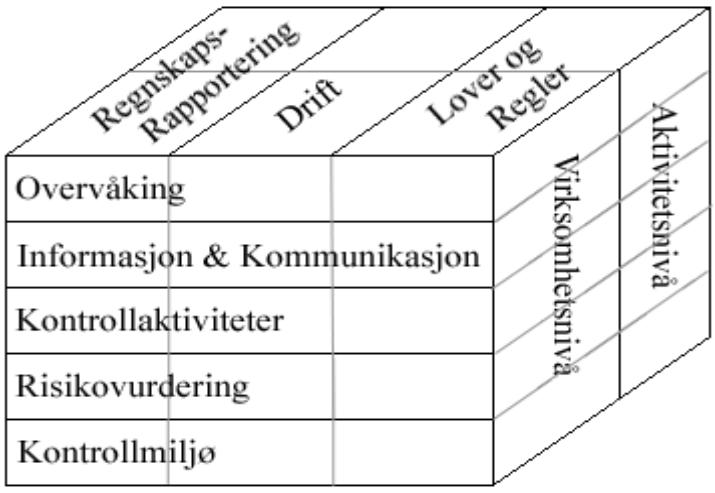
- ***Pålitelig Ekstern Regnskapsrapportering***
- ***Målrettet og Kostnadseffektiv Drift***
- ***Overholdelse av Gjeldende Lover og Regler***

Første kategori omfatter utarbeidelsen av pålitelige offentlige regnskaper, som årsrapporter og kvartalsrapporter. Intern kontroll vedrørende ekstern regnskapsrapportering kan sies å være

effektiv når ledelsen og styret med rimelig sikkerhet kan si at regnskapsrapporteringen er pålitelig. Andre kategori inneholder et foretaks grunnleggende forretningsmessige mål, og er effektiv når en kan se at virksomhetens operative mål nås. Siste kategori dreier seg om å overholde de lover og regler som virksomheten er underlagt, og er effektiv når disse overholdes.

Oppsummert vil dette si at intern kontroll består av de tiltak og handlinger, autorisert av ledelsen, som gjennomføres for å drive påvirkning i retning av ønsket resultat.

2.2 COSOs Rammeverk



Figur 2.1

Figuren viser en oversikt over rammeverket COSO, og dets tredimensjonelle beskrivelse av internkontroll.

En bedrift bør implementere intern kontroll for alle tre målsettingskategoriene **Regnskapsrapportering**, **Drift**, og **Lover og Regler**. I forhold til revisjon vil nok intern kontroll vedrørende regnskapsrapportering være mest relevant. I tillegg stiller SOX kun krav til intern kontroll ved finansiell rapportering. Intern kontroll vedrørende effektiv drift, samt overholdelse av lover og regler vil derfor ikke bli behandlet i denne utredningen.

Rammeverktøyet består av de fem komponentene **Kontrollmiljø**, **Risikovurdering**, **Kontrollaktiviteter**, **Informasjon og Kommunikasjon**, og **Overvåking**. Komponentene går også igjen i RS315 (§43). Figuren illustrerer at alle fem komponentene er relevante for alle målsettinger. COSO lister opp en rekke **Faktorer** for hver av de fem kontrollkomponentene, faktorer som ledelsen bør ta ugangspunkt i ved utarbeidelsen av kontrollsystemet. Imidlertid

vil ikke alle faktorer som er nevnt i COSO-rammeverket være av betydning for pålitelig regnskapsrapportering. Betydningen av de ulike faktorene vil for øvrig variere med bransje og virksomhetens størrelse.

Siste dimensjon forteller at intern kontroll må implementeres på virksomhetens overordnede nivå, og for de ulike enkeltaktivitetene. COSO legger dermed opp til at kontrollkomponentene skal vurderes både på **Virksomhetsnivå** og på **Aktivitetsnivå**. Enkelte komponenter (som for eksempel kontrollmiljøet) vil virke mest inn på virksomhetsnivå, mens andre (for eksempel kontrollaktiviteter) vil ha mer innflytelse på aktivitetsnivå. Ramos (2004) forklarer betydningen av virksomhetsnivå og aktivitetsnivå gjennom å benytte en skole som eksempel. For at en elev skal kunne skryte av læringsmiljøet; det være seg gode skolebøker eller dyktige lærere (som her kan sammenlignes med aktivitetsnivå), må enkelte grunnleggende forutsetninger, slik som penger, være til stede. Det at skattebetalerne betaler skatt gjør at skolen har råd til å kjøpe de gode bøkene, og ansette de dyktige lærerne. I en noe overført betydning kan en si at sammenhengen er tilsvarende for kontroller på virksomhets- og aktivitetsnivå. For et effektivt kontrollsystem på aktivitetsnivå, må det eksistere et effektivt kontrollsystem på virksomhetsnivå.

2.2.1 Kontrollmiljø

Kontrollmiljøet setter tonen i en organisasjon (COSO, 1992). Dets betydning for et effektivt kontrollsystem, kan sammenlignes med skjelettets betydning for kroppen. Skjelettet er kroppens byggeklosser; byggeklosser vi ikke kan se fra utsiden. Dog vil mangler (eller brudd) i skjelettet straks merkes ved at flere av kroppens funksjoner lammes. På samme måte vil ikke alltid kontrollmiljøet være synlig utenfor virksomheten, men mangler i kontrollmiljøet vil like fullt ha en negativ innvirning på effektiviteten av kontrollsystemet.

Kontrollmiljøet påvirkes av virksomhetens historie og kultur, og påvirker de ansattes holdninger, handlinger og kontrollbevissthet. Det påvirker også utformingen og funksjonaliteten til kontrollaktiviteter, informasjons- og kommunikasjonssystemer samt overvåkingsaktiviteter. Kontrollmiljøet består av ulike faktorer, som vil bli behandlet i det følgende

- ***Integritet og Etiske Verdier***
- ***Styret og Revisjonskomiteen***
- ***Kompetanse***
- ***Ledelsesfilosofi og Driftsform***
- ***Organisasjonsstruktur***
- ***Ansvars- og Myndighetsfordeling***
- ***Personalpolitikk***

2.2.1.1 Integritet og Etiske Verdier

Effektiviteten i virksomhetens interne kontrollsystemer kan aldri bli bedre enn integriteten og de etiske retningslinjene til de som lager, administrerer og overvåker dem. (COSO, 1992)

Det er flere hensyn som må tas når en skal etablere etiske verdier. Dette bidrar til å komplisere oppgaven. Bedriften, dens ansatte, eiere, leverandører, kunder, og samfunnet er alle eksempler på interesser en bør ta hensyn til, og partenes interesser vil ikke alltid stemme overens. Eksempelvis kan en nedleggelse av en ulønnsom fabrikk bidra til å sikre et selskaps videre eksistens. På den ene siden har man da et etisk ansvar ovenfor de ansatte, deres familie, og samfunnet på det stedet hvor fabrikken nedlegges, mens man på den andre siden har et ansvar ovenfor bedriftens øvrige ansatte, eiere, og andre samfunn hvor virksomheten har fabrikker.

Ledelsens integritet og etiske adferd vil være et produkt av virksomhetens bedriftskultur; som består av etiske og moralske standarder, måten de kommuniseres på og hvordan de forsterkes i praksis. Av sistnevnte fremgår det at ledelsens adferd også bidrar til å forme bedriftskulturen, avhengig av hvorvidt ledelsen går foran som et godt eller mindre godt eksempel.

Moralsk Veiledning.

Et selskap kan ha mange fine formuleringer hva ledelsens etiske verdier angår, men så lenge ledelsen selv ikke følger disse, dannes en ukultur i bedriften. Vissheten om at ledelsen har handlet ”etisk riktig” når de har vært konfrontert med etiske dilemmaer, vil fungere som et sterkt signal til de ansatte i bedriften, og dermed øke sannsynligheten for at de ansatte også

handler ”etisk riktig” når de konfronteres med ulike dilemmaer. I tillegg til å følge egne retningslinjer, bør også ledelsen være i stand til å kommunisere disse til selskapets ansatte.

Et eksempel fra virkeligheten, nært knyttet til undertegnede, var Andersen & Werring. Selskapets kjernevirksomhet var eksport av hermetisk krabbe. I 1960 var store deler av selskapets kapital bundet opp i varer som skulle eksporteres til England. Imidlertid gikk det engelske selskapet konkurs, og Andersen & Werring, som ikke maktet å finne kjøpere for varene, opplevde et akutt likviditetsproblem. Etter å ha betalt løpende fordringer, måtte eierne velge mellom å betale offentlige utgifte eller lønninger. Man valgte å betale lønninger, og selskapet ble dermed slått konkurs av staten, samtidig som staten også anmeldte eierne. Dersom de ansatte skulle gått uten lønning for arbeid, ville det for flere av de ansatte og deres familier fått katastrofale konsekvenser. Tilsvarende dilemmaer var utbredt i kystkommuner på midten av nittenhundretallet.

Incitamenter og Fristelser

En bedriftskultur hvor de ansatte stadig opplever press om å levere urealistiske resultater, vil kunne skape incitamenter til uetiske handlinger. Salgspersonell som føler seg presset av ledelsen, vil kunne benytte salgsteknikker der kundene settes under press eller holdes for narr. Kunder som opplever dette vil trolig ikke komme tilbake, og bedriften skades. Ansatte som føler et press for å oppnå urealistiske resultater vil også ha incitamenter til å ta del i svindel og tvilsom regnskapsføring for å oppnå forventede resultater. Dersom kontrollrutinene for å oppdage slik adferd oppleves som ineffektive, eller manglende, vil dette øke sannsynligheten for at slike handlinger finner sted. På den andre siden vil ledelsens håndtering når slike tilfeller avdekkes være med å skape bedriftskulturen. Måten slike handlinger straffes på sender et signal til bedriftens ansatte om hvorvidt denne typen adferd aksepteres eller ikke.

2.2.1.2 Styret og Revisjonskomiteen

På samme måte som at ledelsens adferd bidrar til å forme bedriftskulturen, vil styret og revisjonskomiteens adferd og holdninger påvirke ledelsen. Faktorer som vil virke inn inkluderer hvorvidt styret og revisjonskomiteen er uavhengig av ledelsen, medlemmenes erfaring og status, i hvilken grad styret og revisjonskomiteen er villige til å foreta granskninger, og måten de handler på i ulike situasjoner.

For å sikre at styret og revisjonskomiteen er villige til å foreta granskninger og de ”riktige” handlingene, vil det være avgjørende at styret har eksterne medlemmer. Et styre og en revisjonskomité som innehar tilstrekkelig med erfaring, status og ekspertise, og med riktig innstilling, vil kunne sørge for nødvendig kontroll og veiledning og vil derfor være essensiell for en effektiv intern kontroll.

2.2.1.3 Kompetanse

Kompetanse relaterer seg til hvilke kunnskaper og ferdigheter som kreves av de ansatte for å utføre ulike oppgaver. Det vil således være en avveining mellom kompetanse og kostnader. Eksempelvis blir det uhensiktsmessig for et lite gatekjøkken å ansette en egen statsautorisert revisor for å føre regnskap.

I forhold til interne kontroller er det viktig at ansatte som utfører kontroller og overvåker prosesser har nødvendig kompetanse til å identifisere feil, og til å foreta de rette handlinger når feil blir identifisert.

2.2.1.4 Ledelsesfilosofi og Driftsform

Ledelsens filosofi og driftsform påvirker måten virksomheten drives på, inkludert den typen forretningsrisiko som aksepteres (COSO, 1992). For eksempel vil ledelsen i bedrifter som har satset på høyrisikoprosjekter og lyktes med det, kunne ha et helt annet syn på kontrollmiljøet, enn tilfelle er for ledelsen i bedrifter som havnet i økonomisk uføre. Sistnevne virksomheter vil antakeligvis være mer forsiktige med å påta seg risiko, og vil antakeligvis også i større grad søke et effektivt kontrollmiljø.

Ledelsens holdninger vedrørende å påta seg og overvåke risiko, ledelsens holdninger og handlinger i forhold til finansiell rapportering, samt ledelsens fokus på å nå økonomiske mål er alle viktige sider ved ledelsesfilosofi, og vil ha stor innflytelse på kontrollmiljøet i en organisasjon. (Ramos, 2004)

2.2.1.5 Organisasjonsstruktur og Fordeling av Ansvar og Myndighet.

Organisasjonsstrukturen er utgangspunktet for styring av en virksomhets aktiviteter. Hvordan virksomhetens aktiviteter planlegges, utføres, kontrolleres og overvåkes har betydning for hvorvidt virksomhetens målsettinger nås. En tilfredsstillende organisasjonsstruktur identifiserer nøkkelaktiviteter, ofte omtalt som virksomhetens "verdikjede".[1]

De ulike transaksjonene i verdikjeden må kartlegges, og en ansvarsfordeling må være klar. Her bør det fremgå hvem som er autorisert for, og hvem som har ansvaret for utførelsen av ulike aktiviteter, hvordan transaksjoner skal registreres, i tillegg til at det bør foreligge klare prosedyrer for hvem man rapporterer til. Delegering av myndighet og ansvar viser hvorvidt virksomheten oppmuntrer arbeidstakere til å ta initiativ med hensyn til problemløsninger, og hvor grensene for denne myndigheten går. Eksempelvis bør en selger ha myndighet til å gi visse rabatter ved store ordre, dog må det selvfølgelig være visse rammer for hvor store rabatter som kan gis. Tilsvarende bør en innkjøpsansvarlig kunne velge leverandør for små enkeltkjøp, mens vedkommende i andre tilfeller kan være bundet av avtaler med faste leverandører.

En mangelfull organisasjonsstruktur kan medføre at ansatte ikke er klar over sine ansvarsområder, hvilket innebærer høy risiko for at feil ikke oppdages eller korrigeres i rimelig tid. Et effektivt kontrollmiljøet bør også bære preg av at aktørene er klar over at de stilles til ansvar for sine handlinger, dersom de for eksempel handler utover hva de har autorisasjon for, eller utover sine rammebetingelser.

2.2.1.6 Personalpolitikk

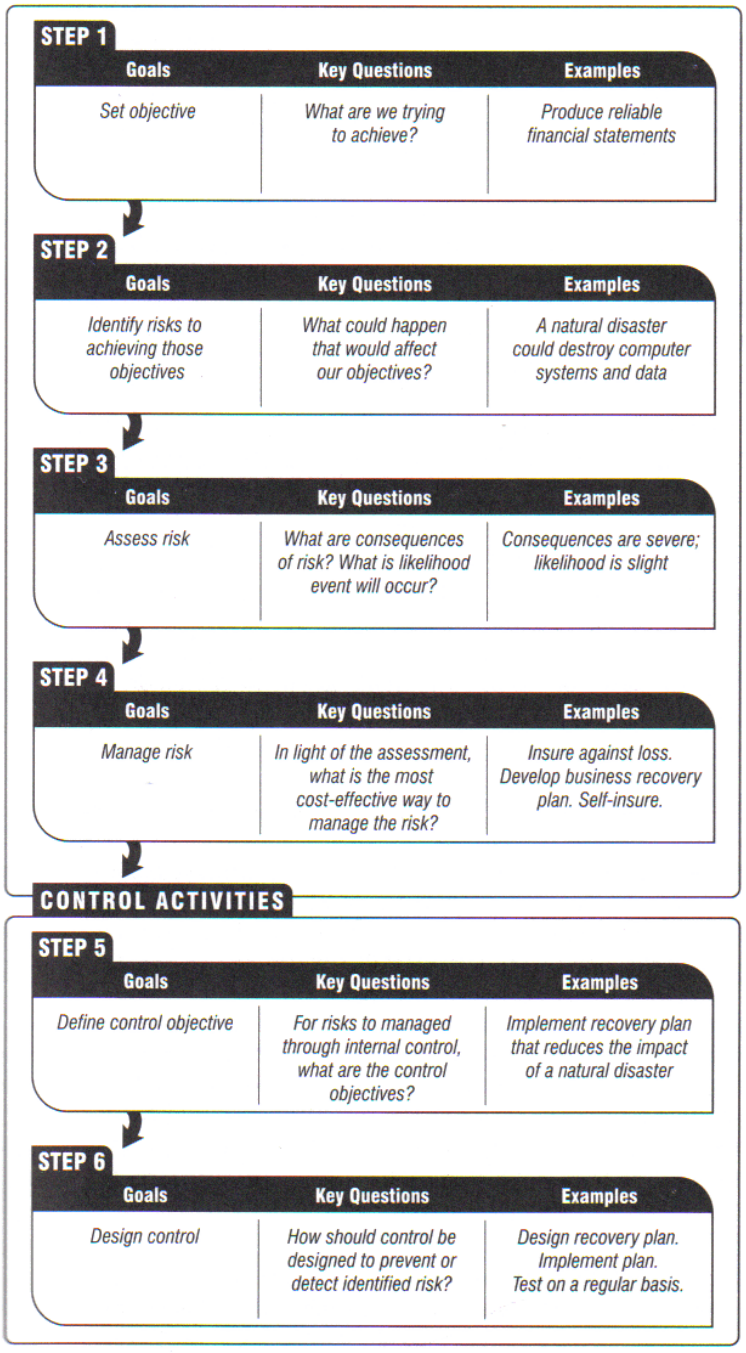
Personalpolitikk (Human Resource) omhandler selskapets retningslinjer i forhold til å ha kompetente ansatte. Politikken involverer de forventninger som stilles til ansatte når det gjelder integritet, etisk adferd og kompetanse; både med hensyn til nyansettelser og forfremmelser. Prosedyrer for kursing, rådgivning, evalueringer, utforming av lønnsystemer og disiplinære reaksjoner er vesentlig i utformingen av en fungerende personalpolitikk. Ved rekruttering bør spesifikke retningslinjer sikre at kandidatene har riktige kvalifikasjoner og

[1] Verdikjedens hovedaktiviteter består av inngående aktiviteter som mottak av ordrer og varer, produksjon, utgående aktiviteter som leveranser, markedsføring, service, med mer. I tillegg kommer støtteaktiviteter, slik som infrastruktur (ledelse, planlegging, finans, jus etc), Human Resource, utvikling, med mer.

etiske retningslinjer. Dette vil for eksempel bedriften kunne sikre gjennom å benytte erfarne og dyktige intervjuere i jobbintervjuer. Skriftlige stillingsbeskrivelser vil være med å sikre at ansatte kjenner sine ansvarsområder og sine myndigheter.

2.2.2 Risikovurdering

"Enhver virksomhet står ovenfor en rekke eksterne og interne risiki som den må forholde seg til. En forutsetning for å kunne vurdere disse er etablering av internt forenlige ***Målsettinger*** *som er knyttet til hvert enkelt nivå i bedriften. Risikovurdering består av* ***Identifisering*** *og* ***Analyse*** *av risiki som er relevante når det gjelder oppnåelse av virksomhetens målsettinger. Identifiseringen og analysen danner så et grunnlag for hvordan risiko skal håndteres."* (COSO, 1992)



Figur 2.2,
Kilde: Ramos, 2004

Figuren viser sammenhengen mellom risikovurdering og kontrollaktiviteter
(Trinn 1-4 inngår i risikovurdering, trinn 5-6 er kontrollaktiviteter)

2.2.2.1 Målsettinger

Uten målsettinger blir det vanskelig for ledelsen å vite hvilke risiki som skal identifiseres. Følgelig blir det også vanskelig å ta riktige beslutninger for å håndtere risiko. Det er derfor av stor betydning å fastsette målsettinger. Målsettinger vedrørende **Pålitelig Regnskaps-rapportering** settes både på virksomhets- og på aktivitetsnivå, dog vil det her være en naturlig overlapping. For eksempel vil risikovurdering på det overordnede nivå danne utgangspunkt for risikovurdering i de enkelte prosessene. På bakgrunn av identifiserte

risikofaktorer, kan ledelsen vurdere vesentlighet, og vurdere hvilke aktiviteter og hvilke deler av bedriften som berøres. Tilsvarende vil en gjennom en effektiv risikohåndtering på aktivitetsnivå bidra til å redusere risiko for vesentlige feil på virksomhetsnivå.

Pålitelig regnskapsrapportering innebærer å utarbeide regnskaper som presenters på en forsvarlig måte og i samsvar med relevante, **Generelt Aksepterte Regnskapsprinsipper**. *American Institute of Certified Public Accountants (*AICPA) har listet opp enkelte punkter som forklarer hva det vil si å presentere regnskapet på en forsvarlig måte. For øvrig benyttes de samme punktene også i COSOs rammeverk:

- ***Regnskapsprinsippene som anvendes er generelt aksepterte***
- ***Regnskapsprinsippene er passende, forholdene tatt i betraktning***
- ***Regnskapsprinsippene er informative med hensyn til forhold som kan påvirke bruken, forståelsen og fortolkningen av dem.***
- ***Informasjonen som presenteres er klassifisert og satt sammen på en fornuftig måte*** (verken for detaljert eller for enkelt)
- ***Regnskapene reflekterer de underliggende transaksjoner og begivenheter som påvirker selskapets resultat, økonomiske situasjon og kontantstrømmer innefor akseptable grenser*** (fornuftige og praktiske grenser)

(AICPA, Statement on Auditing Standards No. 69)

Til grunn for disse målsettingene ligger **Regnskapspåstandene**. Når ledelsen rapporterer sitt årsresultat, og offentliggjør sine regnskaper, er det visse påstander ledelsen kommer med angående selskapets økonomiske situasjon. Disse regnskapspåstandene kan vi dele inn i tre grupper; påstander vedrørende **Transaksjoner**, **Kontoer**, og **Presentasjon og Innhold**

Ledelsens påstander vedrørende virksomhetens transaksjoner og hendelser i perioden:

Gyldighet	Transaksjonene og hendelsene har faktisk funnet sted, og vedrører virksomheten.
Fullstendighet	Alle transaksjoner og hendelser som skal registreres, er registrert.
Nøyaktighet	Opplysninger (herunder beløp) knyttet til transaksjonene er riktig registrert.
Periodisering	Transaksjoner fant sted i løpet av perioden.
Klassifisering	Transaksjoner og hendelsene er registrert på riktig konto.

Figur 2.3 – Regnskapspåstander vedrørende transaksjoner og hendelser

Ledelsens påstander angående kontosaldoer ved periodens slutt:

Eksistens	Eiendeler, forpliktelser og egenkapital eksisterer.
Rettigheter og Forpliktelser	Eiendeler, forpliktelser og egenkapital tilhører virksomheten.
Fullstendighet	Alle eiendeler, forpliktelser, og all egenkapital som skal registreres er registrert.
Verdsettelse og fordeling	Eiendeler, gjeld og egenkapital er registrert med riktig beløp

Figur 2.4 - Regnskapspåstander angående kontosaldoer

Ledelsens påstander om regnskapets presentasjon og innhold:

Gyldighet	Hendelser, transaksjoner og andre forhold som det er redegjort for, har forekommet.
Rettigheter og Forpliktelser	hendelser, transaksjoner og andre forhold som det er redegjort for, vedrører virksomheten.
Fullstendighet	Alle opplysninger som skal inkluderes er registrert.
Klassifisering og forståelighet	Informasjon er presentert og beskrevet på en formålstjenlig måte, og opplysninger er klart uttrykt.
Nøyaktighet og verdsettelse	Informasjon er rettvisende presentert og med korrekte beløp.

Figur 2.5 - Regnskapspåstander om presentasjon og innhold
Kilde: (RS500, §17)

2.2.2.2 Identifisering av Risiko

Identifisering av risiko bør være en kontinuerlig prosess i enhver virksomhet. På virksomhetsnivå kan nye risiki oppstå som følger av eksterne endringer, for eksempel ny regnskapslovgivning. Kravet om at alle norske børsnoterte selskaper må rapportere konsernregnskap i henhold til IFRS[2] er et slikt eksempel. Risiko kan også stamme fra interne faktorer, slik som risiko for at informasjonssystemer bryter sammen. Risiko på aktivitetsnivå handler om å vurdere risikomomenter for viktige enkeltaktiviteter og funksjoner, slik som

[2] For å sikre mer entydighet mellom regnskapsrapportering på tvers av landegrensene, har EU vedtatt at alle børsnoterte selskaper i EU skal føre konsernregnskap i samsvar med International Financial Reporting Standards (IFRS) senest i 2005. Norge har, som EØS-medlem vedtatt regler som innebærer krav om rapportering av konsernregnskap etter IFRS fra 1. Januar 2005 for børsnoterte selskaper.

risiko knyttet til feil i salgsavdeling, produksjonsavdeling etc. Eksempelvis kan dette være risiko for at ikke alle salg registreres i en salgsavdeling.

Faktorer som bør undersøkes når risiko skal identifiseres inkluderer (Ramos, 2004):

- ***Tidligere erfaring med mangelfull måloppnåelse***
- ***Ansattes kvalifikasjoner og kompetanse***
- ***Endringer som vedrører selskapet, slik som konkurranse, lovgivning, personell.***
- ***Hvorvidt bedriften er spredd over flere geografiske steder, spesielt gjelder dette for bedrifter som opererer i flere land.***
- ***Aktiviteters betydning for virksomheten***
- ***Aktiviteters kompleksitet***

SWOT-analyser (Styrker, Svakheter, Muligheter, Trusler), PEST-analyser (Political, Economical, Sociological, Technological), Porters 5-forces, og innhenting av bransje- og trendanalyser er eksempler på tiltak ledelsen kan gjøre for å identifisere ulike risiki i en virksomhet. For å sikre at all relevant risiko blir tatt med i betraktning kan det være hensiktsmessig å identifisere risiko uavhengig av en analyse av sannsynlighet og konsekvens. Når risiki er identifisert, kan deres betydning vurderes.

2.2.2.3 Vurdering av Risiko

I analyse av risikoen bør virksomheten vurdere to momenter. **Sannsynligheten** for at hendelsen vil inntreffe, eventuelt hvor ofte begivenheten som er forbundet med risiko vil inntreffe, bør vurderes. Videre bør også **Konsekvensen** av at hendelsen inntreffer vurderes. Risiko som ikke har noen praktisk betydning for virksomheten, og risiko som med svært liten sannsynlighet vil inntreffe (som at en satellitt skulle falle ned og treffe en av virksomhetens fabrikker) behøver en ikke ta hensyn til. Derimot vil en rette stor oppmerksomhet mot de hendelser som med stor sannsynlighet kan inntreffe, og de hendelser som kan få store konsekvenser, for eksempel i form av gedigne erstatningskrav.

2.2.2.4 Håndtering av Risiko

Når virksomheten har vurdert konsekvens og sannsynlighet, bør man avveie hvorvidt risikoen bør håndteres (kostnad/nytte i forhold til å sikre seg mot risikoen). Er identifiserte risiko verd å ta hensyn til, eller blir det uhensiktsmessig dyrt? Kan risikoen overføres, som for eksempel gjennom å tegne forsikringer, eller ved å benytte finansielle instrumenter i hedgingstrategier? Kan risikoen reduseres eller forebygges gjennom for eksempel å implementere nye prosedyrer, eller vil interne kontroller redusere risikoen? Endelig vil virksomheten i enkelte tilfeller være nødt til å akseptere risikoen.

2.2.2.5 Håndtering av Endringer

Enhver virksomhets omgivelser er i kontinuerlig endring. Tilsvarende endrer virksomhetens egne aktiviteter seg. Dette medfører at en intern kontroll som fungerte for en tid tilbake, ikke nødvendigvis er effektiv i dag. Det er derfor essensielt å etablere prosesser som bidrar til å identifisere endringer som kan påvirke virksomheten. Disse prosessene vil enten være en del av den ordinære ”risikovurderingsprosessen”, eller en parallell prosess. Prosessen skal i tillegg til å identifisere endringer i omgivelsene, også analysere muligheter og trusler som følger av endringene. Dermed vil for eksempel en SWOT-analyse også være aktuell i håndtering av endringer.

2.2.3 Kontrollaktiviteter

Som vist i figur 2.2 er kontrollaktivitetene knyttet til risikovurderingsprosessen. En kontrollaktivitet skal sikre at prosedyrer for å redusere risiko utføres på riktig måte. Aktivitetene skal dermed dekke over så vel tilsiktede som utilsiktede feil (misligheter). Siden det her først og fremst er snakk om intern kontroll for pålitelig regnskapsrapportering, vil de relevante kontrollene i all hovedsak gjelde hvordan transaksjoner autoriseres, initieres, registreres, behandles og rapporteres.

Virksomheter varierer med tanke på kompleksitet, størrelse, aktiviteter, målsettinger, risiko, etc. Selv i situasjoner hvor to bedrifter opererer noenlunde likt, og med noenlunde like målsettinger, vil personer involvert i selskapene ha forskjellige preferanser i forhold til

vurderinger og skjønn. Det kan derfor ikke forventes at to virksomheter har identiske kontrollaktiviteter.

Aktivitetene kan deles inn i to elementer; **Planer** og **Rutiner**. Planene forteller hva som skal gjøres, og rutinene er de handlinger som foretas for å følge planene. Eksempelvis kan en handlingsplan være å sammenligne regnskapets registrerte salgstall og selgerprovisjoner med daglige salgstall fra distriktssjefene. Rutinene blir da å skaffe informasjon om salgstall ved de ulike avdelingene, og å sammenligne disse med regnskapet.

Rutinene kan igjen deles inn i to typer kontrollaktiviteter, de som skal forhindre feil og de som skal oppdage feil; henholdsvis **Forebyggende Kontroller** og **Oppdagende Kontroller**:

Forebyggende Kontroller består av prosedyrer som er designet for å forebygge feil og misligheter, og er typisk anvendt på individuelle transaksjoner.

Oppdagende Kontroller er prosedyrer som er designet for å oppdage og rette feil som, hvis ikke oppdages, vil få innflytelse på regnskapene. Oppdagende kontroller anvendes typisk på transaksjonsgrupper. Selskapets kontroller bør være en kombinasjon av begge kontrolltypene, ledelsen kan altså ikke ene og alene basere evalueringen på én type kontroller. For eksempel vil det kunne oppstå vesentlige feil i regnskapsposter som påvirkes av kompliserte transaksjoner, selv om det eksisterer forebyggende kontroller.

Kontrollene kan være etablert som **Manuelle Kontroller** og som **Automatiserte Kontroller**:

Manuelle Kontroller består blant annet av godkjennelsesprosedyrer, gjennomgåelse av aktiviteter, og avstemminger (RS315, §58). Førstnevnte vil være et eksempel på en forebyggende kontroll, mens sistnevnte er en oppdagende kontroll. Eksempelvis vil en manuell forebyggende kontroll være at innkjøpsordrer skal godkjennes før varer bestilles. En manuell oppdagende kontroll vil for eksempel være en bankavstemming, som skal kunne gi svar på hvorvidt banktransaksjoner er registrert, hvorvidt de er ekte, og hvorvidt de er registrert med riktig beløp. På samme måte vil avstemminger ovenfor kreditorer kunne sikre at selskapets registreringer samsvarer med kreditors.

Automatiserte (Systembaserte) Kontroller skal bidra til å forebygge eller oppdage manuelle feil, i tillegg til å avdekke risiko for feil som har blitt identifisert, vedrørende iverksetting, registrering, behandling og rapportering av transaksjonsstrømmene. For eksempel vil en slik automatisert (forebyggende) kontroll være et datasystem som kredittsjekker alle kunder som bestiller varer på kreditt. Dersom kundene bestiller innenfor gitte kredittrammer, autoriseres bestilte varer for forsendelse. Automatiserte kontroller er mindre utsatt for overstyringer og menneskelig svikt enn manuelle kontroller, mens de derimot kan være utsatt for feil programmering.

2.2.3.1 Informasjonsbehandling

Svært mye av en bedrifts virksomhet registreres i datasystemer. Generelle kontroller av datasystemer (operativsystemer, systemprogramvare etc fungerer som del skal), samt applikasjonskontroll (transaksjoner behandles nøyaktig og riktig) er derfor essensielt for en effektiv internkontroll. I tillegg er det stor risiko knyttet til tilgangskontroll og autorisasjon. Dersom passord endres svært sjeldent, og dersom tidligere medarbeideres brukernavn/passord ikke slettes fortløpende innebærer dette en risiko for at uautoriserte ”brukere” får tilgang til informasjon som de ikke skulle hatt. I verste fall kan uautoriserte personer endre, slette eller legge til vilkårlig data, og dermed undergrave riktigheten av registrerte opplysninger.

2.2.3.2 Fysisk Kontroll

Under begrepet fysiske kontroller ligger sikring av eiendeler, varelagre, økonomiske verdier, samt regelmessig varetelling, og sammenligning med registrerte beløp. Fysiske kontroller bør ses i sammenheng med risiko for svinn. For eksempel bør en gullsmed ha tilstrekkelig alarmsystem og sikre at smykker er tilstrekkelig innelåst når forretningen er stengt. Små, verdifulle smykker kan heller ikke ligge lett tilgjengelig for nasking. Derimot er det ikke av like stor betydning for et sagbruk å låse inn sitt tømmer.

2.2.3.3 Ansvarsfordeling

Gjennom fornuftig ansvarsfordelig minsker risikoen for feil eller misbruk. I en større bedrift bør ikke en og samme person ha ansvaret for å ta imot bestillinger, sende ut varer, ta imot betaling, samt ansvaret for å føre regnskapet. Vedkommende vil ha en helt spesiell anledning

til å manipulere regnskapet, da det vil være vanskelig for tredjeparter å avdekke mislighetene. En fornuftig ansvarsfordeling som sikrer at ansvaret for godkjenning av transaksjoner, registrering av transaksjoner, samt håndtering av aktiva er delt, er avgjørende for å kunne si at kontrollsystemet fungerer.

2.2.4 Informasjon og Kommunikasjon

En virksomhet kan ha de beste rutiner for å avdekke og håndtere risiko, på papiret. Den kan også ha etablert meget tilfredsstillende rutiner for kontrollaktiviteter. Dog hjelper det lite med en teoretisk effektiv internkontroll dersom ikke de ansatte vet hva de skal gjøre. Ledelsen må vurdere hvilken informasjon som er relevant for å kunne styre bedriften, og formidle denne – til den tid og i den form – som behøves av de ansatte for å kunne gjennomføre sine ansvarsoppgaver og kontrollaktiviteter.

Informasjonssystem i forbindelse med økonomisk rapportering består av rutiner og regnskapsbøker som er opprettet for å initiere, registrere, behandle og rapportere virksomhetens transaksjoner og hendelser, samt kontroll med tilknyttede eiendeler, forpliktelser og egenkapital (RS315 vedlegg 2, §9).

Iverksetting kan foregå enten manuelt eller automatisk gjennom programmerte prosedyrer. Registrering består i å identifisere og ta vare på relevant informasjon vedrørende transaksjoner og hendelser. Behandling inkluderer funksjoner som redigering, godkjenning, beregning, måling, verdsettelse, summering og avstemming. Rapportering relaterer seg til bearbeidelse av de økonomiske rapportene, i tillegg til annen informasjon; elektronisk eller skriftlig, som virksomheten bruker i overvåking og i andre funksjoner (RS315, vedlegg 2, §9 ; AU319).

Følgelig omfatter informasjonssystem de metoder og registre som gjør det mulig å registrere opplysninger i samsvar med regnskapspåstandene:[3]

- ***Identifisering og registrering av alle gyldige transaksjoner***
- ***Beskrivelse av transaksjoner i rett tid, og i tilstrekkelig detalj, slik at en kan klassifisere transaksjoner for økonomisk rapportering på en riktig måte***

[3] Se figurene 2.3 - 2.5

- ***Måling av verdien av transaksjoner slik at en kan registrere deres reelle pengeverdi***
- ***Fastsettelse av hvilken periode transaksjonene oppstod i, slik at en kan periodisere transaksjonene i riktig periode.***
- ***Tilfredstillende presentasjon av transaksjoner og tilleggsopplysninger i de økonomiske rapportene.***

(RS315, vedlegg 2, §10)

Kommunikasjon i et internkontrollperspektiv består i å formidle informasjon til de ansatte vedrørende deres roller og ansvar i forbindelse med intern kontroll over økonomisk rapportering. De ansatte må forstå betydningen av sine oppgaver i forhold til økonomisk rapportering og i forhold til andres arbeid, samt forstå fremgangsmåten for å rapportere avvik til riktig overordnet instans i foretaket (RS315, vedlegg 2, §11). Eksempelvis viser COSO til at det ikke er tilfredsstillende kun å identifisere avvik i en avviksrapport. For at tiltak skal kunne iverksettes, hvilket er noe av hensikten med intern kontroll, må en også avdekke hvor og hvorfor avvikene har oppstått. Åpne kommunikasjonskanaler bidrar til å sikre at avvik rapporteres og håndteres.

Informasjon behøves på alle nivåer i organisasjonen for at man skal kunne drive foretaket i retning av fastsatte målsettinger. Informasjon bør samles fra, og kommunikasjon bør foregå, **Eksternt** så vel som **Internt**. På det interne plan skal medarbeiderne blant annet forstå sin betydning i det interne kontrollsystemet, forstå hvilket ansvar vedkommende har, samt vite hva og til hvem vedkommende skal rapportere. Fra eksterne kilder vil en også motta signaler angående kontrollsystemets effektivitet. For eksempel vil gjentatte klager på beløp i fakturaer kunne signalisere feil utstedte fakturaer, og dermed en svakhet i kontrollsystemet.

Det er viktig å hente inn all type informasjon når en skal sikre en effektiv internkontroll. **Økonomisk Informasjon** vil for eksempel brukes til å ta beslutninger i bedriften, i tillegg til utarbeidelse av regnskapsrapporter. Også en del **Ikke-Økonomisk Informasjon** vil være av betydning for å sikre pålitelige regnskapsrapporter. For eksempel vil informasjon om dagens og fremtidens markedsforhold hjelpe virksomheten til å kunne anslå hvor stor del av et varelager som forventes å kunne bli ukurant.

Endelig er det verd å merke seg den gjensidige sammenhengen mellom **Informasjon og Kommunikasjon**, og **Kontrollaktiviteter**. På den ene siden skal effektiv kommunikasjon og

et effektivt informasjonssystem gjøre de ansatte bevisst på sine roller i forhold til å utføre kontrollaktiviteter. På den andre siden skal kontrollaktiviteter bidra til å avdekke mangler og feil i informasjonssystemet og kommunikasjonen.

2.2.5 Overvåking

En virksomhets interne kontroller tilpasses endringer i virksomhetens omgivelser, prosesser, nye ansatte, etc. Det er derfor nødvendig med overvåking av det interne kontrollsystemet for å sikre at de interne kontrollprosessene fungerer effektivt og etter hensikten. Overvåkningen foregår både som **Kontinuerlig Overvåkning** og som **Frittstående Evalueringer**.

Kontinuerlig Overvåkning foregår gjennom den daglige ledelse og kontroll med at virksomhetens daglige aktiviteter utføres slik som forventet, gjennom resultatrapporter og avviksrapporter, feilmeldinger, kommunikasjon med ansatte, og gjennom kommunikasjon med intern og ekstern revisor. I tillegg vil klager fra eksterne parter, for eksempel klager på feil fakturering, indikere mulige feil i selskapets systemer.

Frittstående Evalueringer vil ofte ta form av egenevaluering, hvor ansvarlige for ulike aktiviteter vurderer effektiviteten av internkontrollen tilknyttet sin aktivitet. Dette kan for eksempel foregå gjennom etablering av en database, hvor alle mellomledere skal rapportere endringer i sine prosesser, kontrollsystemer, aktivitetsnivå, i tillegg til å rapportere feil som har blitt begått eller oppdaget i løpet av perioden. Utover dette vil sammenligning med andre bedrifters internkontroll (benchmarking) også fungere som en viktig del av systemets overvåkning.

Selv en minimal feil har en bakenforliggende årsak. Gjennom å rapportere selv de minste feil, kan ledelsen se på foranledningen til feilen, og dermed rette opp eventuelle svakheter i systemet. COSO anfører derfor viktigheten av å rapportere selv *bagatellmessige* feil og mangler. En mangel er ifølge COSO et "…*forhold i det interne kontrollsystemet som man bør kikke nærmere på*", og kan dermed være "…*en oppfattet, potensiell eller reell feil eller ufullkommenhet, eller en mulighet til å forbedre det interne kontrollsystemets evne til å gi større sannsynlighet for oppnåelse av virksomhetens målsettinger*" (COSO, 1992). For eksempel vil en feil i provisjonsutbetaling kunne oppstå på som følger av feil salgspris på

varer. Dermed vil en feilrapport vedrørende for liten provisjon kunne avsløre feil i systemet for prising av varer. Videre vil ikke det at en ansatt underslår én krone, én gang ha noen praktisk betydning for selskapets resultat. Derimot vil det å se mellom fingrene på et slikt underslag gi et lite ønskelig signal til vedkommende (og til de øvrige ansatte). Rapportering av alle underslag vil derfor være viktig i forhold til å vise at slik adferd ikke aksepteres.

3 Intern Kontrolls Betydning for Revisjon

Revisor må opparbeide seg en forståelse av foretaket og dets omgivelser, herunder foretakets interne kontroll, som er tilstrekkelig til å identifisere og vurdere risikoene for vesentlig feilinformasjon i årsregnskapet.

- (RS315, §2)

Revisor skal, som en del av **Risikovurderingsprosessen** i et revisjonsoppdrag, skaffe seg en forståelse av virksomhetens interne kontroll. Denne forståelsen bruker revisor "*…til å identifisere typer av mulig feilinformasjon, til å vurdere faktorer som påvirker risikoene for vesentlig feilinformasjon og til å utforme type, tidspunkt for utførelse og omfang av de videre revisjonshandlingene.*" (RS315, §41). Formålet med forståelsen av internkontrollen er dermed å kunne planlegge hvilke og hvor omfattende **Revisjonshandlinger** som skal foretas i forbindelse med revisjon av en klient.

Revisjonshandlingene kan vi dele inn i to ulike typer (eller formål), henholdsvis **Substanskontroller**[4] og **Tester av Kontroller** (RS330, §10). Generelt kan vi si at dess dårligere en klients interne kontroll virker å være, dess mindre kan revisor stole på virksomhetens interne kontroll, og dess flere substanskontroller må derfor revisor foreta. Imidlertid er valg av revisjonshandling også avhengig av hvilken regnskapspåstand[5] revisor skal undersøke. (RS330, §10)

3.1 Forståelse av Virksomhetens Interne Kontroll

Revisor skal skaffe seg en forståelse av en virksomhets interne kontroll ved å undersøke kontrollenes design, og hvorvidt kontrollene er iverksatt. Kjennskap til kontrollenes design får revisor ved forespørsler av ledelsen og ansatte, ved å inspisere dokumenter, ved å observere bruken av kontrollene, og ved å følge transaksjoner gjennom informasjonssystemene. Revisor

[4] Subtanskontroller utføres for å avdekke vesentlig feilinformasjon i transaksjonsklasser og kontosaldoer (i kroner), samt tilleggsopplysninger (Eilifsen, 2006). Substanskontroller kan enten være tester av detaljer - hvor transaksjoner, saldobalanser og tilleggsopplysninger vurderes for feil, eller analytiske kontrollhandlinger - hvor revisor vurderer om opplysninger i transaksjonsklasser og saldobalanser virker korrekt, på bakgrunn av analyser av trender, forholdstall i forhold til historiske eller bransjedata, og sammenhenger.

[5] Se avsnitt 2.2.2.1

bør ta utgangspunkt i et rammeverk, for eksempel COSO, i arbeidet med å skaffe seg forståelsen av interkontrollen. Eksempelvis vil svakheter i **Kontrollmiljøet** få stor betydning for de revisjonshandlingene som skal foretas. I den grad revisor, på tross av svakheter i kontrollmiljøet, velger å teste kontroller som en vesentlig del av revideringen, bør revisor i alle fall nøye vurdere metode, tidspunkt og omfang av tester.

Revisors mål vil imidlertid ikke være å undersøke hvorvidt kontrollene er "riktig" klassifisert i henhold til et rammeverk, men snarere å identifisere vesentlige kontroller som forebygger, eller avdekker og korrigerer, **Vesentlig Feilinformasjon** knyttet til regnskapspåstandene (RS315, §44). Dette vil si at vi kan dele kontroller inn i to typer, de som skal **Forebygge** feil, og de som skal **Oppdage** feil. Siden det her er snakk om økonomisk rapportering, vil de relevante kontrollene i all hovedsak gjelde hvordan **Transaksjoner** knyttet til **Vesentlige Regnskapsposter** autoriseres, initieres, registreres, behandles og rapporteres. Kontrollene kan bestå i politikker, prosedyrer, rapporter, metoder og systemer (Protiviti, 2004).

Revisor benytter seg av skjønn når han skal vurdere om kontroller er relevante i forhold til risiko for vesentlig feilinformasjon. Til grunn for dette skjønn bør revisor ta hensyn til visse forhold, herunder revisors **Vesentlighetsvurdering**, den aktuelle **Komponenten** (jfr COSO), og virksomhetens **Størrelse, Art og Kompleksitet** (RS315, §48).

I det følgende vil først internkontrollens begrensning bli forklart, før vesentlighet og vesentlige regnskapsposter defineres. Deretter vil identifikasjon av betydelige selskaper og forretningsområder, samt vesentlige transaksjoner og prosesser bli behandlet. Videre blir risiko og sannsynlighet omtalt. Dette er elementer som danner utgangspunkt for revisors forståelse av virksomhetens interne kontroller, som igjen danner utgangspunkt for valg av revisjonshandlinger.

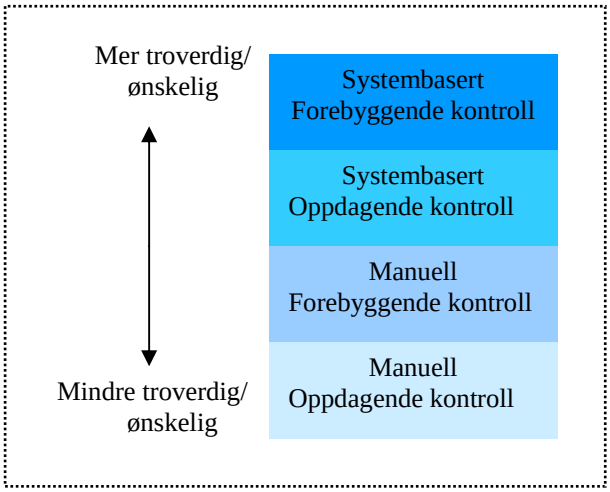
3.1.1 Begrensninger i Intern Kontroll

Intern kontroll, uansett hvor godt den er utformet eller gjennomført, kan bare gi foretaket rimelig sikkerhet med hensyn til oppfyllelsen av foretakets mål for økonomisk rapportering.

- (RS315, §64)

Begrensninger i de interne kontrollssystemene påvirker sannsynligheten for at målsettinger nås. Uansett hvor effektivt en kontroll er planlagt og utformet, vil det alltid eksistere en viss risiko for at feil ikke forebygges eller oppdages. Feil kan oppstå fordi menneskelig skjønn og vurderinger i beslutningsprosessen kan være feilaktige. På samme måte kan feil oppstå i utførelsen av, eller overvåkingen av, den interne kontrollen. Spesielt er manuelle kontroller mer utsatt for feil enn automatisert kontroller, da manuelle kontroller lettere kan omgås, ignoreres og overstyres (RS315, §62). Derfor kan en effektiv intern kontroll kun gi rimelig sikkerhet for at feil ikke forebygges eller oppdages (COSO, 1992). Når sannsynligheten for feil er større i manuelle kontroller enn tilfelle er i systembaserte kontroller, skulle dette tilsi at det vil være fordelaktig å benytte systembaserte kontroller.

En kontrolls pålitelighet, og dermed verdien, kan illustreres som på figuren. Behovet for, og verdien av, system-baserte kontroller øker med økt omfang av transaksjoner, og med virksomhetens bruk av IT. Samtidig viser figuren at forebyggende kontroller har større verdi enn oppdagende, da det er sikrere å forhindre en feil i å oppstå enn det er å oppdage feilen. (Protiviti; 2004)



Figur 3.1 Kilde: Protiviti, 2004

En virksomhet må hele tiden foreta en avveining mellom kostnad og nytte, og revisor må også ha forståelse for at 100 % intern kontroll ikke er mulig å oppnå. Et effektivt internt kontrollsystem er derfor et system hvor revisor med rimelig sikkerhet kan si at regnskapsrapporteringen er pålitelig. Det er dog viktig å forstå at selv en god intern kontroll over økonomisk rapportering ikke kan ses på som en absolutt garanti for validiteten av selskapets regnskaper. Det skyldes blant annet at mennesker er involvert, og at disse kan ta feil beslutninger, og det kan være sammensvergelser blant flere involverte parter.

3.1.2 Vesentlighet og Vesentlige Regnskapsposter

Begrepet vesentlighet i forbindelse med økonomisk rapportering knytter seg til et korrekt bilde av perioderegnskapene. RS320(§3) definerer i så måte: "Informasjon er vesentlig hvis feil i, eller utelatelse av, informasjon kan påvirke økonomiske beslutninger som treffes av brukerne på grunnlag av regnskapet. Vesentlighet avhenger av størrelsen av regnskapsposten eller feilen, sett i forhold til omstendighetene rundt utelatelsen eller feilen…"[6] Vesentlighet er dermed en skjønnsmessig vurdering, som baserer seg på kvantitative faktorer (som størrelsen på regnskapsposten og feilen), og kvalitative faktorer (som omstendighetene rundt feilen).

Revisor vurderer vesentlighet både i forhold til årsregnskapet totalt og i forhold til transaksjonsklasser, kontosaldoer og noteopplysninger (RS320, §7). Typisk vil en kvantitativ vurdering av vesentlighetsnivået for årsregnskapet totalt ta utgangspunkt i siste års, eller gjennomsnitt av siste tre års: resultat før skatt, driftsresultat, eiendeler eller inntekter (Eilifsen et.al, 2006); og en viss prosentandel av gitte forhold. Dette vil så danne utgangspunktet for vesentlighetgrensen for de ulike postene.

En regnskapspost er vesentlig ut i fra et kvantitativt mål dersom det er mer enn en fjern sannsynlighet[7] for at posten kan inneholde feil som alene, eller sammen med andre feil, kan ha en vesentlig effekt på regnskapet (AS2, §61). I tillegg vil vesentlige regnskapsposter avhenge av en rekke kvalitative faktorer. PCAOB gir i AS2 (§65) en del kvalitative faktorer som er relevante i forhold til identifikasjon av en vesentlig regnskapspost.

- ***Hvorvidt posten er utsatt for feil eller misligheter*** (iboende risiko)
- ***Volum og kompleksitet av transaksjoner som påvirker regnskapsposter, og i hvilken grad transaksjonene er standardiserte***
- ***Regnskapspostens karakter***
- ***Hvorvidt føring og rapportering av regnskapsposten er komplisert***
- ***Hvor utsatt virksomheten er for tap som følger av feil i regnskapsposten***
- ***Sannsynligheten for at posten kan påføre virksomheten en betinget forpliktelse***
- ***Transaksjoner med nærstående parter***
- ***Endringer i regnskapspostens sammensetning***

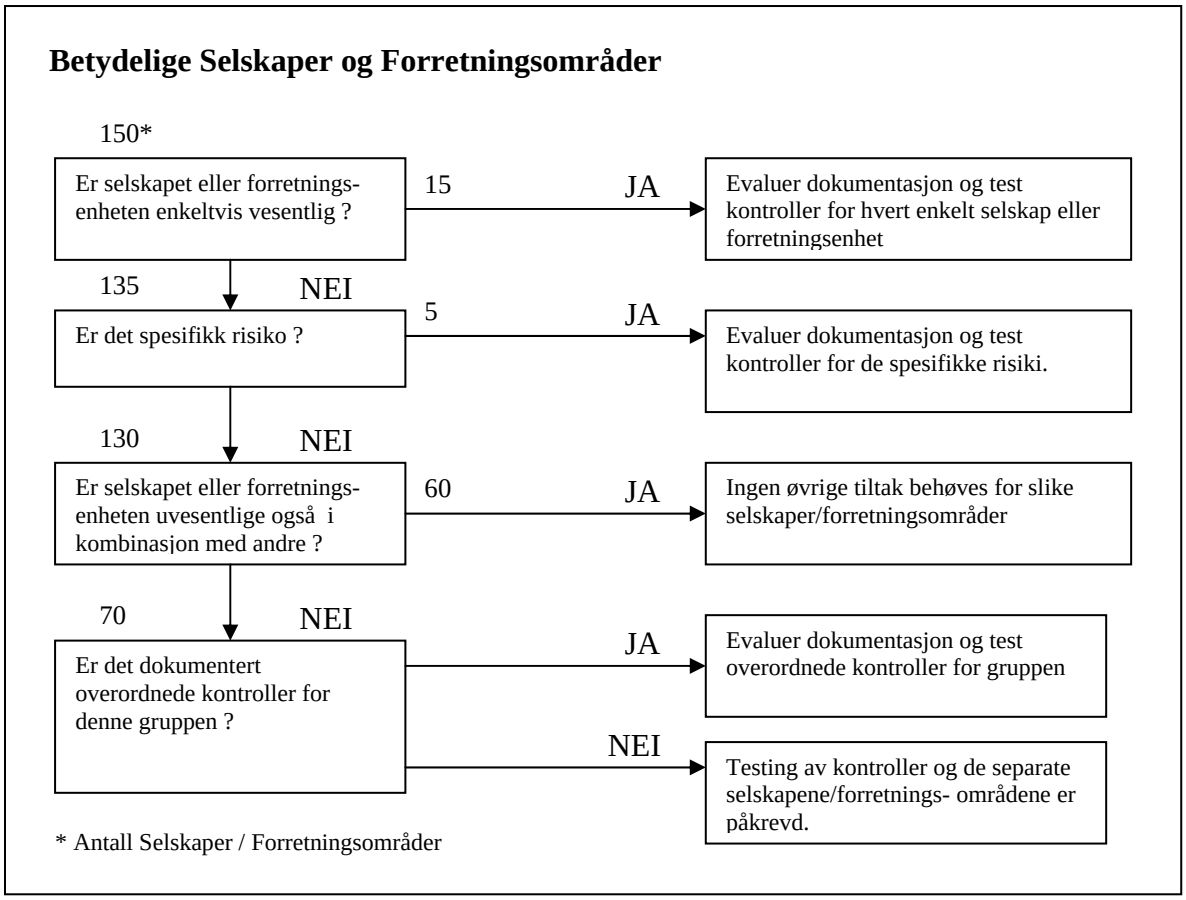
[6] Basert på: International Accounting Standards Board's "Framework for the Preparation and Presentation of Financial Statements"
[7] Begrepet "fjern sannsynlighet" forklares i avsnitt 3.1.5

For eksempel kan en naturlig vesentlighetsgrense for resultat før skatt være 3-5 %, mens vesentlighetsgrensen til en gitt post kan være 2-15 % (Eilifsen et.al, 2006). Dermed kan vi ende opp med en situasjon hvor den kombinerte vesentligheten av de involverte postene overgår vesentlighetsgrensen for virksomhetens resultat som helhet. Dette kan være fornuftig da det ikke forventes at hver enkelt post vil inneholde maksimalt tillatt feil (vesentlighetsgrensen), og da forskjellige personer er involvert i prosessene for å avdekke feil. Det vil vanskelig la seg gjøre kontinuerlig å holde seg oppdatert over hvor mange feil alle andre personer involvert har avdekket.

En kvalitativ faktor kan bidra til å *senke* vesentlighetsgrensen, men den kan derimot ikke bidra til å *øke* vesentlighetsgrensen. For eksempel vil en post som innebærer transaksjoner mellom nærstående parter kunne ha en lavere terskel for vesentlighet enn tilsvarende ville vært dersom det ikke var nærstående parter involvert. Kvalitative faktorer vedrørende årsregnskapet totalt inkluderer hvorvidt dette er første års oppdrag, eventuelt om det typisk har vært mange feil forbundet med klientens regnskaper fra tidligere, endringer i ledelsen, og risiko for misligheter.

3.1.3 Betydelige Selskaper og Forretningsområder.

Når revisor har vurdert vesentlighet, bør neste skritt være å identifisere betydelige selskaper og forretningsområder, hvor feil kan oppstå. PCAOB har i AS2, appendiks B, anført visse kriterier for utvelgelse av vesentlige selskaper og forretningsenheter, og delt disse inn i fire kategorier.



Figur 3.2 Kilde: PCAOB, Auditing Standard 2, Appendix B, Illustration B1

Selskaper og Forretningsområder som Enkeltvis er Vesentlige for Årsrapporten.

Et selskap eller et forretningsområde er enkeltvis vesentlig når det utgjør en betydelig del av konsernets samlede drift eller finansielle stilling. Vurdering av vesentlige kontroller skal da foretas separat for hver enkelt enhet.[8]

Selskaper og Forretningsområder som Inneholder Spesifikk Risiko som kan Medføre Vesentlige Feil i Årsrapporten.

Enheter som faller inn under denne kategorien er ikke vesentlige i seg selv ut i fra en kvantitativ betraktning, men har en latent risiko som kan medføre vesentlige feil i konsernregnskapet. Eksempelvis kan dette gjelde et produkt som omsetter relativt lite, men hvor en eventuell erstatningssum for produktfeil vil være høy. Her skal vurdering av kontroller for de spesifikke risikoer foretas separat for hver enkelt enhet.[9]

[8] PCAOB; AS2; Appendix B (B4)
[9] PCAOB; AS2; Appendix B (B6)

Selskaper og Foretningsområder som er Vesentlige Sammen med Andre Selskaper og Forretningsområder.

For enheter som ikke kommer inn under de to foregående kriteriene skal det vurderes hvorvidt de sammen med andre enheter vil få en vesentlig innflytelse på regnskapet. Det fremgår ikke av PCAOBs standard hvilke vilkår som må oppfylles for at to eller flere enheter sammen skal komme inn under denne beskrivelsen. Gath & Christiansen (2003) beskriver kriteriet slik: ”*…men som sammen med ensartede selskaper eller forretningsområder til sammen udgjør en betydelig del af koncernens samlede drift eller finansielle stilling.”* En viss sammenheng mellom ulike selskaper/ forretningsområder bør dermed antakeligvis eksistere for at de skal komme inn under denne beskrivelsen. I forhold til de to foregående beskrivelsen, bør muligens en slik sammenheng enten være gjennom enheter med en viss likhet i forretningsaktiviteter og transaksjoner, eller gjennom enheter som har en spesifikk risiko (som ikke i seg selv kan medføre vesentlig feil i årsrapporten), som sammen med andre enheter med lignende risiko kan gi vesentlig feil i årsrapporten. Vurdering av vesentlige kontroller skal for disse enhetene tas samlet.

Selskaper og Forretningsområder som ikke krever testing.

Enkelte enheter har verken aktiviteter eller risiko som kan knyttes til andre enheter. Dersom eventuelle feil ikke vil få vesentlig innflytelse på regnskapet, behøves ikke gjennomgang av enhetene. Rimelig sikkerhet for at feil som kan få vesentlig innflytelse på regnskapet ikke vil oppstå, vil en få gjennom etablerte overordene kontroller. Særlig gjelder dette kontroller vedrørende overvåking av driften for den enkelte enhet, kontrollmiljøet og risikovurderingsprosessen.

Er det ikke etablert effektive overordende kontroller for de enkelte selskaper og forretningsområder, bør revisor velge ut noen enheter hvor vesentlige kontroller identifiseres og testes. AS2, B10 oppgir en del retningslinjer som revisor må ta hensyn til i utvelgelsen av enheter.

- ***Den enkelte enhets relative regnskapsmessige vesentlighet.***
- ***Risiko for vesentlige feil knyttet til enheten***
- ***I hvilken grad selskapene og forretningsenhetene har like aktiviteter og interne kontroller***
- ***Sentralisering av prosesser***

- ***Kontrollmiljøets effektivitet, særlig toppledelsens kontroll over den lokale ledelsen, og toppledelsens muligheter for å overvåke ulike aktiviteter enheten.***
- ***Den enkelte enhets transaksjoner og tilhørende aktivas omfang og karakter.***
- ***Risiko for at ikke-registrerte forpliktelser, som kan påføre konsernet en vesentlig forpliktelse, eksisterer i enheten.***
- ***Ledelsens risikovurderingsprosess, og hvorvidt ledelsen ekskluderer visse selskaper eller forretningsenheter fra den generelle vurderingen av effektiviteten av selskapets internkontroll.***

3.1.4 Analyse av Transaksjonsstrømmer og Vesentlige Prosesser

Når datterselskap og forretningsenheter som genererer transaksjoner til de vesentlige regnskapspostene har blitt identifisert, bør neste skritt være å analysere transaksjoner hos de identifiserte enhetene. Dermed vil revisor ha et grunnlag for å identifisere de kontrollene i virksomheten som er vesentlige, i forhold til hvorvidt de kan forebygge, eller avdekke og korrigere, vesentlig feilinformasjon knyttet til regnskapspåstandene. Transaksjoner kan deles inn i tre hovedtyper (AS2, §72):

Rutinetransaksjoner; hyppige transaksjoner som regelmessig inngår i selskapets kjernevirksomhet. Eksempler er salg, kjøp, innbetaling, utbetaling, lønn, med mer.
Ikke Rutinemessige Transaksjoner; transaksjoner som kun forekommer periodevis, eller som er unormale er ikke-rutinemessige transaksjoner. Eksempler på periodevise transaksjoner kan være lagerregulering, kalkulering av skatt etc. Unormale transaksjoner kan for eksempel være fusjoner, salg av kraftverk etc.
Skjønnsbaserte Transaksjoner; transaksjoner hvor ledelsen må benytte vurderinger i fastsettelsen av regnskapsmessige verdier. Eksempler vil være nedskriving for ukurans på varelager, garantiavsettelse, etc.

Det vil være forskjellige iboende risiko knyttet til de ovenfor nevnte kategoriene. En bør forstå at det er større risiko for feil knyttet til transaksjoner som er uregelmessige og transaksjoner som i stor grad baseres på skjønn, enn tilfelle er for rutinemessige transaksjoner. Prosesser knyttet til ikke-rutinemessige transaksjoner foregår gjerne ad hoc (i tilfeldig

rekkefølge), og kontrollene er ofte mer uformelle (Protiviti, 2004). Det bør derfor være et mål å forstå og dokumentere hvilken av de tre kategoriene en transaksjon kommer inn under.

Når en har fått en forståelse av transaksjonene involvert i de vesentlige selskaper og forretningsområder, bør en skaffe seg en oversikt over prosessene som er involvert i transaksjonene. Identifisering av prosessene kan gjøres på to måter (Protiviti, 2004):

- Summere transaksjonsstrømmer for de transaksjoner og tilhørende regnskapssystemer som har vesentlig innflytelse på regnskapsrapportering. Dette gjøres ved å splitte virksomheten og dens regnskapssystem i et antall transaksjonsstrømmer. Eksempel på slike transaksjonsstrømmer er inntekter, kjøp, lønningslister, og økonomisk rapportering
- Segmentere bedriften i ulike prosesser. Når en har foretatt en oppdeling av virksomheten i ulike prosesser, kan en identifisere hvilke prosesser som er kritiske og som derfor bør gjennomgås med tanke på risiko og kontroll. Kritiske prosesser identifiseres på bakgrunn av deres betydningen for regnskapet, og sannsynligheten for at det eksisterer mangler i kontrollen.

Det er ikke noe fasitsvar på hvor mange prosesser en bør identifisere. Videre vil det være avhengig av skjønn hvor snevert begrepet prosess skal defineres. En bedrift kan se på selve transaksjonsstrømmene som prosesser, mens en annen bedrift kan dele opp en transaksjonsstrøm, slik som kjøp, i ulike prosesser som anskaffelse, mottak, leverandørgjeld, etc. Vedlegg 1 viser et illustrerende eksempel på ulike prosesser som kan forventes å inngå i en lønnsutbetaling.

3.1.5 Risiko og Sannsynlighet

Begrepet risiko i forbindelse med økonomisk rapportering knytter seg til faren for feil som kan gjør regnskapene ikke-pålitelige. Dette avsnittet vil omhandle revisors identifikasjon av risikoer for feil i regnskapene, samt sannsynligheten for at feil kan oppstå. For øvrig ble teori vedrørende risikovurdering behandlet i avsnitt 2.2.2, som en av komponentene som inngår i rammeverket til COSO.

For at det eksterne regnskapet skal være pålitelig, må transaksjoner og kontoer bli riktig regnskapsmessig behandlet. Ledelsen påstår at så er tilfelle gjennom regnskapspåstandene. Av dette følger at regnskapet ikke er pålitelig dersom regnskapspåstandene ikke medfører riktighet.

Når revisor skal identifisere risikoer, kan han først ta utgangspunkt i analysen og identifikasjonen av vesentlige transaksjonsstrømmer og prosesser, som ble omtalt i forrige avsnitt. Som en illustrasjon kan en ta utgangspunkt i transaksjonen *varesalg*. En av prosessene som inngår i et varesalg er innbetaling, altså salgsinntekter. Et av målene (en av regnskapspåstandene) vil da være at alle salgsinntekter er autentiske - at de bygger på et faktisk salg - og at de skal regnskapsføres. I forhold til at salgsinntektene bygger på et faktisk salg er en generell regel at inntekter skal føres når de er opptjente[10] (NRS, 1996). Det vil si når det er sannsynlig at den økonomiske fordelen vil komme virksomheten til gode. NRS sier videre at inntekt fra varesalg vil være opptjent (skal inntektsføres) når risiko og kontroll knyttet til varen er overført (NRS, 1996). Dermed kan en risiko knyttet til salgsinntekter være at varen faktisk ikke er sendt. En kontrollaktivitet for å møte denne risikoen vil være at salg kun regnskapsføres når godkjente bestillinger samt tilhørende fraktdokument foreligger. På samme måte bør revisor vurdere risikoer for at de enkelte regnskapspåstandene ikke stemmer for hver enkelt av de vesentlige transaksjonsgruppene/prosessene.

En viktig del av risikovurderingsprosessen er å vurdere betydningen av den aktuelle risiko - og sannsynligheten for, eller hvor ofte, hendelsen vil inntreffe. Betydningen av risikoen bedømmes ut i fra hvorvidt risikoen forventes å gi høy, middels eller lav effekt på de økonomiske rapportene. I forhold til å klassifisere sannsynlighet for at en risiko vil inntreffe, kan en ta utgangspunkt i standarder som behandler sannsynlighet for usikre forpliktelser. Både Norsk Regnskapsstandard 13 og Statement of Financial Accounting Standards No. 5 (3)[11] klassifiserer sannsynlighet i ulike kategorier.

Sistnevnte klassifiserer sannsynligheter i følgende kategorier:

- **Sannsynlig** – Det er sannsynlig at hendelsen inntreffer.
- **Rimelig sannsynlig** – Det er mer enn en fjern sannsynlighet for, men mindre enn sannsynlig at hendelsen inntreffer,

[10] NRS(D) – Diskusjonsnotat fra Norsk RegnskapsStiftelse - Regnskapsføring og Inntekt, 1996
[11] Financial Accounting Standards Board

- **Fjern –** Sannsynligheten for at hendelsen inntreffer er meget liten.

NRS13 operer med flere kategorier, og forsøker også å kvantifisere de ulike kategoriene.

- **Så godt som sikkert** – Nesten 100 % sikkert at hendelsen inntreffer
- **Rimelig sikkert** – Over 90 % sannsynlighet
- **Betydelig sannsynlighetsovervekt** – Mellom 70% og 90 % sikkert
- **Sannsynlighetsovervekt** – Sannsynlighetsintervall mellom 50% og 70 %
- **Lite sannsynlig** – Sannsynlighet mellom 10% og 50 %
- **Svært lite sannsynlig** – Svarer til en sannsynlighet under 10 %

Antakeligvis vil det være vanskelig å beregne sannsynlighet for hver enkelt risiko så omfattende som Norsk Regnskapsstandard gjør. Ved å kombinere de to klassifiseringene, vil en derimot kunne ha et rimelig godt utgangspunkt for å kvantifiseres sannsynligheten.

- **Sannsynlig** – Det er sannsynlighetsovervekt (>50 %) for at hendelsen inntreffer
- **Rimelig sannsynlig** – Sannsynlighet mellom 10 % og 50 %
- **Fjern** – Det er meget liten (<10 %) sannsynlighet for at hendelsen inntreffer

En risiko som er sannsynlig, og hvor betydningen på de økonomiske rapportene er stor bør være gjenstand for effektive interne kontroller. Derimot er det ikke nødvendigvis like avgjørende å ha den samme grad av interne kontroller ovenfor risikoer som har liten betydning for de økonomiske rapportene, og hvor det bare er en fjern sannsynlighet for at hendelsen inntreffer.

4 Sarbanes-Oxley Act of 2002

> **Overall, the rules we passed Tuesday should do a lot of great things. I believe that they will cause improvements to internal control structures, strengthen audits, provide important information to investors, reduce the chances of material financial statement errors and irregularities, and, quite possibly, resolve the middle east conflict. Ok, maybe they won't accomplish that last one. And I'll tell you what else they won't do — they won't eliminate financial statement fraud. No rule can do that, because, as many have said over and over in the recent past, nobody can legislate ethics.**
>
> - (Taub, 2003)

Sitatet over er hentet fra en tale holdt i mai 2003, av Debuty Chief Accountant i SEC, Scott A. Taub, og oppsummerer på mange måter Sarbanes-Oxley Act.

Denne delen av utredningen vil først ta for seg bakgrunnen for Sarbanes-Oxley Act; finansskandalene i USA på begynnelsen av dette århundret. Enron har nok vært det mest fremtredende tilfellet, og vil derfor bli brukt som eksempel på noe av den ukulturen som regjerte i enkelte selskaper. Etter en innføring i bakgrunnen for SOX, vil de meste sentrale aspektene ved loven bli presentert.

4.1 Enron – Den Amerikanske Drømmen

Påstander og opplysninger i det følgende er hentet fra boken ”The Smartest Guys in the Room”.[12]

Enron var regnet som prakteksempelet på den amerikanske drømmen. Kenneth Lay (CEO) stod bak oppbygningen av Enron fra å være et ”lite” Houston-basert selskap i 1984 (*Houston Natural Gas*) til et multinasjonalt konsern med en markedsverdi på rundt 70 milliarder $ i 2000. Per Oktober 2000 hadde selskapet gitt investorene svimlende 1400 % i avkastning siden 1990, tre ganger det S&P500 hadde gitt i den samme perioden.

[12] McLean, Bethany & Elkind, Peter; ”The Smartest Guys in the Room – The Amazing Rise and the Scandalous Fall of Enron”

Enron var et eventyr. Av Fortune ble de kåret til ”det mest innovative selskap i verden” seks år på rad. Superlativene haglet. Uttalelser som ”Enron er bokstavelig talt uslåelige i alt de foretar seg” av analytikeren David Fleischer i Goldman Sachs, og ”Industriens standard for fremragende dyktighet” av Deutsche Banks Edward Tirello gikk igjen. Alle elsket Enron.

4.1.1 Enron – Skandalene

28 November 2001 var det hele derimot brått slutt. Etter en rekke negative avsløringer og hendelser nedgraderte ratingselskapet *Standard & Poor* Enrons obligasjoner til ”junk”. Nedgraderingen medførte at gjeld på 3,9 milliarder $ måtte betales umiddelbart. Samme dag endte Enrons aksjekurs på 61 cents. Til sammenligning hadde aksjene vært verd 90 dollar på det meste![13] Enron maktet ikke å betale sin gjeld, dermed var ikke lengre Enron liv laget. Fire dager etter nedgraderingen, 2 Desember 2001 var den til da største konkursen i historien et faktum.[14]

4.1.2 Markedsverdiprinsippet

Det har vist seg at mye var merkelig med Enrons føringer. Et eksempel er bruk av markedsverdiprinsippet. Finansielle instrumenter kunne ifølge SEC føres til markedsverdier ved kontraktsinngåelse. Markedsverdiprinsippet vil si at det er kjøp og salg av selve kontraktene som genererer inntekter. Handel med *naturgass - future kontrakter* var regnet som et slikt instrument. Enron, på sin side, førte også en hel del annet til markedsverdi, deriblant kontrakter på elektrisk kraft. Dermed behandlet Enron kontrakter på elektrisk kraft som om det var kjøp og salg av kontraktene som genererte inntekter, og ikke leveransen av selve kraften. Enron inntektsførte på den måten all fremtidig fortjeneste fra kraftleveransen på tidspunktet for avtaleinngåelse, i stedet for å periodisere inntektene (jamfør opptjenings-prinsippet). Mot slutten av 90-tallet var markedsverdiprinsippet grunnlag ved beregninger for hele 35 % av Enrons eiendeler. Resultatet var at inntektene ble blåst opp i de årene avtalene ble inngått.

[13] 23. August 2000
[14] Enron var til da den største konkursen i historien med aktiva verd ca 63 mrd dollar. WorldCom kom senere, og hadde til sammenligning eiendeler til en verdi av ca 104 mrd dollar. (Tall hentet fra http://bankrupt.com)

4.1.3 Tvilsomme Føringer

Enron forsøkte i det lengste å unngå å vise tap. Særlig gjaldt dette for områder som kunne regnes som selskapets kjernevirksomheter; trading og risikostyring. Ett av disse var Enron Energy System (EES). Første kvartal 2001 hadde EES i realiteten et tap på 500 millioner dollar. Dette var et tap Enron vegret seg for å offentliggjøre. I stedet kom man opp med en løsning; skjule tapene i en annen av Enrons divisjoner (Engros divisjonen), med det utfallet at EES kunne vise til en profitt på 40 millioner $.

En kan også finne en rekke områder hvor det var inkonsistens mellom måten inntekter og kostnader ble ført på. I Mai 2001 førte Enron salget av tre kraftverk pålydende 1 millard dollar som ordinære inntekter. Inntekter på en milliard dollar, fra *Raptor*'ene, noen av Enrons mange Special Purpose Entities, hadde først blitt ført som ordinære inntekter i regnskapet. Når kontraktene med Raptorene senere ble kansellert ønsket Enron å behandle kostnadene som ekstraordinære.

4.1.4 Skjule Virkeligheten

Det var flere merkverdigheter i Enrons regnskaper. Spesielt gjelder dette Enrons flittige bruk av "off-balance-sheet financing". Deres mange Special Purpose Entities som *Jedi*, *Chewco*, *LJM1* og *LJM2* og *Raptor*'ene skulle sikre Enrons investeringer, samt kjøpe aktiva fra Enron. Disse ble også i stor grad benyttet for å skjule gjeld.

4.1.5 Rettslig Etterspill

Andrew Fastow stod bak utformingen av flere av Enrons tvilsomme SPE. Fastow erklærte seg i Januar 2004 skyldig i konspirasjonsanklager. Flere andre har også erklært seg skyldig for forskjellige forseelser i kjølvannet av Enrons konkurs, inkludert Enrons CAO, Richard Causey, som erklærte seg skyldig i verdipapirsvindel i Desember 2005. 25 Mai 2006 ble for øvrig tidligere CEO, Kenneth Lay, dømt på seks punkter for svindel – mens tidligere CEO og CFO, Jeffrey Skilling, ble dømt for konspirasjon, for innsidehandel og på 17 punkter for svindel.

4.1.6 ARTHUR ANDERSEN

Tilfellet Enron omhandlet ikke bare selve Enron. Også selskapets revisor, Arthur Andersen var innblandet i skandalen. I oktober 2001 virket det sannsynlig at SEC ville starte en etterforskning av Enron. Arthur Andersen, som i Februar 2001 blant annet hadde diskutert hvorvidt de fortsatt ønsket å beholde Enron som klient, begynte en massiv destruering av papirer, under skalkeskjulet at det var Arthur Andersens policy å makulere arbeidspapirer. 15 Juni 2002 ble AA funnet skyldig i å ha ødelagt bevis.[15] Arthur Andersen påstod på sin side at de, som så mange andre, var ofre – ofre i en politisk motivert forfølgelse, og et offer for Enron. Det har vært delte meninger om hvorvidt AA var delaktig i regnskapsmanipuleringen, eller ble ført bak lyset av Enron. I alle tilfeller mistet Arthur Andersen mye av sin troverdighet, og avviklet revisjon av selskaper i August 2002.

4.1.7 "Economic Failure"

Kort tid etter Enrons konkurs fortalte Arthur Andersens CEO, Joseph Berardino, i et intervju med NBCs *Meet the Press* at Enron falt som følge av økonomisk svikt " *This is a company whose business model failed. The accounting reflects the results of business activities. And the way these events were being accounted for were clear to management and to the board…. But at its base, this is an economic failure…"* (Berardino, 2002)

4.1.8 Svar på Skandalene – Sarbanes Oxley

I tillegg til Enron, måtte også selskaper som Adelphia Communication, WorldCom[16] og Global Crossing[17] søke beskyttelse etter "Chapter 11" etter avsløringer av uregelmessigheter i regnskapsføringen. Regnskapssnusk hos disse, samt selskaper som blant annet Tyco og Xerox medførte et krav fra allmennheten om at noe måtte gjøres. Svaret kom i form av en ny lov, hvis navn ble gitt etter den amerikanske senatoren Paul Sarbanes og kongressmedlemet

[15] Dommen mot Arthur Andersen ble senere (Mai 2005) opphevet av amerikansk høyesterett.
[16] Det er interessant å legge merke til at WorldComs revisor var nettopp – Arthur Andersen.
[17] Global Crossing gikk ikke formelt konkurs. De fikk godkjent en plan for å "komme seg" etter Chapter 11-beskyttelse. Ironisk nok var revisor for Global Crossing… Arthur Andersen

Michael Oxley som var ansvarlige for utformingen. Sarbanes-Oxley Act of 2002 ble undertegnet av president George W. Bush 30 Juli 2002.[18]

4.2 Hva er Sarbanes-Oxley Act of 2002 ?

> **…Sparked by dramatic corporate and accounting scandals, the Act represents the most important securities legislation since the original federal securities laws of the 1930s. The Act effects dramatic change across the corporate landscape to re-establish investor confidence in the integrity of corporate disclosures and financial reporting.**
>
> - (Donaldson, 2003)

Sarbanes-Oxley Act of 2002 er, jfr William H. Donaldson, formann i *US Securities and Exchange Commision*, den mest omfattende regnskaps- og selskapslovgivning i USA siden 1930-tallet.[19] SOX kan kort oppsummeres som reguleringer og krav innen områder som revisjon, ledelse, og økonomisk rapportering. I det følgende gis en beskrivelse av de mest sentrale elementene i SOX.

4.2.1 Revisjon

Tidligere har den amerikanske revisjonsbransjen selv hatt ansvaret for å sette standarder for revisjon av børsnoterte selskaper, gjennom *American Institute of Certified Public Accountants (AICPA)*. Etter Sarbanes Oxley Acts **Paragraf 101 til 103** overføres dette ansvaret til en ny og uavhengig organisasjon, ***Public Company Accounting Oversight Board*** *(PCAOB)*. Ethvert revisjonsselskap som reviderer selskaper notert på amerikanske børser er pliktig å registrere seg hos PCAOB. Loven kommer med klare begrensninger til hvilke oppgaver et revisjonsselskap kan påta seg for sin revisjonskunde.[20] Videre stiller SOX krav til rotering av revisor, hvilket innebærer at ingen enkeltperson kan ha hovedansvar for revisjon av samme

[18] Det er verd å merke seg at dette kun var ni dager etter WorldComs konkurs. SOX har for øvrig blitt kraftig kritisert for å bære preg av å være en ”hastelov”.
[19] Securities Act of 1933 og Securities Exchange Act of 1934
[20] Section 201

firma lengre enn i fem etterfølgende år.[21] Endelig stilles det krav til at ethvert selskap notert på amerikanske børser skal ha en egen (uavhengig) revisjonskomité, som ekstern revisor skal rapportere til.[22] Dersom det ikke eksisterer en egen revisjonskomité vil hele styret fungere som dette.

4.2.2 Ledelse

Sarbanes-Oxley Act stiller nye, og større, krav til ledelsen og dens ansvar. En svært sentral paragraf i loven er **Section 302.** Her stilles det krav til at ledelsen skal vedkjenne seg det ansvar som ligger i selskapets finansielle rapport, gjennom å skrive under på at de har gjort seg kjent med rapporten. Videre signeres det på at opplysningene, så langt ledelsen vet, gir et riktig bilde på selskapets finansielle situasjon.

Paragraf 406 pålegger selskapene å opplyse om det foreligger etiske retningslinjer for ansatte i sentrale økonomiske posisjoner. Videre forventes det, av **Paragraf 407**, at enhver revisjonskomité (som nevnt i forrige avsnitt) har en økonomisk ekspert. I den grad etiske retningslinjer ikke foreligger, eller ingen av medlemmene i revisjonskomiteen er såkalte økonomisk eksperter, kreves en skriftlig begrunnelse for disse "manglene".

Sarbanes-Oxley Act skjerper også straffebestemmelsene. **Paragraf 304** innfører krav om tilbakebetaling av incentivbaserte utbetalinger (som bonuser og gevinster på opsjoner) gitt til CEO og CFO dersom selskapet, på grunn av feil i regnskapene som skyldes besvikelser fra ledelsen, må korrigeres sine regnskaper. Samtidig risikerer ledelsen strengere straffer enn tidligere for dokumentforfalskning, dokumentødeleggelse, bedrageri, med mer.[23] Særlig betydningsfull er **Section 906** - vedrørende strafferammen for å signere på riktigheten av selskapets regnskaper i henhold til paragraf 302, vel vitende om at virksomhetens økonomiske rapportene ikke er i overensstemmelse med gjeldende krav. Maksimumsgrensen på bøter økes fra 1.000.000 $ til 5.000.000 $, og fengsel fra maksimum 10 års til 20 års fengsel, for tilsiktede handlinger.

[21] Section 203
[22] Section 301 & 204
[23] Section 802

Etter **Paragraf 402**, forbys personlige lån til ledelsen, dog med visse unntak som for eksempel varekjøp på kreditt. Bakgrunnen for denne bestemmelsen ligger i tidligere praksis, med enorme personlige lån til lederne i selskaper som WorldCom og Tyco. For eksempel lånte Bernard Ebbers 408 millioner dollar av WorldCom mens han var leder for selskapet. Dennis Kozlowski lånte på sin side 242 millioner $ fra Tyco for å dekke utgifter til eiendom, kunst, med mer (Ebeling, 2004).

4.2.3 Økonomisk Rapportering.

Den enkeltbestemmelsen i Sarbanes-Oxley Act som har vært gjenstand for mest diskusjon, er bestemmelsen om intern kontroll over økonomisk rapportering.[24] **Section 404** pålegger ledelsen i børsnoterte selskaper å gi en vurdering av effektiviteten av selskapets interne kontroll over økonomisk rapportering. I tillegg kreves det at revisor skal attestere ledelsens vurderinger. Både ledelsens evaluering av effektiviteten av det interne kontrollsystemet, samt revisors attest skal legges ved selskapets årsrapport. Paragraf 404 må ses i sammenheng med paragraf 302 om ledelsens ansvar, og paragraf 906 om straffeansvar ved å opptre uansvarlig.

Virksomheter plikter, etter **Paragraf 401,** å opplyse om betydelige transaksjoner off-balance, blant annet som følger av Enrons omfattende bruk av Special Purpose Entities (Christiansen; 2003). Dermed skal det ikke være mulig å skjule gjeld i *off-balance sheet vehicles*. Videre kreves det at alle spesielle ordninger og alle forpliktelser (også betingede forpliktelser) som har, eller kan forventes å få, vesentlig innflytelse på regnskapene blir opplyst.

Endelig plikter ethvert selskap - innen rimelig tid - og på en forståelig måte- å opplyse om betydelige endringer i deres økonomiske situasjon[25]. Manglende prosedyrer for å fange opp endringer i omgivelsene vil dermed ikke begrenses til en svakhet i kontrollsystemet, men vil også bli å betrakte som et brudd med loven.

[24] I vedlegg 5 er Securities and Exchange Commission's definisjon av intern Kontroll over økonomisk rapportering (Internal Control over Financial Reporting) gjengitt.
[25] Section 409. I lovteksten benyttes formuleringen "*in plain English*" for å understreke at rapporteringen skal være forståelig.

4.2.4 Øvrige Bestemmelser

SOX inneholder en del sentrale elementer som ikke direkte berører områdene revisjon, ledelse eller økonomisk rapportering. For eksempel gir **Section 806** beskyttelse for ”whistleblowers”. En whistleblower er en ansatt som rapporterer brudd på aksjelovbestemmelsene til eksterne parter, slik som SEC, media, etc. Etter paragrafen er det straffbart å reagere på slik rapportering med virkemidler som trakassering, degradering, suspensjon eller oppsigelse.

Paragraf 307 pålegger advokater å rapportere vesentlige brudd på verdipapirlov som avdekkes i virksomheten - til ledelsen, eventuelt til revisjonskomiteen eller styret, dersom ledelsen ikke handler passende i henhold til bevisene.

5 Revisjon av Interne Kontroller over Økonomisk Rapportering.

Plikt til å ha en viss regnskapsmessig internkontroll er ikke en ny tanke i USA. I 1977, som et resultat av Watergate-etterforskningen, begynte statlige interesser å fatte interesse for intern kontroll (COSO, 1996). Den påfølgende loven om korrupt forretningsskikk ovenfor utlandet[26] inneholdt krav om at selskaper registrert hos SEC må ha et regnskapsmessig internt kontrollsystem for å sikre at ledelsen har kontroll, myndighet og ansvar ovenfor selskapets eiendeler.[27] Året etter offentliggjorde COHEN-kommisjonen[28] sin rapport. COHEN-rapporten gikk ett skritt videre, i det de foreslo å pålegge ledelsen å rapportere effektiviteten av selskapets interne kontroll, samt pålegge revisor å attestere på hvorvidt de er enige med selskapets beskrivelse (COHEN, 1978). Det tok 24 år før forslagene fra COHEN-rapporten skulle bli formelle krav, gjennom SOX §404.

Users of financial information have a legitimate interest in the condition of the controls over the accounting system and management's response to the suggestions of the auditor for correction of weaknesses. Those matters should be disclosed in the proposed report by management. It is consistent with the normal responsibilities for financial reporting that primary reporting responsibility be assigned to management, with a report by the auditor on management's representations. The auditor should report on whether he agrees with management's description of the company's controls and should describe material uncorrected weaknesses not disclosed in that report.

- (COHEN, 1978)

Utdrag fra sammendraget av COHEN-rapporten.

Public Company Accounting Oversight Board forteller i Auditing Standard 2, §27: "*…Because of the potential significance of the information obtained during the audit of the financial statements to the auditor's conclusions about the effectiveness of internal control over financial reporting, the auditor cannot audit internal control over financial reporting without also auditing the financial statements.*"

[26] Unlawful Corporate Payments Act of 1977
[27] US Code, Title 15, Chapter 2B, §78m – (b)(2)(B)
[28] COHEN: "The Commission on Auditors' Responsibilities" - nedsatt I 1974 av AICPA

Med dette sier de altså at revisjon av en virksomhets interne kontroller over økonomisk rapportering krever at revisjonsselskapet også reviderer virksomhetens regnskaper. Dette er for øvrig konsistent med beskrivelsen i SOX § 404, hvor det heter "…*Any such attestation shall not be the subject of a seperate engagement*". Ut i fra dette bør revisor kunne bygge på det arbeidet han har gjort med å skaffe seg en forståelse av intern kontroll gjennom revisjonsoppdraget. Derfor vil også jeg, i dette kapittelet om revisjon av intern kontroll over økonomisk rapportering, bygge på de to foregående delene om intern kontroll.

AS2, punkt 28, forteller hva revisor må foreta seg i forbindelse med revisjon av interne kontroller:

- ***Planlegge oppdraget.***
- ***Evaluere ledelsens vurderingsprosess.***
- ***Skaffe seg en forståelse av interne kontroller over økonomisk rapportering.*** (Dette temaet har blitt nøye behandlet i kapittel 2 og 3, og vil således ikke bli utdypet i denne delen).
- ***Teste og evaluere designeffektiviteten av interne kontroller over økonomisk rapportering.***
- ***Teste og evaluere den operative effektiviteten av interne kontroller over økonomisk rapportering.***
- ***Danne seg en mening av effektiviteten av interne kontroller over økonomisk rapportering.***

5.1 Mangler i Internkontroll

Det er av stor betydning at revisor identifiserer mangler i de interne kontrollene. En mangel i et kontrollsystems utforming forefinnes når en nødvendig kontroll ikke eksisterer, eller ikke er tilstrekkelig utviklet (AS2, §8). Da vil målet med kontrollen ikke kunne nås, på tross av at kontrollen fungerer slik den er designet. Ergo er det en mangel i utformingen. I så måte er det viktig å undersøke hvorvidt kontrollene er i stand til å hindre feil, som kan relateres til regnskapspåstandene, i å oppstå. (Ernst & Young, 2003). En mangel i iverksettingen av en kontroll eksisterer når en kontroll ikke fungerer slik den er designet, eller når de som skal utføre kontrollene ikke innehar riktig kompetanse eller riktig autorisasjon for å gjennomføre kontrollen på riktig måte (AS2, §8).

5.1.1 Betydelig Mangel

En mangel i en kontroll, eller en kombinasjon av kontrollmangler kan ha en negativ innvirkning på en virksomhets evne til å autorisere, initiere, registrere, behandle og/eller rapportere økonomiske data i henhold til god regnskapsskikk. Konsekvensen kan bli feilaktige økonomiske rapporter. Dersom det er mer enn en fjern sannsynlighet for at kontrollen ikke bidrar til å hindre slike feilaktige finansielle rapporter, og feilen er ikke-ubetydelig, er mangelen **Betydelig** (AS2, §9).

5.1.2 Vesentlig Svakhet

Med utgangspunkt i definisjonen for en betydelig mangel, kan det også tenkes at en feil i de økonomiske rapportene ikke bare er "ikke-ubetydelige", men at feilen også må betraktes som vesentlig. I en situasjon hvor en mangel i en kontroll medfører mer enn en fjern sannsynlighet for en feil i de økonomiske rapportene som må betraktes som vesentlig, vil mangel være en **Vesentlig Svakhet** i den interne kontrollen (AS2, §10).

5.2 Planlegging

Revisor må, på samme måte som i forbindelse med revisjon av regnskaper, også sørge for tilstrekkelig planlegging i revisjon (attestering) av interne kontroller over økonomisk rapportering. PCAOBs AS2, punkt 39 oppsummerer en rekke forhold som må vurderes når revisor skal planlegge revisjonsoppdraget:[29]

Revisor vil ha fått kjennskap til virksomhetens intern kontroll over økonomisk rapportering gjennom øvrige oppdrag. Denne kunnskapen må revisor ta med i betraktningen. Revisor må også vurdere type og omfang av allerede tilgjengelig bevis som relaterer seg til internkontrollens effektivitet. Revisor må ta hensyn til eventuelle svakheter i kontrollene som har blitt meddelt virksomhetens revisjonskomité eller virksomhetens ledelse på et tidligere

[29] Flere av elementene som inngår i AS2, §39, om planleggingen av revisjon av interne kontroller over økonomiske rapportering finner en igjen i planleggingen av revisjon av regnskaper – og vil derfor ha flere fellestrekk med elementene som inngår i norsk RS315 "Forståelse av foretaket og dets omgivelser og vurdering av risikoene for vesentlig feilinformasjon".

tidspunkt, og hvorvidt det har blitt foretatt endringer som følger av dette. Eventuelle strafferettslige forhold eller reguleringer som vedrører virksomheten må også vurderes.

Revisor må skaffe seg en forståelse av de forhold som influerer bransjen hvor selskapet opererer, slik som lover og reguleringer, bransjens økonomiske situasjon og utsikter, og hva som er vanlig å bruke av rammeverk for økonomisk rapportering. Videre må revisor skaffe seg en forståelse av foretakets art. Slike forhold er virksomhetens eierskap og kontroll, finansiering, organisering, og struktur.

Revisor må danne seg et foreløpig bilde av vesentlighet, risiko, og andre faktorer av betydning for å kunne bestemme hva som vil være en **Vesentlig Svakhet**.

På bakgrunn av disse momentene danner revisor seg et foreløpig inntrykk av internkontrollens effektivitet.

5.3 Evaluere Ledelsens Vurderingsprosess

Når en virksomhet har implementert et system for internkontroll, skal ledelsen selv evaluere dens effektivitet. Tradisjonelt har intern kontroll ofte vært forbundet med revisjon av et selskap, hvor målet har vært å avdekke hvilke og hvor omfattende revisjonshandlinger revisor skal foreta. Når ethvert børsnotert selskap nå plikter å implementere, og deretter evaluere sin egen intern kontroll, kan sistnevnte ses i sammenheng med krav til revisors uavhengighet. Dersom et selskap skulle kontaktet revisor for å få en evaluering, ville det i praksis betydd at revisor attesterte sitt eget arbeid. Dette ville ikke samsvart med krav om revisors uavhengighet, og forbudet mot å revidere eget arbeid (Taub, 2003). Derfor pålegges ledelsen å evaluere kontrollsystemets effektivitet, mens revisor skal vurdere ledelsens evaluering, og konkludere med hvorvidt de er enige i ledelsens vurdering. Imidlertid anerkjenner SEC behovet for koordinasjon mellom revisor og ledelsen i forhold til å teste og dokumentere effektiviteten av interne kontroller over økonomisk rapportering.[30]

[30] SEC Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports (II)(B)(3)(b)

Ledelsen skal skaffe til veie og opprettholde tilstrekkelig bevis, inkludert dokumentasjon, for å kunne støtte opp under vurderingen av effektiviteten av interne kontroller over økonomisk rapportering. En kan således dele ledelsens vurderingsprosess inn i tester av kontroller og dokumentasjon. Revisor må her ta hensyn til at metodene for å evaluere intern kontroll over økonomisk rapportering vil, og skal, variere fra selskap til selskap (SEC, Final Rule).

5.3.1 Tester av Kontroller

Auditing Standard 2, paragraf 40, lister opp en rekke forhold som revisor må undersøke om ledelsen har tatt hensyn til. Det mest sentrale i denne paragrafen er at ledelsen skal ha testet vesentlige kontroller, og evaluert sannsynligheten for at svikt i kontrollene kan resultere i feil i de økonomisk rapportene – betydningen av slike feil – og om det eventuelt er andre kontroller som vil oppnå de samme målene. Ledelsen skal i så måte ha evaluert både design- og iverksettingseffektiviteten av kontrollene. Dersom det er mangler i kontrollene (se kapittel 5.1), det være seg i designet eller i iverksettingen, må ledelsen vurdere hvorvidt manglene er betydelige, og eventuelt hvorvidt de representerer en vesentlig svakhet. Kontrollene ledelsen bør teste inkluderer:

Kontroller Vedrørende Vesentlige Regnskapsposter som er Inkludert i de Økonomiske Rapportene. Dette er en meget vid definisjon, da det inkluderer initiering, autorisering, registrering, behandling, rapportering og avstemming av kontoer og transaksjoner som inngår i perioderegnskapene.

Kontroller Vedrørende Regnskapsføringens Overensstemmelse med Generelt Aksepterte Regnskapsstandarder. Da SOX er en lov som omhandler selskaper notert på amerikanske børser, vil generelt aksepterte regnskapsstandarder først og fremst forstås som USGAAP. Dersom en tilsvarende bestemmelse om intern kontroll blir vedtatt i Norge, eller EU, vil IFRS og norsk god regnskapsskikk bli mer aktuelt.

Programmer og Kontroller som skal Forhindre, Identifisere og Oppdage Bedrageri. Dette inkluderer bedrageri på alle plan i virksomheten. Å forhindre og oppdage svindel er for øvrig et av hovedmålene til Sarbanes-Oxley Act. Det kan en blant annet se av de økte straffebestemmelsene som følger av loven, og gjennom flere paragrafer som omhandler

programmer for å forhindre, eller identifisere og oppdage bedrageri. Et eksempel på et program for å forhindre bedrageri er ”kravet” til etiske retningslinjer for personer i sentrale økonomiske posisjoner (§406). Et eksempel på et program som skal identifisere og oppdage bedrageri finner vi i §301(4). Der stilles det krav om å opprette prosedyrer som gir ansatte anledning til (konfidensielt) å rapportere mulige uregelmessigheter og tvilsomheter vedrørende regnskaps-føring/revisjon. I tillegg stilles det krav til prosedyrer for håndtering av slike klager. Revisjonskomiteen har det formelle ansvar for at slike prosedyrer eksisterer.
Kontroller, oftest Generelle IT-Kontroller, som Danner et Grunnlag for at andre Kontroller Fungerer som de skal.

Kontroller av Vesentlige Ikke-Rutinemessige Transaksjoner, og Transaksjoner og Poster som Involverer Elementer av Skjønn og Subjektive Vurderinger. I avsnitt 4.1.3 ble det nevnt at Enron solgte tre kraftverk til en milliard dollar, og førte dette som ordinære inntekter. Et slikt salg er nok ment å komme inn under ”ikke-rutinemessige transaksjoner”, hvilket tilsier at salget skulle vært gjenstand for skjerpede kontroller. Salg av halvfabrikata (ofte som intern-salg i bedrifter), hvor markedspriser ikke eksisterer, vil typisk være transaksjoner som inneholder stor grad av skjønn og subjektive vurderinger.

Kontroller på Bedriftsnivå. Disse omhandler blant kontrollmiljøet - som inkluderer ledelsens integritet og etiske verdier, ansvarsfordeling og myndighet, og adferdsregler. Kontroller ved periodeslutt - herunder prosedyrer som nyttes i forbindelse med å føre transaksjoner inn i hovedboken. Kontroller vedrørende ledelsens risikovurderingsprosess, kontroller for å overvåke resultater, samt kontroller for å overvåke andre kontroller – slik som aktiviteten til internrevisjonen og revisjonskomiteen.

5.3.2 Dokumentasjon

Dokumentasjon av interne kontroller er ikke nytt i amerikansk lovgivning. Securitites Exchange Act krever at selskaper notert på amerikanske børser registrerer og tar vare på opplysninger som i tilstrekkelig grad reflekterer selskapets transaksjoner og kontoer.[31] Dermed blir det nye med Sarbanes-Oxley først og fremst at ledelsen skal evaluere effektiviteten av det interne kontrollsystemet, og at dette skal rapporteres (Taub, 2003).

[31] Securities Exchange Act §13(b)(2)(A)

Karakter og omfang av dokumentasjon av intern kontroll, og de vurderinger som ligger til grunn for evaluering av kontrollers effektivitet, har vært gjenstand for mye debatt. Først og fremst skyldes nok dette at de fleste virksomheter ønsker å oppfylle de formelle krav og unngå anmerkninger som følger av mangelfull dokumentasjon. Samtidig har det vært begrensede (manglende) retningslinjer i Sarbanes-Oxley Act så vel som fra SEC hva angår dokumentasjonsomfanget.

Imidlertid er det, i Auditing Standard 2 - punkt 42, listet en del krav til dokumentasjonen som må være oppfylt for at revisor skal kunne anse dokumentasjonen som tilstrekkelig for å støtte opp under ledelsens vurdering av effektiviteten av internkontrollen. Siden ledelsen ønsker å unngå anmerkninger som følger av utilstrekkelig dokumentasjon, vil denne listen kunne fungere som en sjekkliste også for ledelsen.

- Dokumentasjonen må beskrive designet av kontroller for alle relevante regnskapsmål relatert til alle vesentlige regnskapsposter og opplysninger i de økonomiske rapportene. Dokumentasjonen må inneholde de fem komponentene i en internkontroll, og kontroller på både aktivitets og virksomhetsnivå.
- Det må være beskrevet hvordan vesentlige transaksjoner initieres, autoriseres, registreres, behandles og rapporteres.
- Tilstrekkelig informasjon om transaksjonsstrømmer til å identifisere hvor vesentlige feil og mangler kan oppstå
- Kontroller designet for å forebygge og oppdage bedrageri, også med tanke på de som utfører kontrollene. Ansvarsfordeling og separasjon av ulike funksjoner bør fremgå.
- Dokumentasjon vedrørende årsoppgjørsprosessen
- Dokumentasjon vedrørende beskyttelse av eiendeler
- Resultatet av ledelsens tester og evalueringer

Når PCAOB i punkt 43 åpner for forskjellig utforming av dokumentasjonen, det være seg gjennom kombinasjoner av virksomhetspolitikk, prosessmodeller, flowcharts, jobbeskrivelser, dokumenter, eller skjema, har de på en fornuftig måte tatt hensyn til at virksomheter varier, både konkret i forhold til andre virksomhet, og med tanke på utforming av internkontrollen.

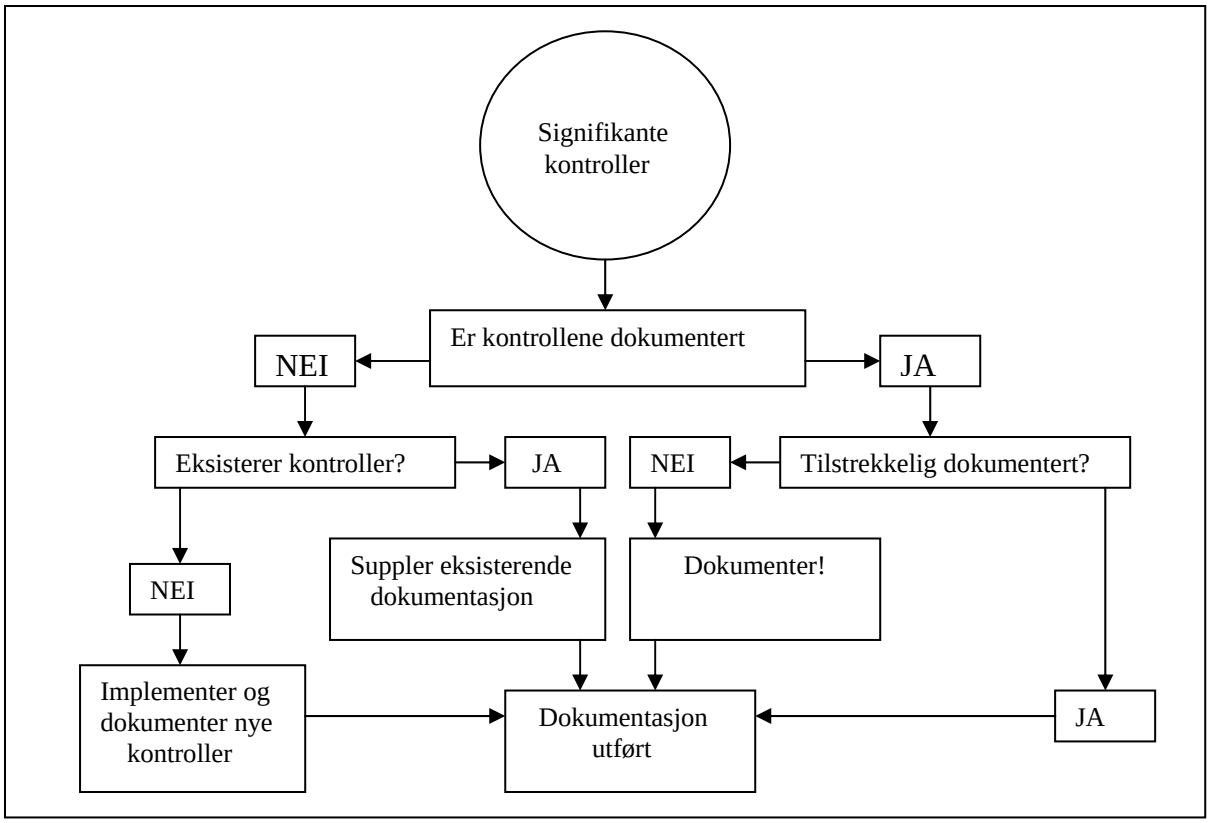


Fig 5.1 - Vurdering av dokumentasjons tilstrekkelighet. Kilde: Ramos, 2004

Dokumentasjon gir ikke konkrete bevis på at kontrollsystemet er effektivt. For eksempel vil en positiv kunngjøring vedrørende selskapets verdier gi et inntrykk av at selskapet har et sterkt kontrollmiljø, men det vil ikke være bevis i seg selv på at kontrollmiljøet fungerer. Tilsvarende vil ikke mangelfull dokumentasjon nødvendigvis bety at interne kontroller ikke eksisterer og fungerer. Dokumentasjon skal derimot øke påliteligheten av de interne kontrollene - gjennom å gjøre informasjon vedrørende de prosedyrer som gjennomføres, når, og av hvem lettere tilgjengelig. Dermed bidrar dokumentasjonen til å bekrefte at de interne kontrollene samsvarer med de risiki som har blitt identifisert. Dokumentasjon skal også identifisere endringer. Endringer i dokumentasjonen skal representere endringer i de interne kontrollene. Dermed vil en gjennom tilstrekkelig dokumentasjon, og overvåking av dokumentasjonen, også overvåke endringer i det interne kontrollsystemet. (Ramos, 2004).

5.3.3 Ledelsens Rapport[32]

SEC har i final rule, *Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports*, laget en liste over hva internkontrollrapporten må inneholde:[33]

- En erklæring på ledelsens ansvar for å etablere og opprettholde tilstrekkelig intern kontroll for finansiell rapportering.
- Det skal fortelles hvilket rammeverk som er benyttet for å evaluere effektiviteten av selskapets internkontroll.
- Ledelsens vurdering av effektiviteten av selskapets internkontroll, slik den vurderes ved regnskapsårets slutt. Som en del av vurderingen skal ledelsen avgi en erklæring på hvorvidt internkontrollen er effektiv eller ikke. Det skal opplyses om identifiserte vesentlige svakheter i den interne kontrollen. Er det en eller flere vesentlige svakheter, kan **ikke** ledelsen konkludere med at selskapets internkontroll er effektiv.
- En erklæring på at selskapets eksterne revisors attestasjon til den interne kontroll er inkludert i årsrapporten.

5.3.3.1 Ledelsens Ansvar[34]

Første punkt omhandler ledelsens ansvar, jfr Sarbanes Oxley Act, section 302 og 404. CEO, CFO eller personer som innehar tilsvarende oppgaver skal signere på at man har gjort seg kjent med årsrapporten. Signerende personell skal da bekrefte at de ikke har kjennskap til vesentlige feil i rapporten. Det er da selvfølgelig ikke tilstrekkelig å lukke øynene for eventuelle vesentlige feil. Tvert imot skal ledelsen aktivt gå inn for å sikre en autentisk regnskapsrapportering. En viktig del blir derfor å sikre at interne kontroller over økonomisk rapportering er tilfredsstillende. SOX gir ledelsen det formelle ansvar for at selskapet har tilstrekkelig intern kontroll, og pålegger ledelsen å erkjenne at dette ansvaret. Eventuelle vesentlige svakheter som ledelsen har avdekket i den interne kontrollen, eller misligheter som ledelsen har kjennskap til, skal meddeles selskapets revisor og revisjonskomité. Endelig kreves det at selskapet skal opplyse om eventuelle betydelige endringer i det interne kontrollsystemet i løpet av regnskapsåret.

---

[32] Vedlegg 2 viser et eksempel på ledelsens rapport, fra ledelsen og revisjonskomiteen i Pfizer Corp, for regnskapsåret 2006.
[33] (II)(B)(3)(a)
[34] Vedlegg 4 viser et eksempel på en ansvarserklæring, tilhørende FORM 10-K, slik den er utrykt av CEO i Exxon, Rex W. Tillerson (2006).

5.3.3.2 Bruk av Rammeverktøy

Punkt 2 omhandler bruk av rammeverktøy. SOX er ikke i seg selv et rammeverk for implementering av intern kontroll. Det er derfor forventet at et på forhånd godkjent rammeverk benyttes, og at det er opplyst om hvilket rammeverk som er brukt. De fleste selskaper vil nok benytte rammeverktøyet COSO, men også rammeverktøyene Guidance on Assessing Control (Canada) og Turnbull (UK) er nevnt som passende rammeverk for implementering av intern kontroll.[35] Royal Dutch Shell er et eksempel på selskap som sannsynligvis vil bruke et annet rammeverk enn COSO i sin implementering av internkontroll, når de innen utgangen av 2006 skal møte kravene. I årsrapporten sendt til SEC, FORM 20-F for 2005, skriver Royal Dutch Shell: *"…The Group's financial, operational and compliance controls are subject to regular review by the Board in respect of process and effectiveness. The Directors consider that these internal control arrangements are compatible with the guidance for directors published in September 1999 (known as the Turnbull Guidance) in relation to the internal control provisions of the Combined Code."*

5.3.3.2 Ledelsens Erklæring Vedrørende Internkontroll Over Økonomisk Rapportering

Prosessen som skal lede fram til ledelsens erklæring har, med unntak av selve testingen av kontroller, blitt behandlet så langt i utredningen. Tester og evaluering av interne kontroller vil bli behandlet i avsnitt 5.3 og 5.4. Når ledelsen skal teste og evaluere de interne kontrollene, vil det i stor grad foregå på samme måte som når revisor skal teste og evaluere virksomhetens interne kontroller. Selv om revisor og ledelsen bør koordinere arbeidet, må imidlertid begge parter gjennomføre tester av, og evaluere, de interne kontrollenes effektivitet.

Sammen med revisors uttalelser, vil ledelsens erklæring på de interne kontrollenes effektivitet være det mest sentrale i internkontrollrapporten. Derfor stiller også SEC krav til innholdet. Vurderingen skal inneholde en konklusjon på hvorvidt virksomhetens interne kontroll over økonomisk rapportering er **Effektiv**, i tillegg til spesifikt å inneholde opplysninger om eventuelle **Vesentlige Svakheter** som ledelsen har avdekket.

[35] SECs final rule *" Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports" (II)(B)(3)(a)*

En fullverdig vurdering av det interne kontrollsystemet, uten vesentlige merknader, vil kunne se slik ut:

> **Management assessed the effectiveness of the Company's internal control over financial reporting as of December 31, 2005. In making this assessment, management used the criteria set forth by the Committee of Sponsoring Organizations of the Treadway Commission in Internal Control-Integrated Framework. Based on our assessment and those criteria, management believes that the Company maintained effective internal control over financial reporting as of December 31, 2005**
>
> - (Pfizer, 2006)

Utdraget er hentet fra årsrapporten til Pfizer Inc.

5.3.3.3 Erklæring på Revisors Kjennskap til Ledelsens Vurdering

Siste punkt omhandler revisors rolle. Ekstern revisor skal ha blitt gjort kjent med ledelsens vurdering av den interne kontrollen, og ledelsen skal her erklære at så er tilfelle.

5.4 Evaluering av Interne Kontrollers Utformingseffektivitet

Internkontroll over økonomisk rapportering er effektivt utformet når kontrollene, så fremt de er iverksatt, forventes å forhindre eller oppdage feil eller misligheter som kan forårsake vesentlig feilinformasjon i en virksomhets regnskaper. Revisor vil gjennom forespørsler av ledelse og personell, gjennomgang av dokumenter, observasjon av kontroller, og gjennom å følge informasjonsgangen gjennom hele transaksjonsstrømmer, kunne skaffe seg en oversikt over hvordan systemet er designet. Ernst & Young (2003) beskriver tre steg som må gjennomføres for at utformingen av kontrollene skal kunne dokumenteres og evalueres:

1. Fastslå hvorvidt identifiserte signifikante risiki berøres av en eller flere av de identifiserte kontrollene.
2. Fastslå hvorvidt kontrollene som retter seg mot de identifiserte risiki er tilstrekkelig designet for å oppdage vesentlig feilføringer, både i forhold til feil og misligheter.
3. Gjennomgå signifikante kontroller for å fastslå hvorvidt de faktisk er iverksatt.

De prosedyrene revisor foretar for å evaluere effektiviteten av internkontrollenes utforming, vil også bidra til å sørge for bevis vedrørende kontrollenes iverksettingseffektivitet. Det er begrenset hvor meningsfullt det vil være å lage prosedyrer for å teste kontroller som ikke er godt nok designet, og kontroller som ikke blir benyttet.

5.5 Testing og Evaluering av Interne Kontrollers Iverksettingseffektivitet

En kontrolls operative effektivitet tar hensyn til hvordan kontrollen har blitt anvendt, konsekvensen av anvendelsen, og hvem som har anvendt den (AU 319). Effektiviteten av iverksettingen finner en gjennom å teste kontrollene. For at det skal være hensiktsmessig å utføre tester på kontrollene, bør kontrollenes utforming allerede ha blitt vurdert til å være effektive. I motsatt fall vil det ikke være hensiktsmessig å teste kontrollene. Anta for eksempel at en person registrerer en transaksjon, for deretter selv å utføre kontrollen. I en slik situasjon er det relativt stor risiko for at kontrollen ikke fungerer effektivt, selv om den i utgangspunktet kunne bidratt til å hindre en feil i å oppstå. På samme måte som at revisor ikke bør revidere sitt eget arbeide, bør heller ikke en ansatt kontrollere sitt eget arbeide.

5.5.1 Valg av Kontroller for Testing

Når revisor skal teste den operative effektiviteten av kontrollene, bør vedkommende ta hensyn til at ikke alle identifiserte kontroller må testes. For eksempel kan étt spesifikt regnskapsmål støttes opp av flere kontroller. I slike tilfeller er det tilstrekkelig kun å teste enkelte nøkkelkontroller. Tilsvarende vil det i andre tilfeller kunne være en spesifikk kontroll som dekker mer enn én regnskapspåstand. Da holder det selvfølgelig å teste kontrollen én gang. Hvilke kontroller som skal testes avhenger av revisors vurdering av hvorvidt kontrollene effektivt vil støtte opp under de tilknyttede regnskapspåstandene, og hvorvidt enkelte kontroller kan testes mer effektivt enn andre (Ernst & Young, 2003).

Valg av hvilke kontroller som bør testes henger sammen med hvilke kontroller som avdekker identifiserte risiko i forhold til de enkelte regnskapsmålene. De kontrollene som anslagsvis gir størst overbevisning om at regnskapspåstandene er korrekte er også de kontrollene hvor en

bør fokusere testene (AU 319). Særlig bør det rettes oppmerksomhet mot de kontroller som har en viss risiko for ikke å fungere, til tross for effektivt design. PCAOB angir i AS2 (§83) enkelte slike indikasjoner:

- ***Hvorvidt det har vært endringer i omfanget eller karakteren av transaksjoner - som kan påvirke en kontrolls utformings- eller iverksettingseffektivitet på en uheldig måte.*** (Dette forstås som risiko for at de som utfører kontrollene ikke er oppmerksomme på nye former for feil eller risiki.)
- ***Endringer i kontrollers design.***
- ***I den grad en kontroll avhenger av effektiviteten av andre kontroller.*** (For eksempel en kontroll som avhanger av et effektivt kontrollmiljø.)
- ***Hvorvidt det har vært endringer av nøkkelpersonell som utfører eller overvåker kontrollene.*** (Dette forstås som risiko for at de som utfører kontrollene ikke har nok erfaring.)
- ***Hvorvidt kontrollene er manuelle eller systembaserte.***
- ***Kontrollenes kompleksitet.***

I kapittel 5.3.1 ble det beskrevet en del kontroller ledelsen bør teste. Når revisor retter oppmerksomheten mot kontroller som har en viss risiko for ikke å fungere, gjelder dette først og fremst de kontrollene som er beskrevet i nevnte kapittel.[36]

I forhold til punktene over må en skille mellom forventninger og risiko. Kontroller som har en viss risiko for ikke å fungere bør som nevnt testes. Dersom en imidlertid på forhånd forventer et større antall feil i kontrollene, vil kontrollene ikke kunne beregnes som effektive, og det vil være lite hensiktsmessig i det hele tatt å teste kontrollene.

[36] Kontroller vedrørende vesentlige regnskapsposter som er inkludert i de økonomiske rapportene; kontroller vedrørende regnskapsføringens overensstemmelse med generelt aksepterte regnskapsstandarder; programmer og kontroller som skal forhindre, eller identifisere og oppdage bedrageri; kontroller som danner et grunnlag for at andre kontroller fungerer som de skal; kontroller av vesentlige ikke-rutinemessige transaksjoner, og transaksjoner og poster som involverer elementer av skjønn og subjektive vurderinger, og kontroller på bedriftsnivå (herunder kontroller vedrørende regnskapsavslutningen).

5.5.2 Valg av Metode for Testing

Testene vil normalt bestå av prosedyrer som forespørsler av ledelse og ansatte, gjennomgang av dokumenter, rapporter og elektroniske filer, observasjon av utførelsen av kontrollen, og gjennomføring av selve kontrollen (AU 319). Gjennomgang av selve kontrollen vil for eksempel kunne være å foreta en avstemming. Gjennom å foreta avstemming av en eller flere poster, kan revisor få en bekreftelse på hvorvidt prosedyrene er riktig fulgt. Observasjon kan være å overvåke selve avstemmingen, mens gjennomgang av dokumenter kan være å se på hvordan avstemningen har blitt foretatt. Forespørsler vil, i forhold til samme eksempel, typisk kunne være å spørre ansatte hvorfor og hvordan de foretar en avstemming. Forespørsler kan bestå av både muntlige så vel som skriftlige spørsmål, og det bør stilles spørsmål vedrørende hva ansatte gjør, og hva ansatte ville gjort, i ulike tenkte situasjoner.

Selv om forespørsler nok vil bli mest benyttet, bør det være naturlig med en kombinasjon av flere av ulike typer tester. Merk at forespørsler alene ikke er tilstrekkelig (AS2, §95; RS315, §55), da det kan være uoverensstemmelser mellom hva som blir sagt og hva som blir gjort. Dette kan skyldes at den personen som utfører (eller burde utført) kontrollen, antakeligvis vil bekrefte kontrollens funksjon, enten fordi det er personens overbevisning, eller for å unngå reprimande. I forhold til behovet for å teste kontroller viser AS2 (§97) til et eksempel, hvor en kontrollfunksjon innebærer å signere på fraktbrev. Imidlertid gir ikke signaturen i seg selv noen bekreftelse på at varene er gjennomgått. For å få en bekreftelse på at forsendelsen inneholder riktige varer og riktig antall, vil en test av kontrollen kunne være å gjennomgå forsendelsen på nytt.

5.5.3 Valg av Tidspunkt for Test av Kontroller

Når, og over hvor lang tid de ulike kontrollene skal testes vil i utgangspunktet være en vurdering av revisor. Imidlertid er det et par hensyn som bør tas i forbindelse med valg av tidspunkt. Først og fremst må testene foregå over en periode som i tilstrekkelig grad kan gi svar på hvorvidt de vesentlige kontrollene er operativt effektive ved det tidspunktet evalueringen foretas. (Eilifsen et.al, 2006). Hvor langt denne perioden strekker seg, vil derimot være en skjønnsmessig avgjørelse for revisor, basert på hvilken type test som gjennomføres, hvor ofte kontrollen foretas, og de ulike prosessene som involveres. (Ernst & Young, 2003).

Revisor må ta hensyn til at kontroller som har blitt testet i begynnelsen av året, ikke nødvendigvis er like effektive nesten et år senere. På den andre siden må han også ta hensyn til at dersom testene foretas nært opp til årsoppgjøret, vil det være liten tid til å foreta rettelser i henhold til oppdagede svakheter. Spesielt gjelder dette i tilfeller hvor det foretas undersøkelser. Personer som blir spurt må få tilstrekkelig tid til å svare, og ved manglende svar må revisor ha tilstrekkelig tid til å purre på svarene. I tillegg krever det en viss tid til å evaluere svarene (Ramos, 2004). Endelig finnes det enkelte tester som kun kan foretas etter at året er ferdig, som for eksempel tester av kontroller som vedrører årsoppgjøret.

5.5.4 Omfanget av Test av Kontroller

Omfanget av tester av kontroller vil på samme måte som metode og tidspunkt for testene avhenge av revisors vurderinger, og kunne variere fra år til år. Det vesentlige er at testene gjør revisor i stand til å evaluere hvorvidt kontrollene for å sikre korrekt finansiell rapportering fungerer effektivt. For eksempel vil omfanget av tester av systembaserte kontroller kunne reduseres i forhold til for tilsvarende manuelle kontroller, da systembaserte kontroller i utgangspunktet er sikrere enn manuelle kontroller. I enkelte tilfeller vil testing av én enkelt systembasert kontrolls iverksetting være tilstrekkelig for å sikre en relativt høy grad av sikkerhet for at kontrollen er effektiv, gitt at de generelle IT-kontrollene også fungerer effektivt (AS2, §105).

Alt i alt vil det være opp til revisor å avgjøre hvilke og hvor mange kontroller som skal testes, når, og i hvilken grad. Ernst & Young (2003) oppgir imidlertid et par faktorer som bør hensynstas i forhold til å fastsette omfanget av testene.

Hyppigheten i Kontrollenes Utførsel.

En manuell kontroll som utføres sjeldent, for eksempel en gang i måneden, krever færre tester enn en kontroll som utføres ofte, for eksempel for hver transaksjon. Dette fordi feil akkumulert sett kan få vesentlig innflytelse på regnskapene. Som nevnt tidligere vil forebyggende kontroller ofte bli utført i sammenheng med enkelte transaksjoner, mens oppdagende kontroller ofte utføres på grupper av transaksjoner. Derfor bør det utføres flere tester for forebyggende kontroller, enn tilfelle er for oppdagende kontroller, for å oppnå samme grad av sikkerhet vedrørende kontrollens effektivitet.

I Hvilken Grad Feil som Kontrollen er Ment å Oppdage vil få Vesentlig Innflytelse på Regnskapene.

Kontroller som har vesentlig betydning for avdekking av en spesifikk risiko, eller kontroller som avdekker risiko som er vurdert som sannsynlig, eller vurdert å få stor konsekvens, må testes mer omfattende enn mindre betydningsfulle kontroller (selv om også de sistnevnte godt kan være definert som vesentlige). Dette gjelder også for kontroller som dekker flere regnskapsmål, hvilket tilsier at en svakhet i disse kontrollene vil få større total betydning i regnskapene enn tilfellet er ved svakheter i andre kontroller.

I Hvilken Grad Revisor Ønsker å Basere Evalueringen på en eller flere Kontroller

I den grad revisor ønsker å basere vurderingen av en regnskapspåstands riktighet på test av én enkelt kontroll, bør denne testes grundigere enn tilfelle ville vært om flere kontroller kontrollerte samme regnskapspåstand.

I Hvilken Grad en Kontroll Virker å Fungere Effektivt.

Dersom det er mye som tyder på at en kontroll fungerer effektivt, kan en begrense antall tester i forhold til om det ikke er noen indikasjoner på kontrollens effektivitet. I motsatt fall, dersom utførelsen av en kontrollaktivitet ikke kan gi nevneverdig bevis for at kontrollen i det hele tatt fungerer, vil det ikke engang være noe poeng i å teste kontrollen, da kontrollen i seg selv antakeligvis er bortkastet. Ved komplekse eller skjønnsbaserte kontroller bør kompetansen til de personer som utfører kontrollene også tas med i betraktning når omfanget av kontroller skal bestemmes.

5.5.4.1 Bruk av Statistiske Metoder

I en del tilfeller vil revisor støtte seg til statistiske metoder for å beregne stikkprøvestørrelser når han skal vurdere hvor mange kontroller som skal testes. Utgangspunktet er da at man basert på en stikkprøve kan vurdere sannsynligheten for at kontrollene faktisk er effektive. Ved bruk av statistiske metoder må en forstå (og akseptere) at feil kan oppstå. En operer da med to typer feil; Type I- og Type II-feil.

I forhold til revisjon og intern kontroll definerer en Type I-feil som tilfeller hvor en konkluderer at en intern kontroll ikke er effektiv, mens den i virkeligheten er det. Type II-feil

blir da tilfeller hvor en konkluderer at en intern kontroll er effektiv, mens den i virkeligheten ikke er det (Eilifsen et al, 2006). Intern kontroll over økonomisk rapportering etter Sarbanes-Oxley Act, har som mål å sikre korrekt finansiell rapportering. Det overordnede målet vil derfor først og fremst være å forhindre Type II-feil i å oppstå. Revisor, som skal vurdere effektiviteten av det interne kontrollsystemet, bør derfor søke å unngå tilfeller hvor en konkluderer at en kontroll er effektiv, dersom den i virkeligheten ikke er effektiv.

Når revisor skal ta stikkprøver av kontrollene, bør han ha klart definert hva som er populasjonen. Betydningen av dette forstår en ved hjelp av følgende eksempel, som er hentet fra Eilifsen et.al (2006): Gitt at kontrollen som skal testes er *hvorvidt alle forsendelser blir fakturert*. I så måte er det antall forsendelser som er populasjonen. Dersom fakturaer benyttes som populasjon, vil ikke de forsendelser som ikke har blitt fakturert inkluderes, og poenget med testen er borte. Videre er det essensielt å forstå at feil kan opptre systematisk. For eksempel kan feil oppstå én fast dag i uken, fordi en ansatt (som kun arbeider denne dagen) ikke utfører prosedyrene riktig. Derfor bør utvalget, altså stikkprøven, plukkes tilfeldig fra hele populasjonen, slik at kontroller foretatt alle dager har lik mulighet for å bli valgt. Systematisk utplukking av stikkprøven, eksempelvis test av kontroller foretatt på tirsdager, vil ikke inkludere feil som er begått fredag, og testen vil miste mye av sin verdi.

I forhold til hvor stor stikkprøve bør være, oppgir Eilifsen et al (2006) tre(fire) faktorer som vil ha innvirkning på valg av stikkprøvens størrelse.

Konfidensnivå

Første faktor er konfidensnivå. Det vil si den akseptable risiko for at kontrollen feilaktig vurderes å være effektiv. For eksempel kan målet være å kunne si, med 95 % sikkerhet (konfidensnivå), at en kontroll er effektiv i minst 99 % av tilfellene. Større stikkprøve betyr at en med høyere sikkerhet kan oppnå målet.

Akseptert Avvik

I beskrivelsen over er akseptert feilmargin 1%. Normalt vil en (lav) akseptert feilmargin være i område 3-5 %. Dess høyere feilmargin en aksepterer før en konkluderer med at kontrollene ikke er effektive, dess mindre behøver stikkprøven å være.

Forventet Feilmargin

Tredje faktor er forventet feilmargin i populasjonen, ofte basert på historiske data. Dersom en forventer at feilmargingen er større i populasjonen, enn hva som kan aksepteres i stikkprøven, vil det ikke være hensiktsmessig å utføre statistisk testing. Det lar seg ikke gjøre å få større sikkerhet i en stikkprøve enn tilfelle er i populasjonen stikkprøven er en del av.

Populasjonsstørrelse

Siste faktor er kun gjeldende i tilfeller med små populasjoner (altså få kontroller). I en populasjon på over 500 vil imidlertid ikke denne faktoren være gjeldende, da høyere stikkprøver ikke vil øke graden av sikkerhet. Populasjonsstørrelsen kan derimot ha betydning i kontroller som utføres én gang daglig. Det skulle i tilfelle tilsi 365 kontroller i året. Dess flere kontroller som gjennomføres (inntil 500) – dess flere tester må gjennomføres for å få rimelig sikkerhet for kontrollenes effektivitet.

Med utgangspunkt i faktorene nevnt over, kan statistiske beregninger avdekke hvor mange stikkprøver som må tas. Størrelsen av stikkprøven avhenger av regnskapspåstandenes vesentlighet (Ernst & Young, 2003). Dersom regnskapspåstandene er av vesentlig betydning, bør testene gi 95 % sannsynlighet for at feilmarginen ikke overstiger 5 %. Dermed skulle, så fremt feil ikke oppdages, en stikkprøvestørrelse på 60 kontroller være tilstrekkelig. I tilfeller hvor feilene ikke betraktes som like vesentlige, vil 90 % sikkerhet for at feilmarginen ikke overstiger 10 % være nok. I så fall er et utvalg på 25 kontroller tilfredsstillende.

5.5.4.2 Bruk av Andres Arbeid.

> **In all audits of internal control over financial reporting, the auditor must perform enough of the testing himself or herself so that the auditor's own work provides the principal evidence for the auditor's opinion.**
>
> - (AS2, §108)

Revisor kan altså benytte seg av det arbeidet som er gjort innad i en virksomhet for å evaluere internkontrollenes effektivitet. Dette arbeidet kan blant annet være foretatt av en særskilt opprettet prosjektgruppe, internrevisjonen, eller revisjonskomiteen. Imidlertid skal revisor selv stå for hovedtyngden av bevisene som leder til revisors vurdering.

I den grad revisor velger å benytte andres arbeid som en del av bevismaterialet, må revisor ta hensyn til enkelte faktorer. Dess større effekt en eventuell feil vil ha på regnskapene, dess viktigere er det at revisor selv tester og kommer fram til bevis for effektiviteten av kontrollen(e) som skal forhindre eller avdekke feilen. Videre bør ikke revisor benytte seg av andres arbeid når det gjelder kontroller hvor effektiviteten bestemmes av subjektive vurderinger og skjønn. Revisor skal ikke basere sin vurdering på andres arbeid når det gjelder kontrollmiljøet, ei heller i tilfeller hvor det er risiko for at ledelsen overstyrer kontrollene (AS2, §112).

Dersom revisor, etter å ha vurdert de forhold som er nevnt over, velger å benytte andres arbeid – må revisor foreta en vurdering av kompetansen og objektiviteten til de personene, hvis arbeid revisor ønsker å benytte. Dess bedre kompetanse (formell utdanning og erfaring), dess mer kan revisor stole på deres arbeid. Eksempelvis vil en kunne forvente at internrevisjonen i en virksomhet har en relativt høy grad av kompetanse. Imidlertid vil ikke revisor kunne stole på arbeidet fra personer som har en lav grad av objektivitet, selv om vedkommende har høy kompetanse. En faktor som kan bidra til redusere objektiviteten vil for eksempel være et tilfelle hvor det er en nærstående slektning av den som utfører kontrollen som tester hvorvidt kontrollene er riktig utført (AS2, §§117-121).

For å få rimelig sikkerhet for kvaliteten og effektiviteten av det arbeidet andre har gjort, må revisor foreta tester av deres arbeid. Revisor bør da enten gjenta tester av kontroller, eller teste kontroller som tilsvarer de kontrollene som allerede har blitt testet (AS2, §123).

5.6 Revisors Vurdering

Når revisor skal danne seg en mening om effektiviteten av virksomhetens intern kontroll over økonomisk rapportering, må revisor evaluere de bevis han har fått gjennom revisjonshandlingene. Revisor skal da ta hensyn til resultater fra substanskontroller som er foretatt som en del av revideringen av regnskapet og de resultater han har fått gjennom tester og evaluering av kontrollers design og utforming. Revisor skal vurdere nøyaktigheten av ledelsens vurdering av de interne kontroller, og hvorvidt vurderingen er tilstrekkelig

dokumentert. Revisor går også gjennom eventuelle svakheter som har blitt oppdaget i de interne kontrollene (AS2, §127).

5.6.1 Revisors Rapport

Revisor skal i rapporten gi svar for hvorvidt han er enig med ledelsens vurdering av effektiviteten av interne kontroller over økonomisk rapportering, og avgi sin egen erklæring på hvorvidt han mener de interne kontrollene er effektive. En ren beretning i en revidering av interne kontrollers effektivitet er en beretning hvor revisor anser de interne kontrollene som effektive. Revisor kan kun utstede en ren beretning når det ikke har blitt oppdaget **Vesentlige Svakheter**, og når det ikke har forekommet **Begrensninger i Revisors Arbeid** (AS2, §129).

5.6.1.1 Begrensninger i Revisors Arbeid

Rammeverk for Attestasjonsoppdrag (§55) viser til to typer vesentlige begrensninger i revisors arbeid. Revisor kan bli hindret i å innhente nødvendig bevis som følger av omstendighetene rundt oppdraget, og revisor kan bli pålagt en begrensning i å innhente bevis av den ansvarlige eller engasjerende part. Ved slike begrensninger skal revisor utstede en attest med forbehold, en konklusjon på at han ikke kan uttale seg, eller trekke seg fra oppdraget (AS2, §178). Hva revisor velger å gjøre avhenger imidlertid av omfanget av begrensningen. Dersom begrensningene skyldes påleggelser fra ledelsen, bør imidlertid revisor enten frastå fra å konkludere, eller trekke seg fra oppdraget.

5.6.1.2 Vesentlig Svakhet

Revisor må vurdere identifiserte mangler i internkontrollen, for å avgjøre om manglene er betydelige, og i så fall, hvorvidt de også innebærer en vesentlig svakhet i internkontroll over økonomisk rapportering. Mangler har blitt behandlet i kapittel 5.1, men det kan likevel være på sin plass med en gjentakelse av definisjonen av en vesentlig svakhet: *I en situasjon hvor en mangel i en kontroll medfører mer enn en fjern sannsynlighet for en feil i de økonomiske rapportene som må betraktes som vesentlig, vil mangel være en vesentlig svakhet i den interne kontrollen.* Vesentlige feil er, som nevnt i avsnitt 3.1.2, feil som *kan påvirke økonomiske beslutninger som treffes av brukerne på grunnlag av regnskapet.*

Når revisor vurderer betydningen av en mangel, vurderer revisor størrelsen på feilen som mangelen, eller kombinasjonen av mangler, kan resultere i. Revisor vurderer også sannsynligheten for at en slik feil kan oppstå (AS2, §131).

Sannsynligheten for at en mangel kan resultere i en feil som får innflytelse på regnskapene avhenger blant annet av hvorvidt det er nærstående parter involvert i transaksjonene; hvor komplisert transaksjonene er; om priser bygger på subjektive vurderinger; hvorvidt eiendeler er utsatt for tap eller underslag; og mulige fremtidige konsekvenser av mangelen. Størrelsen på feilen avhenger først og fremst av mengden og størrelsen på de transaksjoner og de kontoer som berøres av feilen.

Mangler som Betraktes som Betydelige – eller Vesentlige Svakheter.

Dersom revisor i løpet av revideringen av internkontrollen, eller revidering av regnskapene, oppdager vesentlige feil som virksomhetens internkontroll ikke har identifisert, er dette en betydelig mangel, og en sterk indikasjon på en vesentlig svakhet i internkontrollen. (AS2, §140)

Ikke tilstrekkelig dokumentasjon, og ikke tilstrekkelig bevis til å større opp under ledelsens vurdering av effektiviteten av internkontroll over økonomisk rapportering er en mangel i kontrollsystemet. Revisor vurderer hvorvidt mangelen er så graverende at det regnes som en betydelig mangel, og eventuelt en vesentlig svakhet. Manglende dokumentasjon vil også kunne ses på som en begrensning i grunnlaget for attesteringen. (AS2, §§45-46,138).

En ineffektiv revisjonskomité regnes som en betydelig mangel, og ofte også en vesentlig svakhet. En ineffektiv revisjonskomité har en blant annet dersom revisjonskomiteen ikke kjenner sine arbeidsoppgaver, ikke har tilstrekkelig oversikt over regnskapsrapporteringen og internkontrollen, eller ikke har tilstrekkelig formell kompetanse (AS2, §§55-59,140). I SOX kreves det dessuten at alle medlemmene i revisjonskomiteen skal være uavhengig av virksomheten.[37] Imidlertid har dette vært gjenstand for en del debatt, da enkelte land, for eksempel Tyskland, krever at minst en av medlemmene i revisjonskomiteen faktisk er tilknyttet virksomheten. Revisjonskomiteen regnes som en del av kontrollmiljøet i en

[37] §301, 3.

virksomhet. For øvrig er et ineffektivt kontrollmiljø, også utover en ineffektiv revisjonskomité, regnet som en betydelig mangel i en virksomhets internkontroll.

Dersom det er identifisert bedrageri som kan relateres til ledelsen, vil dette være en vesentlig svakhet i internkontroll over økonomisk rapportering.

Revisor kan vurdere en kombinasjon av flere mangler til å være en vesentlig svakhet. For eksempel kan en virksomhet ha manglende fordeling av ansvar, det kan være flere ikke-vesentlige transaksjoner som ikke har blitt korrekt ført i hovedboken, og manglende avstemming av kontoer (som berøres av de nevnte transaksjoner). Sammen vil disse manglene utgjøre en vesentlig svakhet i internkontroll over økonomisk rapportering (AS2, vedlegg D-3)

5.6.1.3 Revisors Konklusjon.

Dersom revisor ikke avdekker vesentlig svakheter i internkontrollen, kan revisor konkludere med at de vurderer intern kontroll over økonomisk rapportering til å være effektiv.

> **In our opinion, management's assessment that Pfizer Inc and Subsidiary Companies maintained effective internal control over financial reporting as of December 31, 2005, is fairly stated, in all material respects, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Also, in our opinion, Pfizer Inc and Subsidiary Companies maintained, in all material respects, effective internal control over financial reporting as of December 31, 2005…**
>
> - (KPMG LLP, 2006)

Utdrag fra KPMGs rapport på effektiviteten av Pfizers internkontroll for regnskapsåret 2005.
Hele rapporten kan ses i vedlegg 3.

6 Avslutning

I utredningen har jeg først forklart begrepet intern kontroll. Intern kontroll skal hindre eller oppdage feil som kan få vesentlige konsekvenser for regnskapene. Gjennom å basere implementeringen av internkontroll på et fungerende rammeverk, vil virksomheten på en systematisk måte kunne luke ut eller oppdage feil i tide. Et eksempel på et slikt rammeverk er COSO - dette rammeverket har jeg beskrevet i første del av utredningen. Basert på et slikt rammeverk, og kjennskap til virksomheten og dens omgivelser, vil revisor skaffe seg en forståelse av en virksomhets internkontroll. Denne forståelsen benytter revisor for å bestemme type, tidspunkt og omfanget av revisjonshandlinger i revideringen av en virksomhets regnskaper. I USA er alle børsnoterte virksomheter, som følger av flere finansskandaler, lovpålagt å implementere et system for interne kontroller over økonomisk rapportering. Ledelsen skal evaluere dette, og deretter konkludere med hvorvidt de anser de interne kontrollene som effektive. Virksomhetens revisor[38] skal så vurdere ledelsens evaluering, i tillegg til selv å konkludere med hvorvidt han anser virksomhetens intern kontroll som effektiv (Sarbanes-Oxley Act of 2002, §404).

Bestemmelsene om konkludering på effektiviteten av intern kontroll over økonomisk rapportering, jfr SOX, skulle i utgangspunktet trådt i kraft (for *alle* berørte selskaper) allerede i 2003. Imidlertid har denne fristen, som følger av den betydelige arbeidsmengden bestemmelsene har medført, stadig blitt utsatt. For større amerikanske selskaper har bestemmelsene vært gjeldende siden november 2004, mens bestemmelsene trår i kraft i juli 2006 for større ikke-amerikanske selskaper. Det betyr at norske selskaper som Hydro, Smedvig, Statoil, og Telenor ved fremleggelsen av regnskapet for 2006 også skal ha evaluert effektiviteten av sin interne kontroll. Først da kan vi forvente å få en fullstendig oversikt over kostnadene de norske selskapene har hatt i forbindelse med oppfyllelse av bestemmelsen.

Derimot foreligger data om kostnadene knyttet til kravene for de amerikanske selskapene som implementerte SOX §404 i løpet av 2004. En undersøkelse foretatt av Susann W. Eldridge og Burch T. Kealey ved universitet i Nebraska viser at revisjonskostnadene for amerikanske

[38] Revisor som reviderer regnskapet.

Fortune 1000-selskaper i gjennomsnitt økte med 40 % fra 2003 til 2004.[39] Et selskap som General Electric opplevde en økning i revisjonskostnader på 41,4 % til 78,2 millioner dollar i samme periode. Rapporten forteller at økningen i kostnadene i hovedsak er knyttet til implementering av SOX §404. De absolutte kostnadene øker, mens grensekostnaden minker dess større selskapet er (Eldridge et.al, 2005). En undersøkelse av Thomas E. Hartman viser samme tendens, der gjennomsnittlige revisjonskostnader for S&P-500 og S&P Small Cap–selskaper økte med henholdsvis 55 % og 84 % fra 2003 til 2004[40] (Hartman, 2005).

I forhold til å implementere bestemmelser tilsvarende SOX §404 i Europa, sier European Federation of Accountants (FEE) ”*…FEE is currently not convinced about the usefulness of introducing across the EU published effectiveness conclusions on internal control over financial reporting as required by Section 404 of the Sarbanes-Oxley Act. However, it will be important to take account of the views of investors and companies and forthcoming evidence about the usefulness, costs and benefits of such conclusions to investors as Section 404 of the Sarbanes-Oxley Act is implemented…”*

17. Mai 2006 opplyste PCAOB at de skal gjennomgå, og foreta endringer i Auditing Standard 2. Endringene skal i større grad sikre at revisors hovedfokus i revisjonen blir på de områder som er utsatt for misligheter og vesentlige feil. I tillegg skal PCAOB presisere begrepene vesentlighet, betydelig mangel, og vesentlig svakhet; og det skal bli mer opp til revisors skjønn å vurdere hva som er sterke indikasjoner på vesentlige svakheter i internkontrollen. PCAOB opplyser også at de forestående endringene skal understreke betydningen av å integrere revisjon av internkontroll med revisjon av regnskaper.

I det videre vil det bli interessant å se hva kravene om å konkludere på effektiviteten av internkontroll over økonomisk rapportering koster de berørte norske (og europeiske) selskapene. Det blir også interessant å følge med på utviklingen i USA, blant annet gjennom de annonserte endringene i Auditing Standard 2. FEE har uttrykt at de for øyeblikket ikke ønsker krav om å pålegge selskaper å konkludere på effektiviteten av internkontrollen. Dermed gjenstår det å se hva skjer neste gang en stor finansskandale rulles opp. Undertegnede har vanskelig for å tro at vi har sett den siste finansskandalen.

[39] Fra 3,5 millioner til 5,8 millioner dollar.
[40] For S&P500: Fra 4,8 millioner til 7,8 millioner dollar. For S&P Small Cap: Fra 567.000 til 1.042.000 dollar.

Kilder

Bøker:

Eilifsen, Aa. ; Messier jr, W.F. ; Glover, S.M. ; Prawitt D.F. ; "Auditing & Assurance Services (International Edition)"; *McGraw-Hill Education*; Maidenhead, UK; 2006

McLean, Bethany og Elkind, Peter; "The Smartest Guys in the Room – The Amazing Rise and the Scandalous Fall of Enron"; *Pinguin – Viking*; London, UK; 2001. pp 127, 158, 229, 239, 244, 303, 317, 339, 368, 381, 382, 393, 403, 406

Moeller, Robert; "Brink's Modern Internal Auditing"; 6th edition; *John Wiley & Sons Inc*; Hoboken; NJ; 2005

Ramos, Michael J.; "How to Comply With Sarbanes-Oxley Section 404 : Assessing the Effectiveness of Internal Control"; *John Wiley & Sons Inc;* Hoboken, NJ; 2004

Rapporter, Avhandlinger, Uttalelser, Artikler:

Berardino, Joseph; "Meet the Press"; *NBC*; 20 Jan 2002

Christiansen, Brian; " Ny amerikansk regulering – Sarbanes-Oxley Act"; *INSPI*; Apr 2003

Cohen-rapporten; "The Commission on Auditors' Responsibilities"; 1978

Committee of Sponsoring Organizations of the Treadway Commission (COSO); "*Intern kontroll – et integrert rammeverk";* 1992. Norsk oversettelse: Solberg, Marte; Cappelen Akademisk Forlag as; Oslo; 1996

Committee of Sponsoring Organizations of the Treadway Commission (COSO); "*Helhetlig risikostyring – et integrert rammeverk. Sammendrag*"; 2004. Norsk oversettelse: Øvsthus, Kari; Norges Interne Revisorers Forening (NIRF); Oslo; 2005

Donaldson, William H.; "Testimony Concerning Implementation of the Sarbanes-Oxley Act of 2002 – Before the Senate Committee on Banking, Housing and Urban Affairs"; 09 Sep 2003

Ebeling, Ashlea (2004); "The Lending Game; New rules say top executives can't borrow money from their company anymore. But every rule has its exceptions"; *Forbes*; Volume 173 Issue 10 – 10 Mai 2004.

Eilifsen, Aasmund; "Forelesning 6; Kapittel 5 – Planlegging og Tester"; *Norges Handelshøyskole*; 15 Feb 2006

Eldridge, Susan W og Kealey Burch T.; "SOX Costs: Auditor Attestation Under Section 404"; *University of Nebraska at Omaha*; Jun 2005

Ernst & Young; "Evaluating Internal Controls – Evaluating Overall Effectiveness, Identifying Matters for Improvement, and Ongoing Assessment of Controls"; 2003

Tillerson, Rex W.; "Certification by Chief Executive Officer - Exhibit 31.1 til FORM 10-K til SEC"; Exxon; 28 Feb 2006

European Federation of Accountants; "Risk Management and Internal Control in the EU Discussion Paper"; FEE; Mar 2005

Gath, Peter og Christiansen, Brian; "Sarbanes-Oxley Act § 404 – Ledelsens vurdering af interne kontroller og revision af interne kontroller"; *Revision og Regnskapsvæsen*; Nr 9; Sep 2003

Hartman, Thomas E.; "The Cost of Being Public in the Era of Sarbanes-Oxley"; *Foley & Lardner LLP*; 16 Jun 2005

Howell W.A.; "Audit Committee's Report – Pfizer"; Pfizer Inc., 2005 Financial Report; 24 Feb 2006

KPMG; ”Report of Independent Registered Public Accounting Firm on Internal Control Over Financial Reporting – 24 Feb 2006”; Pfizer Inc., 2005 Financial Report; 24 Feb 2006

Public Company Accounting Oversight Board; “Board Announces Four-Point Plan to Improve Implementation of Internal Control Reporting Requirements”; PCAOB; 17 Mai 2006

McKinnell, H.A. ; Levin A.G. ; Cangialosi L.V. ; “Management’s Report on Internal Control Over Financial Reporting - Pfizer”; Pfizer Inc., 2005 Financial Report; 24 Feb 2006

Protiviti Inc; “Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements – Frequently Asked Questions Regarding Section 404”; 3rd edition; 2004

Royal Dutch Shell; “FORM 20-F - Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 For the fiscal year ended December 31, 2005”; *SEC*; 2006

Taub, Scott A.; “The SEC’s Internal Control Report Rules and Thoughts on the Sarbanes-Oxley Act”; *University of Southern California Leventhal School of Accounting SEC and Financial Reporting Conference*; Pasadena, CA; 23 Mai 2003

Thain, John; ”Sarbanes-Oxley: Is the Price Too High”; *The Wall Street Journal*; 27 Mai 2004.

http://www.bankrupt.com

Standarder, Lover

AS2; “Auditing Standard no 2 - An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements”; *Public Company Accounting Oversight Board (PCAOB);* 09 Mar 2004

AS2; “Auditing Standard no 2 - An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements – Appendix B”; *Public Company Accounting Oversight Board (PCAOB);* 09 Mar 2004

AU319; “AU Section 319 - Consideration of Internal Control in a Financial Statement Audit”; *American Institute of Certified Public Accountants (AICPA) Professional Auditing Standards;* SAS no 55, 78 & 94

FAS05; “Statement of Financial Accounting Standards No. 5”; *Financial Accounting Standards Board*; Mar 1975

NRS(D); ”Diskusjonsnotat fra Norsk RegnskapsStiftelse – Regnskapsføring av inntekt”; Norsk RegnskapsStiftelse; Okt 1996

RS315; ”Forståelse av foretaket og dets omgivelser og vurdering av risikoene for vesentlig feilinformasjon”; *Den norske Revisorforening*,

RS315; ”Forståelse av foretaket og dets omgivelser og vurdering av risikoene for vesentlig feilinformasjon – Vedlegg 2”; *Den norske Revisorforening*

RS320; ”Vesentlighet” *Den norske Revisorforening*

RS330; ”Revisjonshandlinger for å håndtere anslått risiko”; *Den norske Revisorforening*

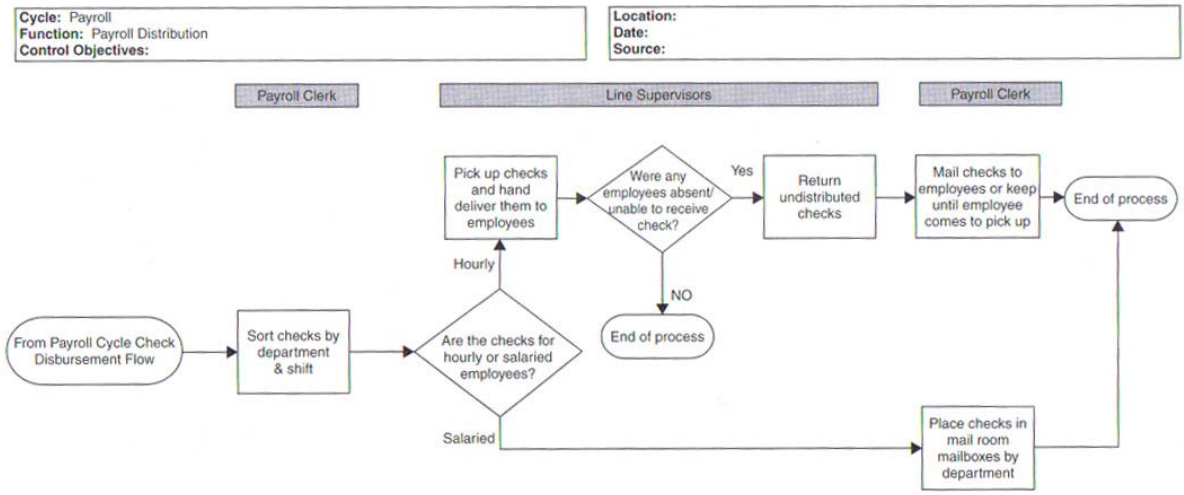
RS500; ”Revisjonsbevis”; *Den norske Revisorforening*

Sarbanes-Oxley Act of 2002

SEC, Final Rule; “Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports”; 06 Nov 2003

Vedlegg

Vedlegg 1:



Kilde: Moeller; 2005; p.134.

Figuren viser et eksempel på en transaksjonsstrøm tilknyttet lønnsutbetaling.

Vedlegg 2:

Management's Report on Internal Control Over Financial Reporting

Management's Report
We prepared and are responsible for the financial statements that appear in our 2005 Financial Report. These financial statements are in conformity with accounting principles generally accepted in the United States of America, and therefore, include amounts based on informed judgments and estimates. We also accept responsibility for the preparation of other financial information that is included in this document.

Report on Internal Control Over Financial Reporting
The management of the Company is responsible for establishing and maintaining adequate internal control over financial reporting as defined in Rules 13a-15(f) and 15d-15(f) under the Securities Exchange Act of 1934. The Company's internal control over financial reporting is designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles in the United States of America. The Company's internal control over financial reporting includes those policies and procedures that: (i) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the Company; (ii) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the Company are being made only in accordance with authorizations of management and directors of the Company; and (iii) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the Company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate. Management assessed the effectiveness of the Company's internal control over financial reporting as of December 31, 2005. In making this assessment, management used the criteria set forth by the Committee of Sponsoring Organizations of the Treadway Commission in Internal Control-Integrated Framework. Based on our assessment and those criteria, management believes that the Company maintained effective internal control over financial reporting as of December 31, 2005.

The Company's independent auditors have issued their auditors' report on management's assessment of the Company's internal control over financial reporting. That report appears in our 2005 Financial Report under the heading, *Report of Independent Registered Public Accounting Firm on Internal Control Over Financial Reporting*.

Henry A. McKinnell
Chairman and
Chief Executive Officer

Alan G. Levin
Principal Financial Officer
February 24, 2006

Loretta V. Cangialosi
Principal Accounting Officer

Audit Committee's Report

The Audit Committee reviews the Company's financial reporting process on behalf of the Board of Directors. Management has the primary responsibility for the financial statements and the reporting process, including the system of internal controls.

In this context, the Committee has met and held discussions with management and the independent registered public accounting firm regarding the fair and complete presentation of the Company's results and the assessment of the Company's internal control over financial reporting. The Committee has discussed significant accounting policies applied by the Company in its financial statements, as well as alternative treatments. Management represented to the Committee that the Company's consolidated financial statements were prepared in accordance with accounting principles generally accepted in the United States of America, and the Committee has reviewed and discussed the consolidated financial statements with management and the independent registered public accounting firm. The Committee discussed with the independent registered public accounting firm matters required to be discussed by Statement of Auditing Standards No. 61, *Communication With Audit Committees*.

In addition, the Committee has reviewed and discussed with the independent registered public accounting firm the auditor's independence from the Company and its management. As part of that review, the Committee received the written disclosures and letter required by the Independence Standards Board Standard No. 1, *Independence Discussions with Audit Committees* and by all relevant professional and regulatory standards relating to KPMG's independence from the Company. The Committee also has considered whether the independent registered public accounting firm's provision of non-audit services to the Company is compatible with the auditor's independence. The Committee has concluded that the independent registered public accounting firm is independent from the Company and its management.

The Committee reviewed and discussed Company policies with respect to risk assessment and risk management.

The Committee discussed with the Company's internal auditors and the independent registered public accounting firm the overall scope and plans for their respective audits. The Committee met with the internal auditors and the independent registered public accounting firm, with and without management present, to discuss the results of their examinations, the evaluations of the Company's internal controls, and the overall quality of the Company's financial reporting.

In reliance on the reviews and discussions referred to above, the Committee recommended to the Board of Directors, and the Board has approved, that the audited financial statements be included in the Company's Annual Report on Form 10-K for the year ended December 31, 2005, for filing with the Securities and Exchange Commission. The Committee has selected and the Board of Directors has ratified, subject to shareholder ratification, the selection of the Company's independent registered public accounting firm.

W.R. Howell
Chair, Audit Committee
February 24, 2006

The Audit Committee's Report shall not be deemed to be filed or incorporated by reference into any Company filing under the Securities Act of 1933, as amended, or the Securities Exchange Act of 1934, as amended, except to the extent that the Company specifically incorporates the Audit Committee's Report by reference therein.

Vedlegg 3

Report of Independent Registered Public Accounting Firm on Internal Control Over Financial Reporting

To the Board of Directors and Shareholders of Pfizer Inc:

We have audited management's assessment, included in the accompanying Management's Report on Internal Control Over Financial Reporting, that Pfizer Inc and Subsidiary Companies maintained effective internal control over financial reporting as of December 31, 2005, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Pfizer Inc and Subsidiary Companies' management is responsible for maintaining effective internal control over financial reporting and for its assessment of the effectiveness of internal control over financial reporting. Our responsibility is to express an opinion on management's assessment and an opinion on the effectiveness of the Company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, evaluating management's assessment, testing and evaluating the design and operating effectiveness of internal control, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion. A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (i) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (ii) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (iii) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements. Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, management's assessment that Pfizer Inc and Subsidiary Companies maintained effective internal control over financial reporting as of December 31, 2005, is fairly stated, in all material respects, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Also, in our opinion, Pfizer Inc and Subsidiary Companies maintained, in all material respects, effective internal control over financial reporting as of December 31, 2005, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the consolidated balance sheets of Pfizer Inc and Subsidiary Companies as of December 31, 2005 and 2004, and the related consolidated statements of income, shareholders' equity, and cash flows for each of the years in the three-year period ended December 31, 2005, and our report dated February 24, 2006 expressed an unqualified opinion on those consolidated financial statements.

KPMG LLP
New York, NY
February 24, 2006

Vedlegg 4
Exhibit 31.1 til FORM 10-K (2005) for Exxon; Rex W. Tillerson; CEO Exxon; 28. Feb. 2006

CERTIFICATION BY CHIEF EXECUTIVE OFFICER

EXHIBIT 31.1

Certification by Rex W. Tillerson
Pursuant to Securities Exchange Act Rule 13a-14(a)

I, Rex W. Tillerson, certify that:

1. I have reviewed this annual report on Form 10-K of Exxon Mobil Corporation;

2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4. The registrant's other certifying officers and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

   (a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

   (b) Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

   (c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

   (d) Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

5. The registrant's other certifying officers and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

   (a) All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

   (b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: February 28, 2006

/s/ REX W. TILLERSON
Rex W. Tillerson
Chief Executive Officer

Vedlegg 5

Rule 13a-15[41] (f)

"The term internal control over financial reporting is defined as a process designed by, or under the supervision of, the issuer's principal executive and principal financial officers, or persons performing similar functions, and effected by the issuer's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

1. Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;
2. Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and
3. Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisitions, use or disposition of the issuer's assets that could have a material effect on the financial statements."

[41] Issuer's Disclosure Controls and Procedures Related to Preparation of Required Reports